# INFORMATION WARFARE AND INTERNATIONAL LAW ON THE USE OF FORCE

JASON BARKHAM*

## I. INTRODUCTION

Information Warfare (IW)[1] is a new type of weapon that has the potential to alter modern warfare significantly. IW first became a popular topic with the publication of several high profile articles, which created images of American "cyber-soldiers" armed only with computers and of entire wars being fought without a single shot fired.[2] While no one knows exactly how IW will develop or what shape the weapons or strategies associated with it will take, we can hypothesize about some of the challenges it might create for international law.

Despite general peace among developed countries and a lack of major interstate warfare in the last generation, there are still plenty of opportunities for conflict. The threat of nuclear war has driven the growth of small-scale warfare.[3] Instead of full-scale wars between great powers, the threat to peace now arises from limited conflicts with "rogue" states, particularly those that attack major countries or other targets. The United Nations Charter and its prohibition on the use of force in Article 2(4),[4] which were drafted in response to an era of major wars, have had trouble adjusting to an era of smaller wars. IW will strain traditional interpretations of Article 2(4) further. IW tactics may force a search for a clearer boundary

* Law Clerk, Honorable Naomi Reice Buchwald, U.S. District Court for the Southern District of New York; J.D., Harvard Law School, 2001; B.A., Yale University, 1998. The author wishes to thank Professor Anne-Marie Slaughter for her insight and advice in writing this article.

1. This paper primarily uses the term "Information Warfare" rather than terms such as cyberwarfare, cyberattack, or computer network attack. These terms are often used interchangeably in the literature.

2. *See* Douglas Waller, *Onward Cyber Soldiers; The U.S. May Soon Wage War by Mouse, Keyboard and Computer Virus. But It Is Vulnerable to the Same Attacks*, TIME, Aug. 21, 1995, at 38; Neil Munro, *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, WASH. POST, July 16, 1995, at C3.

3. *See* HILAIRE MCCOUBREY & NIGEL D. WHITE, INTERNATIONAL LAW AND ARMED CONFLICT 32-33 (1992).

4. U.N. CHARTER art. 2, para. 4.

of the definition of the use of force because they will blur some of the previously understood distinctions of what constitutes a weapon and a use of force. This will be particularly important if IW spawns the sort of proliferation of low-level force between states and non-state actors that it potentially could.

The inability of international law to address problems of small-scale conflict and attacks on private parties is exacerbated by potential applications of IW. For example, IW will complicate the ability of international law to exclude economic coercion from the use of force as defined by Article 2(4). Conventional warfare has long focused on attacking an enemy's military-industrial complex, whereas IW can achieve conventional goals while minimizing physical damage. This may create many opportunities for these actions, which exploit the gap between traditionally defined acts of force and excluded activities such as economic coercion. It may be impossible to distinguish between a full-scale IW attack and a minor electronic incursion. This would be a major problem in a legal regime that bases the appropriateness of a response on the severity of the attack.

Information Warfare also creates serious proliferation concerns; many non-state actors could acquire IW capabilities with which they could cause serious damage. These new actors, who operate primarily outside of the international legal framework, would place even more strain on the traditional use of force model, which already would face difficult new problems created by states' growing IW capabilities. Alarmists have suggested that IW poses an immediate threat to governments worldwide as well as to individual computer users.[5] Others believe that this threat is less imminent.[6] Either way, IW does pose a challenge to all states, corporations, and indi-

---

5. *See* Winn Schwartau, *An Introduction to Information Warfare*, *in* WAR IN THE INFORMATION AGE: NEW CHALLENGES FOR U.S. SECURITY POLICY 47, 52 (Robert Pfaltzgraff & Richard Schultz eds., 1997) [hereinafter WAR IN THE INFORMATION AGE].

6. "The only publicly available estimate . . . states that the development of even a limited strategic information warfare threat would be unlikely before 2005." GREGORY RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 369-70 (2001).

viduals that have become increasingly reliant on computers and data.[7]

Either Information Warfare will require an expansion of the application of the Article 2(4) definition of the use of force or the international community will need to develop new means of addressing the threat, possibly by treaty. Not expanding the definition of the use of force would mean that some IW attacks might not be prohibited by international law. Conversely, expanding the definition of the use of force would bring these actions into the prohibition, but it also would seem to require including the traditionally-excluded categories of political and economic coercion in the definition. Distinguishing force from economic coercion would be much more difficult because the means of attack—computer network attack—would have some applications that traditionally are considered uses of force as well as others that typically have not been considered acts of force. The nature of IW attacks will make it nearly impossible for states to determine whether or not an incursion is actually a use of force without waiting for a damage assessment.

While a treaty regulating Information Warfare might eliminate the need for a broad expansion of Article 2(4), it would cause its own set of problems. Under a treaty regime, it would be difficult to identify whether or not the attacker was a state actor. Non-state actors, such as multinational corporations and transnational criminal organizations, could develop consequential IW capabilities, but presumably they would not be parties to the treaty, thus seriously undermining the treaty's effectiveness. There would also be serious questions about whether states would sign or comply with such a treaty.

---

7. One of the most serious computer-related threats to states, corporations, and individuals comes from computer activity. This piece will not deal in depth with criminal actions, which states typically prosecute under national laws rather than relying on international law for enforcement. There is a large literature on computer crime. *See, e.g.*, Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931 (1996); David Goldstone & Betty-Ellen Shave, *Essay: International Dimensions of Crimes in Cyberspace,* 22 FORDHAM INT'L L.J. 1924 (1999); John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317 (1997); Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451 (1999). Some aspects of distinguishing IW from computer crime will be addressed *infra* Part V(B)(1)(c).

This paper will examine how Information Warfare works, problems it may create for international law on the use of force, and some of the difficulties involved in possible solutions. Part II will discuss the definition of IW and the various tools that are likely to be used in IW, and will look at some applications of IW. Part III will review the key elements of international law on the use of force. Part IV will examine the effects of IW on traditional use of force analysis and analyze some of the problems that IW will create for the distinction between force and coercion. Part V will discuss the alternative of setting up a treaty regime to regulate IW and will look at some of the obstacles that such a treaty would have to overcome. Part VI will offer some conclusions.

## II. Understanding Information Warfare

### A. *A Working Definition of Information Warfare*

Information Warfare in this paper focuses on computer network attack (CNA), as opposed to psychological operations (PSYOPS) or other information-based operations. In its most conventional applications, IW can be used to accomplish many traditional military goals, such as destroying enemy infrastructure targets, disabling defense systems, or attacking civilian targets.[8]

The term "Information Warfare" has been used to describe the current Revolution in Military Affairs (RMA),[9] where the ability to acquire and transmit information quickly is transforming warfare tactics by creating perfect information for commanders, providing them with complete and accurate information instantaneously available across the theater of war. The goal of the information RMA is to produce "information dominance," whereby one country's forces would be able to see the three-dimensional battlespace so much more accurately than its enemies that it would be able to take decisive action while the enemy is still evaluating the situation during

8. *See, e.g.*, Steve Lohr, *Get Ready. Aim. Zap; National Security Experts Plan for Wars Whose Targets and Weapons Are All Digital*, N.Y. Times, Sept. 30, 1996, at D1.

9. Scholars have suggested that there have been over a dozen revolutions in military affairs, and that they are increasing in frequency. *See* Michael Vickers, *The Revolution in Military Affairs and Military Capabilities*, *in* War in the Information Age, *supra* note 5, at 30. R

the "decision cycle."[10] These capabilities would fundamentally change combat. Although information always has been essential in combat, the increasing reliance on transmitted digital information would give the side with the ability to deny the other access to information a major advantage in the encounter.

In addition, Information Warfare may create new opportunities to manipulate enemy information and perception. The side with information superiority could corrupt its enemy's information, placing phantom troops on the other side's systems and undermining enemy morale through false news broadcasts. These techniques often are referred to as Psychological Operations.[11] Modern PSYOPS using IW capabilities could be a very effective weapon, particularly against the United States or another country that relies heavily on public opinion. During the Balkan Wars, all sides used PSYOPS extensively in attempts to undermine the other side's resolve.[12] If a group were able to create false statements or images and implant them into an adversary's mass media, the effects on enemy morale could be devastating. IW's potential applications in PSYOPS have led some commentators to propose the idea of "noösphere," an entirely new domain in which dominance over ideas, rather than land (geosphere) or populations (biosphere), would be determinative.[13]

While information in war has many applications, IW is limited to situations where information itself is the target.

---

10. *See* John McDonald, *Exploiting Battlespace Transparency: Operating Inside an Opponent's Decision Cycle*, *in* WAR IN THE INFORMATION AGE, *supra* note 5, at 143-45. R

11. *See, e.g.*, Glossary of Information Warfare Terms, *at* http://www.psycom.net/iwar.2.html (revised Dec. 2, 2000) (defining "psychological operations" as "[p]lanned psychological activities in peace and war directed to enemy, friendly, and neutral audiences in order to influence attitudes and behavior affecting the achievement of political and military objectives"); *see also* Martin C. Libicki, *What is Information Warfare?*, 28 STRATEGIC FORUM (May 1995), *at* http://www.ndu.edu/inss/strforum/forum28.html (last visited Jan. 11, 2002).

12. *See* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1082-83 (2000) (citing attempts by the United States, Serbian supporters, and individuals in China to use the Internet to affect perceptions of the conflict).

13. *See* JOHN ARQUILLA & DAVID RONFELDT, THE EMERGENCE OF NOOPOLITIK: TOWARD AN AMERICAN INFORMATION STRATEGY 12-15 (1999).

While IW attacks may have physical effects, the attack actually focuses on disrupting the information system, rather than on destroying a tangible object. The applications of IW most similar to conventional conceptions of warfare are those which occur at the beginning of a conflict or which preclude battle altogether. For example, by destroying enemy information systems and preventing any possible armed response before attacking and causing chaos on the enemy side, the IW attack might force the target to surrender, knowing that it would be completely defenseless against any attack.[14] An IW attack also could attack information systems at major infrastructure targets, the destruction of which could cause massive explosions and significant damage. Information attacks also could be employed as an element of a conventional war. By attacking another state's information system immediately prior to or at the start of a military operation, a state could use IW as a force multiplier.[15] While IW capabilities are in their infancy, they have moved beyond pure theory and actually have been used. The United States has revealed that it attempted to use IW during the Kosovo conflict but has not released any details.[16]

### B. *Tools for IW Attacks*

The tools for cyberwarfare are familiar to any hacker. The simplest type of attack is a virus, which is a code fragment that attaches itself to a program and only operates when its host program begins to run. A virus crashed the AT&T switching system in January 1990.[17] While difficult to direct, viruses can cause significant damage. The "I Love You" virus, released

---

14. *See* JOINT CHIEFS OF STAFF, JOINT DOCTRINE FOR INFORMATION OPERATIONS, JOINT PUB. 3-13, at II-10 (1998), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (last visited Jan. 10, 2002).

15. *See id.* at II-11. The U.S. military defines a force multiplier as "a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment." *See* DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUB. 1-02, at 170 (2001), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jpl_02.pdf (last modified Oct. 15, 2001).

16. *See* Elizabeth Becker, *Pentagon Sets Up New Center for Waging Cyberwarfare*, N.Y. TIMES, Oct. 8, 1999, at A16.

17. *See* BRUCE STERLING, THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER 21-24 (1992).

in the spring of 2000, caused an estimated $6.7 billion in damage.[18] A worm is an independent program that copies itself onto other computers but usually does not change other programs.[19] Worms can cause damage merely by eating up network resources or destroying data and are particularly effective over networks.[20] Trojan Horses are code fragments that disguise worms or viruses and allow attackers to gain access to systems. If deployed correctly, they do not leave a trace. A logic bomb is a particular type of Trojan Horse that activates only when a certain condition is met. It can lie dormant in a system for long periods of time before activating.[21] Trap doors are mechanisms that allow a programmer to access software at any time without the owner's knowledge. Analogous to trap doors, chipping involves embedding hidden functions in the hardware itself to allow the designer access to or control over the chip at a later point, for example, by blacking out radar systems during an attack.[22]

Another type of IW attack is the denial of service attack, which disrupts a system by bombarding it with requests for information, forcing it to shut down. The February 2000 denial of service attacks disabled some of the most popular sites on the Internet including eBay, Yahoo!, and Amazon.com. These attacks prompted widespread public concern over infrastructure protection and increased attention to the threat of hackers disrupting the American economy.[23] While these attacks were not sufficiently widespread or coordinated to impact the

---

18. *See* Sharon Berger, *Internet Insurance—Ahead of Its Time?*, JERUSALEM POST, Feb. 7, 2001, at 14.

19. *See* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 280-81 (1999).

20. *Id.*

21. *Id.* at 258-66.

22. *See* Reto Haeni, An Introduction to Information Warfare, *at* http://www.seas.gwu.edu/~reto/infowar/ (Aug. 23, 1996).

23. *See* Ariana Eunjung Cha & John Schwartz, *Hackers Disrupt Yahoo Web Site: Concerted Online Attack Blamed for 3-Hour Outage*, WASH. POST, Feb. 8, 2000, at A1. The Clinton Administration scrambled to investigate the attacks and assure the country that the Internet was safe and reliable, putting additional resources into critical infrastructure protection. *See* David Johnston, *U.S. Officials Lay Out Plan to Fight Computer Attacks*, N.Y. TIMES, Feb. 17, 2000, at C2. *See also* M.J. Zuckerman, *How the Government Failed to Stop the World's Worst Internet Attack*, USA TODAY, Mar. 9, 2000, at 1A; Ricardo Alonso-Zaldivar & Eric Lichtblau, *High-Tech Industry Plans to Unite Against Hackers*, L.A. TIMES, Feb. 16, 2000, at A13.

functioning of the nation's information infrastructure, they served as warnings of the effects a cyberattack might have and how difficult it might be to prevent. Disruption, rather than destruction, may be the sole objective in an IW attack. Tying up the information infrastructure without attempting to destroy it could cause chaos, much like electronic jamming of enemy radar does on the battlefield.

Information Warfare attacks can affect any type of information system. An attack, such as manipulating a stock market, might cause little physical damage, but would cause serious secondary effects. However, an attack using the same techniques could be directed at a dam, causing a flood that could destroy an entire city.[24] It is often difficult to determine when a cyberattack begins and who the attacker is.[25] Even if the target were able to detect a penetration, it might not know the attacker's purpose and, under international law, would have to refrain from taking any retaliatory action while awaiting a damage and intent assessment.[26] The attack might be indistinguishable from an accidental computer error or routine malfunction,[27] making it difficult for the government to identify the source of the problem as an IW attack.

---

24. *See* Robert Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F. L. REV. 173 (1997).

25. *See* Timothy Thomas, *The Threat of Information Operations: A Russian Perspective*, *in* WAR IN THE INFORMATION AGE, *supra* note 5, at 66. No arrests were made in connection with the February 2000 attacks until April 2000. Even then it took four more months to determine that the suspect in custody was responsible for more than one attack. *See also Canada Broadens Its Case Against Suspected Hacker*, N.Y. TIMES, Aug. 4, 2000, at C5. R

26. *See* LAWRENCE GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 62-63 (1997) (noting that any action taken must be justified to the Security Council or the world community; therefore, the victim would need to ensure that it had determined the source of the attack and the extent of the damage).

27. *Id.* at 59-60.

### C. *Different Types of Information Warfare Attacks*

TABLE 1: SUMMARY OF TYPES OF INFORMATION WARFARE ATTACKS

| Level of Attack | Effects | Potential Actors |
|---|---|---|
| Strategic Information Warfare | Use of the computer network attack to defeat the enemy completely | States with significant financial and organizational resources, particularly intelligence |
| Wide-scale Attacks | Series of attacks, similar to a strategic bombing campaign | States with smaller intelligence capabilities |
| Asymmetric Attacks | Relatively small number of attacks, concentrating on high-value targets | Small states and non-state actors |
| Hacker attacks | Disruption of individual systems | Individuals or small groups |

Information Warfare attacks can be characterized by different tiers of severity. The highest level, Strategic Information Warfare, is the ability to use computer network attack to defeat the enemy without actually fielding a fighting force.[28] It is similar to strategic nuclear warfare, in which the nuclear forces are intended to destroy the enemy and force surrender without a conventional battle. There is some dispute over the resource requirements for Strategic Information Warfare. According to one view, it requires levels of financial and organizational resources that few states, let alone non-state actors, can muster.[29] The most difficult IW component to acquire is intelligence.[30] Others have suggested that the capabilities can be acquired at a much lower cost, citing lower costs for computer hardware and increasingly complex communications

28. *See* RATTRAY, *supra* note 6, at 22. **R**

29. *Id.* at 191-201 (discussing such requirements as the extensive knowledge of the adversary, the ability to estimate effects, human capital, and extensive training).

30. *Id.* at 100. The availability of a vast number of potential nodes that could be subject to an IW attack creates an information problem for the attacker who must know not only how to penetrate a single system, but also how to find the susceptible points of entry and navigate from that system into other interconnected systems without detection. *Id.* at 191.

networks, giving potential actors access to a wide range of infrastructure targets.[31]

A state with significant but substrategic IW capabilities could launch a series of attacks on key enemy infrastructure targets.[32] These capabilities could allow a state to carry out a campaign of attacks intended to undermine the target's will and strategic capacity, forcing it to accept the attacker's demands. Such a campaign itself would not render the target defenseless and, therefore, would not be considered Strategic Information Warfare, but it still could be a significant component in a state's arsenal.

Smaller states and non-state actors could develop more modest IW capabilities that they could use as part of their military strategies.[33] Without the requisite personnel and training, smaller states would not be able to attack entire information infrastructure systems successfully, but IW appears to create many opportunities for these actors to pursue asymmetric attacks, in which a country (or sub-state group) that cannot compete on a conventional battlefield with a dominant power instead focuses its resources on a small number of high-value targets.[34] In a military situation, these could be warships or barracks.[35] In a wider context, these could include unconventional attacks on densely populated cities or other high impact targets.[36] The September 11, 2001, attacks on the World

---

31. *See* ROGER MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR 17 (1997).

32. *See id.* at 24-25. These include telecommunications systems, energy pipelines, electric power grids, transportation control systems, the Federal Funds Transfer System, bank transfer systems, and the health care system.

33. *See* RATTRAY, *supra* note 6, at 186. R

34. *See* Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1054, 1078, 1083 (1998).

35. Such actions could be traditional attacks of terrorism, such as the Khobar Towers and U.S.S. Cole bombings, or a component in a conventional military conflict, such as the Iraqi SCUD missile attacks on U.S. bases in Saudi Arabia and on Israeli cities during the Gulf War. *See* Michael R. Gordon, *Superpower Suddenly Finds Itself Threatened by Sophisticated Terrorists*, N.Y. TIMES, Oct. 14, 2000, at A11.

36. This threat is particularly acute with respect to weapons of mass destruction and rogue states. Particularly worrisome is the ability to deliver a relatively simple device containing a biological warfare agent, such as anthrax, undetected in a major city. The potential effects are catastrophic. *See* H.G. Reza, *2 Anti-Terrorist Teams Forming in State*, L.A. TIMES, Apr. 3, 2000, at

Trade Center and Pentagon were tragic examples of the tremendous damage that asymmetric attacks can cause. The smaller a state's IW capacity, the more likely it would be to pursue terror-level attacks, focusing on a few high-value targets. Finally, at the far end of the spectrum are hacker attacks, which are not carried out by a state and are treated under the criminal laws of the target state.[37]

When facing the threat of IW, potential targets constantly must be ready to defend against an enemy system attack, possibly by counterattacking the attacker's system.[38] In order to gain the intelligence required to conduct an effective network attack, IW officers could probe potential enemies' systems consistently to find weak points to attack. Low-level IW activities could be imperative for preserving intelligence and readiness through system mapping and locating vulnerabilities.

No country has discussed its IW doctrine publicly. Despite the U.S. government's silence on its offensive IW strategy, it announced the formation of a new offensive IW unit in 2000.[39] Many countries have begun to assess both the opportunities and dangers of IW.[40] There is probably too much interdependence for major industrialized states to attack each other. For example, even if the United States could launch an IW attack on another major industrialized state without being identified as the source, the attack would have several effects which ultimately would harm the United States. Such an attack would damage the targeted state's economy, reducing its imports of U.S. goods and services, and would destabilize global equity and capital markets, which also would harm the

---

B1; Pamela Hess, *Study: US Not Ready for Bio-War Attack*, UPI, Sept. 27, 1999, LEXIS, News Library, UPI File.

37. *See* Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 210 (2000).

38. *See* RATTRAY, *supra* note 6, at 135-36. R

39. *See* Andrew Koch, *U.S. to Form New Warfare Centre*, JANE'S DEF. WKLY., Oct. 13, 1999, LEXIS, News Library, Jane's Defence Publications File.

40. *See, e.g.*, Rahul Bedi, *The Jane's Interview*, JANE'S DEF. WKLY., July 14, 1999, LEXIS, News Library, Jane's Defence Publications File (quoting India's Chief of Naval Staff as stating India's intention to develop IW capabilities); *IDF to Focus on IW*, JANE'S DEF. WKLY., Sept. 1, 1999, LEXIS, News Library, Jane's Defence Publications File (discussing Israeli Army IW capabilities); Damon Bristow, *Technology: Information Warfare Grips China*, JANE'S INTELLIGENCE REV.—POINTER 8, Nov. 1, 1998, LEXIS, News Library, Jane's Defence Publications File.

U.S. economy. Nonetheless, IW is a potential threat to any country that has automated systems, and the danger increases the more a country computerizes both in the civilian and military contexts.[41] Even as many societies begin to increase computerization, it has been estimated that one hundred countries have some IW capabilities.[42] Most of these countries lack the capability to conduct strategic IW, but that may not stop them from causing significant damage through the use of isolated attacks. Developing states will spend less on information security as they build up their information capacity. Consequently, they may become increasingly susceptible to extortion by large states that could threaten their economic development by degrading their information systems.

While no country has been the target of a widespread IW attack, the U.S. government has been a frequent target of hacker attacks. In one well-publicized attack in February 1998, two U.S. teenagers, aided by an Israeli, penetrated hundreds of U.S. Air Force computer systems.[43] The Defense Department was so worried that it informed President Clinton that the penetrations could be the beginning of a full-scale IW attack. It took government officials a month to identify and locate the hackers, an operation referred to as Solar Sunrise. This took place eight months after a June 1997 NSA simulation known as Eligible Receiver exposed major weaknesses in computer security for several major military commands as well as power and telecommunications services in several major cities.[44]

---

41. *See World-Wide Threats: Hearing Before the Senate Select Committee on Intelligence*, 106th Cong. 18 (2000) (prepared testimony of George Tenet, Director of Central Intelligence).

42. Michelle Van Cleave, *Infrastructure Protection and Assurance*, *in* SEMINAR ON INTELLIGENCE, COMMAND, AND CONTROL, GUEST PRESENTATIONS, SPRING 1999, at 163 (Anthony Oettinger ed., 2000), *available at* http://pirp.harvard.edu/pubs_pdf/van%20cle/van%20cle-i00-2.pdf (last visited Jan. 10, 2002).

43. *See* Reuters, *U.S. Report: Teen Hackers Plead Guilty to Pentagon Attacks* (July 30, 1998), *at* http://news.zdnet.co.uk/story/0,,t269-s2069023,00.html; *see also* Press Release, U.S. Department of Justice, Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers (Mar. 18, 1998), *at* http://www.usdoj.gov/criminal/cybercrime/ehudpr.htm; *see* Reuters, *Withdrawal Ordered for U.S. Pentagon Hackers* (Nov. 6, 1998), *at* http://lists.jammed.com/ISN/1998/11/0026.html.

44. *See* Bradley Graham, *U.S. Studies New Threat: Cyber Attack; Hackers, Simulation Expose Vulnerability*, WASH. POST, May 24, 1998, at A1; *U.S. Senate Com-*

The extent of the IW threat is uncertain. While the basic tools are known, the uncertainties of the process of evolving from hacker-like penetration to military doctrine leaves much of the future to the realm of speculation. The analysis in Part IV will attempt to extrapolate from the little that is known to suggest tactics and doctrines that can be analyzed under international law.

## III. Traditional International Law on the Use of Force

### A. *Basic Principles*

Modern law on the use of force is based on the U.N. Charter. An analysis of international law and IW begins with the prohibition of the use of force in Article 2(4).[45] The drafters intended to prohibit all types of force, except those carried out under the aegis of the United Nations or as provided for by the Security Council.[46] The principles were similar to the ban on uses of force other than for self-defense set out in the Kellogg-Briand Pact of 1928, which had failed to prevent WWII.[47] The founders wanted to restrict the use of force severely by sharply limiting its use to situations approved by the Security Council.[48]

---

*mittee on the Judiciary, Subcommittee on Technology, Terrorism and Government Information Holds Hearing on Infrastructure Protections*, June 10, 1998, LEXIS, Legislation and Politics Library, FDCH Political Transcripts File.

45. "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2, para. 4. There is a vast literature on the topic of the use of force and Article 2(4), and it is beyond the scope of this paper to discuss it in its entirety. Instead, this paper will attempt to highlight some of the key issues that arise out of the literature and apply them to the problem of IW.

46. *See* Ruth B. Russell, A History of the United Nations Charter 456-57, 673-75, 1067 (1958); *see also* Proposals for the Establishment of a General International Organization (1944).

47. *See* Kellogg-Briand Pact, Aug. 27, 1928, 46 Stat. 2343. *See also* Shabtai Rosenne, *International Law and the Use of Force*, *in* 62 U.S. Naval College Int'l L. Stud.: The Use of Force, Human Rights, and General International Legal Issues 4 (Richard B. Lillich & John Norton Moore eds., 1980) [hereinafter The Use of Force, Human Rights, and General International Legal Issues].

48. The United Nations originally was envisioned as having its own armed forces that would intervene in trouble spots, but this plan broke down

### B. *The Definition of Use of Force*

Neither the Charter nor any international body has defined the term "use of force" clearly. Not all hostile acts are uses of force. The *Corfu Channel* case demonstrates some of the complexities of determining whether there has been a use of force. The Royal Navy had swept the North Corfu Channel for mines in 1944 and 1945 and declared it to be a safe route of navigation.[49] On May 15, 1946, an Albanian gun battery fired at two British warships, which were passing through the Channel.[50] In order to test the Albanian response and to assert their right of free passage, on October 22, 1946, the British sent four warships through the Channel. Two of them struck mines.[51] The International Court of Justice (ICJ) ruled that sending warships through the Channel did not violate Albanian sovereignty,[52] but it did hold that Britain violated international law by sending an armed force into Albanian territorial waters to remove mines on November 12 and 13, 1946. It declared the British action to be a "policy of force," although it did not declare it expressly to be an illegal use of force in violation of Article 2(4). The ICJ, however, characterized Albania's decision to fire on British ships as a "use of force."[53] The ICJ rejected the British claim of acting to preserve evidence for the international tribunal as justification for sweeping the channel. It held that such self-help could lead to "serious abuses" and violated international law.[54] The Court intended that Article 2(4) prohibit forceful actions, regardless of the relative power of the state committing the act, but it adopted a rather narrow interpretation of the actual use of force.

While the precise definition of what constitutes the use of force is unclear, some of the parameters are well known. Conventional weapon attacks are included in Article 2(4). Despite attempts by developing states to include threats of force and economic coercion within Article 2(4) during the drafting of

---

as the Cold War emerged. *See* Andrew Miller, Note, *Universal Soldiers: U.N. Standing Armies and the Legal Alternatives*, 81 GEO. L.J. 773, 775, 779-83 (1993).

49. *See* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 13-14 (Apr. 9).

50. *See id.* at 27.

51. *See id.* at 14, 28, 30.

52. *Id.* at 29-30.

53. *Id.* at 19, 35.

54. *Id.* at 34-35.

the U.N. Charter and as actions of aggression in the Declaration on Friendly Relations, the international community has resisted such efforts;[55] thus, threats of force and economic coercion have been expressly excluded.[56] The boundary of Article 2(4) lies somewhere between actual uses of military force and threats of force.[57] Some scholars have suggested that there are some uses of force that are not covered by Article 2(4).[58] A naval blockade, technically an act of war, would be a use of force because the enforcement requires force,[59] but sanctions, while they achieve a similar effect, would not be a use of force unless force is used to carry them out.[60]

---

55. The International Law Commission also voted to keep the threat of force outside the definition of aggression. Secretary General of the United Nations, *Question of Defining Aggression*, U.N. GAOR, 7th Sess., at 52, para. 372, U.N. Doc. A/2211 (1952), *reprinted in* LOUIS HENKIN ET AL., INTERNATIONAL LAW: CASES AND MATERIALS 681 (2d ed. 1987); *see also* V.S. MANI, BASIC PRINCIPLES OF MODERN INTERNATIONAL LAW: A STUDY OF THE UNITED NATIONS DEBATES ON THE PRINCIPLES OF INTERNATIONAL LAW CONCERNING FRIENDLY RELATIONS AND CO-OPERATION AMONG STATES 263 (1993). Mani discusses the fact that no consensus could be worked out in drafting the Declaration of Friendly Relations regarding whether the "use of force" applied only to armed force or whether it extended to "all other forms of coercion." *Id.* at 11-16. The primary advocates of limiting the definition of the use of force were mostly western industrialized states, while the developing world and the Communist states advocated a broader conception of force. *Id.* at 14-16.

56. *See* Derek Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1 (1972) (stating that the Western powers wanted to confine Article 2(4) to military force and let prohibitions of non-intervention cover other actions); Oscar Schachter, *International Law: The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1624 (1984).

57. "The main problem of the definition of force is whether it should be limited to armed force . . . or whether . . . the concept is now a broader one altogether, including such intangible elements as psychological, economic and political pressures." Rosenne, *supra* note 47, at 5. **R**

58. *See* ANTHONY AREND & ROBERT BECK, INTERNATIONAL LAW AND THE USE OF FORCE 36 (1993). *But see* Schachter, *supra* note 56, at 1623 (stating **R** that in virtually every case the use of force is sought to be justified by reference to the accepted Charter rules).

59. *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 365-66 (1963).

60. *See* Paul Szaz, *The Law of Economic Sanctions*, *in* 71 U.S. NAVAL COLLEGE INT'L L. STUD.: THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM 455, 455-56 (Michael N. Schmitt & Leslie C. Green eds., 1998) [hereinafter THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM] (defining sanctions as an act short of force).

International legal scholarship has developed several factors for determining whether an act is a use of force. First, a use of force requires the use of a weapon.[61] Traditionally, the analysis looks at whether there is kinetic impact (some type of explosion or physical force),[62] but chemical and biological weapons lacked this characteristic. Ian Brownlie, therefore, expanded the analysis beyond kinetic impact and moved toward a result-oriented approach.[63] He focused on whether there was a destruction of life or property.[64] According to this analysis, there is no difference between an attacker firing a missile at a target or spraying it with poison gas; if an action kills people or destroys property, it is a use of force. A use of force can occur only between two states; Article 2(4) does not apply to non-state actors, who are presumably subject to domestic laws.[65] Terrorist bombings, therefore, are tried as criminal actions, even when the attacker is a foreign national and might claim to be waging war against the target state.[66]

There is some debate over how to interpret the U.N. Charter. Many scholars assume that, in order to retain its effectiveness, the Charter evolves to some degree.[67] The extent to which the Charter's definitions evolve is important in apply-

---

61. *See* JAMES BOND, PEACETIME FOREIGN DATA MANIPULATION AS ONE ASPECT OF OFFENSIVE INFORMATION WARFARE: QUESTIONS OF LEGALITY UNDER THE UNITED NATIONS CHARTER ARTICLE 2(4), at 78 (1996); BROWNLIE, *supra* note 59, at 362-63. R

62. *See* BOND, *supra* note 61, at 78; *see also* GREENBERG ET AL., *supra* note 26, at 42-43. R R

63. BROWNLIE, *supra* note 59, at 362-63.

64. *See id.* at 362.

65. *See id.* at 365.

66. *See* John J. Goldman, *N.Y. Trial of 4 Suspects in U.S. Embassy Bombings in Africa Begins Today*, L.A. TIMES, Jan. 3, 2001, at A5 (describing the results of U.S. Embassy bombings, which took place outside the United States of America but on U.S. sovereign property).

67. Bond sets out three approaches to interpreting Article 2(4): textual, subjective, and contextual. Under the textual approach, interpretation focuses on straight analysis of the words used in the Charter as they were applied at the time the treaty was signed, even though they lose effectiveness as time progresses. BOND, *supra* note 61, at 28-29. The subjective approach R (the most prevalent of the three) focuses on the intent of the parties. Its goal is to give effect to the treaty, especially where the treaty is an international constitution. *Id.* at 29-31. Under the contextual approach, interpretation focuses on the objects and purposes of the treaty. It also looks at state practice and changes in the world. It is also known as the "politically oriented jurisprudence" approach. *Id.* at 31-33.

ing use of force analysis under Article 2(4) as new types of warfare develop. If the definition of a use of force is static, then the ban on the use of force gradually will become less effective as new interstate actions occur beyond the boundaries of what the drafters considered.[68] The United Nations has not developed into an international security system regulating the use of force as many of its founders intended.[69] Some scholars, most notably Thomas Franck, have questioned whether Article 2(4) is even relevant in an age of small wars that the United Nations has been largely powerless to stop.[70] In his response to Franck, Louis Henkin emphasizes the normative role of Article 2(4) and argues that its effectiveness continues because, at a minimum, it forces many states to attempt to justify their actions even if they lack authorization.[71] Even if Article 2(4) has ceased to be effective as a rule and an accurate predictor of behavior, some have argued, it still has a core meaning that influences state behavior.[72] Other scholars have questioned whether Article 2(4) retains any normative impact at all, arguing that the willingness of states to violate it and its failure to address internal conflict have eroded its normative value.[73] If Article 2(4) loses its relevance, international law will have lost its primary analytical tool for evaluating hostile acts. This would impair significantly any effort to classify or regulate Information Warfare under the U.N. Charter.

---

68. *Id.* at 29.

69. *See* Richard Falk, *The Decline of Normative Restraint in International Relations*, 10 YALE J. INT'L L. 263, 264 (1985).

70. *See* Thomas M. Franck, *Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States*, 64 AM. J. INT'L L. 809, 812-20 (1970); *see also* AREND & BECK, *supra* note 58, at 181-82 (citing Franck and listing numerous violations of 2(4) which undermine the credibility of the claim that a norm against the use of force still persists). **R**

71. *See* Louis Henkin, Comment, *The Reports of the Death of Article 2(4) Are Greatly Exaggerated*, 65 AM. J. INT'L L. 544 (1971); *see, e.g.*, H.R. DOC. NO. 101-127 (1990).

72. Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L L. 271, 273 (1985).

73. *See* Franck, *supra* note 70, at 809. *See generally* Eugene V. Rostow, *The Legality of the International Use of Force by and from States*, 10 YALE J. INT'L L. 286, 290 (1985). **R**

### C. *The Self-Defense Exception to Article 2(4)*

One of the only exceptions to the U.N. Charter's prohibition on the use of force is the right of individual or collective self-defense set out in Article 51.[74] Self-defense under the Charter is a justifiable act of force undertaken by a state that is the victim of an armed attack or by the allies of an attacked state acting in its defense. All armed attacks are uses of force, but not all uses of force are armed attacks. Created to protect the legal status of the Act of Chapultepec, signed by the states of North and South America, and the Pact of the Arab League, Article 51 preserved the legality of mutual defense alliances.[75] Article 51 is the only way states can use force legitimately when the United Nations fails to act, which often may happen as the result of a veto by a permanent member of the Security Council.

The scope of Article 51 is the subject of considerable controversy among scholars. Some argue that only armed attacks can trigger the right of self-defense under Article 51.[76] The Security Council has taken a restrictive view of Article 51, declining to approve of actions taken that were not in specific response to an armed attack.[77] Others claim that the drafters did not intend to curb the traditional right of self-defense.

---

74. *See* Schachter, *supra* note 56, at 1620 (noting that the other exception occurs when the Security Council authorizes the use of armed force). Article 51 states that: R

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence 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. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

U.N. CHARTER art. 51.

75. *See* BROWNLIE, *supra* note 59, at 270. R

76. *See id.* at 269-78; *see also* LOUIS HENKIN, HOW NATIONS BEHAVE 141 (2d ed. 1979).

77. *See* James J. McHugh, *Forcible Self-Help in International Law*, *in* THE USE OF FORCE, HUMAN RIGHTS, AND GENERAL INTERNATIONAL LEGAL ISSUES, *supra* note 47, at 150 (citing Security Council denunciations of Israeli actions and of British actions against Yemen in 1964 in which the British claimed they were defending the South Arabian Federation). R

The issue is whether the term "in the event of armed attack" was intended to be the exclusive situation in which the right survived.[78] The traditional right of self-defense is based on the *Caroline* standard, set out by U.S. Secretary of State Daniel Webster in response to a British attack on a U.S. ship during the Canadian uprising of 1837.[79] The British claimed that they destroyed the Caroline in an act of self-defense because the U.S. government could not protect them from raids across the border.[80] In accepting the British apology for the event made five years later, Webster acknowledged that an act of self-defense was permitted when the "'necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'"[81] The *Caroline* standard permitted the threatened state to respond before the predicate attack actually occurred, an action referred to as anticipatory self-defense.

Many modern scholars believe that Article 51 can be triggered only in response to an armed attack, but not by the threat of attack or even low-level use of force. In *Nicaragua v. United States*, the ICJ held that "armed attacks" included the sending of armed bands, irregulars, and mercenaries, but did not include assistance to rebels, which the Court believed to be only a threat of force or an unlawful intervention in the internal affairs of another state.[82] Merely sending troops across an international border also did not constitute in itself an armed attack. Thus, the Court ruled that, because Nicaragua's actions in El Salvador did not constitute an armed attack,

78. *See* MYRES MCDOUGAL & FLORENTINO FELICIANO, THE INTERNATIONAL LAW OF WAR: TRANSNATIONAL COERCION AND WORLD PUBLIC ORDER 235 (1994) (stating that "[i]t is of common record in the preparatory work on the Charter that Article 51 was not drafted for the purpose of deliberately narrowing the customary-law permission of self-defense against a current or imminent unlawful attack by raising the required degree of necessity"); *see also* Schachter, *supra* note 56, at 1633-34. R

79. *See* JOHN BASSET MOORE, 2 DIGEST OF INTERNATIONAL LAW §217, at 410 (1906).

80. *See id.*

81. *Id.* at 412 (quoting Daniel Webster).

82. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 103-04 (June 27).

El Salvador's right of collective self-defense had not been triggered, and the U.S. intervention violated international law.[83]

While all scholars agree that states have a right to self-defense in response to an armed attack, some scholars have argued that states should have a right to anticipatory self-defense when an enemy attack is imminent under the *Caroline* standard. Opponents of anticipatory self-defense claim that such a view undermines the whole system prohibiting use of force under the Charter and that Article 51 is a narrower exception than what existed in international law prior to the U.N. Charter.[84] They suggest that the drafters of the Charter intended to narrow the customary right of self-defense. Henkin and Brownlie both generally oppose the legality of anticipatory self-defense,[85] but others scholars, such as Derek Bowett, Myres McDougal, and Oscar Schachter have advocated its legality, at least in some circumstances where an attack is imminent.[86] Even though anticipatory self-defense is controversial, Israel relied heavily on it to justify its 1981 bombing of the Osirak reactor in Iraq.[87] While not expressly supporting anticipatory self-defense, Yoram Dinstein argues for an expansive

---

83. *Id.* at 123 (noting also that the U.S. claims to be acting in defense of Honduras and Costa Rica were also groundless).

84. *See* HENKIN, *supra* note 76, at 141. R

85. *See* BROWNLIE, *supra* note 59, at 278. Henkin does accept, however, that: R

> If the reason for a new reading of the Charter permitting anticipatory self-defense is the hypothetical case of a country which learns certainly and unimpeachably that another is about to destroy it, responsible readings of the Charter and responsible concern for international order would limit the new reading to that extreme case.

HENKIN, *supra* note 76, at 143. R

86. *See* Derek Bowett, *Reprisals Involving Recourse to Armed Force*, 66 AM. J. INT'L L. 1, 4 (1972); MCDOUGAL & FELICIANO, *supra* note 78, at 234-40 (assuming a high degree of imminence). Some observers like Schachter have also expressed that "[i]t is not clear that article 51 was intended to eliminate the customary law right of self-defense and it should not be given that effect. But we should avoid interpreting the customary law as if it broadly authorized preemptive strikes and anticipatory defense in response to threats." Schachter, *supra* note 56, at 1634. R R

87. *See* Anthony D'Amato, Comment, *Israel's Air Strike Upon the Iraqi Nuclear Reactor*, 77 AM. J. INT'L L. 584, 587-88 (1983); *see also* Schachter, *supra* note 56, at 1635. By contrast, note that the U.S. naval quarantine of Cuba in 1962 did not rely on Article 51. *See* William O. Miller, *Collective Intervention and the Law of the Charter*, *in* THE USE OF FORCE, HUMAN RIGHTS, AND GENERAL INTERNATIONAL LEGAL ISSUES, *supra* note 47, at 92-94. R R

conception of an imminent threat as part of his conception of "interceptive self-defense." Dinstein argues that there can be legitimate acts of self-defense before the enemy has fired a shot, but that the key is the presence of an irreversible course of action by the enemy. According to Dinstein, if a state responds to an attack after it has begun but before the invasion force reaches the border, the response is consistent with Article 51.[88] The critics' main problem with anticipatory self-defense is that it permits threatened states to make their own decisions as to how imminent a threat is or how likely the enemy is to carry out an attack; thus, anticipatory self-defense can erode the whole notion of a prohibition on the use of force.[89]

### D. *Responses Other than Article 51*

It is less clear what states are permitted to do in response to uses of force that do not constitute armed attacks. In *Nicaragua v. United States*, the International Court of Justice recognized this gap in international law but did not proffer a solution.[90] Collective self-defense is not an option, nor is an armed attack in response permitted. Most scholars agree that reprisals for hostile actions are not permitted.[91] Nonetheless, while reprisals violate international law, they have become increasingly common.[92] Retorsion, which consists of legally per-

---

88. *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 187-91 (2d ed. 1994) (arguing that an armed attack may begin before the force is actually used).

89. *See* HENKIN, *supra* note 76, at 295. R

90. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 103-04 (June 27).

91. *See* Bowett, *supra* note 86, at 1. *But see* Richard B. Lillich, *Forcible Self-Help Under International Law*, *in* THE USE OF FORCE, HUMAN RIGHTS, AND GENERAL INTERNATIONAL LEGAL ISSUES, *supra* note 47, at 131. Retaliatory acts of R force are illegal unless they are justified as self-defense under Article 51. This suggests that there may be room for legitimate reprisals, at least under traditional international law. In order for the reprisal to be legal, there must be an illegal act by another state; the state making the reprisal must request reparations; and the reprisal must be proportionate to the original act. Lillich notes that Brownlie observes that the U.N. Charter prohibits all reprisals involving the use of force. *Id.* at 132.

92. *See* AREND & BECK, *supra* note 58, at 42-43. *See* Bowett, *supra* note 86, R at 1-2 (stating that armed reprisals violate international law but noting that there is a low level of compliance with the prohibition). *See generally* William O'Brien, *Reprisals, Deterrence, and Self-Defense in Counterterror Operations*, 30 VA. J. INT'L L. 421 (1990) (discussing the Security Council's responses to repri-

missible but unfriendly acts that have a retaliatory purpose, is an option. Acts of retorsion might include suspending treaty obligations, seizing assets, making political decisions adverse to the offending state, limiting diplomatic relations, withholding benefits such as financial aid, imposing trade barriers, or denying ships of the opposing state access to ports. Although they are coercive actions, because they are legal, they cannot be considered uses of force.[93] Historically, retorsions were responses in kind. More recently, retorsion has re-emerged in international relations. U.S. trade sanctions against Haiti, China, and Pakistan declared in 1993 would qualify as retorsions, as would the trade embargo declared against the Federal Republic of Yugoslavia in response to Serbian actions in Bosnia-Herzegovina.[94]

Some preventive measures also may be legal, provided they do not become reprisals. Brownlie permits such measures against low-level attacks, provided that the line of prevention is drawn at the border. Any broader measures of prevention, he asserts, depend on the status of anticipatory action under the law.[95] As Dinstein also notes, this depends on when the attack actually has begun. Unlike Dinstein, Brownlie does not believe that the attack has begun until the potential attacker's forces have violated the potential victim's territorial integrity, including its airspace and territorial waters.[96] At that moment, in Brownlie's view, the attack has begun and the victim can defend itself under Article 51. However, Brownlie notes that "in certain cases technical means of countering the instrument of aggression will not adequately ensure protection if action is only taken when the object enters the territorial domain."[97] Specifically, he accepts the reasonability of an interception system that would operate against rockets over the

---

sals since 1971, and arguing that, while reprisals are relatively common, they remain legally impermissible).

93. *See* Lillich, *supra* note 91, at 130-31; *see also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS, § 905 cmts. a, f (1987). R

94. *See* GERHARD VON GLAHN, LAW AMONG NATIONS: AN INTRODUCTION TO PUBLIC INTERNATIONAL LAW 535 (7th ed. 1996). Glahn also provides a list of acts of retorsion taken during the second half of the twentieth century. *See id.* at 533-34.

95. BROWNLIE, *supra* note 59, at 372. R

96. *Id.* at 373-74.

97. *Id.* at 367.

high seas, airspace of third party states, or outer space. He attempts to distinguish rocket attacks from fast aircraft on the grounds that any expansion of the exception would increase the possibility of abuse.[98] In effect, Brownlie accepts a minimum deviation from his opposition to anticipatory self-defense by taking a step towards Dinstein's more expansive view of when an attack begins. Brownlie's recognition that technological changes could require re-interpretation of the beginning of an attack opens the possibility that IW might require a more thorough reconsideration of use of force analysis.

## IV. IW AND ARTICLE 2(4)

### A. *IW and the Traditional Conception of the Use of Force*

At the moment of an IW attack, the target might have no idea of the attacker's intent or the amount of damage it has incurred. A computer network attack could take many forms; it could be the beginning of an all-out attack, or it could cause no harm at all. The problem for use of force analysis is how to fit IW into a framework in which some penetrations might be considered force while others are not; meanwhile, the target might not know which type of action it is until after the attack.

#### 1. *Information Warfare as a Weapon that Does Not Preclude the Determination of a Use of Force*

While Information Warfare attacks often do not fit into traditional use of force analysis, some types of computer attacks easily can be determined to be uses of force. Since the determination of a use of force requires that a weapon be used, there first must be a method of analogizing IW attacks to weapons. Given Brownlie's shift of the traditional use of force analysis from a purely kinetic analysis (based on physical force being applied to the target) to a result-based analysis, evaluating IW attacks is not limited to focusing on the method of the attack.[99] A result-based analysis requires looking at whether there is a kinetic result, rather than whether the weapon itself is kinetic. Otherwise, a computer attack that destroyed an enemy aircraft might not be considered a use of force, even though there is clearly no difference in result between using a

98. *Id.*

99. *See* Schmitt, *supra* note 34, at 1071-72. **R**

computer and using a missile.[100] Thus, using computers to destroy targets certainly should be considered a use of force. As long as the method of computer attack seems to work like a weapon by causing damage instantaneously and in a manner analogous to a conventional weapon, it is relatively easy to consider at least some types of IW attacks uses of force.[101]

### 2. *Responding to IW Attacks*

TABLE 2: PERMITTED RESPONSES TO IW ATTACKS

| Type of Attack | Permitted Response |
|---|---|
| Strategic IW | Self-defense under Article 51 |
| IW as prelude to conventional attack | Self-defense under Article 51 |
| Series of IW attacks—significant damage | Self-defense under Article 51 |
| Isolated IW attack | No right of self-defense; possibility of retorsion |
| Series of IW attacks—minor damage | No right of self-defense; possibility of retorsion |

Many types of IW attacks will fit comfortably within the framework of Articles 2(4) and 51. Strategic level IW would be a clear violation of Article 2(4); launching an all-out war, which would cause widespread damage and significant casualties, certainly would trigger the victim's right of collective self-defense.[102] Similarly, if the IW attack were a prelude to a conventional one, it, too, would be a use of force triggering Article 51's right to self-defense.[103]

---

100. *See* BOND, *supra* note 61, at 84-85; *see also* Hanseman, *supra* note 24, at 185 (arguing that using an IW attack on an enemy command center by cutting off the power, inserting a computer virus, or preventing all communications would be the same as dropping a bomb on an enemy under the law of armed conflict). R

101. *See* BOND, *supra* note 61, at 78. R

102. *See* Hanseman, *supra* note 24, at 184; GREENBERG ET AL., *supra* note 26, at 85; *see also* Todd Morth, Note, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, 30 CASE W. RES. J. INT'L L. 567, 595-96 (1998). R

103. *See* Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 929-32 (1999).

Evaluating a widespread series of IW attacks would depend on the consequences and frequency of the strikes. As noted above, the fact that the strikes are computer-based does not change the analysis of Strategic IW. If the attacks are on a small enough scale, they might be analogous to the mere sending of troops across a border without causing significant damage.[104] For example, a state might launch a series of small incursions into the computer systems of an opposing country, causing a few system disruptions and perhaps causing the target minor damage in terms of reduced network performance or brief outages and destroying small amounts of data. The incursions might be considered a use of force but not an armed attack, so that the attack would not trigger the target's right of self-defense under Article 51.[105] Another problem for the victim would occur if there were an isolated IW attack that causes damage but is not followed up by any further attacks. This could be a brief attack but one which causes more significant damage, such as causing a small explosion at a factory or power plant. In that case, after the instant of the attack, there would be no further threat of damage and therefore no possible claim of self-defense. Any response, therefore, would be retaliation, which would violate international law. Plausibly, the target might attempt to justify its response on the grounds that further attacks would have been imminent and that the right of self-defense would still apply, but if the attacker made it clear that the attack was a one-time action, then the response would be an illegal act of retaliation.

The instantaneous nature of IW attacks further complicates the permitted responses. The extent of an IW penetration could be the implantation of a worm that would be activated in the future, without further action by the attacker. Immediately after the intrusion there might be no damage, and the attack might not be imminent. Viewed on an immediacy basis, the threat of attack would fail to meet the *Caroline* standard. Even though an IW attack is instantaneous, allowing states to act when they perceive an IW attack to be "imminent" remains a major problem.

---

104. This would be analogous to the ICJ's holding on Nicaragua's actions against El Salvador, which were found not to trigger Article 51. *See* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 103-04 (June 27).

105. *See* BOND, *supra* note 61, at 84-85. R

According to traditional analysis, if the IW attacks were to be preliminary to a full-scale attack, then the target could respond to the initial wave of IW attacks, but if the attacker were to have Strategic IW capabilities, the target might be too crippled to respond after the initial attack had occurred. While not decimated physically, the victim might not be able to repair its information systems, leaving it defenseless. If the IW attack is the prelude to a conventional attack, a response launched after the information systems are disabled may be too late to stop the invasion. This is similar to Brownlie's reasoning on the problem of the beginning of an armed attack and ICBMs, but allowing countries to respond before they even know whether they are being attacked might allow acts which would undermine the U.N. Charter's prohibition on the use of force. A state might try to justify its actions on the grounds that IW attacks by a hostile state are always imminent. A rule permitting wide-ranging responses would allow targeted states too much latitude in determining the extent of the appropriate response and would eviscerate Article 51's purpose of limiting the times where self-defense actions would be appropriate.

If a target state were to detect an IW attack in progress, traditional international law would require it to wait until damage occurred to know whether or not the action would qualify as an armed attack. While the target's best opportunity to respond would be the instant it traces the attacker,[106] the attack might still be pending at this point. An automatic response might be the only way to take action while the incursion is ongoing. The problem with automatic responses in conventional situations is that sometimes the response is incorrect and innocent civilians die. Such an event occurred in July 1988, when an Iranian Airbus was shot down by the U.S.S. Vincennes.[107] This could happen with IW as well. There might

106. *See* Bob Brewin, *Report: Allow Cyberwar Response*, FED. COMPUTER WK., Mar. 29, 1999, http://www.fcw.com/fcw/articles/1999/FCW_032999_255.asp.

107. *See* Walker, *supra* note 12, at 1179 (discussing the accidental shooting of an Iranian airliner that was thought to be a military plane). *See also Iran Airbus Crash Tied to U.S. Errors; Mistakes Were in 'Fog of War,' Report Says of Fatal Gulf Incident*, L.A. TIMES, Aug. 21, 1988, LEXIS, News Library, Los Angeles Times File; John H. Cushman Jr., *11 Minutes to Downing of an Airliner*, N.Y. TIMES, Aug. 20, 1988, at 5. For problems that occur when countries have R

be a legitimate accessing of a system that appears suspicious, or an illegal penetration from a source that, if the victim were to attempt to disable the attacker, could have adverse consequences. The consequences of these scenarios might not be as serious as the 290 civilian deaths in the Vincennes incident, but shutting down an attacking computer could have a cascade effect with unpredictable consequences.[108] If a target were to respond automatically to an incursion by counterattacking the detected system, it might penetrate a system that it has not yet mapped. As noted above, system mapping is essential to carrying out an effective IW attack. Without knowing the contours of a system, an IW officer penetrating a hostile computer system might not be able to distinguish adequately between military and civilian targets. Much like the Vincennes incident, an inadequately prepared defense could cause damage to civilian targets.

Small-scale IW attacks could exploit the gap between Articles 2(4) and 51. The limited means of prevention that Brownlie suggests do not translate well to cyberspace where there are no borders at which to take preventative measures to stop the attack. Since reprisals violate international law, a target state cannot retaliate by attacking the other side's information systems. If state A were to shut down B's power grid temporarily, causing a few casualties but little permanent damage, could state B respond? If there were no threat of further action, there would be no basis for state B to act in self-defense. Any response would be disproportionate to the threat.[109] An attempt to shut down state A's power grid in a similar manner would be a reprisal. If state B suspects that an attack is imminent but the force would not be overwhelming, there would not be even an arguable claim for anticipatory self-defense because the legitimacy of the action still would depend on whether the responding state could justify its action under the *Caroline* standard.

While prevention is permitted, its effectiveness would be very limited; cyberattacks are difficult to prevent.[110] The as-

---

aggressive rules of engagement, see George C. Wilson, *Are We Trigger-Happy? Our Shoot-First, Question-Later Policy Is Risky*, WASH. POST, Jan. 15, 1989, at C1.

108. *See* RATTRAY, *supra* note 6, at 132-33. R

109. *See* GREENBERG ET AL., *supra* note 26, at 88. R

110. *See* Walker, *supra* note 12, at 1187. R

sault cannot be stopped at the border. Other than increasing computer security at key nodes, there is very little that a potential target can do to prepare. Even if the victim were to detect the attack in progress, its ability to respond under traditional international law principles would be limited.[111] Shutting down the attack would mean striking at the attacker's server, which would require crossing the border. Such an act would be beyond the scope of prevention under Brownlie's traditional analysis. The detection of the computer penetration could signal the beginning of the armed attack because it would be the initial territorial breach, analogous to the penetration of airspace or territory. If so, the target would be permitted to respond. The problem is that, at the moment of detection, the target would not know the severity of the penetration. If the penetration caused little damage, then the victim might not be permitted to take defensive action. If the intrusion were the equivalent of a minor border breach, that would not be an armed attack. The target's only legal recourse to a minor incursion might be an act of retorsion. The difficulty in evaluating minor IW attacks might suggest that all IW attacks should be considered uses of force, but that proposal contradicts the prior distinctions that have been made in excluding acts of political and economic coercion from Article 2(4).

### B. *IW Attacks and the Distinction Between Force and Coercion*

IW's potential applications create serious problems for the existing distinction between force and coercion under Article 2(4).[112] Including all IW actions within the use of force would require a major expansion of Article 2(4). There is a sensible argument for such a categorical classification; IW attacks are, in essence, territorial penetrations, which violate the victim's sovereignty. But such an expanded definition of the use of force would make it very difficult to continue to exclude acts of coercion from Article 2(4) because international law would have to distinguish IW acts that do not cause physical damage, such as electronic incursions and blockades, from acts of economic and political coercion, such as economic

111. *See* GREENBERG ET AL., *supra* note 26, at 85, 88. **R**

112. This distinction is important because the Charter, through Article 2(4), bans the use of force, but acts of coercion do not violate international law because they are not uses of force. *See* U.N. CHARTER art. 2, para. 4.

sanctions, which traditionally and specifically have been excluded from Article 2(4), but which often have the same effect.[113] There would not be a logical basis to exclude only certain types of economic aggression from an expanded Article 2(4).[114] In any event, the drafters of the Charter and the Declaration of Friendly Relations explicitly rejected this, and a general consensus has emerged that economic aggression is not a use of force.[115]

None of the approaches to solving the problem of how to regulate IW using Article 2(4) is satisfactory. Michael Schmitt has proposed a framework that attempts to evaluate IW attacks under Article 2(4). Having established that IW attacks can have effects that range across the continuum from armed force to economic coercion, he argues for evaluating the attack on the basis of six criteria: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[116] Applying these criteria determines whether the attack is "armed force" or political or economic coercion. According to Schmitt, looking only at the result does not adequately preserve the distinction created by Article 2(4). He argues that his framework preserves better consistency between evaluating computer attacks and traditional attacks.[117] Once the IW attack is deemed to be a use of force, the extent of the attack can be measured to determine whether there has been an armed attack, which would trigger Article 51.

There are some major flaws in Schmitt's framework. A primary problem is his use of presumptive legitimacy as a factor. If the question is whether IW is a use of force or coercion, and coercion is legitimate and force is not, then we cannot ask whether the action is legitimate to determine whether the action is force or coercion. In effect, Schmitt's approach is backwards, because it requires determining the legitimacy of an attack under international law (i.e., distinguishing between acts

113. *See* BOND, *supra* note 61, at 59; *see also* Schmitt, *supra* note 103, at 906-07. R

114. *See* Jordan J. Paust & Albert P. Blaustein, *The Arab Oil Embargo–A Threat to International Peace*, 68 AM. J. INT'L L. 410, 415-19 (1974).

115. *See* Romana Sadurska, *Threats of Force*, 82 AM. J. INT'L L. 239, 253-54 (1988) (noting development of a general consensus that Article 2(4) does not prohibit economic coercion).

116. *See* Schmitt, *supra* note 103, at 912-15. R

117. *Id.* at 917.

of coercion and uses of force) by asking whether the attack is legitimate.

There are other problems with Schmitt's framework. First, unlike other types of warfare, IW attacks cannot be assessed readily at the time of the attack to determine their magnitude and the permitted responses. This problem will arise with any framework that requires an ex post analysis. The difficulty of tracing IW attacks will undermine severely any state's willingness to wait out the attack before responding because its best opportunity to respond effectively occurs if it detects the attack in progress and responds immediately.[118] Also, Schmitt's analysis does not provide enough guidance as to how to deal with lower-level IW attacks that do not trigger Article 51.

One potential alternative framework would be a broad, result-oriented test. The problem with the result-oriented approach to electronic actions is that it would blur the distinction that excludes economic coercion from the use of force. If the time requirement were expanded, the destruction caused by some economic actions might suggest that they also should be included in Article 2(4). Economic sanctions, for example, can have the same effects over long periods of time as missile attacks aimed at infrastructure targets. An electronic attack might be launched months or years before it has an actual impact on the target, either by slowly attacking the enemy's system or by lying dormant until either triggered by a timing mechanism (time bombs) or a particular sequence of events or commands (logic bombs). If the use of force analysis relies on the result-oriented approach, there may be no meaningful way to exclude economic acts. This problem is why Schmitt objects to a purely result-oriented analysis.[119] According to Schmitt, taking a purely result-oriented approach to solve the "dilemma of how to account for non-kinetically based harm with a system designed to regulate kinetic activities" would not function as an interpretive guide to Article 2(4) but instead "would constitute a new standard."[120]

---

118. Automatic responses, however, would generate the problems discussed above. *See supra* text accompanying notes 106-08. **R**

119. *See* Schmitt, *supra* note 103, at 912-14.

120. *Id.* at 917.

The examples below demonstrate some of the difficulties that different types of IW actions present for the analysis of IW under Article 2(4) and demonstrate the inadequacies of expanding Article 2(4) to include all IW and of trying to evaluate IW attacks on the basis of their similarity to actual uses of force.

1. *Attacks with Delayed Effects*

While an IW attack might cause damage instantaneously, the damage also might not appear for years after the penetration if the attacker merely inserts a Trojan Horse or trap door.[121] As discussed above, this time delay exposes problems in the result-oriented approach. Some types of IW attacks are closely analogous to weapons with delayed effects that are nevertheless considered uses of force. For example, biological weapons might not always have immediate effects, particularly if the disease that is spread has a long incubation period.[122] Delayed effects also are associated often with coercive acts. If the kinetic-action requirement were removed, trade sanctions would be difficult to distinguish from certain conventional strikes. Trade sanctions might have instant effects such as increased prices and eroded economic strength, as well as long-term effects, which might include civilian deaths from poverty and malnutrition.[123] The only remaining difference between sanctions and a conventional strike would be the casualties occurred at the time of the direct strike, which might be minimized in any event by precision-guided munitions. Under a result-oriented approach, it would be extremely difficult to exclude categorically sanctions from the use of force.[124] In effect, the time delay involved in the effects of conventional weapons typically thought of as having a kinetic (physical) impact drove Brownlie's development of the result-oriented approach. The

121. *See supra* text accompanying notes 21-22.

122. Schmitt follows Brownlie's analogy to include biological and chemical weapon attacks within the use of force. *See* Schmitt, *supra* note 103, at 913. R

123. For the case against economic sanctions, see generally John Mueller & Karl Mueller, *Sanctions of Mass Destruction*, FOREIGN AFF., May/June 1999, at 43.

124. Minor sanctions still would not be uses of force because their results would not be as devastating. Not all economic sanctions, therefore, would be included, even in an expanded Article 2(4).

problem is that once the analysis focuses on the results rather than the physical impact, it becomes difficult to preserve the distinction between uses of force, which typically have an instantaneous impact, and acts of coercion, which do not.

The long time horizon during which an IW attack could incubate raises other potential problems by allowing presumed "friendly" parties access to computer systems.[125] For example, the discovery that members of the Aun Shinriko sect had been programmers for important Japanese government computer systems created a fear that they could launch another attack.[126] It is certainly possible that such an actor could plant a logic bomb or leave a trap door in the software which could have potentially disastrous consequences years after it was inserted.[127] The potentially long time horizon for IW attacks could make identifying the attacker hard and make carrying out an appropriate response very difficult.

### 2. *Destruction of Data*

Information Warfare attacks that destroy physical property fit easily within Article 2(4), but extending Article 2(4) to attacks on data requires some expansion of the notion of kinetic impact. Otherwise, neither the weapon nor the result will be kinetic. The analysis depends upon whether there is destruction of life and property. Whether a particular IW attack is a use of force depends on whether the target is considered property, and whether it actually is destroyed. This problem requires extending the definition of property to include data. Destroying a database is analogous to bombing a factory; in both cases the attack destroys property. However, even though destroying data has an analogous economic effect to destroying a factory, there is no actual violence caused by the destruction of the data itself. If the analysis depends only on the destruction of property, there is an attack and therefore a use of force. Given that technological advances have increased the strategic importance of the information industry, there is a clear argument for equating data with property.[128]

---

125. *See* Van Cleave, *supra* note 42, at 173. **R**

126. *See* Warren P. Strobel, *A Glimpse of Cyberwarfare*, U.S. NEWS & WORLD REP., Mar. 13, 2000, at 32.

127. *See* RATTRAY, *supra* note 6, at 400. **R**

128. *See* Schmitt, *supra* note 34, at 1063. **R**

### 3. *Subversion of Property*

Attacks that undermine the value of data create more problems for Article 2(4) use of force analysis than attacks that actually destroy data. Unlike attacks that destroy property, acts of subversion, which could include interfering with satellites, stock market manipulation, denial of service attacks, and industrial espionage, could rob the property of its value without causing any actual physical damage.

Under a traditional Article 2(4) analysis, there would be no weapon used and no property destroyed, so the act would not be a use of force.[129] Assuming data were considered property, would the mere manipulation of the data be a use of force? If the answer depends on the consequences of the manipulation, which might not be immediate, then it becomes very difficult to distinguish manipulation of stock markets, financial transactions, and telecommunications systems from other types of economic coercion, such as sanctions. The target might be whole afterwards, but the parties would be harmed as a result. Another interesting example would be that of manipulating a satellite. The satellite itself would not be damaged; the attacking state interferes only with the victim's ability to receive the satellite imagery. There clearly would be no kinetic impact, nor any damage to property. However, applying more liberal interpretations of the prohibition against force could enable a finding of the use of force on the grounds that the security provided by the satellite had been impaired, and the attacker might be using the victim's blindness to act elsewhere.[130] Expanding the use of force to include acts that undermine the target's security seems to run counter to the long-standing acceptance of espionage as a legitimate action under Article 2(4).[131]

---

129. *See* BOND, *supra* note 61, at 95-96. **R**

130. *Id.* at 88-93.

131. Such an approach could destroy the long-standing distinction between force and espionage. *See* Sean P. Kanuck, Note, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L. J. 272 (1996). Kanuck notes the following distinction:

> [A] tripartite legal distinction exists under international law. The first class of observational, data-collection activities are [sic] simply subject to domestic regulations. The second tier of activities, proactive efforts to influence domestic affairs short of armed engagement, are [sic] most often violations of domestic law and are also

Industrial espionage, in which states use their national intelligence capabilities to benefit their companies, is another form of subverting property.[132] States might use their IW capabilities to further their economic espionage activities by setting back a foreign company's development of certain technology or a key product. In such a scenario, there would be state action that would cause damage to property. The purely economic nature of the actions suggests that economic espionage is an act of economic coercion and therefore is excluded from the definition of use of force. However, applying the consequence-based approach, the attack on the company (and by extension the company's home state) would appear to be a use of force. States that would be victims of economic espionage would not need to rely on Article 2(4) to justify a response. Since the parties involved are typically allies and trading partners, there would be numerous channels through which the aggrieved state would be able to seek redress. Economic espionage illustrates a common problem with a result-oriented approach because including it within Article 2(4) would prohibit an action that many countries consider legal.

Acts of property subversion also highlight the difficulty of classifying some IW attacks as force while excluding others. Since the computer attack intended to steal information is indistinguishable from the attack intended to destroy the information or cause physical damage, when a state conducts computer operations aimed at stealing secrets from a foreign company's systems, these operations are also seemingly a use of force. However, the problem with this reasoning is that it re-

---

"condemned" by international law. Finally, threats or actual use of force are expressly proscribed by the United Nations Charter as well as customary international law.

*Id.* at 276.

Some authors have excluded espionage from the definition of IW entirely. In a cyberattack, the information is destroyed, whereas in an act of espionage, it is merely copied. But this distinction is anachronistic in a digital age where the value of the information is destroyed when it is copied. As data becomes property and data's value is based on its exclusivity, the destruction of the data might occur merely from copying it. If copying the data destroys the value of that data, then that has caused a loss of property by the same means as an attack, which could have destroyed property by kinetic means. *See* Morth, *supra* note 102, at 579-80. **R**

132. *See* Thierry Olivier Desmet, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 97-98 (1999).

quires that any economic espionage committed in cyberspace be considered a use of force when traditional forms of economic espionage—which have the same effects—are not.

4. *Electronic Blockades*

The notion of an electronic blockade presents a trichotomy among electronic blockades, naval blockades, and economic sanctions that cannot be evaluated coherently under Article 2(4). Traditionally, a blockade is an act of war carried out by naval forces.[133] Naval blockades are uses of force because of the violence required in their enforcement, but there is little real difference between electronic blockades and economic sanctions, particularly those sanctions regimes that are enforced vigorously.

According to a kinetic analysis, only a naval blockade would be a use of force. Schmitt's framework probably would exclude electronic blockades from the use of force because they lack immediacy, there is no immediate destruction, the effects are difficult to measure, and the actions are not invasive.[134] While the blockade does create a direct effect, the impact on the target is not immediate and its severity is questionable. According to this analysis, the electronic blockade seems as though it is too similar to coercion to be a use of force.

There are two major problems caused by not defining electronic blockades as uses of force. First, it would make them legitimate under international law. One could argue that an electronic blockade could be a form of quarantine, similar to that imposed by the United States during the Cuban Missile Crisis, but the key to the legitimacy of the quarantine was that it was justified as a defensive action under the Organization of American States Charter.[135] Uses of force conducted with U.N. Security Council authorization have similar legitimacy, but if electronic blockades were left outside of Article 2(4), then states would be free to employ them without multilateral justification.

Second, it would be illogical to differentiate between naval blockades and electronic blockades. An electronic block-

133. *See* Jane Gilliland, Note, *Submarines and Targets: Suggestions for New Codified Rules of Submarine Warfare*, 73 GEO. L.J. 975, 992 n.121 (1985).

134. *See* Schmitt, *supra* note 103, at 911-12.

135. *See* ABRAM CHAYES, THE CUBAN MISSILE CRISIS 88 (1974).

ade potentially could disrupt all communications into and out of the target state and impair seriously the flow of commerce, which could have similar effects to a naval blockade.[136] If the embargo were to shut down the target state's information systems by disabling its servers or by a denial of service attack, that seemingly would be a use of force, since the act would take place within the opposing party's systems and, by extension, its territory. Even if the embargo were accomplished by blocking data transmission before it reached the routers within the target state, this would be analogous to a naval blockade, which is a use of force. Thus, the target state could argue that the blockading state used force in acting against its data transmissions. Electronic blockades cannot be distinguished from naval blockades on the grounds that naval blockades are more effective. While international law traditionally has required that formal blockades be effective, blockades of that nature have long ceased to exist.[137]

While the futility of attempting to differentiate between naval blockades and electronic blockades seems to require including electronic blockades within the definition of use of force, it is similarly difficult to distinguish electronic blockades from economic sanctions. In both electronic blockades and economic sanctions, there is no physical violence, and much of the damage does not occur instantly, but over time.[138] However, the result-oriented approach, which drives the argument for including electronic blockades in the definition of use of force, has its own flaws. If, as a result of sanctions, the target state were unable to repair and maintain its armed forces for lack of spare parts, the target state would be in the same position that it would have been in if the machines had been destroyed in a conventional action.

---

136. *See* GREENBERG ET AL., *supra* note 26, at 12. R

137. One of the conditions of traditional blockade status was that the blockade be effective. While an information blockade likely would not be declared by a belligerent under traditional maritime law, British officials noted before WWI that modern realities dictated abandoning the traditional formality of a complete close-in blockade. *See* James McNulty, *Blockade: Evolution and Expectation*, *in* THE USE OF FORCE, HUMAN RIGHTS, AND GENERAL INTERNATIONAL LEGAL ISSUES, *supra* note 47, at 183-84. For an introduction R to the basic elements of a blockade, see Michael N. Schmitt, *Blockade Law: Research Design and Sources*, *in* 12 LEGAL RESEARCH GUIDES 1, 2-8 (1991).

138. *See* Schmitt, *supra* note 34, at 1071-72. R

### 5. *Electronic Incursions*

While some data manipulations may be uses of force even though they do not destroy their targets, the lowest level of IW attacks further complicates the use of force analysis because such attacks neither cause damage nor substantially impair the target network. When one state probes the servers of another, there is neither harm to life or property nor any physical impact whatsoever. The problem is that, to the target, these electronic incursions do not look any different from those that do cause damage.[139] Under international law, the victim must gauge its response by the amount of damage it sustains; it cannot defend itself unless an attack is underway and it has suffered damage. But by the time a damage assessment is complete, the attack may be over. The victim would have lost its opportunity to defend itself or neutralize the attack.

Probing an adversary's computer systems is similar to the U.S. Air Force practice during the Cold War of sending bombers into Soviet airspace with no intention of causing any damage.[140] The Cold War probes were designed to find the vulnerabilities in Soviet air defenses and learn its response tactics. It is a tactic that did not end with the Cold War; between March 1998 and May 1999, Russian hackers repeatedly penetrated U.S. military information systems in an operation now referred to in the United States as Moonlight Maze.[141] In both instances the goal was the same: In order to be prepared to attack, one must know the enemy's systems.

Due to the massive intelligence requirements, knowing the design and vulnerabilities of the enemy information infrastructure is essential to developing IW capacity.[142] Gathering this intelligence requires frequent probing. While probing servers is intelligence gathering, which has its own set of rules under international law,[143] the nature of IW makes it very difficult for the target state to distinguish intelligence gathering from an attack.

---

139. *See* GREENBERG ET AL., *supra* note 26, at 59-60. **R**

140. *See* MICHAEL BESCHLOSS, MAYDAY: EISENHOWER, KHRUSHCHEV, AND THE U-2 AFFAIRS 77 (1986).

141. Bob Drogin, *Yearlong Hacker Attack Nets Sensitive U.S. Data*, L.A. TIMES, Oct. 7, 1999, at A1.

142. *See* RATTRAY, *supra* note 6, at 142. **R**

143. *See* Kanuck, *supra* note 131, at 276. **R**

### C. *Problems with Relying on Article 2(4) to Regulate IW*

Unlike the case of the U.S. bombers during the Cold War, where the Soviets clearly could know whether the bombers actually had launched any weapons, it is difficult to assess an IW intrusion. There is also the problem that the intelligence itself has value to the victim; the attack erodes the target's security, but international law could not consider every action that affects another country's security to be a use of force.[144] There are too many legitimate actions, such as forming alliances, building up military capabilities, and aiding an unfriendly state's neighbors, which nonetheless affect other states' security, particularly as states increasingly view their national security in terms of their economic strength. Under such a standard, any adverse trade action then could be considered to be a use of force. While it seems unreasonable to consider any action that affects another state's security to be a use of force, it may not be possible to establish reasonable boundaries on how much security must be diminished before an IW attack is considered a use of force. For example, a stock market manipulation might cause a financial loss and damage the target's economy and security, but an adverse trade action might have the same effect, and the latter seemingly would not be a use of force. The actions left outside of Article 2(4) are difficult to distinguish from those covered by Article 2(4).

Either IW attacks must be divided into acts of force and coercion, or the definition of force must be expanded significantly to encompass all IW attacks. Neither solution seems satisfactory. Either similar means or similar results must receive different treatment. The problem with failing to expand Article 2(4) is that it would become underinclusive. IW, like economic sanctions, would become a legal act under international law that many in the international community nonetheless would oppose. That would undermine respect for the prohibition on the use of force, but expanding it might have the same effect. If Article 2(4) prohibited too much conduct that many states deemed integral to their national security,

144. Even though intelligence gathering degrades the target's security, there is a "well established right of nations to employ spies. As such, resort to that practice involves no offense against international law." W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 435 (John Norton Moore et al. eds., 1990).

they would be even more willing to violate Article 2(4), and the prohibition against force might lose its already questioned normative effect.

Even under an expanded Article 2(4), some IW actions might not be considered force, but they still could be potentially destabilizing. If many types of IW strikes were not considered uses of force, some states would be less likely to forgo using these strikes because the strikes would be perceived as being permissible activities, notwithstanding the general norms against intervention. Relying on expanding Article 2(4) requires believing that the U.N. Charter's ban on the use of force can be effective, and that the effectiveness can be maintained if its scope is broadened. Some scholars have argued that international law needs to move beyond the paradigm of Article 2(4) and develop a new paradigm to regulate the use of force because Article 2(4) is so often violated.[145]

Given the difficulties with applying Article 2(4) to some types of IW, it may not prohibit many IW activities effectively. If Article 2(4) cannot be expanded to cover IW while maintaining its effectiveness, then it may be more sensible to seek another method for regulating IW. A treaty on IW would address that concern, though it would raise new problems of its own, such as how to deal with the problems of non-state actors, corporations, and criminal organizations that may acquire IW capabilities.

## V. Other Potential Regimes to Regulate IW

### A. *Existing Treaty Regimes*

There are already treaties that create norms that ultimately could be used to regulate IW. The International Telecommunications Convention prohibits harmful interference with telecommunications.[146] While the effectiveness of the

145. Arend and Beck argue that because Article 2(4) is no longer "authoritative and controlling," it therefore cannot be the standard for international law. Arend & Beck, *supra* note 58, at 194. R

146. *See* International Telecommunication Convention, Oct. 25, 1973, arts. 4, 35, 28 U.S.T. 2495, 2512-13, 2530-31, 1209 U.N.T.S. 255, 257-58, 269. *See also* Roger Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 Naval L. Rev. 57, 62 (1998).

treaty is limited by its state security exception,[147] the creation of a norm analogizing network space to airspace is important to the development of international law in cyberspace, just as the creation of a norm analogizing airspace to territory was important.[148] A violation of the International Telecommunications Convention does not constitute a per se use of force; it is only a violation of international law, the violation of which does not necessarily generate the same opposition.[149] There is nothing in international law specifically designating a disruption of telecommunications as a use of force. The Agreement on the Prevention of Dangerous Military Activities, signed by the United States and the Soviet Union in 1989, which prohibits harmful interference with enemy command and control systems, suggests a possible emergent norm that could make such attacks a use of force.[150]

These norms suggest some concern about the interruptions with telecommunications that would occur in IW. However, none of them seems to go far enough to serve as the predicate for a norm that would prohibit low-level IW activities like economic incursions. Even at higher levels of IW activities, such as electronic blockades that cause little damage, any IW attack could be carried out under a unilateral claim of state security, so the existing treaties would not prohibit such attacks.

### B. *Challenges for a Treaty Regulating Information Warfare*

Article 2(4) and other existing treaty regimes do not create a clear legal prohibition of many types of IW attacks. For international law effectively to address IW attacks, there must be a treaty that directly addresses the issue. While no formal

---

147. "Members also reserve the right to cut off any other private telecommunications which may appear dangerous to the security of the State. . . ." International Telecommunication Convention, art. 19(2), 28 U.S.T. at 2525, 1209 U.N.T.S. at 266; *see also* Scott, *supra* note 146, at 63. R

148. *See, e.g.*, Convention on International Civil Aviation, Dec. 7, 1944, 1948 U.N.T.S. 296; *see also* 1923 Hague Draft Rules of Aerial Warfare, art. 12, *reprinted in* DOCUMENTS ON THE LAWS OF WAR (Adam Roberts & Richard Guelff eds., 3d ed. 2000).

149. *See* BOND, *supra* note 61, at 59 n.102. R

150. *See* Morth, *supra* note 102, at 591-92 (citing Agreement on the Prevention of Dangerous Military Activities, June 12, 1989, U.S.-U.S.S.R., 28 I.L.M. 877). R

treaties dealing with IW have been proposed, there have been calls made for such a treaty.[151] There are, however, numerous potential obstacles involved in regulating IW by treaty. If a treaty regime's flaws are too serious, then states will not comply with it. This section lays out some of the problems such a treaty would have to address.

1. *Problems of Determining Whether There is a State Actor*

a. The Hacker Threat

Not all network incursions are attempts by hostile states to penetrate information systems to attack, or even to gather intelligence for a possible future attack. Currently, the biggest threat to information infrastructure systems is not foreign military IW units, but hackers.[152] The identity of and relationship between the parties is particularly important in determining whether an incursion is a use of force by a state or a criminal act by a private actor.[153] IW attacks may make it very difficult to determine the identity of the attacker.

---

151. *See, e.g.*, Matthew Campbell, *'Logic Bomb' Arms Race Panics Russia*, TIMES (London), Nov. 29, 1998, at 28; *see also* Michael J. Robbat, Note, *Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm*, 6 B.U. J. SCI. & TECH. L. 10, 53-54 (2000).

152. The U.S. government has not systematically evaluated the relative likelihood of different types of IW attacks. However, strategic level IW threats are not likely before 2005. *See* RATTRAY, *supra* note 6, at 509. Anecdotally, hacker-level attacks have been the only publicized IW attacks to take place so far. It is important to note that, while some of these attacks may have been state sponsored, such as the Russian Moonlight Maze penetrations, they have been small-scale attacks and not the type that could be the pretext for widespread operations. While attempting to make the case for the imminent danger of IW, Winn Schwartau focuses almost exclusively on individual "information warriors" who can offer their services to parties looking to use IW for economic gain, but does not focus on states building up Strategic IW capabilities. *See* Schwartau, *supra* note 5, at 55-59. R R

153. *See* JAMES ADAMS, NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE 196 (1998). In Adams's illustrative example, a computer in the United States penetrates a key nuclear facility somewhere on the Korean Peninsula. The victim's identity is crucial. If the victim is South Korea, then the act is a criminal violation, but if a U.S.-based computer has attacked a North Korean facility, the act is hostile and potentially could be considered a use of force. *See also* GREENBERG ET AL., *supra* note 26, at 65-66. R

There are important state responsibility issues as countries that have supported bands of terrorists also might choose to use computer attacks to reach their goals, and the damage could become more widespread. Hackers present another major problem. If they are not controlled or supported by the state, is the state responsible for their actions? The hacker wars between China and Taiwan bring this question into sharp focus, as the distinction between hackers motivated by nationalistic desires and organized, state-sponsored attacks may be impossible to determine.[154] As the ICJ held in the *Iran* case, the actions of a state's citizens can be attributed to the government if the citizens "acted on behalf on [sic] the State, having been charged by some competent organ of the Iranian State to carry out a specific operation."[155] While the Court did not find enough evidence to attribute the actions of the citizens to the government, the Court found that the Iranian government was nonetheless responsible because it was aware of its obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff, was aware of the embassy's need for help, had the means to assist the embassy, and failed to comply with its obligations.[156] Neither of these methods of determining state responsibility is likely to be sufficient in an IW context.

b. Identifying the Source of IW Attacks

Tracing an attack to a state-supported group is difficult enough when the attack is kinetic and the attackers leave physical evidence behind, as in the recent terrorist attacks of September 11, 2001. However, an IW attack might allow geography to mask the actual location of the group initiating the attack. The *Nicaragua* decision noted that an armed attack could include irregulars, which could prove to be a realistic

154. *See China-Taiwan Hacker Wars*, FOREIGN REP., Oct. 21, 1999, LEXIS, News Library, Jane's Defence Publications File. The article notes that while the initial attacks have been limited to hacking into websites, China and Taiwan may be at an early stage in developing the capacity to penetrate and attack each other's critical information infrastructure.

155. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 29 (May 24).

156. *Id.* at 32-33.

analogue to state-sponsored hackers.[157] States might not be willing or able to take the time to litigate the issue of responsibility for hacker attacks before an international tribunal and instead might hold responsible the state in which the hackers are located even if the individuals were in fact acting on their own and not as proxies for the state.[158]

One serious concern would arise if IW attackers were to mask their identities in order to confuse the victim. Assuming that a state reasonably believed it was the victim of an armed attack and that the threat persisted, a response would be legitimate on self-defense grounds. If the victim were to respond against a presumed attacker rather than the actual attacker, it would have attacked a potentially innocent party. A treaty would have to establish mechanisms for dealing with the identification of the attacker as well as the victim's permitted re-

non-state actors could hire hackers to attack banks, communications networks, and stock exchanges for both criminal and political purposes.[160] The attacking government might provide the resources and the hackers would get to keep all or a portion of whatever they were able to steal.[161] Computer crime can be very lucrative, and it could be even more so if the hacker can receive governmental protection to reduce the risk of punishment.[162] This is a potential model for countries that could recruit IW forces to attack countries like the United States at much lower costs—the hackers need not work for military wages in order to achieve their country's military goals. Such symbiotic arrangements could present a very difficult problem for target states attempting to respond to IW attacks where states use private actors as proxies. Such attacks would appear to originate from a private source and could mask government involvement. Unless a pattern of attacks were to develop, it could be very difficult to identify the government involved. This is similar to Solar Sunrise, in which an Israeli, who was not actually at his computer, masterminded the attack.[163] If the sponsor of an attack were to take pains to conceal itself, it might be even more difficult to link the sponsor to the proxies.

d. Determining the Identity of the Victim

Just as the identity of the attacker raises difficult questions for any potential IW treaty, so does the identity of the victim. In an IW context, it becomes necessary to ask whether an attack on a company is an attack on a whole country. It is not necessarily clear that the state in whose territory the injured party resides is the injured state. Suppose the French office of

160. *See* RATTRAY, *supra* note 6, at 198-99 (discussing information mercenaries). R

161. *See* BOND, *supra* note 61, at n.20 (suggesting "strategic criminal operations," though seemingly not really referring to states carrying them out, but only to individuals or transnational criminal organizations). R

162. Vladimir Levin stole $10 million from Citibank's computer system but was caught, and most of the money was recovered. M.J. Zuckerman, *Security on Trial in Case of On-line Citibank Heist*, USA TODAY, Sept. 19, 1997, at 12A.

163. *See generally* Reuters, *U.S. Report: Teen Hackers Plead Guilty to Pentagon Attacks*, *supra* note 43; U.S. Department of Justice, *supra* note 43; Reuters, *Withdrawal Ordered for U.S. Pentagon Hackers*, *supra* note 43.

a U.S. company were the victim of a cyberattack. In a conventional attack, the country where the attack is located has been attacked because its territorial integrity has been violated. Under a traditional use of force analysis focusing on territory, France would have been attacked because that would be the location of the strike. The impact of an attack on the company likely would be borne by the company itself and its shareholders; however, the loss would be felt in the United States, not France. If there were no physical damage, France's sovereignty would not have been infringed at all. Under the destruction of property analysis, the U.S. company would have suffered the damage, so the United States would be the victim of the attack. The effect on the United States would be the same as if that company's U.S. factory were bombed but no one was hurt. The action could be analogized to the attacking state violating trade laws that hurt the U.S. company. While the U.S. government is not injured directly by illegal trade actions, such as its allegations that steel is being dumped onto the U.S. market, under international trade law the state must bring the grievance even though it is the company that suffers the damage. A traceable electronic attack on a U.S. company would create a situation similar to that in the *Chorzow Factory* case, where Germany recovered monetary damages against Poland for its actions against German companies.[164]

2. *Problems of Non-State Actors*

Any attempt to craft an IW treaty also must deal with the problem of the increasing power of non-state actors. Non-state actors have become increasingly powerful at the expense of nation-states. This creates problems for international law as a whole, but would be especially troublesome in the context of an IW treaty.[165] IW will exacerbate non-state actors' impact on the power of the nation-state. This section will explore the general issues that non-state actors possessing IW capabilities cause, and then turn specifically to the problems caused by

164. *See* Chorzow Factory (Ger. v. Pol.), 1928 P.C.I.J. (ser. A) No. 17 (Sept. 13).

165. Michael Schmitt writes: "As might be expected, state-centrism will continue to weaken in the face of the growing influence of intergovernmental and nongovernmental organizations, multinational corporations, and even terrorist groups and international criminal syndicates." Schmitt, *supra* note 34, at 1054. **R**

multinational corporations and transnational criminal organizations (TCOs).

The problems inherent in identifying attackers and victims in IW attacks become even more complicated when the analysis turns to examining non-state actors who cannot be controlled by domestic laws. As non-state actors acquire deadly force in growing amounts with the development and proliferation of IW capabilities, they will put more pressure on the already weakening state system. Attacks carried out by non-state actors cannot be uses of force under Article 2(4),[166] but many potential IW actors are non-state actors. Individuals or small groups could be classified adequately as criminals, but larger non-state groups could cause major problems because they are too big to be controlled by a nation-state. While their actions still would be criminal, law enforcement agencies are unlikely to have the capability to stop them, and the attacks do not fit within the usual conception of criminal action.

Non-state actors do not fit into a traditional use of force analysis.[167] International law focuses on states, but the growing power of non-state actors, such as insurgent groups, multinational corporations, transnational criminal organizations, and non-governmental organizations, is a challenge for traditional international law. Using IW, these groups could attack anywhere and the results would be the same as if a recognized government had committed the act. These questions become particularly difficult when a sub-state actor actually controls significant amounts of territory, as the Revolutionary Armed Forces of Colombia (FARC) does in Colombia.[168]

IW enables non-state actors to increase their military capabilities significantly, more cheaply, and with a lower risk of detection than they could with conventional weapons.[169] The increased geographical range of IW capabilities could enable such groups to attack a target state without ever setting foot in it. This could eviscerate the effectiveness of domestic crimi-

166. *See* U.N. CHARTER art. 2, para. 4. *See also* Kanuck, *supra* note 131, at 276.

167. Louise Doswald-Beck, *Implementation of International Humanitarian Law in Future Wars*, *in* THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM, *supra* note 60, at 39, 58-59. R

168. The FARC controls an area of Colombia the size of Switzerland. *See Hopes and Fears in Colombia*, ECONOMIST, July 17, 1999, at 15.

169. *See* MOLANDER ET AL., *supra* note 31, at 17-18. R

nal/anti-terrorist laws and allow such groups to evade internal security forces. If the threat from non-state actors increases, international law will have to change in order to permit state actors to defend themselves against non-state actors based outside the target country.[170] Also, non-state actors are often much harder to identify than states, particularly when the line between the non-state actor and the harboring state blurs. However these groups are classified, their IW capabilities could create serious problems for potential target states that would not be able to prevent or punish attacks if they could not identify the perpetrators.[171] As political groups, sub-state groups function analogously to states in some ways. They potentially can transform into the state itself, either by taking over the government or by reaching a negotiated settlement to join the government.

Non-state actors who try to build IW forces will have some difficulties. While there are many hackers with the necessary skills, there are nevertheless problems inherent in building what are, in effect, mercenary armies.[172] While non-state actors probably could not obtain strategic IW capabilities, they could still do a lot of damage.[173] IW could increase their military capabilities significantly, making it even harder to distinguish between interstate war and terrorism.

IW creates another problem: If a non-state actor within country A were to attack a target in country B, would state B have the right to defend itself against state A's national information infrastructure (which the non-state group may have coopted) or must it target its response to the non-state group itself?[174] If the victim must limit its response to the non-state

170. *See* Schmitt, *supra* note 34, at 1073-74. R

171. *See* Hanseman, *supra* note 24, at 198. R

172. RATTRAY, *supra* note 6, at 273-74. R

173. The long-term planning and intelligence capabilities that al-Qaeda demonstrated in orchestrating the attacks of September 11, 2001, suggests that non-state groups could acquire the technical requirements to carry out IW attacks.

174. The precedent set by the United States in responding to the September 11, 2001, attacks by bombing the Taliban regime in Afghanistan suggests that a victim's response to a cyberattack may not be limited to moving against the group itself in situations where the sub-state group operates with the assistance of a country, but attacks by insurgent groups still would not enable the victim to respond directly against the state in whose territory the attacker resides.

group, the response almost certainly would not be an IW attack, as that would target state A's national information infrastructure. For example, suppose that the FARC were to launch an IW attack on the United States and that the United States could not rely on the Colombian government to prosecute the FARC. By responding directly against the FARC, the United States would violate Colombia's territorial integrity and conceivably permit Colombia to take action against the United States. At a minimum, it would anger the Colombians by subjecting them to an attack because they could not police their territory adequately. If the victim knew that the attack came from a non-state actor, then the attack would take place outside of the U.N. Charter, and the victim could not rely on Article 51 as a justification for an action taken in self-defense. However, because the attack would have taken place outside the bounds of the Charter, the victim could defend an armed response on the grounds of the traditional right of self-defense. IW increasingly will enable non-state actors to acquire the means of making war, one of the foundations of the definition of the state in international law. If this type of attack were to become common, it would expose a major flaw in the U.N. Charter system and significantly reduce states' willingness to adhere to it.

a. Multinational Corporations

The growth in the size and influence of multinational corporations (MNCs) has created a powerful group of actors who are outside the state-based international law framework. Despite their increasing power, corporations are not considered "subjects" of international law. In fact, corporations benefit from receiving many of the protections of international law through their host states without the obligations international law imposes.[175] Leaving corporations out of international law only works on the assumption that states can control MNCs' actions sufficiently. If corporations cannot be controlled by individual states, the international community as a whole will

175. *See* Peter Malanczuk, *Multinational Enterprises and Treaty-Making—A Contribution to the Discussion on Non-State Actors and the "Subjects" of International Law*, *in* MULTILATERAL TREATY-MAKING: THE CURRENT STATUS OF CHALLENGES TO AND REFORMS NEEDED IN THE INTERNATIONAL LEGISLATIVE PROCESS 62 (Vera Gowland-Debbas ed., 2000).

need to devise a new arrangement for corporate interactions with states.

MNCs' capacity to develop IW capabilities threatens to augment their power, particularly because they already have the technological capability and resources needed to conduct IW operations.[176] They also have begun to develop their own intelligence capabilities.[177] Corporations have become very powerful but are still largely excluded from the political system. Though they often face extraterritorial regulation through competition laws and anti-corruption measures such as the Foreign Corrupt Practices Act,[178] they still maintain significant operating autonomy in their international operations.

In limited circumstances, MNCs might choose to use their IW capabilities. They are unlikely to unleash Strategic IW attacks against opponents, but they might undertake attacks with more limited goals. MNCs could attack each other without causing serious collateral damage, but the possibility that such battles could cascade through the world economy with devastating effects is probably a sufficient deterrent to large-scale attacks.[179] However, a credible threat of an IW action could be sufficient to allow a company to extract important concessions from a competitor or even a state. Companies might try to destroy proprietary information or launch attacks against competitors at critical production times or on critical network nodes. A well-timed denial of service attack could delay a key inventory shipment or production segment and seriously harm a competitor.

---

176. *See* CYBERCRIME . . . CYBERTERRORISM . . . CYBERWARFARE . . . : AVERTING AN ELECTRONIC WATERLOO 26 (Center for Strategic and Int'l Stud. ed., 1998).

177. According to abcnews.com, 82% of companies with revenues in excess of $10 billion have their own intelligence units. *See* Katherine Hobson, *Corporate Intelligence Seen as a Necessity—Spies Like Us*, *at* http://www.mnemotrix.com/texis/cust/rwipromo/+IwqBme-DmhWmwww/article.html (Sept. 24, 1998); *see also* Karen Sepura, Note, *Economic Espionage: The Front Line of a New Economic War*, 26 SYRACUSE J. INT'L L. & COM. 127, 135-36 (1998).

178. *See* PETER MUCHLINSKI, MULTINATIONAL ENTERPRISES AND THE LAW 126-27 (1999). For more on the Foreign Corrupt Practices Act, see Symposium, *A Review of the Foreign Corrupt Practices Act on Its Twentieth Anniversary: Its Application, Defense and International Aftermath*, 18 Nw. J. INT'L L. & BUS. 263 (1998).

179. *See supra* text accompanying note 108. **R**

The potential costs of economic disruption and antitrust laws may not be strong enough to deter a MNC's desire to attack its competitors. While companies have an incentive to obey the law, they also have an incentive to remain as close to the law's boundaries as possible in order to maximize profits. IW gives companies another tool to conceal anti-competitive actions against their competitors. As MNCs grow more powerful, national governments may have more trouble enforcing laws against them. MNCs that use IW against their competitors might do so through proxies so that the actions cannot be traced to the MNC itself. They also could locate the attacks in states where they might be exempt from competition laws.

MNCs also might be able to use IW against states. While no company would attack a major industrialized state, IW could be a potent threat to less developed states. For example, a corporation that installed an infrastructure system in a developing country potentially could hold that state hostage by threatening to destroy or manipulate the system. The MNC might leave a trap door in the software it installs through which it could re-enter if it chose to do so at a later date. Such threats could give the corporation leverage on future contracts or conceivably even influence over national policy.

MNC information warfare capability could give companies many of the same powers as nation-states, and they would have the ability to influence nation-state activity on the strength of their economic and military power. Anthony D'Amato has raised the issue of how to apply public international law to corporations, questioning whether international law would be used, or a new "intercorporate law" would evolve to handle "intercorporate warfare." He hypothesizes that the largest corporations might set up their own governing body based on the pursuit of profit.[180] Given this reality, nation-states may be forced to look to corporations as partners in international agreements, giving them a recognized status under international law.

b. Transnational Criminal Organizations

Criminal organizations are an interesting hybrid of sub-state groups and corporations. Their illegitimate activities are

180. Anthony D'Amato, *Megatrends in the Use of Force*, *in* THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM, *supra* note 60, at 1, 14-15. R

similar to those of sub-state groups, but their profit-seeking objectives drive them to act like corporations. In effect, they are rogue corporations, not bound by the laws that constrain legitimate corporations. They have many of the same capabilities as states.[181] In some places, they also take on state responsibilities such as the provision of social welfare services.[182] They will take whatever measures are necessary to protect their business operations, but they do not want to cause too much damage to the economies where they do business. While difficult to calculate, the estimates of global organized crime activities are staggering.[183] Criminal organizations have no qualms about using violence, maintain near-total secrecy, and have tremendous organizational flexibility.[184] They have the same resources and incentives as corporations to use IW but do not face any of the deterrents. There are also significant ties between criminal organizations and sub-state groups. The Tamil Tigers, FARC, and Somali warlords all maintain significant ties to drug trafficking in order to finance their wars.[185]

Criminal organizations have the resources to conduct widespread IW operations and already commit large-scale computer crime.[186] Their goals are typically to evade the state, and they are willing to use terror against governments in order to deter investigations.[187] They certainly could use the threat

---

181. Peter A. Lupsha, *Transnational Organized Crime Versus the Nation State*, 2 TRANSNAT'L ORGANIZED CRIME 21, 34-35 (1996).

182. Louise I. Shelley, *Transnational Organized Crime: The New Authoritarianism*, *in* THE ILLICIT GLOBAL ECONOMY AND STATE POWER 25, 35-36 (H. Richard Friman & Peter Andreas eds., 1999).

183. It is estimated that TCOs launder $300-$500 billion per year, 60-70 percent of which is not drug related. *See* Carol Hallett, *The International Black Market: Coping with Drugs, Thugs, and Fissile Materials*, *in* GLOBAL ORGANIZED CRIME: THE NEW EMPIRE OF EVIL (Linnea Raine & Frank Cilluffo eds., 1994). Organized crime activities extend far beyond drugs to smuggling illegal immigrants; trafficking in arms and nuclear materials; prostitution; vehicle smuggling; trading in illegal animals; trafficking of cultural objects and art pieces; smuggling precious metals; and trading vital organs for transplants. These groups also earn large commissions for money laundering. *See* Phil Williams & Ernesto U. Savona, *The United Nations and Transnational Organized Crime: Problems and Dangers Posed by Organized Transnational Crime in the Various Regions of the World*, 1 TRANSNAT'L ORGANIZED CRIME 1, 21-29 (1995).

184. *See* Lupsha, *supra* note 181, at 34-35. **R**

185. *Id.* at 28.

186. *Id.*

187. Williams & Savona, *supra* note 183, at 24-25. **R**

of violence as an intelligence-gathering tool. They might be inclined to use IW in order to attack national law enforcement systems, or threaten IW attacks on civilian or infrastructure targets to persuade governments to cease their investigations. A powerful IW threat could lead to a familiar pattern of tacit agreements between TCOs and states whereby the TCO limits violent actions in return for the state's failing to pursue them.[188]

c. Increased Power of Non-State Actors Presents a Challenge to International Law

The ability of non-state actors to acquire IW capability presents a difficult problem. These groups are not subject to the U.N. Charter, and their actions do not constitute uses of force under Article 2(4). Nonetheless, IW presents them with the capability to make war on a level with many states. IW attacks could enable them to bend states to their will on a scale that traditional terrorist activities have not been able to do. Furthermore, IW would enable them to possess a real war-making capability. If the state system is based on the recognition of those parties who are able to fight and win wars, these groups seemingly cannot be excluded, but there are dangers inherent in recognizing all parties who have IW capabilities, because granting such recognition only would encourage more groups to develop them. The problem is similar to the non-proliferation dilemma surrounding nuclear weapons where greater status typically is accorded to nuclear states even as the nuclear states attempt to persuade the non-nuclear states not to develop their capabilities.

Non-state groups traditionally have had an undefined role in international law.[189] IW threatens to change the balance of power between non-state actors and states by giving the non-state actors some of the same war-making capabilities as states. If the original basis for state recognition was the ability to make war, then the increased military capacity of non-state ac-

188. *Id.* at 35.

189. *See, e.g.*, Karsten Nowrot, *Legal Consequences of Globalization: The Status of Non-Governmental Organizations Under International Law*, 6 IND. J. GLOBAL LEGAL STUD. 579, 580 (1999); Julie Mertus, *From Legal Transplants to Transformative Justice: Human Rights and the Promise of Transnational Civil Society*, 14 AM. U. INT'L L. REV. 1335, 1375-76 (1999).

tors as a result of proliferation of IW capabilities could undermine the Westphalian system.[190] The possibility of an IW treaty raises the question of whether these non-state actors can participate in the process. Both criminal organizations and corporations make agreements with their competitors and with states.[191] Sub-state insurgent groups frequently have contacts with the government that they are resisting, as well as with other governments and insurgent groups. Of the three types of groups, corporations would be the most likely to join an agreement on IW; they do follow most laws and they have an interest in limiting the IW threat. On the other hand, substate insurgent groups and criminal organizations could not easily become parties to a treaty, since their host states and many others are committed to eradicating them. Their exclusion would not render an IW treaty regime meaningless, but it would undermine its effectiveness.

### C. *Will Countries Comply with an IW Treaty?*

There are many variables involved in determining whether a treaty would be an effective way of dealing with the threat of IW. The first issue is whether states actually would sign an effective treaty. While major industrialized states would have the most to lose from widespread IW use, many might be uncomfortable foreclosing, or at least stigmatizing, an undeveloped area of military doctrine.[192] Unlike chemical or biological weapons, cyberwarfare does not seem inherently immoral—many effects of an IW attack are similar to those of conventional attacks. Another major question is whether the U.S. Senate would ratify such a treaty. Given its historical reti-

---

190. IW simply creates the possibility that non-state actors will have the capacity to wage war to a much greater extent than they previously had.

191. *See* CLAIRE STERLING, THIEVES' WORLD: THE THREAT OF THE NEW GLOBAL NETWORK OF ORGANIZED CRIME 14 (1999) (describing the commonplace nature of agreements among criminal organization alliances). Sterling also notes that the Cuntreras crime family had a long-standing, though unofficial, agreement with the government of Venezuela that allowed it to control the island of Aruba. *Id.* at 21-22. Multinational corporations frequently form joint ventures with competitor corporations. *See Coca-Cola and Proctor & Gamble Form Joint Venture to Produce Juices and Snacks*, FOOD & DRINK WKLY., Feb. 26, 2001, LEXIS, News Library, All News Group File.

192. GREENBERG ET AL., *supra* note 26, at 101. **R**

cence in agreeing to treaties,[193] it may reject the treaty or weigh it down with reservations.

In determining whether states would sign and comply with an IW treaty, it would be helpful to examine why nations observe international law. Certainly, as Henkin notes, "almost all nations observe almost all principles of international law . . . almost all of the time."[194] However, the realist critique of international law is that without an enforcement regime, it is not really law. The rationalist view is that nations only obey international law when it is in their self-interest to do so.[195] Echoing this view, Henkin writes that "barring an infrequent nonrational act, nations will observe international obligations unless violation promises an important balance of advantage over cost."[196] The question, therefore, is whether an IW treaty will survive a cost-benefit analysis.

How would states perceive a prohibition on IW? The United States, for example, has more to lose by damaging interconnected global financial markets than any other actor.[197] Furthermore, most of the best targets are either U.S. allies or countries where U.S. corporations have invested heavily because these countries have the highest level of computerization. Other industrialized states, such as Japan, Germany, France, and Great Britain, with large potential IW capabilities may be similarly deterred because they see cyberattacks, even against potential rivals, as adversely affecting their own economies due to the interconnected global economy and the cascading effects of IW attacks. Russia and China, who are the strongest opponents to perceived U.S. hegemony and states with the potential to field Strategic IW capabilities, might

---

193. *See, e.g.*, Eric Schmitt, *Senate Kills Test Ban Treaty in Crushing Loss for Clinton; Evokes Versailles Pact Defeat*, N.Y. TIMES, Oct. 14, 1999, at A1; Apple, Jr., *supra* note 159, at A1 (reporting the Senate's rejection of the Comprehensive Test Ban Treaty). R

194. HENKIN, *supra* note 76, at 47. R

195. *See* Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 YALE L.J. 2599, 2602 (1997) (describing the rationalist and realist views of international law).

196. HENKIN, *supra* note 76, at 50. Franck also acknowledges that nations obey rules when the benefits of complying exceed the costs. *See* Franck, *supra* note 70, at 836; Koh, *supra* note 195, at 2642. R R

197. *See* BOND, *supra* note 61, at 95 n.162 (noting that the United States would "probably be wise to not set precedents establishing the practice of data manipulations"). R

make a different calculation. While they too would suffer secondary damage if they were to launch a series of IW attacks, they might perceive the benefits of such attacks—damaging the economies of the United States and its allies and the prestige value of having countered U.S. imperialism—as greater than the economic costs of the secondary effects they would bear. Smaller states, which will be able to develop smaller—but still dangerous—IW capabilities, might make the same calculation despite the damage to their international standing from the inevitable condemnations for violating international law with their attacks.

## VI. Conclusion

As IW strategy and technology evolve, international law scholars will have to fit this new kind of warfare into an analytical framework developed to address a very different conception of war. Article 2(4) was drafted to prevent another world war. Today, that fear has been replaced by the threat of many small wars using a wide array of weapons: conventional, economic, or possibly electronic. Article 2(4) has excluded actions such as economic aggression and threats of force, which makes states more willing to take these actions. Leaving many IW actions out of Article 2(4) could provide states with a loophole through which to evade the prohibition on the use of force.

The problem IW poses for Article 2(4) does not derive from its large-scale applications, but from attacks that do not destroy life or property, such as subversion of property, electronic blockades, and incursions. The large-scale attacks are similar to conventional methods of warfare and fit comfortably within traditional use of force analysis. The lower-level attacks present the problem for Article 2(4). They cannot be analyzed readily under Article 2(4) because they threaten to erase the distinction between acts of force and acts of coercion. The severity of an IW attack cannot be identified readily, so it would not be feasible to require a victim to conduct a damage assessment to determine whether an IW penetration were a use of force or merely of coercion. More importantly, while an intrusion might have been detected, the full extent of the attack might not be known for some time. IW attacks that are

acts of force cannot be distinguished readily from those that are not.

The tools for analyzing conventional actions under Article 2(4) do not lend themselves well to IW. Neither Michael Schmitt's six-factor test nor the result-oriented approach is adequate. Schmitt's approach does not deal with low-level IW attacks adequately, as these attacks would be excluded from the use of force under his analysis. While more serious attacks would be included, the target may not know which type of attack it had suffered. The result-oriented test does not provide any way to differentiate between acts of force and coercion: If the kinetic impact of an attack is not relevant, the resulting damage may be the same whether the victim suffers a missile attack or economic sanctions.

Given Article 2(4)'s inability to cope with electronic incursions and blockades and subversion of property using IW, a treaty regime may be a better solution to regulate IW. A treaty, however, would face some major obstacles. One major challenge would be the problem of non-state actors, particularly corporations and criminal organizations. While such groups present problems for international law as a whole, their challenge to an IW treaty is especially problematic. Such groups would not be bound by a treaty; furthermore, IW technology could increase dramatically their military capabilities. The lack of regulation of their IW activities combined with their growing power could create serious problems for many national governments and for the state-based international system as a whole.

Even without the growth in power of non-state actors, an IW treaty would have to overcome serious problems arising out of the nature of IW attacks themselves. The identity of an IW attacker can be more readily concealed than that of a conventional attacker. It also might be possible for private citizens of a state to launch an IW attack on a hostile state, with or without their government's complicity. A treaty with any type of compliance regime also would have to address serious sovereignty concerns as potentially millions of computers would be subject to search.

Finally, even if all of these concerns were addressed, a treaty would face the challenge of whether states actually would comply with a ban on IW. The increased interdepen-

dence that the electronic age has brought suggests that many countries would decide that launching an IW attack was not in their best interest. But some states might decide that the benefits of attacking outweigh the costs. It is too early in the development of IW to state with any certainty which direction the technology will take or how the law will have to adjust to future developments, but it is very likely that international law will need new tools and conceptual categories in order to address these new weapons.