REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
26-Sep-97

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE
Information Warfare: Few Challenges for Public International Law

5. FUNDING NUMBERS

6. AUTHOR(S)
Gerald H. Meader

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Georgetown University Law Center

8. PERFORMING ORGANIZATION REPORT NUMBER
97-026

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

19971006 070

14. SUBJECT TERMS

15. NUMBER OF PAGES
52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT

18. SECURITY CLASSIFICATION OF THIS PAGE

19. SECURITY CLASSIFICATION OF ABSTRACT

20. LIMITATION OF ABSTRACT

DTIC QUALITY INSPECTED 3

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

Information Warfare: Few Challenges for Public International Law

by Gerald H. Meader

LAWG-728-11

Graduate Seminar: International Law at the End of the Century

Professor Robert E. Dalton

Georgetown University Law Center

DTIC QUALITY INSPECTED 3

Information Warfare: Few Challenges for Public International Law

by Gerald H. Meader

Page

I. INTRODUCTION 1

A. INFORMATION WARFARE IS OF RISING CONCERN 2

1. U.S. Dependence on the National Information Infrastructure 2
2. An Extremely Attractive Weapon 4

B. INFORMATION WARFARE DEFINED: *INTERNATIONAL, SOVEREIGN, BELLIGERENT* 4

1. Information Warfare is *Not* Purely Domestic 5
2. Neither is it Individual 6
3. General Definition of "Information Warfare" 7
4. Narrowing the Scope: What is *New* about Information Warfare? 7
5. Getting Specific: Categories or Types of IW 10

II. *INFORMATION WARFARE:* THE LAW IS THERE (IF YOU LOOK HARD ENOUGH) 13

A. RESORTING TO ARMED FORCE ("AGGRESSION") 13

1. Aggression and IW Generally 14

a. When is IW Illegal "Aggression" 14
b. Self Defense 20
c. Humanitarian and Other Intervention 22
d. Reprisal 23
e. International Responsibility, Counter-Measures, and Reparation 24

2. Application of the Law Concerning Aggression to IW 26

a. Command-and-Control Warfare 26

HYPOTHETICAL 1 (First strike on command communications)..... 27
HYPOTHETICAL 2 (First strike on command personnel) 28

b. Intelligence-Based Warfare 30

HYPOTHETICAL 3 (Sensitive intelligence stolen from military computers) 31

c. Electronic Warfare 33
d. Psychological Warfare 33
e. "Hacker" Warfare 33

HYPOTHETICAL 4 (Throwing a Presidential election) 33
HYPOTHETICAL 5 (IW attack on U.S. stock markets) 34

B. THE LAW OF ARMED CONFLICT (LOAC) 36

1. LOAC and IW Generally 36
2. Application of LOAC to IW 40

a. Command-and-Control Carfare 40
b. Intelligence-Based Warfare 40
c. Electronic Warfare 41
d. Psychological Warfare 41
e. "Hacker" Warfare 41

C. THE LAW OF NEUTRALITY 42

1. Neutrality and IW Generally 42
2. Application of the Laws of Neutrality to IW 45

a. Command-and-Control warfare 45
b. Intelligence-Based Warfare 45

HYPOTHETICAL 6 (Freely-available tactical satellite information) 45

c. Electronic Warfare 48
d. Psychological Warfare 48
e. "Hacker" Warfare 48

III. A COMMENT ON TERRORISM 48

IV. CONCLUSION 50

Information Warfare: Few Challenges for Public International Law

by Gerald H. Meader

I. INTRODUCTION

In an article entitled *Onward Cyber Soldiers*, Time Magazine describes a classic information warfare (IW) scenario:

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. U.S. planes, specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot.[1]

This story illustrates only some of the potential aspects of IW. Unlike this fictional account, many aspects of IW have already been tested on the battlefield. For example, in the Persian Gulf War, the allied forces gave the Iraqi army an "involuntary lobotomy" by bombing communications networks and electrical power grids in Baghdad and using the Army's Sandcrab jammer that disrupted long range radio traffic throughout Iraq.[2]

These events, and books such as the Tofflers' *War and Anti-War*,[3] greatly popularized this subject, and a great many studies and reports—more or less apocalyptic—have contributed to the growing library by authors of various stripe.[4] At least three things are true

---

[1] Douglas Waller, *Onward Cyber Cyber Soldiers,* Time Magazine, August 21, 1995. This article was the cover story for this edition.

[2] Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor,* The Washington Post, July 16, 1995, A1.

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

[4] There is also a wealth of information on this subject to be found on the internet at, *e.g.*, <http://www.fas.org/irp/wwwinfo.html#infowar>.

about this subject. First, it is stubbornly resistant to definition. Second, IW does pose some threat to our national security and war-fighting abilities. Third, despite the relative novelty of IW, existing international law is largely adequate to address the issues that surround its use. In other words, despite the novelty, gravity, and the perceived need for new international law on the subject,[5] there are actually few real legal challenges for international public law.

To demonstrate how IW issues may be addressed through the existing international law, IW will be defined and subdivided into five types, some of which overlap. These different types of IW will then be viewed in three different general settings—IW between nations at peace ("aggression"), IW between belligerent nations, and IW as it relates to neutral nations. Hypothetical situations will be used for illustrative purposes. Throughout, existing international law will provide answers to the issues which arise. A comment on international terrorism follows this analysis.

A. Information Warfare is of Rising Concern

A threshold question is, "Why address this issue at all?" It deserves a look because our increasing dependence on information and information technologies makes us ever more vulnerable to this attractive, elegant weapon.

1. U.S. Dependence on the National Information Infrastructure

According to a recent report by a Defense Science Board Task Force,[6] the information infrastructure of the United States is increasingly vulnerable.[7] Indeed, because the U.S. is so

---

[5] *See, e.g.,* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 Harvard Int'l L.J. (1996, v.37, n1, Winter, pp. 272-292), and M.E. Bowman, *Essay: International Security in the Post-Cold War Era: Can International Law Truly Effect Global Political and Economic Stability? Is International Law Ready for the Information Age?* 19 Fordham Int'l L.J. 1935 (June 1996, pp.1935-1946).

[6] *Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D),* November 1996. The task force was established at the direction of the Under Secretary of Defense for Acquisition and Technology. It was directed to "focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence."

very dependent on information technology, it is one of the *most* vulnerable nations to IW attack.[8] This vulnerability extends to infrastructures related to military C4I,[9] oil and gas control, water supply, government operations, mass media, civil emergency services, transportation control, finances (national and global), and production, inventory and process controls.[10] They are vulnerable because all of these systems use increasingly complex, interconnected network control systems. These infrastructures are also *inter*-dependent such that an attack on one could have a cascade effect on others.

The U.S. Department of Defense (DoD) alone has over 2.1 million computers, over 10,000 local area networks (commonly known as "LANs"), and over 100 long-distance networks; it depends on computers to coordinate and implement aspects of every element of its mission, from designing weapon systems to tracking logistics.[11] The Defense Information Systems Agency (DISA) found that 86 percent of DoD unclassified computers could be penetrated by exploiting the trusted relationships between machines on shared networks. Only two percent of the penetrations were detected, and only five percent of those were reported. That means that only about one in one thousand intrusions are both detected and reported.[12] In 1995, the DISA responded to 210 computer intrusions. This means that as many as 210,000 intrusions may actually have occurred, and this is only the DoD.[13] Once the intruders enter the computer, they may gain information or passwords, install "trap doors" so they might

---

[7] *Id.* at ES-1.
[8] *Id.* at 2-9.
[9] Command, control, communications, computers and information.
[10] *Id.* at 2-10.
[11] *Id.* at 2-7.
[12] *Id.* at 2-15.
[13] *Id.*

readily re-enter at a later date, modify, steal or destroy data, or even shut down computers or networks.

The DoD is not alone in this. It is generally true that our increasing use of computers and information technology has raced far ahead of our ability to keep the systems secure. This fact, coupled with our growing dependence on information systems, leaves us vulnerable.

2. An Extremely Attractive Weapon

Moreover, an enemy would find this an extremely cost-effective means of warfare. Computers are inexpensive, portable, the available hacking software is increasingly user-friendly, and the expertise needed to use the software is widespread. Twenty years ago, none of these things would be true.

Anonymity can also be achieved through use of the internet and by surreptitiously breaking into and jumping off from other computers. This can provide valuable deniability, if a hostile State so chooses.

Other factors that make IW attractive include the vast number of available targets; the lack of spatial, temporal, or political boundaries; the lack of any quick preventive measures; and the potential psychological effects. Today, no fewer than 30 countries are working on IW techniques.[14]

Unfortunately, however, the term "information warfare," as it commonly used, is far more broad than the mere military applications alone. In order to proceed, it is essential that IW be defined for further analysis in the context of international law.

B. INFORMATION WARFARE DEFINED: INTERNATIONAL, SOVEREIGN, BELLIGERENT

[14] Report of the National Communication System, December 1994. This DISA-managed unit is charged with assuring that a core of the nation's information networks remains operational during any crisis.

Information warfare is defined in different ways by different people, for different purposes. A small business entrepreneur might define information warfare as an aggressive advertising campaign to defeat a local rival. Government officials might use to the term to describe a hacker's effort to tie up the White House e-mail server by flooding it with a huge volume of e-mail messages. The banking industry might consider it to be the actions of a disgruntled bank employee who inserts software into a bank computer resulting in loss of customer data or embezzled funds. The military might view it as the efforts of an agent of a foreign power using the internet to remotely break into a computer to steal sensitive information. There are many, many other variations on this theme.[15] Perhaps the best way to approach a working definition of IW for an international law analysis is do define what IW is *not*.

1. Information Warfare is Not Purely Domestic

There is nothing at all new about the use and abuse of information. The manipulation of information has been a societal concern since the dawn of history. Over the years, societies have written myriad laws addressing the manipulation of information when it results in anti-social ends. Classic examples of such crimes include forgery, perjury, and embezzlement, "larceny by trick," counterfeiting, obstruction of justice through the destruction of evidence, and others, all of which employ the manipulation or destruction of information.

Adding a modern electronic twist to these acts in no way negates the offense. For instance, it makes no difference whether an embezzler falsifies a written ledger or manipulates

[15] There are a great many variables, such as *who* the actor is (a national or foreigner, an employee, a terrorist, an agent of a nation), *where* the act occurs (at the affected computer's keyboard or remotely through the internet or other long-distance communication system), *how* the act occurs (using telecommunication or computer switches in neutral territories or satellites), or the *effect* of the act (a taking of information only or the interference or destruction of information or an information system), to name a few.

a computerized database—the crime is still committed.[16] The distinguishing factor between these crimes and IW is, primarily, the domestic nature of the activity. Being domestic in nature, these actions are not subject to international law. Accordingly, we may exclude, for our purposes, the actions of the local hacker who creates electronic mischief or perpetrates petty theft. Domestic industrial espionage and competitive business practices are similarly excluded. Whether the act is or is not a crime, the domestic nature of the action excludes the act from the definition of IW.

2. Neither is it Individual

If information warfare is *warfare* in any traditional international sense, then it must involve hostilities between sovereigns or, more broadly, between or among actors which each claim to be acting in a sovereign capacity (as in the case of a civil war). Thus, an independently acting terrorist who causes an aircraft to crash by manipulating the information received by the aircraft and pilot, might bring into play extradition and legal assistance treaties, but this act is generally not a belligerent act between sovereigns. The same is true of international hacking and international industrial espionage.

This is not meant to infer that we should not be concerned about information crime or independent terrorism because it is not, as it is herein define, IW. Rather, this type of information activity is addressed either through domestic law or international law *other than* those which deal with warfare generally or, more specifically, the initial resort to military force, the law of armed conflict, or the laws governing neutrality and state-sponsored terrorism.

[16] However, whether the domestic law is sufficient to address the variety of criminal activity which may be committed using information technology is beyond the scope of this paper.

3. General Definition of "Information Warfare"

Having cleared away some aspects of the more popular definitions of IW, the question remains: What *is* IW? Even when narrowed to international, belligerent acts between sovereigns, different definitions abound. The U.S. Navy has defined it this way:

> [A]ction taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. [17]

The U.S. Air Force describes it thus:

> [A]ny action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.[18]

The Joint Chiefs of Staff define it this way:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer based networks.[19]

There is a lot of commonality among these descriptions. However, these definitions are too broad and, therefore, require further definition.

4. Narrowing the Scope: What is New about Information Warfare?

Ultimately, through centuries of bloodshed, nations began to impose rules of warfare on themselves, many of these rules springing from religious beliefs. As these practices among the "civilized" nations became common, they were increasingly regarded as rules binding on

---

[17] OPNAVINST 3430.26 1 (18 Jan 95) (Operational Naval Instruction).
[18] Department of the Air Force, *Cornerstones of Information Warfare* 3-4 (1995).
[19] CJCSI 3210.01, 1996 (Chairman, Joint Chiefs of Staff, Instruction)

them all. Ultimately, these customary international laws were codified in various conventions including the Hague Convention and the 1949 Geneva Conventions. Included among these Laws of War were prohibitions against the improper use of a national flag, insignia, or a flag of truce.[20] Setting aside any moral constraints, this brand of information manipulation was deemed counterproductive due to the adverse reactions it engendered from neutral countries; fear of reciprocity; and increased resentment which, in turn, made the settlement of hostilities that much more difficult. These kinds of ancient *IW* rarely ever brought about any decisive advantage anyway.

On the other hand, international law holds many forms of information manipulation lawful during armed conflict. Ruses and deceptions are expressly permitted.[21] Thus, a nation may plant false information, set up fake equipment for satellite observation, pretend to attack a target when no such attack is planned, and so forth. A nation may also seek to gain and exploit enemy information under international law.[22]

Interdiction of enemy communications has also become an acceptable custom of war—both in the sense of destroying the enemy's ability to communicate and of intercepting and exploiting the communications. For instance, a military force may in wartime drop gravity bombs onto command and control bunkers, disrupt military communication through jamming, cut or destroy communication cables, or otherwise interdict military communications. Eavesdropping and code breaking have long become venerable wartime sciences. Use of

---

[20] Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex to the Convention, 1 Bevins 631, signed on October 18, 1907, at The Hague, Article 23, "In addition to the prohibitions provided by special Conventions, it is especially forbidden: ...(f) To make improper use of a flag of truce, of the national flag, or the military insignia and uniform of the enemy, as well as the distinctive badges ... "

[21] *Id.* Article 24, "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."

[22] *Id.*

photographs to capture enemy information is also nothing new, and radar is an aging, but still effective, technique to gather information about the enemy.

Psychological operations also employ information aspects. Examples include dropping leaflets on the enemy telling them they have no hope of winning, educating the civilians as to the intent of friendly forces and what may be expected from them, and broadcasting radio messages to demoralize the enemy.

These basic notions of IW have evolved over the last century. Now the task is to see whether, and to what extent, these pre-existing notions of IW extend to newly emerging or more heavily relied upon information tools—such as satellite communications and computer networks.

What is *new*, then is (1) the availability of new sources of information; (2) the mushrooming reliance on inexpensive, miniaturized, enormously capable automated data systems for both civilian and military purposes; and (3) the widespread interconnection of these systems via extensive, virtually instantaneous communications nets. Computers and communications channels are subject to jamming, eavesdropping, destruction, corruption of data, and even to hostile seizure of control. Reliance on these systems for military purposes without adequate protection endangers the military operations that depend upon them.

The bottom line then is, that military control and exploitation of information are nothing new. What *is* new, however, is the extent to which military forces have become dependent upon it. Setting aside those military actions readily addressed above, this paper will focus on new situations in order to determine whether, and to what extent, existing law governs. Those areas where IW raises no new issues will merely be noted.

5. *Getting Specific: Categories or Types of IW*

How do these new methods of warfare manifest themselves? In many different ways. In fact, it is very easy and common to talk about IW generally, without ever getting specific. Is IW hacking into civilian computers? Is it jamming radars on the battlefield? It turns out, it can be all of these things. A very useful categorization of *types* of IW can be found in a paper written by Martin Libicki.[23] He describes different types of IW, many of which overlap, as follows:

• Command-and-control warfare that seeks to sever a military's command and control function from the forces in the field. This may be accomplished by directly attacking the command center with bombs or by otherwise disabling the command function by, for example, cutting off power to the command center. Alternatively, the command function may be severed from the troops by breaking the communication links between command and forces. Communication links may be severed by bombing or otherwise disabling communication lines, buildings or structures (such as telephone switching centers or microwave towers); jamming the communications; or interrupting supporting power supplies. The focus is on attacking the enemy's ability to command and control.

• Intelligence-based warfare which consists of the ability to provide real-time or near real-time information about where the enemy is on the battlefield and what the enemy is doing so the individual shooter in the field can better fight. This may be accomplished through satellites, radar, unmanned aerial vehicles, and other sensors (laser-ranging, acoustic, infrared, optical, *etc.*). An example of this type of warfare would include the case of the individual tank

[23] Martin Libicki, National Defense University, *Advanced Concepts and Information Strategy Paper 3*, with credit to the Institute for National Strategic Studies, Washington DC. ISSN 1071-7552. This paper may be obtained

commander who can "sense" the enemy tanks' locations, directions and speeds for accurate shooting. It also encompasses the denial of information to the enemy by negating the enemy's sensors through stealth technology, concealment, ruses or decoys. This represents an increasing tilt from the traditional use of intelligence by commanders to *prepare* a battlefield (which will, of course, continue) toward the use of intelligence by the individual to *master* the battlefield in real time. The focus is on the application of information to the battlefield, not only to prepare the battlefield, but especially as an integral component of the weapon system itself.

• Electronic warfare is an aging art primarily concerned with jamming of radars and anti-jamming techniques. Aircraft and missiles remain heavily dependent on this technology. Libicki also includes encryption in this category. The focus is on the communications media generally, especially as it relates historically to radar.

• Psychological warfare in which information is used to change the minds of friends, neutrals, and foes. The focus here is on the minds of others.

• "Hacker" warfare in which military or civilian computer systems are attacked remotely (although it could be done on-site as well) in order to gain information, undermine the war-fighting ability or will of the enemy. The focus is on the unique *method* of warfare. This is aspect of IW is commonly confused with the more overarching concept of IW. Its focus is on the clandestine use of others' computer systems, usually from afar.

Libicki also includes two other types of IW he characterizes as economic information warfare and "cyberwarfare." Economic information warfare involves blocking information or channeling it to pursue economic dominance. It deals primarily with information *embargoes*.

---

through the internet or purchased through the U.S. Government Printing Office, Superintendent of Documents,

Although perhaps useful in times of armed conflict, this type of "warfare" is beyond the scope of this paper. [24]

Cyberwarfare is a grab bag of futuristic scenarios, entirely out of science fiction. It includes fanciful scenarios where battles are simulated between nations—the results being used to dissuade the "loser" from engaging in real warfare. It envisions battles carried out by computerized "virtual warriors" like those out of modern day movies.[25] This category is only included, as Libicki puts it, "Because to judge what otherwise sober analysts choose to include as information warfare... the range of what can be included in its definition is hardly limited to reality."[26] Because the nature of this type of "warfare" is so bizarre and improbable, it is considered beyond the scope of this paper.

For purposes of analysis, international law will be divided into several pieces, "resorting to military force," the law of armed conflict (LOAC), neutrality, and terrorism.[27] This will allow a comprehensive look at (1) how that legal relationship known as "war" is

---

Mail Stop: SSOP, Washington DC 20402-9328.

[24] The rigorous embargo the United States has enforced against Cuba since the early 1960s, with the stated aim of inducing Cuba to change its form of government, has not been considered by the world community to be a use of force. Neither has the Arab states' embargo of Israel. No state other than Iraq complained when the United States imposed unilateral financial sanctions against Iraq after its invasion of Kuwait, including blocking of all Iraqi property and accounts, a ban on Iraqi imports and exports, travel restrictions to Iraq, and suspension of all contractual rights in the United States or with a U.S. person. These U.S. sanctions were later made consistent with sanctions ordered by the U.N. Security Council. Lesser economic sanctions were also used by the U.S. against Nicaragua, Panama, South Africa, and Iran, without significant protest. Information is increasingly seen as an intangible asset to be traded like any other. Accordingly, there is no reason to believe that an "information embargo," whether total or otherwise, would end in a different result.

[25] *E.g.*, the movie *Tron* envisioned computer-generated people doing battle entirely within the computer circuitry.

[26] *Advanced Concepts and Information Strategy Paper 3, Supra,* Ch. 9.

[27] *See, generally,* THE LAWS OF WAR: A COMPREHENSIVE COLLECTION OF PRIMARY DOCUMENTS ON INTERNATIONAL LAW GOVERNING ARMED CONFLICT, edited with an introduction and commentary by W. Micheal Reisman and Chris T. Antoniou (Vintage Books (a division of Random House), 1994). The terms "law of war," "law of armed conflict," and "international humanitarian law" are the subject of widely divergent definitions. This extremely useful text breaks down the "Laws of War" into several sub-categories, including those listed. Other categories in the text not addressed in this paper include prisoners of war, belligerent occupation, and war crimes. Issues surrounding occupation and the treatment of prisoners of war are essentially irrelevant to a discussion of IW. War crimes issues, dealing with the attribution of individual responsibility for violations of the laws of war or international humanitarian law, are beyond the scope of this paper.

entered into, (2) how the actors may lawfully act once in it, and (3) what the non-players have at stake. Terrorism is addressed briefly in a later chapter. After discussing and defining each of these dimensions of war, each of the five aforementioned types of IW will be measured against them.

II. *INFORMATION WARFARE:* THE LAW IS THERE (IF YOU LOOK HARD ENOUGH)

Before continuing, it is important to distinguish between a solely IW attack on the one hand, and an armed attack which incorporates aspects of IW on the other. An armed attack using elements of IW will be characterized under international law, not by the IW, but by the armaments. The effects of such a coordinated attack, however magnified by information technologies, will be seen as the result of the armed attack, without any particular regard to the IW aspects. International law has long dealt with the analysis of armed attacks. From a legal perspective, then, attacks involving the use of conventional weaponry—even those elegantly enhanced by IW—pose no new legal issues.

Therefore, in order to dissect IW issues, it is necessary to look at IW methods in isolation—that is, without any concurrent armed attack. In this way, the temptation toward easy answers based on the armed aspect of an attack is minimized.

As will be seen, there are few areas where IW and international law intersect to raise issues. Where they do, the issues are usually readily disposed of by using existing international law. There are, however, a few interesting issues.

A. Resorting to Armed Force ("Aggression")

This is, perhaps, the most difficult area for IW issues. There are many abstract issues, including whether international law outlaws, permits, or is silent regarding a particular use of IW between nations who are non-belligerents. Another abstract issue is whether any form of

pure IW targeted against an otherwise non-belligerent country rises to a level where an armed response is lawful. In other words, can any type of IW be considered equivalent to a "first strike" such that the laws of war are invoked and the legal status of the parties with respect to each other and other non-belligerents is changed? If the IW attack does not rise to the level where armed self-defense is lawful, how should the IW attack be construed and what kind of lawful responses are available to the aggrieved parties? Fortunately, these issues are largely *abstract* and, when reduced to plausible scenarios, yield fairly straight-forward answers.

1. Aggression and IW Generally

The first step in the analysis is to see whether any type of IW against a non-belligerent may be characterized as "aggression" under international law. If an IW attack can be considered aggression, then, as will be shown, it is contrary to international law.

a. When is IW Illegal "Aggression"

At some point, a peaceful relationship between states may be legally altered by what was once called an "act of war" and is now termed "aggression."[28] War is a legal relationship, initiated by a declaration of war or by an "act of aggression," *i.e.*, an act demonstrating an intention to be at war, or constituting such a serious breach of the rights of another nation that it would be justified in declaring war. For example, the United States was at war with Japan immediately after Pearl Harbor,[29] but it was not at war with Germany until a declaration of

[28] Much of the information and reference material used in this Chapter was gleaned from a paper prepared by Colonel Phillip A. Johnson, Chief, International and Operations Law Division, Headquarters United States Air Force. The paper and other materials were provided from the Air Force Judge Advocate General School, Maxwell Air Force Base, Alabama. The author expresses his appreciation for making this material available.
[29] Roosevelt's famous speech following declared that the U.S. was in a state of war from the time of the bombing of Pearl Harbor. [get the cite]

war was enacted by Congress. An "act of war" was traditionally limited to an armed attack. But, can an IW attack constitute an act of aggression?

This begs the question, "What is 'aggression?'" A good starting point is the Kellogg-Briand Pact of 1928 which provides in relevant part, as follows:

> Article I: The High Contracting Parties solemnly declare in the names of their respective peoples that they condemn *recourse to war* for the solution of international controversies, and renounce it as an instrument of national policy in their relations with one another.
>
> Article II: The High Contracting Parties agree that the settlement or solution of all disputes or conflicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by *pacific* means. [30]

Although this is a renunciation of war as an extension of politics,[31] it begs the question of whether IW alone can amount to "recourse to war." The Charter of The United Nations also sheds some light:

> Article 2: The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles...
>
> (3) All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
>
> (4) 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. [32]

---

[30] General Treaty for Renunciation of War as an Instrument of National Policy of August 27, 1928 (Kellogg-Briand Pact), T.S. No. 796 (emphasis added). There were 63 parties to this agreement at the outset of the Second World War, including Germany, Japan, Canada, Czechoslovakia, France, Hungary, the Netherlands, Norway, Poland, Romania, the USSR, the United Kingdom, and the United States.

[31] Carl von Clausewitz, *On War* (Anatol Rapoport ed., 1968) ("War is a mere continuation of policy by other means.").

[32] Charter of the United Nations, October 24, 1945 (emphasis added).

Clearly, all members of the U.N. have the duty to refrain from endangering international peace and security. However, the specific injunction in Article 2(4) is against the use of "force." Whether force includes the manipulation of information is unclear.

The United Nations General Assembly further defined these clauses in a declaration in 1970:

> Every State has the duty to refrain in its 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. Such a threat or use of force constitutes a violation of international law and the Charter of the United Nations and shall never be employed as a means of settling international issues.
>
> A war of aggression constitutes a crime against the peace for which there is responsibility under international law.
>
> ...
>
> Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a *threat or use of force.*
>
> Nothing in the foregoing paragraphs shall be construed as enlarging or diminishing in any way the scope of the provisions of the Charter concerning cases in which the *use of force* is lawful.[33]

This seems to be a dead end. The terms "force" and "armed force," taken in context, seem synonymous. Perhaps the key is to look to definitions of the term "aggression." The United Nations General Assembly defined aggression as follows:

> Article 1. Aggression is the use of *armed force* by a State against the sovereignty, territorial integrity or political independence of another State, or in

[33] Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, General Assembly Resolution 2625 (1970). [Extracts of an 8-page text.]

> any other manner inconsistent with the Charter of the United Nations, as set out in this Definition. [34]

Once again, we are back to armed force. At first blush, it would seem that Article 1 limits the definition of aggression to "the use of armed force," meaning some form of physical, military intrusion. It goes on--

> Article 2. The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of *sufficient gravity.* [35]

This article also discusses armed force, but also throws in the requirement that the force employed be of sufficient gravity. This will be a factor in future analysis because IW attacks may not meet this criterion. The next article provides a laundry list of acts which constitute aggression. It is difficult to fit IW into any of the listed categories:

> Article 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:
>
> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
>
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of *any weapons* by a State against the territory of another State;
>
> (c) The blockade of the ports or coasts of a State by the armed forces of another State;
>
> (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;

[34] "Definition of Aggression" Resolution, General Assembly of the United Nations, December 14, 1974; G.A.Res. 3314 GAOR, Supp. 31 (A/9631) at 142 (emphasis added).
[35] *Id.* (emphasis added).

(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein. [36]

However, Article 3(b) does allow for "other weapons" to be considered. But, this reference is clearly in relation to alternate types of "bombardment" (in the kinetic sense). Continuing--

Article 4. The acts enumerated above *are not exhaustive and the Security Council may determine that other acts constitute aggression* under the provisions of the Charter. [37]

Article 4 allows the Security Council to determine whether "other acts" constitute aggression. Whether Article 4 envisions other acts of armed force, on the one hand, or other acts apart from armed force, on the other, is an open question. Perhaps the expansive view is most appropriate, given the Security Council's recent growing propensity to interpret liberally and to generally expand its lawmaking abilities.[38] Other relevant portions of the Resolution include--

Article 5(1) No consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression.

---

[36] *Id.* (emphasis added).

[37] *Id.* (emphasis added).

[38] The United Nations Security Council (UNSC) creates international law through UNSC Resolutions which are enforceable through peaceful means and armed force. The International Court of Justice (ICJ) has shown the UNSC great deference when the UNSC acts to confront a breach of international peace and security. For example, the ICJ has never had occasion to struck down a UNSC Resolution. Indeed, it is unclear whether the ICJ even ha the authority to conduct judicial review of UNSC Resolutions. *But see, Constitutionalism, Judicial Review, and the World Court*, by G.R. Watson, Harvard Int'l L.J., Winter 1993, vol. 34, no. 1, pp. 1-45, for the view that such judicial review may be evolving.

(2) A war of aggression is a crime against international peace. Aggression gives rise to international responsibility.

(3) No territorial acquisition or special advantage resulting from aggression is or shall be recognized as lawful.

Article 6. Nothing in this Definition shall be construed as in any way enlarging or diminishing the scope of the Charter, including its provisions concerning cases in which the use of force is lawful.[39]

This doesn't help resolve whether IW may ever constitute armed force or aggression, *per se*. But, there is another source for the interpretation of law.

In *Nicaragua v. U.S.,*[40] the International Court of Justice (ICJ) ruled that the provision of arms by Nicaragua to the leftist rebels in El Salvador did *not* constitute an armed attack on El Salvador, so it could not form the basis of a collective self-defense argument that would justify the laying of mines in Nicaraguan waters—or certain attacks on Nicaraguan ports, oil installations and a naval base—acts that were "imputable" to the United States.[41] The Court said it had insufficient evidence to determine whether certain cross-border incursions by Nicaraguan military forces into the territory of Honduras and Costa Rica constituted armed attacks.[42] The ICJ thus declined to give an expansive view to the definition of armed attack and refrained from finding that armed incursions were tantamount to an armed attack absent clear evidence..

In sum, the inescapable conclusion then is that the terms "use of force," "armed attack," and "aggression" are interchangeable; that all of these deal, at a minimum, with physical intrusions or assaults against the sovereignty of a State; and that there are no

[39] Definition of "Aggression" Resolution, *Supra.*
[40] 1986 I.C.J. 1 (June 27, 1986).
[41] *Id.* at sections 230, 292.
[42] *Id.* at section 94.

precedents or international agreements that address the extent to which IW may be considered the equivalent of an armed attack or the use of force.

This is not to say, however, that the effects of an IW attack may *never* be considered the equivalent of that done by more traditional weapons. For example, if it could be clearly shown that several aircraft crashes occurred as a result of IW-style guidance system tampering, or that power grids were disabled during a period of extreme cold (or heat), resulting in the death of the elderly or inform, might the effects of these events be seen as the equivalent of an armed attack? Perhaps we are looking at this the wrong way around. Perhaps it is better to look not at when the act of the aggressor gives rise to an act of war (or armed force or aggression), but rather to focus on the targeted State in order to focus on when that State has the right to *respond* with armed force to the effects of an IW attack.

b. Self Defense

Referring again to the Charter of the United Nations, Article 51 provides, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." Once again, we are back to responding to an "armed attack." This, also, seems to lend no clear IW guidance with regard to self-defense.

Another aspect of self-defense is the doctrine of *anticipatory* self-defense. Under this doctrine, a nation may attack another *before* being attacked when "the necessity of self-

defense is instant, overwhelming, and leaving no choice of means, and no moment of deliberation."[43]

The U.N. Charter, however, threw a monkey wrench into this doctrine when it brought Article 51 into force. As noted above, Article 51 allows self defense if an armed attack *occurs*.[44] Clearly, the buildup of hostile military forces on the border of a country does not, by itself, give rise to any right of armed response. Rather, it should result in the threatened nation forwarding its concerns to the U.N. Security Council or General Assembly under Article 35 of the U.N. Charter.[45] The Security Council is then charged with addressing the situation in order to maintain international peace and security.[46]

This notion of anticipatory self defense is a troublesome one. Its use as a justification for a first strike is not at all conducive to international peace and security because of the risk of abuse. On the other hand, if a threatened State spends time consulting with the U.N., it may doom itself, missing what may be its only opportunity to avert a national disaster. Still, requiring an actual armed attack as the trigger for self-defense has the virtue of giving the defender a clear and unambiguous justification for its response—justification which is readily provable and not as easily subject to manipulation. Despite the Article 51 requirement that an

---

[43] *Dicta* in *The Caroline,* 2 Moore, Digest of International Law 412 (1906).

[44] The language of Article 51 does not provide that self defense may be taken *only* if an armed attack occurs. However, usage indicates this is the intent.

[45] *Charter of the United Nations, supra*, Article 35 provides, in part—

1. Any Member of the United nations may bring any dispute, or any situation of the nature referred to in Article 34 [any dispute or any situation which might lead to international friction or give rise to a dispute], to the attention of the Security Council or of the General Assembly.
2. A state which is not a Member of the United Nations may bring to the attention of the Security Council or of the General Assembly any dispute to which it is a party ...

[46] *Id.,* Article 24 provides, "In order to ensure prompt and effective action by the United Nations, its members confer on the Security Council *primary* responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf." [Emphasis added.] The Security Council than has all those rights found in Chapters VI and VII of the U.N. Charter at its disposal to deal with the situation.

armed attack actually occur, anticipatory self-defense has been used with some success in extreme circumstances where armed attack appeared imminent, without significant negative backlash.[47] It may be concluded, then, that anticipatory self-defense is acceptable, but only in cases where the need is clear and the criteria aforementioned are unambiguously met.

Nevertheless, as it relates to IW, anticipatory self-defense will rarely serve as justification for any armed attack simply because most forms of IW attack are of insufficient gravity to trigger the right of self-defense, as will be discussed further, below.

c. Humanitarian and Other Intervention

As far as humanitarian intervention is concerned, it is difficult to imagine a case where an IW attack could create a Somalia- or Haiti-type situation which would require or justify such an intervention. Even if it did, any intervention would most likely be by invitation in the *affected* state, not the aggressor state. Thus, the laws of war are not invoked.

The U.S. is increasingly reluctant to enter into humanitarian operations. After the painful lesson in Somalia where, for a variety of reasons, the armed forces were dragged across the "Mogadishu line" (from non-combatant to combatant status), the US will likely be reluctant to provide humanitarian relief unless specifically requested by the host government (if there is one) and unless armed force is used only as a means of self-defense.

Even when the U.S. does act on humanitarian grounds, its efforts are not always applauded. The example of the recent cruise missile attack against Iraq for humanitarian violations against the Kurds in northern Iraq serves as an example of armed humanitarian intervention against an aggressor state. However, the legality of the U.S. attack was widely disputed. The U.S. justification was based not on any customary international law or treaty

[47] *See e.g.,* the Israeli attacks on Arab armies, 1967, and the Israeli bombing of Iraqi nuclear weapons plant. *But*

regime, but rather, on a tortured interpretation of Security Council Resolutions. This fact would tend to leave the U.S. even more reluctant to act, even if an IW attack caused some widespread calamity. It may be concluded, therefore, that humanitarian intervention has no practical application to IW.

Other grounds for an armed intervention might include intervention to support self determination, to protect democracy (the Reagan Doctrine), or to protect socialism (the Brezhnev Doctrine), but none of these seem likely candidates for justification for an armed response to an IW attack. One reason why this is so, is simply because an IW attack alone would either be ineffective in a third world country where dependence on an information infrastructure is relatively non-existent, or of limited effect in countries which are so dependent.

Even in the United States, perhaps the most vulnerable nation to an IW attack, a concerted IW attack would fail to cripple the nation. It is hard to conceive of a nation sufficiently affluent to possess complex information infrastructures, being brought to its knees by the temporary disruption of the phone and utility systems and concurrent destruction of numerous aircraft or trains, however tragic and outrageous these events might be.[48] Thus, these types of intervention have no application to IW.

d. Reprisal

Traditionally, a reprisal was the use of armed force, short of war, to bring about another state's compliance with international law, to gain reparation for a specific illegal act, or in retaliation therefor. Notice and an attempt at peaceful resolution of the dispute was a precondition for a reprisal. For example, in 1914, when U.S. armed forces occupied Veracruz

---

see, MacChesney, Some Comments on the "Quarantine" of Cuba, 57 A.J.I.L. 592 (1963).

in response to a variety of affronts and indignities committed against the U.S. by Mexico, Congress made it clear through a joint resolution that the U.S. disclaimed any hostility to the Mexican people or any purpose to make war upon Mexico. Reprisal is distinct from the lawful and proportionate use of armed force for self-defense in that a reprisal may occur when there is no significant threat of invasion or armed aggression.

However, reprisal is no longer a lawful means of retaliation against another state for a perceived wrong. This is almost certainly due to the risk of abuse and the potential for acts of reprisal to escalate into full-fledged war. Reprisal was specifically outlawed in the Protocol I Additional to the Geneva Conventions.[49] Article 51(6) provides, "Attacks against the civilian population or civilians by way of reprisals are prohibited." The United Nations General Assembly has also provided, "States have a duty to refrain from acts of reprisal involving the use of force."[50] And, indeed, the practice of reprisal has become exceedingly rare.

e. International Responsibility, Counter-Measures, and Reparation

Most types of IW attacks between non-belligerents fail to qualify as armed attacks (or their equivalents) and, therefore, do not alone give rise to a state of armed conflict between nations. Instead, most types of IW would be seen in international law as "intervention" which would give rise to international state responsibility, the right to employ counter-measures, or the expectation of reparation.

Intervention in foreign nations is governed, in part, by a 1965 General Assembly Resolution which states, as follows:

---

[48] *Report of the Defense Science Board Task Force on Information Warfare—Defense, Supra,* pp. 2-14.
[49] Protocol I Additional to the Geneva Conventions of 1949, 1125 U.N.T.S. 3, adopted on June 8, 1977, at Geneva.
[50] Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, *supra.*

> 1. No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, 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.[51]
>
> ...
>
> 5. Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference *in any form* by another State. [52]

Of course, interference with the political, economic or cultural elements of a State, in a manner short of armed attack does not lend legal justification for an armed response to the interference, despite the fact that such interference is "condemned." Rather, such interference constitutes a breach of international law which gives rise, in turn, to state responsibility, though not necessarily the right to respond militarily.

Other lawful forms of response are also available. For example, as the result of a dispute between France and the United States over the interpretation of a bilateral 1946 Air Services Agreement, France suspended Pan Am flights to Paris. In response, the U.S. suspended French flights to Los Angeles. France sought relief in arbitration, partly on the basis that the U.S. countermeasures were unlawful. The arbitral tribunal ruled for the U.S., stating that "under present-day international law States have not renounced their right to take *counter-measures*" when they perceive that their legal rights have been violated by another state.[53] Of course, in order to avoid the legal proscriptions against armed aggression and reprisals, counter-measures must avoid the use of armed force.

---

[51] Ths provision is extensively referenced these days in discussions of how States do not have an *absolute* right to conduct their own internal affairs, especially when the State violates human rights. *See, e.g., Note: Accountability in Chechnya—Addressing Internal Matters with Legal and Political International Norms*, by Duncan B. Hollis, 36 B.C. L. Rev. 793 (July 1995).

[52] Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States, General Assembly Resolution 2131 (1965) (emphasis added).

[53] Case Concerning Air Services Agreement between France and the United States, Arbitral Award of December 9, 1978, 18 U.N.R.I.A.A. 417, 443-46 (emphasis added).

Counter-measures may be taking contrary to the internationally recognized rights of the offending party provided the counter-measure is proportionate to the offense. Also, a state may unconditionally take counter-measures such as the reduction or termination of diplomatic relations and the tightening of controls over entry and exit visas.

The law concerning reparation is long-standing. As early as 1928, the Permanent Court of International Justice provided as follows:

> Whenever a duty established by any rule of international law has been breached by act or omission, a new legal relationship automatically comes into existence. This relationship is established between the subject to which the act is imputable, who must 'respond' by making adequate reparation, and the subject who has a claim to reparation because of the breach of duty. [54]

Most IW attacks are of such a nature that reparation is clearly lawful remedy. Reparation deals primarily with monetary or in-kind compensation for wrongful damage done by one state to another. Whether reparation is actually paid over, is another matter.

2. *Application of the Law Concerning Aggression to IW*

Having outlined the law relating to aggression, the various types of IW will be compared against them.

a. *Command-and-control warfare*

What is the legality of an IW first strike on national or military command and control? If the strike is on a military command center and iron bombs are used, there is no issue. Setting aside issues of anticipatory self-defense, the act is one of aggression and is illegal. If IW is used in conjunction with the dropping of iron bombs, then the attack as a whole would

[54] Chorzow Factory Decision, Permanent Court of International Justice, series A, no. 17 (1928).

be illegal, with the IW considered merely an aspect of the armed attack. The IW attack and the dropping of munitions would be inseparable.

In order to ascertain the practicality of a purely IW strike against a nation's command and control structure, the following hypothetical is advanced:

HYPOTHETICAL 1. Suppose that a nation engages in a *purely* IW attack against the communication networks used by the command of a second nation. It is conceivable that such an attack, if properly coordinated, could effectively sever the command function from the forces in the field. But, what would be the point? Unless the IW attack was followed up by, or concurrent with, an illegal armed attack, it would serve little purpose except to invite some form of retaliation. Or, it would simply demonstrate the targeted systems' weaknesses, thereby encouraging efforts to prevent a recurrence. Such an attack would also have very temporary effects because of the wide variety of available communication media, not all of which could be affected. Such a useless attack is highly improbable.

Even if such a pure IW attack were to occur, an armed response would clearly be unlawful under Article 51 of the U.N. Charter which permits self-defense only in the case of an actual armed attack. Anticipatory self-defense could serve as a possible justification if there were other factors showing an imminent threat, but a very heavy burden is placed on the nation arguing for anticipatory self-defense; the IW attack would only be one of many factors. In any case, the ultimate determination of lawfulness would require no new international legal framework. The doctrine of anticipatory self-defense, however enfeebled by time, is an existing doctrine of international law. No new international law would be required for the determination.

Diplomatic, economic, and political responses would be in order, as would reference of the matter to the U.N. Security Council—if a threat to international peace and security were perceived.

The simple fact is that it is difficult to conceive of an open IW attack without a concomitant armed attack. Information warfare is typically an *adjunct* of an armed attack, a sort of "force multiplier." [55]

But, is the IW attack itself lawful? Of course not. The act gives rise to international responsibility. Such an act wrongfully interferes in another state's internal military and political controls and clearly gives rise to international responsibility. [56] No new international law is required here, either.

HYPOTHETICAL 2. What if an IW attack has the same *effect* as an armed attack? Suppose a nation is able to affect the avionics or air traffic control system used by Air Force One and other aircraft, causing them to crash, killing the President and key members of his staff, including his top military advisors. Would this act give rise to a right of self-defense? How is this different from shooting down these aircraft with a missile?

It may *seem* different because in the IW case, there may have been no physical invasion of U.S. territory, as in the case of a hacker performing the sabotage from within her home nation. Is the act illegal? Yes, it would quite clearly infringe on the internal controls of the nation. But, assuming, as always, that the perpetrating country could be discovered, what are the lawful responses? It is beyond cavil that a state-sponsored assassination using bullets or missiles would be considered an armed attack against the nation. However, an armed attack

[55] A "force multiplier" is any means of enhancing the capabilities of conventional armed forces or quality of their armaments so that fewer forces are required to accomplish the mission.

alone does not necessarily give the right to armed self-defense. The aggression must also be of sufficient gravity.[57] Is the assassination of the President and his key advisors, together with other facts—such as the belief that similar attacks may continue to occur—of sufficient gravity? Clearly. Wars have started over much less. [58]

The issue remains, then, whether the use of IW is different from the use of a missile. The aggressor state might argue that when the sabotage occurred, nothing physical was affected—only the particular states of energy which comprise computer codes or electronic communication signals were changed. Since nothing *physical* was affected, there can be no international liability. This argument is too nice. In reality, integral components of the aircrafts' operations *were* intentionally affected to bring about the crashes. Also, deliberately changing the state of the "ones and zeroes" which comprise an information stream *is* a measurable, physical change. Just because it is very small, doesn't mean that it does not exist.

The aggressor state might also argue that the sabotage was not an armed attack, *per se*, giving rise to the right of self-defense. But such a narrow interpretation of "armed attack" is inapposite. This issue really becomes whether sabotage can ever be considered an armed attack or aggression. Even though the "Definition of Aggression" Resolution doesn't expressly deal with IW, it also provides in Article 4, "The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter." It is unclear whether *only* the Security Council may make this determination. An expansive reading would allow states to make the determination, as well.

---

[56] Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States, General Assembly Resolution 2131 (1965)

[57] *See,* "Definition of Aggression" Resolution, *Supra.*.

[58] *E.g.,* World War I is said to have started on June 28, 1914, when Archduke Francis Ferdinand, and his wife, of Austria-Hungary, were assassinated by Serbian agitators at Sarajevo, Bosnia.

Where the effects of an IW attack are indistinguishable from the effects of an armed attack, there is a good argument that an armed attack has occurred and the right to self-defense is invoked. [59]

There is also some support for self-defense even when there is no armed attack, as it might be narrowly defined. In his dissenting opinion in *Nicaragua v. United States of America*,[60] Judge Schwebel found that "[a] State is not necessarily and absolutely confined to responding in self-defense only if it is the object of armed attack."[61] He also goes on to describe how, under a too-strict reading of the armed attack requirement, a nation may by denied its only hope for survival.[62] Clearly, then, there is at least some support for the position that the *effect* of a hostile country's act may be the equivalent of an armed attack of sufficient gravity to justify an armed response. It is hard to imagine in a dramatic case such as the one hypothesized, that the opinion of legal scholars worldwide would lean any other way.

b. Intelligence-based warfare

---

[59] *See* U.N. Chart, *supra*, Article 51.

[60] *Nicaragua v. United States v. America*, 1986 I.C.J. 1 (June 27, 1986).

[61] *Id.*, at para. 176.

[62] *Id.*, at para. 177, where Judge Schwebel states, as follows:

> Let us suppose that State A's support of the subversion of State B, while serious and effective enough to place the political independence of State B in jeopardy, does not amount to an armed attack upon State B. Let us further suppose that State A acts against State B not only on its behalf but together with a Great Power and an organized international movement with a long and successful history of ideology and achievement in the cause of subversion and aggrandizement, and with the power and will to stimulate further the progress of what the movement regards as historically determined. If the Court's *obiter dictum* were to be treated as the law to which States deferred, other Great Powers and other States would be or could be essentially powerless to intervene effectively to preserve the political independence of State B and all other similarly situated States, most of which will be small. According to the Court, State B could take counter-measures against State A, but whether they would include measures of force is not said. What is said is that third States could not use force, whether or not the preservation of the political independence—or territorial integrity—of State B depended on the exertion of such measures. In short, the Court appears to offer—quite gratuitously—a prescription for overthrow of weaker governments by predatory governments while denying potential victims what in some cases may be their only hope of survival.

This case is distinct in some ways from the hypothetical, but a central premise remains intact, which is that armed force may not be the only trigger for the right to self defense.

As we see in the newspapers from time to time, intelligence gathering occurs even among the friendliest of allies. It has occurred on the international plain since the dawn of time. When nationals are apprehended selling classified information to a friendly or hostile government, the individuals are dealt with under domestic law. Attempts at espionage involving the use of information systems or computers are also increasingly the subject of domestic law.[63] However, international espionage is not violative of international law.

HYPOTHETICAL 3. What if a friendly or, at least, non-belligerent country uses the internet to tap into a sensitive military network, downloading highly classified information, and installing a trap door to allow easy access to the computer at a later time? Is this an act of war such that armed response is authorized? No, the matter is clearly not of sufficient gravity to rise to the level of an armed response.

Does it give rise to international responsibility? No. It doesn't seem to be a *direct* "interference" in the personality of the State.[64] In the case hypothesized, nothing was altered or destroyed. Even though every nation must have the ability to maintain its secrets, the sheer prevalence of the practice of stealing secrets precludes the assertion of an international custom. Neither is there any convention condemning such an act or its equivalent.

How is this case different from the acquisition by foreign officials of actual classified intelligence documentation? The hypothetical differs primarily because most cases of espionage occur when a foreign agent receives information *freely given* by a disloyal or disgruntled government employee, for pay, politics, or revenge. The hypothetical, on the other

---

[63] *See, e.g.*, 18 USC 793-794, *National Defense Information*; 18 U.S.C. 1029, *Access Device Fraud Act*; 18 U.S.C. 1030, *Computer Fraud and Abuse Act*; 18 U.S.C. 1367, *Interference with the Operation of a Satellite*; 18 U.S.C. 2510 *et seq.*, Electronic Communications Privacy Act; 18 U.S.C. 2511, *Interception & Disclosure of Wire, Oral, or Electronic Communications*; 18 U.S.C. 2701, *Unlawful Access to Stored Communications*; 42 U.S.C. 2000aa, *Privacy Protection Act*; 50 U.S.C. 1801 *et seq.*, *Foreign Intelligence Surveillance Act*.

hand, envisions the government actively seeking to do the taking by defeating the safeguards of the government and by taking the materials from their possessor *in*voluntarily. In a situation like this, it is hard to say that the act is other than a trespass onto the sovereign rights of a nation, but this distinction does not alter the fact that espionage—even the involuntary kind hypothesized—is not unlawful under international law.

How does internet espionage differ from the apparently lawful practice of satellite imagery where super-sensitive cameras orbiting in space take high quality photo intelligence (PHOTINT) of military equipment or operations? How is it different from signals intelligence (SIGINT), which is universally accepted (provided the collection of electronic signals occurs outside the target nation's territory)?

The two cases are distinct in some regards. In the PHOTINT situation, the objects photographed are in plain view from a location where the other party has a right to be—in space. The information contained in a computer is not in a location where it can be freely viewed. On the contrary, safeguards must be broken to gain access. Moreover, although the hacker certainly has a right to sit in his own country while using his computer, the hacker does not have the right to send offensive electronic signals into the U.S. By manipulating the data stream, the hacker is, to use an analogy, throwing a very slender lasso into the country, deftly snagging the information, and pulling it back. Once again, the ethereal quality of electronic signals does not mean that the signals are non-existent. Even so, it is difficult to say that that this is much more than bouncing radar beams off of a ship or other object of a foreign country.

Also, how does this lasso analogy differ from the analogy used with regard to hypothetical two, above, where the data stream was used as a tool to manipulate the avionics

---

[64] Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States, *supra.*

or air traffic control system to cause a plane crash? One difference is in the *result*. In the airplane crash case, the result was one similar to an armed attack or an act of aggression which is universally condemned. In the intelligence computer case, the result is the theft of intelligence data by a foreign power, *i.e.*, espionage—an event evidently not contrary to international law, however it may be condemned domestically.

I conclude, therefore, that the theft of sensitive information as in hypothetical 3 is such that the targeted state may only take counter-measures such as diplomatic protests, reduction of financial support, *etc.*, which are lawful in international law.

c. Electronic warfare

Electronic warfare has no practical application in peacetime and so, there are no legal issues to address.

d. Psychological warfare

It is hard to imagine any new form of psychological warfare among non-belligerents that might be unlawful. Propaganda on the internet might be one form, but this is hardly illegal. Like electronic warfare, there are few new issues associated with psychological warfare.

e. "Hacker" warfare

The difficulty with analyzing hacker warfare is that it may be the *means* of command and control warfare, psychological warfare, or others. Recognizing that an overlap exists, attention will be paid to hacker purposes other than those previously discussed.

HYPOTHETICAL 4. Suppose an unfriendly country wanted to sway public opinion in a closely contested presidential race so that the candidate with policies most favorable to that country had a better chance of winning. The unfriendly country might theoretically do

this by systematically disrupting stock market computers; affecting social security or IRS computers so that denial of benefits letters or audit notices, respectively, were sent to large segments of the population; snarling air or rail transport; planting false records of illegal political party donations; disrupting utility services; or otherwise causing embarrassment.

Are these acts worthy of armed self-defense? No, the effects of the IW do not rise to that level. Are they interfering in the internal political processes of this country?[65] Clearly, and thus, state responsibility attaches. [66] Minimal counter-measures could also be taken. But, what if an internet attack did have a more dramatic results?

HYPOTHETICAL 5. Suppose a foreign power was able to disrupt the various stock market computer systems in a concerted IW attack against the U.S. resulting in widespread financial chaos. Assume that various sectors of the economy were affected—businesses went bankrupt and certain commodities became scarce.

Clearly, this is interference by another State in the internal economic system of the U.S. contrary to international law. Counter-measures by the U.S. would clearly be in order. But does this attack rise to the level where self-defense is authorized?

Once again taking a result-oriented approach to the analysis, such an IW attack is analogous to a blockade, a long-recognized act of aggression. A blockade is an "[a]ction taken against [an] enemy nation so as to isolate, obstruct and prevent communications, commerce, supplies, and persons from entering into or leaving such

---

[65] *Id.*

[66] Paradoxically, if the effort failed, there would likely be little backlash; if it succeeded, the newly elected President would be tempted to minimize the effect of the unfriendly nation's efforts.

nation."[67] Blockades use armed force, or the threat thereof, to enforce this isolation, the purpose of which is to weaken the enemy.

The IW attack on the stock market differs from a blockade in a number of ways. First, the effects of such an IW attack are primarily on the domestic market, whereas a blockade's effect is felt in the international market. However, since the intent of the blockade is to adversely affect the internal market of the country, *through* the international market, the use of the internet is more direct. It is also more potent in that the damage may be done in a single stroke, whereas a blockade would require numerous naval vessels, for example, to remain at a variety of ports for some time to have any significant effect.

There is temptation to view an IW attack on the stock markets as analogous to an embargo. An embargo is a generally lawful act;[68] whereas a blockade is an unlawful act of aggression. Generally, the effects that flow from a lawful act are lawful; those from an unlawful act, unlawful. But this presupposes the conclusion. Why should such an IW attack by viewed as analogous to a blockade versus an embargo?

The analogy to an embargo is inapposite primarily because an embargo is an exercise of sovereignty over the sovereign's own domain, whereas a blockade is a direct intrusion onto the sovereignty of another state. In the hypothetical, the hostile power directly manipulated

---

[67] BLACK'S LAW DICTIONARY 156 (5th ed. 1979).

[68] There have been efforts to include economic coercion, including embargoes, into the definition of aggression. These efforts have been stalled largely due to the fear that, by doing so, the definition of aggression might begin to expand without limit. *See*, 1952 Report on the Question of Defining Aggression, UN Doc. A/2211 at 58. Economic coercion has been generally denounced. *See, e.g.,* Charter of Economic Rights and Duties of States, UN G.A.Res. 3281, 29 GAOR, Supp. 31 (A/9631, at 50 (1974). However, whether international law forbids such conduct is still an open question.

the U.S. stock market computers through the slender thread of the internet. Having no authority to physically intrude into the nation's stock market computers, or to change the characteristics of its magnetic makeup, the act was a direct violation of U.S. sovereignty.

Thus, it may be concluded that, where a concerted IW attack on the stock market causes horrific and widespread calamity similar to that which might be caused by a blockade, necessary and proportionate armed self-defense is lawful to end or preclude further hardship.

B. THE LAW OF ARMED CONFLICT (LOAC)

1. LOAC and IW Generally

In the past, this law was originally known as the *law of war,* but when declarations of war went out of vogue, the term *law of armed conflict* came into widespread use. The law of armed conflict relates to the manner in which nations conduct armed aggression against each other and is codified primarily in the Hague and Geneva Conventions. It should be distinguished from the popular term "international humanitarian law" or "human rights" which are more broad. This distinction is well-described in the text, *The Laws of War:*

> Humanitarian law ... seeks to incorporate key aspects of that part of contemporary international law that is concerned with the protection of human rights.
>
> There are certain common goals in the modern law of war and the international protection of human rights, for both seek to restrain governments' use of power against people subject to them. But the commonality cannot be pressed too far. Human rights documents generally speak in terms of absolute prohibitions on certain government actions against people, while the law of war is premised on the existence of a belligerent situation in which high levels of violence will be directed by governments and their agents against people. Rather than the absolute prohibitions of human rights law, the question in the law of war [LOAC], more often than not, is what level of violence is reasonably necessary and proportional in the context. [69]

[69] W. Michael Reisman and Chris T. Antoniou, *Introduction to* THE LAWS OF WAR, *etc., supra.,* at p. xxi.

A good place to start a review of the applicable LOAC is with the Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex to the Convention.[70] Article 22 provides, "The right of belligerents to adopt means of injuring the enemy is not unlimited." The principles of necessity and proportionality are foundations to an analysis of LOAC as it relates to IW. Article 23(g) especially forbids the destruction or seizure of the enemy's property unless imperatively demanded by the necessities of war. In addition to these principles, the LOAC requires the protection of civilians from bombardment specifically,[71] hostilities generally,[72] and genocide.[73] With reference to IW, the following excerpts from the Protocol I Additional to the Geneva Conventions are particularly relevant:

> Article 48—*Basic Rule*
> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[74]

Thus, as a general rule, during armed conflict, IW must focus on military objectives. But does this Protocol address IW, or is it aimed at kinetic warfare only?

> Article 49—*Definition of Attacks and Scope of Application*
> 1. "Attacks" means acts of violence against the adversary, whether in offense or in defence,

[70] 1 Bevans 631, signed October 18, 1907, at The Hague.
[71] *See,* Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex to the Convention, 1 Bevans 631, signed on October 18, 1907, at The Hage. Articles 25 and 26 apply. *Also See*, the Hague Convention (IX) Concerning Bombardment by Naval Forces in Time of War, 1 Bevans 681, signed on October 18, 1907, at The Hagues, Articles 1 through 4; and the Hague Rules of Aerial Warfare, 32 A.J.I.L. *Supp.) 12 (1938), signed on February 19, 1923, at The Hague; not in force.
[72] Protocol I Additional to the Geneva Conventions of 1949, 1125 U.N.T.S. 3, adopted on June 8, 1977, at Geneva. In particular, Articles 48-58 apply.
[73] Convention on the Prevention and Punishment of the Crime of Genocide, 78 U.N.T.S. 277, adopted by Resolution 260 (III)A of the General Assembly of the United Nations on December 9, 1948.
[74] Protocol I Additional to the Geneva Conventions of 1949, *supra.*

2. The provisions of this Protocol with respect to attacks apply to *all* attacks in whatever territory conducted, including the national territory belonging to a Party to the conflict but under the control of an adverse Party.

3. The provisions of this Section apply to *any* land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They further apply to all attacks from the sea or from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air. ... [75]

We can see from this Article that the text envisions an expansive scope which textually, at least, includes IW. Note, however, that only attacks *on land* are addressed. This leaves open the issue as to whether, for example, civilian satellites are vulnerable to attack. (This issue will be addressed later in this paper.)

The protections afforded civilians are further elaborated below. The protections are not absolute--

Article 51—*Protection of the Civilian Population*

1. The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations. To give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.

2. The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purposes of which is to spread terror among the civilian population are prohibited. [Note to me: Terrorism and propaganda]

3. Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.

4. Indiscriminate attacks are prohibited. Indiscriminate attacks are
   (a) those which are not directed at a specific military objective;
   (b) those which employ a method or means of combat which cannot be directed at a specific military objective;
   (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;

   and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

[75] *Id.* (emphasis added).

5. Among others, the following types of attacks are to be considered as indiscriminate:
   (a) an attack by bombardment ... and
   (b) *an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.*[76]

Paragraph 5(b) permits civilian suffering, but only if the loss of life or damage to objects is not excessive when compared to the military advantage. Thus, an IW attack during armed conflict might be limited by the damage done to civilians or civilian objects.

Article 52—*General Protection of Civilian Objects.*

1. Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2.

2. Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

3. In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be *presumed not to be so used.*[77]

This provision protects civilian facilities and objects from attack and imposes a presumption that civilian facilities are not subject to attack. This provision would apply to some extent to civilian information networks. We will explore later, the extent to which this provision applies. Some civilian objects are *never* subject to attack, however, as may be seen from the following:

Article 54—*Protection of Objects Indispensable to the Survival of the Civilian Population*

---

[76] *Id.* (emphasis added).
[77] *Id.* (emphasis added).

1. Starvation of civilians as a method of warfare is prohibited.

2. It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying then for the sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive. ...

This Article might affect the application of IW against water treatment or water pumping stations, for example, not only because of the water needed for human survival, but because crops and livestock might suffer.

2. *Application of LOAC to IW*

The Law of Armed Conflict poses the least interesting scenarios for the development of new international law. Although not *all* is fair in war, a great deal is. Finding areas where IW can raise new issues for international law is difficult.

a. Command-and-control warfare

Unlike the situation in hypotheticals one and two, attacks on command personnel (including the President as Commander-in-Chief) and on the communications used by command are clearly lawful during a period of armed conflict. Neither can any situation be easily imagined where an IW attack on command and control would be unlawful. Accordingly, it seems that there are no new challenges to address.

b. Intelligence-based warfare

The most dramatic examples of information warfare during periods of armed conflict occur on the battlefield. Information resources, such as laser range-finding or infrared sighting, are capable of sending information to the tank commander for pinpoint shooting. Laser-guided munitions receive information about the exact location of the target so that the

force of the munitions is maximized. If anything, this results in a *more* humane form of warfare, at least compared, for example, with the so-called carpet bombing which was popular in the World War II. Because of its precision, the risk of collateral damage, injury and death—although not eliminated—is significantly reduced

Once again, however, there are no particularly new forms of IW that might subject themselves to a need for new international law.

c. Electronic warfare

There are no particularly new types of electronic jamming or jamming countermeasures, either. Rather, these technologies are merely evolving into more advanced forms. Thus, there are no new issues to address in this area.

d. Psychological warfare

Once again, the bounds described by the law of armed conflict are so very wide that no IW issues—except those with obvious resolutions—present themselves for analysis.

e. "Hacker" warfare

The general prohibition against attacking civilian targets is particularly applicable to hacker warfare. Could an enemy benefit from trying to disrupt the stock market, airline and rail transportation, communications, and the utilities that support them? Undoubtedly. Might some of these be indiscriminate weapons? Perhaps, but it would depend on the use of the information technology and its effects. Information warfare is, in this way, like any other weapon—subject to the rules as laid out above. Issues surrounding IW hacker warfare are as amenable to a LOAC analysis as are, say, dropping a bomb on the stock market or destroying aircraft, trains, or communications systems with missiles. Focusing on the effects of IW in

this area makes the analysis of any IW issue fairly straight-forward. Thus, it may be concluded that IW as it relates to armed conflict, poses no new or interesting issues.

C. THE LAW OF NEUTRALITY

The belligerents aren't the only players during armed conflict. Often, neighboring states suffer just as much as those doing the fighting. Fortunately, international law addresses these countries' concerns. The laws of neutrality pose a few interesting issues for IW:

1. Neutrality and IW Generally

Neutral nations are generally immune from attack, but are required to refrain from assisting belligerents. Failure to live up to these requirements will subject the neutral state to the loss of its protection as a neutral. The laws of neutrality are codified in the Hague Convention.[78] The relevant portions include the following:

> Article 1. The territory of neutral Powers is inviolable.[79]
>
> Article 2. Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.

These Articles describe the general rules, but there are many exceptions. Especially relevant are those rules and exceptions regarding communications. Continuing in the Hague Convention--

> Article 3. Belligerents are likewise forbidden to:
>
> (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea.[80]

---

[78] Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in case of War on Land, 1 Bevans 654, signed on October 18, 1907, at The Hague.

[79] *See also,* Rights and Duties of Neutral Powers in Naval War, 1 Bevans 723, signed on October 18, 1907, at The Hague. Article 1 thereof is similar, but more expansive.

[80] *See also,* Maritime Neutrality (Inter-American), 2 Bevans 721, signed on February 20, 1928, at Havana. Article 4(b) contains substantially similar language as it relates to the establishment of such apparatus in neutral waters.

(b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.[81]

. . .

Article 7. A neutral Power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, or arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet.[82]

Article 8. A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or Companies or private individuals.[83]

Article 9. Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied to both belligerents.

A neutral Power must see to the same obligation being observed by Companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.

Article 10. The fact of a neutral Power resisting, even by force, attempts to violate its neutrality cannot by regarded as a hostile act.

Article 7 of the referenced Hague Convention expressly forbids the export or transport of anything of use to a belligerent. However, Articles 8 and 9 make an exception to this general prohibition by permitting the neutral power to allow belligerents to use communications equipment, provided the use is impartial as among the belligerents.

These rules deal with the use of a neutral land and extend, by application of the *Rights and Duties of Neutral Powers in Naval War*,[84] to underwater cables or other communications facilities at sea. But, does this protection extend to satellite communications?

---

[81] *See also,* Maritime Neutrality, *supra,* Article 4(b) which contains substantially similar language as it relates to the use of such apparatus in neutral waters.

[82] *See also,* Rights and Duties of Neutral Powers in Naval War, *supra.* Article 7 contains similar language.

[83] *See also,* Maritime Neutrality, *supra.*, Article 24, which provides, "The use by the belligerents of the means of communication of neutral states or which cross or touch their territory is subject to the measures dictated by the local authority."

[84] Rights and Duties of Neutral Powers in Naval War, *supra.,* Article 1 provides, "Belligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality." Thus, submarine cables owned by neutrals, in neutral waters, are protected provided they are made available to all belligerents indiscriminately.

The *Outer Space Treaty* of 1967 generally prohibits the stationing of nuclear weapons or other weapons of mass destruction in orbit around the Earth, on the moon or other celestial bodies, or otherwise in space.[85] It also limits the use of the moon and other celestial bodies (but *not* space, *per se*) to peaceful purposes. The treaty is silent on the use of Earth orbit for military purposes other than the stationing of weapons of mass destruction. Relevant provisions include:

> Article I. ... Outer space, including the Moon and other celestial bodies, shall be *free for exploration and use by all States* without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies. ...
>
> Article II. Outer space, including the Moon and other celestial bodies, is *not subject to national appropriation by claim of sovereignty*, by mean of use or occupation, *or by any other means.*[86]

Thus, satellites in space remain, in effect, in neutral territory (Articles I and II), and use of communications satellites in neutral space very closely parallels the use of telegraphy and other communications apparatus as described in the Hague Convention, Articles 8 and 9 (excerpted above). Provided these neutral communications nodes are offered to the belligerents impartially, the analogy is an exact match and international law would render the communications satellites inviolable.

Another interesting issue is whether United Nations forces are considered neutral for purposes of IW, even if they are engaged in a coercive peacekeeping operation such as that conducted in Somalia or Northern Iraq. However, as interesting as this issue is it is focused more on the nature of U.N forces than it is on IW. In other words, if U.N forces are

---

[85] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies ("The Outer Space Treaty"), signed at Washington, London, Moscow, January 27, 1967; entered into force for the United States on October 10, 1967.
[86] *Id.* (emphasis added).

determined to be neutrals in such a setting, the usual laws regarding neutrals and the observations in this chapter would apply. This issue of the neutrality of U.N. forces is, thus, beyond the scope of this paper.

2. *Application of the Laws of Neutrality to IW*

A neutral country would be in a situation similar to a noncombatant State as described in the chapter dealing with aggression, above. Accordingly, the same rules would apply with regard to all the various forms of information warfare, with the few exceptions noted below.

a. Command-and-control warfare.

Presumably, a neutral country's command and control system would not be subject to an IW attack any more than any other non-belligerent country's.

b. Intelligence-based warfare

Although the neutral is not engaged in preparing a battlefield or prosecuting battle, the neutral may nevertheless be unintentionally providing critical battlefield intelligence through satellite technology. Weather or location-finding satellites (*e.g.*, Global Position System or "GPS") are just two examples. These satellites, distinct from communications satellites, are typically located at about 22,300 miles above the Earth. They orbit the Earth once every day, thereby maintaining a fixed position over a specific location at the equator. They are thus said to be in geo-synchronous orbit. These satellites frequently broadcast information to anyone with an antenna who chooses to receive it. (Low Earth orbit satellites may also gather information which may be offered to the world and be put to use by a belligerent.)

HYPOTHETICAL 6. What if the information provided by such a neutrally owned satellite is used by the more technologically advanced belligerent force to its decisive advantage? May the technologically inferior belligerent jam or blind the satellite? May it

destroy the satellite by sending a command causing it to continuously fire its station-keeping rockets, thereby sending it spinning off useless in space? Would this give rise to international liability?

The answer is found in the *Outer Space Treaty*.[87] The relevant excerpts include the following:

> Article VI. States Parties to the Treaty shall bear *international responsibility for national activities in outer space*, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for ensuring that national activities are carried out in conformity with the provisions set forth in the present Treaty.
>
> . . .
>
> Article VII. Each state party to the Treaty that launches or procures the launching of *an object* into outer space, including the Moon and other celestial bodies, and each State Party from whose territory or facility an object is launched, is *internationally liable for damage to* another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on Earth, in air space or in outer space, including the Moon and other celestial bodies.
>
> Article VIII. A State Party to the Treaty on whose registry an object launched into outer space is carried *shall retain jurisdiction and control* over such object, and over any personnel thereof, while in outer space or on a celestial body. Ownership of objects launched into outer space, including objects landed or constructed on a celestial body, and of their component parts, is not affected by their presence in outer space or on a celestial body or by their return to the Earth.[88]

Satellites continue to be subject to the jurisdiction and control of the State that has registry (or ownership) of them (Article VIII), and international liability results from damage caused by either national activities in outer space (Article VI) or by the object launched (Article VII).

---

[87] *Id.*
[88] *Id.* (emphasis added).

However, there is no reference, *per se*, to responsibility for damage caused to satellites by *ground* activities, including the seizure of control of the satellite through ground communications. Liability attaches only for national activities *in* outer space (Article VI) or for damage caused by objects that are launched (Article VII).

Liability would attach, however, if the action of seizing the satellite were considered an activity in outer space, in accordance with Article VI. Clearly, when the lawful owners of a satellite cause the satellite to crash into another or to fall from the sky onto a building, those owners cannot claim that their activities were entirely on the ground. Rather, the activity was in outer space, regardless of the location from which the satellite *commands* originated. It is a small step, then, to conclude that the seizure of a satellite, and taking command of it, is an activity in outer space.

However, in a case of seizure, the damage is done to the satellite *itself*. This raises the issue of whether Article VI contemplated damage *to* an object in space, as opposed to damage *by* an object in space. The language of Article VI is neutral. It simply provides that States "...shall bear international responsibility for national activities in outer space..." The text is clear. The seizure and effective destruction of a satellite by rendering it useless, permanently or temporarily, is an activity in outer space which imposes international responsibility. The seizing State would be liable under international law.

It should be noted that the 1971 Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) and the 1976 Convention on the International Maritime Satellite Organization (INMARSAT), were both intended to provide commercial satellite communication services through fixed and mobile ground stations, respectively. The INTELSAT Agreement permits military use of its "public communications

services," but denies the military the use of its "specialized communications services." The INMARSAT Agreement, on the other hand, expressly provides that its services are for peaceful purposes. This does not, however, prevent the military from using its satellites for communications for certain activities. Nations *contract* for services. Therefore, if the contract prohibits the use of all or a portion of the INTELSAT or INMARSAT systems during belligerent activities, then international law does not apply, the State being bound contractually.

c. Electronic warfare

Neutrals enjoy the same protection from electronic warfare as non-combatants, as described in Chapter IV above.

d. Psychological warfare

Neutrals enjoy the same protection from psychological warfare as non-combatants, as described in Chapter IV above.

e. "Hacker" warfare

Once again, neutrals enjoy the same protection from hacker warfare as non-combatants, as described in Chapter IV above.

III. A COMMENT ON TERRORISM

Terrorism conducted by a political, social, cultural, environmental or other group, not affiliated or sponsored by a State is simply criminal activity and is addressed through national and international criminal mechanisms. For example, the seizure, control or destruction of aircraft is addressed internationally through, *inter alia*, Aviation: Offenses and Certain Other

Acts Committed on Board Aircraft;[89] Suppression of Unlawful Seizure of Aircraft (Hijacking);[90] and the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation.[91] There is no distinction in these international agreements for the use of computers, information, or information systems as the means to these illicit ends. Other international conventions exist for a variety of other terrorist crimes.[92]

It appears that terrorist acts taken by a group struggling to gain freedom is, under many circumstances *not* unlawful under international law. The U.N. General Assembly pronounced in 1973 as follows:

> The struggle of peoples under colonial and alien domination and racist regimes for the implementation of their right to self-determination and independence is legitimate and in full accordance with the principles of international law.[93]

The prominent case where this becomes an issue is with regard to the Palistinian Liberation Organization's struggle with Israel. Fortunately, these kinds of struggles do not currently directly affect the United States; they are increasingly few; and, in developing countries without significant infrastructures, IW poses little threat. Accordingly, this narrow issue will not be addressed. However, many of the general principles in this paper would apply to such an internal struggle.

---

[89] 20 U.S.T. 2941, convention done on September 14, 1963, at Tokyo; entered into force for the United States on December 4, 1969.

[90] 20 U.S.T. 1641, convention done on December 16, 1970, at The Hague; entered into force for the United States on October 14, 1971.

[91] 24 U.S.T. 565, done on September 23, 1971, at Montreal; entered into force for the Untied States on January 26, 1973.

[92] *See, e.g.,* Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, 28 U.S.T. 1975, convention adopted by the General Assembly of the United Nations on December 14, 1973, at New York; entered into force for the United States on February 20, 1977; and the International Convention Against the Taking of Hostages, G.A. Res. 146, U.N. GAOR, 34th Sess., Supp. No. 46, at 245, U.N. Doc. A/34/46 (1980), adopted by the General Assembly of the United Nations on December 17, 1979, at New York.

[93] G.A. Res. 3103, 28 U.N. GAOR at 512, U.N. Doc. A/9102 (1973), quoted in *Tel-Oren v. Libyan Arab Republic*, 726 F.2d 774 (1984).

However, terrorists are increasingly funded, equipped, trained, protected, or otherwise sponsored by States. This is especially true when this type of conduct is, because of significantly inferior economic or military might, an attractive weapon. Assuming that a reasonably clear connection could be made between an IW terrorist attack and a sponsoring State, the issue arises as to whether such a terrorist attack differs from a "belligerent" act.

There is no real difference. Although States may seek to characterize their terrorist acts (including terrorist acts perpetrated by a State's agents) as having some moral authority, such acts are universally condemned by, *inter alia*, a United Nations Resolution of December 9, 1985

which--

> 1. Unequivocally condemns as criminal all acts methods and practices of terrorism wherever and by whomever committed, including those which jeopardize friendly relations among States and their security;
>
> ...
>
> 6. Calls upon all States to fulfill their obligations under international law to refrain from organizing, instigating, assisting or participating in terrorist acts in other States, or acquiescing in activities within their territory directed towards the commission of such acts; [94]

The leaders of seven industrial democracies also issued strong language condemning State involvement in terrorism:

> We, the heads of state or government of seven democracies and the representatives of the European Community, assembled here in Tokyo, strongly reaffirm our condemnation of international terrorism in all its forms, of its accomplices and of those, *including governments*, who sponsor or support it. [95]

---

[94] Resolution adopted by the United Nations General Assembly to Prevent International Terrorism, G.A. Res. 61, U.N. GAOR, 40th Sess., Supp. No. 53, at 301, U.N. Doc. A/40/53 (1986), adopted December 9, 1985.

[95] Texts of the Statements Adopted by Leaders of Seven Industrial Democracies [at the Tokyo Summit Meeting, Concerning Terrorism], May 5, 1986, Weekly Compilation of Presidential Documents, Volume 22, Number 19, at 583 (emphasis added).

The statement goes on to levy against States sponsoring terrorism certain sanctions including arms embargoes, reduction or elimination of diplomatic relations, and stricter immigration laws.

It is clear from the above that terrorist acts by States are simply other forms of aggression. If anything, the voice of condemnation against terrorism may be added to that against aggression. This being the case, it will be in a nation's interest to characterize aggression, whenever possible, as terrorism. This is so both because it carries this extra international weight and because terrorism—which indiscriminately uses innocent civilians as it primary target—strikes closer to home.

IV. CONCLUSION

Information warfare is much touted of late, but the threat is generally overblown. The very diverse and redundant nature of information services in this country serve as our greatest protection. Even a *concerted* attack on the country's information infrastructure would fail to come close to bringing this nation to its knees. Instead, it would likely result in a response—whether diplomatic, economic or military—that would render the attack too costly, thereby deterring any future IW attacks.

While it is true that the nature of the internet could render such an attack anonymous, this issue is more for defense planners and strategists. For, if an attack is anonymous, then there is no point to an international analysis because the IW "attack" could be an accident, domestically produced, or the handiwork of unaffiliated terrorists. In short, if the attack is anonymous, the legal analysis is rendered moot.

When looking at the types of issues that might arise with IW, there are very few issues that cannot be addressed within the existing international legal regime. There are a few, to be

sure, but even these are capable of resolution, especially when the *effects* of IW are scrutinized (the destruction of an aircraft, for example), and less weight is placed on the means of bringing them about. Excessive focus on the unique *means* of warfare—the seemingly insubstantial nature of the weapon itself and the territoriality issues surrounding the internet, to name a few—loses sight of the larger question which is the issue of *what* may one nation do to another.

Despite the hype, while IW remains a terribly serious concern for military planners and national policy makers, there are few challenges for public international law.