Information Warfare as International Coercion: Elements of a Legal Framework

Christopher C. Joyner* and Catherine Lotrionte**

Abstract

Worldwide interconnectivity through massive computer networks now makes states vulnerable to new threats. Foreign governments can launch computer-based assaults, or acts of information warfare, on another state's domestic systems such as energy grids, telecommunications, and financial facilities that could severely damage or disrupt national defence or vital social services. Even realizing the new forms of computer-generated weapons and changing concepts of sovereignty and territory brought about by global interdependence, international law is likely to rely on UN Charter principles to define the legal boundaries of cyberspace. While perhaps not armed force literally, resort to cyberforce may be viewed as a form of intervention that can produce harmful or coercive effects, and put at risk the national security of another state. There is need for modern international law to define more precisely the criteria used to distinguish which state actions are permissible as normal computer-generated transborder data flow from those cyberactivities that might qualify as an 'armed attack' against a state. Clearer rules are also needed for what responses are permissible as self-defence by a state targeted in an information warfare situation and how international institutions might facilitate the attainment of these objectives.

1 Introduction

Alvin and Heidi Toffler's *The Third Wave* proclaimed in 1991 the dawn of the Information Age. They depicted the history of the world in three waves — the

* Professor of International Law, Department of Government, Georgetown University.

** Assistant General Counsel, Office of the General Counsel, Central Intelligence Agency; Adjunct Professor, National Security Studies Program, Georgetown University. The authors would like to thank Anthony Clark Arend, Professor Dorothy Denning and Phillip Johnson for assistance and comments made during the preparation of this study. The views expressed in this article are those of the authors alone and do not necessarily reflect the position of the United States Government.

agricultural wave, the industrial wave, and the information wave.[1] A decade later, the Information Age has fundamentally transformed the way in which the world operates. Global proliferation in computer interconnectivity, most notably the profound growth in use of the Internet, has revolutionized the way governments, societies and much of the world communicates and conducts business.[2]

At the same time, the technology-intensive Information Age brings with it opportunities for 'cyber-crime', 'cyber-war' or, as more aptly put, the prosecution of 'Information Warfare'. Western societies have spent years building information infrastructures that are interoperable, easy to access and easy to use. Attributes such as openness and ease of connectivity that promote telecommunications efficiency and expedite customer service also now render a society's information infrastructure vulnerable to attacks from other computerized systems.[3] The implications of these developments are clear. Particularly regarding how governments conduct wars and use military force, the Information Age promises profound changes in the future. The manners and means in which states interact internationally are dramatically changing.[4] Given such realities, international legal rules also must be dramatically adapted if new cyberspace technologies are to be regulated, or even managed, in their increasingly pervasive transnational applications.

This study examines known techniques of Information Warfare (IW) and the international legal implications generated by their use. For purposes of definition, our study considers IW to be a subset of Information Operations that is 'conducted during time of crisis or conflict to achieve or promote specific objectives over a specific

[1] See Alvin and Heidi Toffler, *The Third Wave* (1991). See also Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (1993) (the emerging knowledge-based society will use knowledge-based systems to conduct warfare).

[2] Stocks are purchased on-line. Applications for employment are made on-line. Work is done on-line. University degrees are earned on-line. Airplane tickets are bought on-line. Communications with friends occur on-line. People even register to vote on-line. The benefits of the computer-based Internet system are enormous. Vast amounts of information are literally at the fingertips, facilitating research on virtually every topic imaginable. Financial and other business transactions can be executed almost instantaneously. Electronic mail, Internet websites and computer bulletin boards allow instantaneous communications quickly and easily with virtually an unlimited number of persons or groups.

[3] A General Accounting Office report stated that the Defense Department was subjected to 250,000 information warfare attacks in 1995. See US General Accounting Office, 'Information Security: Computer Attacks at Department of Defense Pose Increasing Risks', Report No. GAO/T-AIMD-96–92 (1996) www.access.gpo.gov/su_docs/aces/aces160.shtml?/gao/index.html (visited 18 July 2001). The Pentagon asserts that there were only 500 incidents this year. See Maier, 'Is US Ready for Cyberwarfare?', *Insight on the News*, 5 April 1999, at 18. Today, financial institutions can be defrauded on-line. Trade secrets can be stolen on-line. Extortion and blackmail can be committed on-line. People can be impersonated on-line. Commerce can be disrupted on-line. Persons can be stalked on-line. Even a war can be started on-line. See Cilluffo *et al.*, 'Cybercrime ... Cyberterrorism ... Cyberwarfare, Averting an Electronic Waterloo' (Center for Strategic and International Studies Task Force Report, 1998).

[4] See Alvin and Heidi Toffler, *War and Anti-War* (1993) 2. See Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Senate Commission on Government Affairs, 104th Cong. (1996) 150, at 155 (testimony of Jamie S. Gorelick, Deputy Attorney-General, describing how technology generally, and information networks specifically, play critical roles in the functioning and development of these important areas).

adversary or adversaries'.[5] The realistic potential of instigating IW underscores the changed nature of the globalized world environment, as well as the technological revolution in how transnational conflict might be conducted in the twenty-first century. Coincidentally, both these developments highlight the need to develop or amend the rules and criteria on which factual assertions are based for a state to employ force against another state. The transnational nature of IW suggests that, while international legal norms found in contemporary UN Charter law are helpful, they may not be sufficient for reaching acceptable solutions.[6]

[5] Traditional means of conducting IW include psychological operations, electronic warfare, military deception, physical destruction and information attack. For example, in using IW a government could manipulate the enemy's reasoning (i.e. psychological operations), deny accurate information to the enemy (i.e. electronic warfare), mislead the enemy about its own capabilities and intentions (i.e. military deception), use conventional bombs or electromagnetic pulse weapons targeting information systems of the enemy (i.e. physical destruction) and corrupt information without visibly changing the physical entity within which it resides (i.e. information attacks). The US Air Force defines information warfare as 'any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions'. Department of the Air Force, 'Cornerstones of Information Warfare' (visited 18 July 2001), www.af.mil/lib/corner.html. See also Chairman of the Joint Chiefs of Staff, Joint Publication 1–02, *Dictionary of Military and Associated Terms* (1998) 422, available at www.dtic.mil/doctrine/jel/new_pubs/jp1–02.pdf; Office of the Chief of Naval Operations, Department of the Navy, OPNAVINST 3430.26, at 1 (18 January 1995) ('Information warfare is the action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems'); Dorothy E. Denning, *Information Warfare and Security* (1999) 23 ('Information warfare consists of offensive and defensive operations against information resources of a "win–lose" nature'). For some general discussions on Information Warfare, see Alrich, 'The International Legal Implications of Information Warfare' (US Air Force Institute for National Security Studies Occasional Paper 9, April 1996) 3–5; Martin C. Libicki, *What Is Information Warfare?* (Center for Advanced Command Concepts and Technology, Institute for National Strategic Studies, National Defense University, August 1995) (identifying seven forms of Information Warfare); Stein, 'Information Warfare', *Airpower Journal* (Spring 1995) 31–39; Colonel Richard Szafranski, USAF, 'Theory of Information Warfare: Preparing for 2020', *Airpower Journal* (Spring 1995) 56–65; Winn Schwartau, *Information Warfare: Chaos on the Electronic Highway* (1994) (defining IW into three categories according to the nature of the defence); and Arquilla and Ronfeldt, 'Cyberwar is Coming!', 12 *Comp. Strategy* (April–June 1993) 141 (introduces the concept of 'cyber-war' for the purpose of examining knowledge-based conflict at the military level). See also Haeni, 'An Introduction to Information Warfare' (visited 19 July 2001), www.tangle.seas.gwu.edu/reto/infowar/info-war.html.

[6] These Charter-based rules were designed for a world where military conflict mainly involved large-scale armed attacks by one state against the territory of another, such as those in the First World War, the Second World War and on smaller scales throughout the Cold War. During those conflicts, governments could count an enemy's planes, tanks and ships. From these assessments, a government could decide how to organize its defence based upon its calculations of the enemy's offensive threat capabilities. The use of cyber-space technologies makes the determination of an enemy's assets more difficult and thus complicates arrangements for setting up adequate defensive strategies. See generally Vizard, 'War.Com: A Hacker Attack Against NATO Uncovers a Secret War in Cyberspace', *Popular Science*, 1 July 1999, at 80. It is difficult to manage risks in conflict or to know what assets must be spent on defence, especially when who, where or what IW weapons an enemy possesses remain unknown factors. See also Rattray,

The rise of IW technologies in post-Cold War conflicts[7] provokes questions about the legal definitions of 'armed attack' and 'self-defence' as articulated in the UN Charter, the norms for contemporary state behaviour, and the factual basis involved in IW activities. Claims that a government has surreptitiously penetrated another country's information infrastructure and caused great physical harm raise complex factual issues not previously present when states confronted and openly attacked each another with armies, planes, ships, tanks and conventional weapons. It may be difficult to attribute an IW attack to any particular foreign state, or to characterize that government's motive or intent. An IW attack might be initiated by a foreign private entity or person without state sponsorship. Or a foreign state could hire mercenary-like individuals to carry out an IW attack without attribution to state sponsorship. A cyber-attacker may not be physically near the locations where the attack is launched or where its effects impact. The means of a cyberspace attack may not be readily detectable. A virus sent to a computer via an e-mail attachment will not be readily apparent, as missiles are when they are launched. Under all these circumstances, what lawful action may a state take to respond? The recent availability of IW requires reconsideration of the fact-finding processes and criteria used by governments to make assessments concerning if or when force may be used transnationally through their computer systems.

This article examines how IW is regarded within the context of contemporary international legal rules. It assesses the vulnerabilities of state information infrastructures to these cyberspace technologies, including threats to their national security,[8] and the reality of their international applications. International legal rules regulating the use of force are then analyzed as they apply to the use of IW techniques. This analysis also seeks to determine whether and when cyber-based IW activities might qualify as permissible uses of force. Finally, suggestions are made for criteria that contribute to clarifying the legal nature of IW and to designing a more appropriate regulatory framework. At bottom this study evaluates which legal rules applicable to IW might be used by governments to conduct their foreign policies in compliance with international law and which applications of cyberspace activities present serious legal challenges to maintaining order in contemporary relations among states.

'The Emerging Global Information Infrastructure and National Security', *Fletcher Forum on World Affairs* (Summer–Fall 1997) 81, at 93–95 (describing the need for multilateral efforts to control information warfare and positing several different international mechanisms); see also Anthony Lake, *6 Nightmares* (2000) 57 (citing Deputy Secretary of Defense John Hamre's statements on the difficulties of dealing with the lack of borders in cyberspace).

[7] See Allard, 'The Future of Command and Control: Towards a Paradigm of Information Warfare', in L. Benjamin Ederington and Michael J. Mazarr (eds), *Turning Point: The Gulf War and US Military Strategy* (1994) 161, at 166; Department of Defense, 'Conduct of the Persian Gulf Conflict: Final Report to Congress' (1992); Swalm, 'Joint STARS in Desert Storm', in Alan D. Campen (ed.), *The First Information War* (1992) 167.

[8] For a more extensive discussion of the threats to the national security from abroad see James Adams, *The Next World War* (1998); and Lake, *supra* note 6.

2 Defining the Threat

The pace of developing cyber-technologies and the Internet's ubiquity have brought not only advances in the quality of life, but also new international threats to governments. As nation-based cyber-systems assume increasingly complex, more intricate roles in international commerce, daily life and national defence, these computer networks have become more vulnerable to transnational threats. Interconnectivity aggravates the risk that disabilities affecting one system will also infect other interconnected systems.[9] Massive computer networks provide multiple pathways between and among systems that, if not properly secured, can be operated from remote locations to gain unauthorized access to data and operations in other states. The resultant damage can vary, depending on the type and extent of the IW threat. Critical system operations can be disrupted or otherwise sabotaged, sensitive data can be read and copied, and data or processes can be altered. There is today significant concern that hostile foreign governments could launch computer-based attacks on critical national or regional systems — such as those supporting energy distribution, telecommunications and financial services — that severely damage or disrupt national defence or other vital social services and result in serious harm to the public welfare.[10]

Western societies are particularly cognizant of cyber-based security concerns.[11]

[9] See Defense Science Board Task Force, *Information Warfare: Defense* (IW-D) (November 1996) 2–15 ('Our task force had many enlightening discussions about the potential for effects to cascade through one infrastructure (such as the phone system) into other infrastructures. No one seems to know quite how, where, or when effects actually would cascade; nor what the total impact would be'). The Office of Science and Technology Policy, Executive Office of the President, highlighted the dilemma: 'The public telephone network, for example, relies on the power grid, the power grid on transportation, and all the sectors on telecommunications and the financial structure ... Most of today's cybernetic networks are actually combinations of networks, interconnected and interdependent. Interactions among these subsystems are critical to overall network performance. Because the system also interacts with the real world environment, the interactions among subsystems are not necessarily predictable and sequential, like the steps of an assembly process, but can be essentially random, unsynchronized, and even unanticipated.' IW-D, *ibid.*, at 2–14.

[10] See Graham, 'US Studies New Threat: Cyber Attack', *Washington Post*, 24 May 1998, A1. In mid-1997, a National Security Agency 'hacker team' broke into Defense Department computers and the US electric power grid system as part of the 'Eligible Receiver' exercise. The team simulated a series of rolling power outrages and 911 emergency telephone systems overloads and foiled FBI and Pentagon efforts to trace the attackers. The success of the simulated attack spurred efforts by the government to overcome the vulnerabilities, which still exist. For a detailed description of 'Eligible Receiver', see Denning, *supra* note 5, at 23.

[11] President Clinton recently highlighted the escalating threat posed by IW when he averred that: 'Our security is challenged increasingly by nontraditional threats from adversaries, both old and new, not only hostile regimes, but also international criminals and terrorists who cannot defeat us in traditional theaters of battle, but search instead for new ways to attack by exploiting new technologies and the world's increasing openness.' President Clinton's commencement address to the US Naval Academy, May 1998. See also Woolsey, 'Resilience and Vulnerability in the Information Age', in Stuart J.D. Schwartzstein (ed.), *The Information Revolution and National Security* (1996) 79, at 82–83 (describing

Similarly, the intelligence community is seriously concerned.[12] In the event a state's vital information network infrastructure stops functioning, an Information Age society could be paralyzed and collapse into chaos.[13] Industries that benefit from cyber-technological advances could be immobilized if critical networks providing power, transportation, national defence and medical services are attacked and brought down.[14] The pervasively destructive potential of cyber-based IW presents new international military implications and invites new analytical considerations of where IW fits into the body of contemporary international legal rules pertaining to the use of force.[15]

---

incentives rogue states and terrorist groups have to engage in information warfare); Mann, 'Cyber-Threat Expands with Unchecked Speed', *Aviation Week and Space Technology*, 8 July 1996, 63, at 64 (reporting that CIA Director John Deutch ranks threats of information warfare as 'a close third behind the threats from weapons of mass destruction … and the proliferation and terrorist use of nuclear, biological, and chemical … weapons').

[12] In June 1998 and February 1999, the Director of Central Intelligence (DCI) testified in Senate hearings that several governments now recognize that computer attacks against civilian computer systems represent an option that foreign enemies could use to 'level the playing field' during an armed crisis against the United States. As DCI George Tenet observed: 'Who would consider attacking our nation's computer systems? Yesterday, you received a classified briefing answering this question in some detail. I can tell you in this forum that potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders.' See Cyber Attack: Is the Nation at Risk?, Hearing before the Senate Committee on Government Affairs, 105th Cong. (24 June 1998) 10 (testimony by Director of Central Intelligence George J. Tenet), www.odci.gov/cia/public_affairs/speeches/dci_testimony_062498.html. See also Mann, *supra* note 11, at 64 (reporting that former DCI, John Deutch, ranked threats of information warfare as 'a close third behind the threats from weapons of mass destruction … and the proliferation and terrorist use of nuclear, biological, and chemical … weapons'). More instructively, former Deputy Attorney-General Jamie S. Gorelick provided real world examples that demonstrated the vulnerabilities of US computer systems: 'In 1992, a computer intruder was arrested for tampering with the Emergency 911 systems in Virginia, Maryland, and New Jersey in order to introduce a virus and bring down the systems. Also in 1992, a fired employee of an emergency alert network sabotaged the firm's computer system by hacking into the company's computers, causing them to crash for about 10 hours. During that time, there was an emergency at an oil refinery. The disabled system was therefore unable to alert thousands of nearby residents to a noxious release from the refinery. Finally, a sniffer was introduced into computers of NASA's Goddard Space Flight Center, permitting someone to download a large volume of complex calibration telemetry calculations transmitted from satellites. The sniffer remained undetected for an unprecedented length of time.' The Honorable Jamie S. Gorelick, Deputy Attorney-General of the United States, at the US Air Force Academy, Colorado Springs, Colorado, 29 February 1996, available at www.lawyernet.com/members/jimfesq/wca/1996/28/deep.html.

[13] See Schwartau, *supra* note 5, at 308–310 (describing how a concerted attack against critical financial and communication networks could result in widespread panic and lead to a situation resembling anarchy).

[14] See Laqueur, 'Postmodern Terrorism', *Foreign Affairs*, September–October 1996, at 14 (arguing that a computerized, information-warfare-based attack initiated against the Federal Reserve's main switching terminal in Culpepper, Virginia, would be disastrous to the United States); see also Schwartau, *supra* note 5, at 308–310 (describing the spiralling confusion and panic a concerted series of information-warfare attacks could cause).

[15] The conflict in the Persian Gulf illustrates the importance of infrastructures to US national defence — our domination of Iraq's information and communications ensured victory over a well-armed military force with minimum allied losses. As the Soviet General S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies, noted after the end of the Gulf War: 'Iraq lost the war before it even

Several states are pursuing government-sponsored offensive cyber-programs. These states now include IW in their military doctrine, as well as their war college curricula. Their governments recognize the value of attacking adversary computer systems in order to counter other states' military superiority. The President's Commission on Critical Infrastructure Protection projects that, by the year 2002, 19 million individuals will have the knowledge with which to launch cyber-attacks.[16] Today, more than 120 countries are in the process of establishing information operations competence.[17] While most analyses by the intelligence community regarding IW capabilities of various states is classified, the body of unclassified information regarding the perspectives on and potential use of IW by other states is growing considerably.[18] Many of these governments may pose a sophisticated electronic intrusion threat to national security and emergency preparedness telecommunications and information systems.[19] Russia, China and France have acknowledged developing IW programs; and, according to one estimate, at least 33 other

---

began. This was a war of intelligence, electronic warfare, command and control and counter intelligence. Iraqi troops were blinded and deafened . . . Modern war can be won by informatika and that is now vital for both the US and the USSR.' Briefing by Martin S. Hill, OASD C3I. Presented at the Worldwide PSYOP Conference, November 1995.

[16] See President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure A-48, 9 (October 1997).

[17] See Information Security: Computer Attacks at Department of Defense Pose Increasing Risks: Testimony Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 104th Cong. (1996) (statement of Jack L. Brock, Director, Defense Information and Financial Management Systems Accounting and Information, General Accounting Office). According to the US National Security Agency, more than 100 governments are capable of accessing, attacking, and conceivably disabling America's computers. *60 Minutes*, 9 April 2000.

[18] Both China and Russia have been very active in developing information warfare competence. See Hai Lung and Chang Feng, 'Chinese Military Studies Information Warfare' (Hong Kong PTS Msg 210225Z, February 1996, Subject: PLA Undertakes Study of Information Warfare) (Publications Translations Section, US Consulate General, Hong Kong). See also FitzGerald, 'Russian Views on Electronic and Information Warfare', in National Defense University, *Proceedings of the Third International Command and Control Research and Technology Symposium: Partners for the 21st Century* (1997) 126.

[19] National security and emergency preparedness ('NS/EP') telecommunications and information systems are used to maintain a state of readiness to respond to and manage any event or crisis. NS/EP telecommunications and information systems include the public network and all designated National Communications System primary assets. In testimony before Congress, an intelligence expert testified to the growing threats from foreign nations: 'We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber-warfare programs in other countries. We have identified several, based on all-source intelligence information that are pursuing government-sponsored offensive cyber-programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks. Those nations developing cyber-programs recognize the value of attacking adversary computer systems, both on the military and domestic front. Just as foreign governments and the military services have long emphasized the need to disrupt the flow of information in combat situations, they now stress the power of cyber-warfare when targeted against civilian infrastructures, particularly those that could support military strategy.' Statement for the Record by John A. Serabian Jr, Information Operations Issue Manager, Central Intelligence Agency, before the Joint Economic Committee on Cyber Threats and the US Economy, 23 February 2000, Washington, DC, available at www.odci.gov/cia/public_affairs/speeches/cyberthreats_022300.html.

countries have established sophisticated electronic intrusion programs for intelligence collection.[20] The Russians have stated: 'An attack against the telecommunications and electronic power industries of the United States would, by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction.'[21] More ominously, Chinese newspaper reports suggest that: 'An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the US economy.'[22]

Compared to the military forces and weapons that threatened Western societies in the past, modern technology has made the tools of IW cheap, readily available and easily obtainable.[23] The ubiquity of Internet access and the easy availability of hacker tools on underground Internet sites have significantly reduced both financial and intellectual barriers to launching attacks against critical computer systems. Little special equipment is needed to launch such attacks. The basic attack tools consist of computers, modems, telephones and software, essentially the same instruments used by hackers and cyber-criminals. IW, unlike nuclear warfare, is not just the province of the industrial nation-state. Terrorist groups, whether state-sponsored or independent, domestic or international, as well as organized crime syndicates and individuals, have cyber-technologies at their disposal to launch these attacks.[24]

The first step for any effective response to growing threats is to establish an

[20] National Intelligence Council, 'The Foreign Information Warfare Threat to US Telecommunications and Information Systems' (undated briefing); testimony of Dan Kuehl, National Defense University, before the Joint Economic Committee, 23 February 2000 (depicting China and Russia as two nation-states that are cyber-threats to the US) (hereinafter 'Kuehl testimony'); and Madsen, 'Intelligence Agency Threats to Computer Security', 6 *International Journal of Intelligence and Counter Intelligence* (Winter 1993) 446–487.

[21] See FitzGerald, *supra* note 18, at 126.

[22] Speech by Jim Mackey, Department of Energy, International Association for Counterterrorism and Security Professional Briefing, 8 October 1999, Tysons Corner, VA (unpublished transcript on file with the authors). In an interview on *60 Minutes*, on 9 April 2000, Bill Triplett, a senior staffer on Capitol Hill monitoring cyber-warfare and a specialist on the Chinese military, stated that 'the Chinese probably have the biggest program from the standpoint of being able to attack our infrastructure'. In a recent book published by two Chinese colonels in the People's Liberation Army of China, the two colonels state: 'If we want to have victory in future wars, we must be fully prepared intellectually for this scenario, that is, to be ready to carry out a war which, affecting all areas of life of the countries involved, may be conducted in a sphere not dominated by military actions.' See Kuehl testimony, *supra* note 20, at 31. For a detailed discussion of Chinese views on future warfare and the national security environment, see Mike Pillsbury, *Chinese Views of Future Warfare* (National Defense University Press, 1998) and Mike Pillsbury, *China Debates the Future Security Environment* (National Defense University Press, 1999), available at www.ndu.edu; and Gertz, 'China Plots Winning Role in Cyberspace', *Washington Post*, 17 November 1999, A1.

[23] See Denning, *supra* note 5, at 17 (in comparison to the exorbitant amount of money required to fund conventional forces, Denning suggests that between US$1 million and US$10 million could fund an adept IW team of about 10–20 hackers). See also Schwartau, *supra* note 5, at 308–310.

[24] In April 2000, in an interview with *60 Minutes*, Richard Clarke, the White House's national coordinator for security, infrastructure protection and counterterrorism, described a real possibility for the future. 'One morning we're told by the drug cartel in Colombia, "Either the United States pulls out of Colombia, either the United States stops killing the cocaine plants, or else there'll be an information warfare attack on Houston".'

awareness of the problem's magnitude.[25] Among Western governments, the United States has a leading role in this respect, with executive guidance coming most specifically in Presidential Decision Directive 63 (PDD-63) signed by President Clinton in April 1998.[26] Entitled 'Critical Infrastructure Protection', PDD-63 calls for a national effort to ensure the security of increasingly vulnerable and interconnected infrastructures in the United States, and emphasizes the importance of the partnership between the government and private sectors and the importance of international cooperation. PDD-63 also creates the National Infrastructure Protection Center (NIPC) under the Federal Bureau of Investigation (FBI). The NIPC's mission is to act as the focal agency for gathering information on threats to infrastructure, providing timely warning of attacks, analysis and law enforcement investigation and response.[27] The defence community also created its own crisis reaction centres to monitor its computer networks and react to indications of unauthorized penetration of US defence systems.[28]

As sectors of an industrialized society become increasingly aware of national vulnerabilities and dependence on information infrastructures, a number of countermeasures to minimize threats to these infrastructures have been proposed: information-sharing about incidents, legislation to better define computer crimes, improved law enforcement capabilities, and more focused research and development efforts. While these measures are significant, further action (both legal and technological) is needed for mitigating international threats posed by IW technologies.

[25] For the United States, this public awareness campaign was initiated in July 1996, when the President's Commission on Critical Infrastructure Protection (PCCIP) was established to develop a strategy for protecting and ensuring the continued operation of the nation's computer systems and networks, particularly those governing telecommunications, oil and gas, electricity, bank and financial operations, transportation, water supplies, critical emergency response and government. Executive Order No. 13010, 61 Fed. Reg. 37, 347 (1996). The PCCIP's chairman, Robert Marsh, along with his team of 18, which included former Deputy Attorney-General Jamie Gorelick and former Chairman of the Senate Armed Services Committee Sam Nunn, spent a year investigating the nation's vulnerabilities from computer attacks and formulating policy proposals for how the US was going to protect its infrastructure. In its October 1997 report, 'Critical Foundations: Protecting Americas Infrastructures', the PCCIP described the potentially devastating implications of poor information security from a national perspective and discussed recommendations. While the Report of the PCCIP proposed numerous broad measures of infrastructure security such as IW early warning systems and a cooperative relationship between public and private sector entities, the report makes no mention of the international dimension of the problem of security in cyberspace. 'Critical Foundations, Protecting America's Infrastructures' (Report of the President's Commission on Critical Infrastructure Protection, Washington, DC, October 1997), available at www.pccip.ncr.gov/report_index.html.

[26] White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 22 May 1998, available at www.CIAO.gov/press_release/whitehousefactsheet_pdd63.html.

[27] The White House, 'Protecting America's Critical Infrastructures', PDD-63, The White House, Washington, DC, 22 May 1998.

[28] In 1993, the US Air Force created the Air Force Information Warfare Center (AFWIC), which is responsible for the Air Force's defensive and offensive IW capability. The Navy's equivalent centre is the Fleet Information Warfare Center (FIWC) and the US Army's is called Land Information Warfare Center (LIWC).

So the problem expands. New technologies generate new opportunities, which include options to conduct IW. Paradoxically, greater dependence upon new technologies also breeds enhanced vulnerabilities for technologically advanced societies. To exploit vulnerabilities in information resources, more sophisticated tools are becoming available. For these reasons, IW must be regarded seriously — not merely to know when a cyber-based attack might occur, but more critically to know how to react if such an information attack does occur.

For the interconnected global community to prepare for a cyber-based future, questions pertaining to international law must be addressed: what is the permissibility of IW under international law? Does the use of IW constitute a violation of the proscription against 'use of force' under contemporary international legal norms? Relatedly, under what circumstances may governments permissibly use IW under international law? Does IW engender only the right of self-defence under international law, or can IW engender other legal rights or restrictions beyond that right? This essay treats these questions within the confines of state-sponsored cyber-activities[29] because states remain the fundamental units of the international system, and as such are the actors principally affected by international legal rules.[30] However, as non-governmental organizations, groups and even individuals gain more recognized political and legal status in the international system, those actors will warrant special consideration under a legal analysis of IW.

3 IW as Information Operations

Contemporary international law must adapt to the rapidly changing nature of transnational communications systems. The broad sweep of advanced military technologies and the new ways in which they affect states are labelled 'Information Operations' (IOs),[31] within which IW is considered a subset. These Information Operations provide commanders with the ability to observe the battle space, analyze events and direct forces. Information Operations provide logisticians with the ability

[29] For instance, this article will not address the issue of non-state actors' use of IW under international law, nor will it address the issue of the use of force by states against non-state actors such as recreational hackers, terrorists, organized criminals and other non-state actors.

[30] See Ian Brownlie, *Principles of Public International Law* (4th ed., 1990) 58–59 (noting that international law concerns itself primarily with states). See *ibid.*, at 59.

[31] The US Government has defined 'information operations' as: 'Actions taken to affect adversary information and information systems, while defending one's own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and the interaction of C2 [command and control] and intelligence support. IO are conducted through the integration of many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC [Operations Security], PSYOP [Psychological Operations], military deception, EW [Electronic Warfare], and physical attack/destruction, and could include CAN [Computer Network Attack]. IO-related activities include, but are not limited to public affairs (PA) and civil affairs (CA) activities.' Chairman of the Joint Chiefs of Staff, Joint Publication 3–13, *Joint Doctrine for Information Operations* (1988) I-9 and I-10, available at www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. See also Department of the Air Force, 'Cornerstones of Information Warfare', *supra* note 5, at 12 (information operations are 'any action involving the

to know what weapons are in their inventories and where to focus attention, as well as the information necessary to know where a target is, what the target's defences are, and which weapon will most effectively destroy that target.[32] Four interrelated processes support defensive information operations: information environment protection, attack detection, capability restoration, and attack response. They 'are conducted across the range of military operations at every level of war to achieve mission objectives'.[33] Offensive Information Operations could include the active collection of intelligence about information systems, unauthorized intrusions into information systems, the introduction of vulnerabilities into computer systems, corruption or denial of data, and disabling or destroying information systems.[34]

The implications of exotic IW technologies for the future of warfare is uncertain. Even so, it is clear that the new forms of attack enabled by information technology are qualitatively different from previous forms of military assaults. Some cyber-tools — such as computer intrusions and computer viruses — may push military conflict from the physical world into an electronic universe. Some new weapons may produce scant physical effects on an enemy, while others can cause massive destruction or loss of life. Some instruments require no physical intrusion beyond national borders, while others might be construed as military intervention. Finally, some cyber-weapons impact solely on military targets, while others in the process of disabling military targets also produce collateral damage on civilians. Damage from various forms of IW cyber-attack today is only speculative and remains dependent on what technologies are used when, against what facilities and for what duration. In an IW event, however, severe damage could range from pervasive military and civilian deaths and

---

acquisition, transmission, storage, or transformation of information that enhances the employment of military forces'); Joint Chief of Staff, *Information Assurance: Legal, Regulatory, Policy and Organization Considerations* (Department of Defense, 3rd ed., 1997). For an alternative definition of information warfare, see Denning, *supra* note 5 (Denning provides a theory of information warfare based on the value of information resources to an offence and defence and not necessarily based upon physically destructive acts).

[32] Information operations are both defensive and offensive. Defensive information operations 'ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives'. Joint Publication 3–13, *supra* note 31, at III-1. For Denning, defensive information operations seek to protect information resources from attack by countering the potential for loss of value. See Denning, *supra* note 5, at 10.

[33] Joint Publication 3–13, *supra* note 31, at II-1. Computer network attacks (CNA) are a subcategory of information operations. CNAs consist of '[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'. See Report of the PCCIP, *supra* note 25. Such computer attacks are a form of offensive information operations. For a general discussion of computer network attacks, see Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37 *Columbia Journal of Transnational Law* (1999) 885. Offensive information operations seek to increase the value of a target resource by altering the availability and integrity of the information resources to the benefit of the offence and to the detriment of the defence.

[34] See Colonel Phillip A. Johnson, USAF, Associate Deputy General Counsel (IA), Office of General Counsel, DOD, in 'Opening Shots: Information Warfare and the Law', brief to FY 98, US Air Force Judge Advocate-General School, Legal Aspects of Information Operations Symposium, Maxwell AFB, Alabama, Appendix F, 'Principal DOD Information Warfare Organizations', at F-33–F-34.

extensive computer system malfunctions, to destruction or loss of sensitive government information or national economic crisis, to the denial-of-service of important military or government systems in time of emergency, or merely inconvenience for civilian personal and business populations.

Information Warfare Weapons

A wide variety of IW tools are at present available, both defensively and offensively, for carrying out IW attacks.[35] Such weapons include the following:

- a 'sniffer', executed from a remote site by an intruder that would allow the intruder to retrieve user IDs and passwords as they traverse a network; with user IDs and passwords intruders may gain access to sensitive information related to national defence, corporate proprietary information or trade secrets;[36]
- a 'Trojan horse', remotely installed into the controlling switching centres of the Public Switched Network, which allows an outsider to control the network and causing it to malfunction on command;[37]
- a 'trap door', used to gain unauthorized access and control of air traffic control systems, thereby creating the potential to cause pandemonium and violence in the skies;[38]
- a 'logic bomb', placed within a rail computer system, causing trains to be misrouted and crash;[39]

[35] See Lawrence T. Greenberg *et al.*, *Information Warfare and International Law: Introduction* (National Defense University, 1998).

[36] See *infra* in the text at notes 51–54 for a description of the Solar Sunrise case describing an attack on US national defence computers. See also John Fialka, *War by Other Means* (1997) (discussing corporate espionage).

[37] A 'Trojan horse' contains hidden code that executes potentially malicious acts such as recording passwords entered by legitimate users, installing a virus, and collecting system connectivity information when triggered by an external event. The code can engage in any malicious act within the privileges of the host program, or break out to operate with any other program or by itself. Roger C. Molander *et al.*, *Strategic Information Warfare: A New Face of War* (1996) 64. An example of a 'Trojan horse' was a compromised copy of the 'Dansie Shopping Cart'. See www.securityfocus.com.

[38] Also known as a 'backdoor', a trapdoor provides an undocumented way of gaining access to a computer system or particular software program. A 'backdoor' may be a legitimate feature, installed by a vendor to allow remote maintenance of the system, or a system programmer who wants to break into that computer after he has put it in or after the company no longer employs her. Intruders can use remote network dial-up to access a backdoor and gain unauthorized access to a system.

[39] A 'logic bomb' is a program that lies dormant until a trigger condition causes it to activate and destroy the host computer's files. The execution is usually triggered by a date or time. A 'logic bomb' can be hidden within a 'Trojan horse' or carried by a 'virus'. See Denning, *supra* note 5, at 258.

- 'video morphing', used to make the news broadcasts of a state indistinguishable from an enemy's creation of its version of that same broadcast;[40]
- a 'denial of service attack',[41] executed to prevent critical networks from being able to exchange data with other systems supporting functions such as emergency services, flight safety and war readiness;[42]
- a 'computer worm'[43] or 'virus',[44] which travels from computer to computer across a hospital's computer network, damaging medical data and disrupting vital systems;

[40] See Grier, 'Information Warfare', *Air Force Magazine*, March 1995, 34, at 35; and Graham, 'Military Grappling with the Guidelines for Cyber War', *Washington Post*, 8 November 1999, A1.

[41] In a 'denial-of-service' attack, an intruder executes a program from a remote site that congests or disables the service on the victim computer. By sending forged Internet control message protocol (ICMP) echo request packets (i.e. 'ping' packets) to IP broadcast addresses, the attack can cause network congestion or outage because of the large number of ICMP echo reply packets being sent to the victim site. An overload of this process congests the system, resulting in degraded network performance, or may render the system inoperable. CERT, SEI, CMU, CERT Advisory CA-98.01.smurf, Pittsburgh, PA: CERT, 5 January 1998.

[42] In February 2000, Yahoo, Cable News Network, eBay, Buy.com and ZDNet were all hit with what appeared to be coordinated denial-of-service attacks.

[43] A 'worm' is a self-replicating program that moves from one system to another along a network, as opposed to a virus that attaches itself to legitimate programs or files either destroying them or co-existing with them. A worm does not destroy software or compromise data. A 'worm' uses all available computing resources and saturates communications links, similar to a denial-of-service attack. See Charles P. Pfleeger, *Security Computing* (2nd ed., 1996) 179. In November 1998, a program called the Morris Internet Worm caused the disruption of service to thousands of computers and their users across the Internet. Robert Morris was charged with unleashing this 'worm' and was convicted under 18 USC 1030(a)(5)(A). See *United States v. Morris*, 928 F 2d 504 (2nd Cir.), cert. denied, 502 US 81 (1991) (defining a 'worm' as a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects'). See also Spafford, 'The Internet Worm: An Analysis', at ftp://coast.cs.purdue.edu/pub/Doc/morris_worm/spaf-Iworm-paper-CCR.ps.Z. GAO provided an overview of this worm incident. See ftp://coast.cs.purdue.edu/pub/Doc/morris-worm/GAO-rpt.txt. In a recent worm incident, a malicious VBS script program developed by a Filipino student from Manila flooded network systems, degrading mail, file and web traffic, effecting hundreds of thousands of systems. See www.cert.org/advisories/CA-2000-04.html.

[44] A 'virus', like a 'worm', is a program that infects other programs. The virus becomes active when users access the infected program or file. Once active, the virus has two basic functions: replication and execution. Pfleeger, *supra* note 43, at 179. For a general discussion of computer viruses, see David Ferbrache, *Pathology of Computer Viruses* (1991). In March 1999, a Microsoft Word macro virus (the so-called 'Melissa' virus) developed by 30-year-old David Smith of Aberdeen, New Jersey, propagated itself via e-mail attachments causing system overloads and mail servers to crash. Although the Melissa virus disrupted operations at thousands of companies and some government agencies, it reportedly did not compromise sensitive government data. However, it illustrated the speed with which malicious software can spread in today's interconnected computing environment. See www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html.

- an 'infoblockade', which blocks all electronic information from entering or leaving a state's borders;[45]
- 'spamming',[46] which floods military e-mail communication systems preventing field communications from reaching the troops; and
- 'IP spoofing',[47] which fabricates messages whereby an enemy masquerades as an authorized command authority giving false military information to troops in the field.

Some of these tools can have devastating results if used by criminals or terrorists. For example:

- computer intruders divert funds from bank computers and corrupt data in bank databases, causing disruption or panic, as banks need to shut down to address their problems;[48]
- computer intruders steal and disclose confidential personal, medical or financial information, as a tool of blackmail and extortion, and cause widespread social disruption or embarrassment;[49]
- spies steal classified information from secure government databases and gain information vital to national security;[50] and

[45] Kanuck, 'Recent Development, Information Warfare: New Challenges for Public International Law', 37 *Harvard International Law Journal* (1996) 272, at 289. Interestingly, the UN Charter appears to contemplate these types of electronic interference with a country's communications as 'infoblockades'. Article 41 provides that, in its effort to address breaches of the peace, the UN Security Council may call upon UN members to disrupt an aggressor's 'rail, sea, air, postal, telegraphic, radio, and other means of communication'.

[46] 'Spamming' is an IW tool that clogs the victim's e-mail box with unwanted mail that can interfere with the delivery of desirable messages. See Denning, *supra* note 5, at 122–124. Simply put, it is junk mail sent via e-mail. In 1998, a defendant was held liable to AOL for sending over 60 million pieces of unauthorized bulk e-mail advertisements to customers of AOL. The defendant was found guilty of trespass to chattel under Virginia common law, false designation of origin under the Lanham Act for using 'aol.com' in the spam headers, and dilution by tarnishment because of negative associations with AOL's mark. See 1998 US Dist. LEXIS (ED Va 1998).

[47] 'IP spoofing' is an IW tool that allows an intruder to forge the e-mail 'from' address of a user so that the message appears to becoming from somewhere other than its actual source. In spoofing, the victim receiving the forged message will accept the message believing that it is coming from a trusted source. See Denning, *supra* note 5, at 255–256.

[48] Molander, *supra* note 37, at 74.

[49] Some of these scenarios have been described by James Adams in his book, *The Next World War* (1998) 156–158: 'A CyberTerrorist will remotely access the processing control systems of a cereal manufacturer, change the levels of iron supplement, and sicken and kill the children of a nation enjoying their food … A CyberTerrorist will attack the next generation of air-traffic control systems, and collide two large civilian aircraft … A CyberTerrorist will remotely alter the formulas of medication at pharmaceutical manufacturers.'

[50] In 1994, two hackers penetrated the US Air Force's Rome Laboratory by installing seven 'sniffer' programs that allowed them to read, copy and delete e-mail and read and copy sensitive information. The intruders entered the system over 150 times, copied sensitive data and attacked other linked government facilities and defence contractor systems. Eventually, two British hackers, co-named Kuji and Datastream Cowboy, were determined to be the guilty hackers. See Jim Christy, Rome Laboratory Attacks, Prepared Testimony Before the Senate Governmental Affairs Committee Permanent Investigations Subcommittee, 22 May 1996. In Dorothy E. Denning and Peter J. Denning (eds), *Internet Besieged: Countering Cyberspace*

- terrorists cause an aircraft to crash through the use of a pulse device that disrupts and permanently corrupts the information system components within the aircraft.

These technological tactics may appear more science fiction than actual fact. Today, however, the science is real and the technology is fact. Stock markets and commodity exchanges, electronic power grids, municipal traffic control systems, air traffic control or navigation systems and classified national security information systems can be manipulated or disrupted by any one or a combination of these IW tools, with accompanying economic or societal disruption, physical destruction or loss of life. The status of international law, however, lags behind cyber-technology. Two recent incidents spotlight this disparity and suggest that serious consideration should be given to ways and means that international legal rules may apply to a cyber-attack as a transnational use of force.

A *Solar Sunrise*

In January 1998, tensions flared between the United States and Iraq over United Nations weapons inspections. Saddam Hussein expelled the UN inspectors from Iraq, precipitating a crisis and pushing the US to the brink of renewed military action in the Persian Gulf. On the first Monday in February, analysts at the Air Force's national computer monitoring centre detected an unusual series of red warning flags pop up on their screens, indicating unauthorized intrusions into at least six electronic networks across the country. Several dozen computer systems in US military installations and government facilities were successfully compromised by the intruders, which prompted a full-scale Department of Defense (DOD) response now known as Operation Solar Sunrise.[51]

The attack against DOD computer systems ultimately violated systems belonging to the US Navy and Air Force, as well as federally funded research laboratories. Although no classified systems reportedly were compromised, the attackers obtained system privileges used to read password files, delete files and create 'back doors' for subsequent re-entry. The intruders hid their electronic tracks by routing their attack through computer systems in the United Arab Emirates. They accessed unclassified

---

Scofflaws (1998). In 1992, the Defense Information Systems Agency (DISA) identified 53 attacks on military and DOD systems. In 1995, that number had grown to 559. By the year 2000, the number of attacks was estimated to approach 500,000 a year. See Correll, 'War in Cyberspace', *Air Force Magazine*, January 1998; see also Ted Uchida, School of Advanced Military Studies, US Army Command and General Staff College, *Building a Basis for Information Warfare Rules of Engagement* (1997) 8. 'Cyberespionage' is the term that has been coined to describe the use of computers and networks to obtain secret information. Some foreign governments recruit malicious hackers to help them conduct espionage against the US Government. According to Clifford Stoll in his book, *The Cuckoo's Egg* (1990), the German hackers caught in attacks against the US Government systems were actively conveying information to Russian agents.

[51] See Graham, 'US Studies New Threat: Cyber Attack', *Washington Post*, 24 May 1998, at AI.

logistics, administration and accounting systems that control the US ability to manage and deploy military forces. They gained privileged access to computers by using tools available from a university website and installed 'sniffer' programs to collect user passwords. They created a 'backdoor' to re-enter the system and then used a patch available from a university website to close the vulnerability and prevent others from repeating their exploit.[52]

Despite potentially grave consequences, these attacks were orchestrated neither by an organized terrorist group nor a foreign government; rather, an Israeli teenager code-named 'The Analyzer' and two 16-year-old high school students in Cloverdale, California, broke into these systems, simply to prove that they could.[53] The incident made clear to government policy-makers that such intrusions pose real threats to national security.[54]

B *Moonlight Maze*

In October 1999, Michael A. Vatis, Director of the FBI's National Infrastructure Protection Center (NIPC), testified before a Senate subcommittee in the first public confirmation about the year-long FBI investigation code-named Moonlight Maze.[55] Moonlight Maze revealed the most extensive computer attack aimed at the US Government. According to reports, hackers working from Russia penetrated DOD computers for more than a year and stole vast amounts of sensitive information.[56] Security experts first spotted the intrusions in January 1998 when Air Force and Army computer crime investigators tracked the attacks to an Internet service provider in Russia. According to Pentagon and FBI officials, the Russian hacking was a

[52] Testimony before the House Joint Committee on Preventing Economic Cyber Threats by John A. Serabian Jr, 23 February 2000.

[53] The Israeli National Police, working with US authorities, arrested Ehud Tanedaum and charged him with illegally accessing US and Israeli government computers. The two teenagers, who have been publicly identified, were charged and tried in juvenile court. See Reed and Wilson, 'Suspected Pentagon Hacker Found — FBI Arrests Israeli Teen Who Had Bragged He Couldn't Be Caught', *Seattle Times*, 19 March 1998, at A7.

[54] The United States was then contemplating military action in the Gulf because of Iraqi non-compliance with UN inspection teams. The timing of these cyber-intrusions raised particular concerns in the United States that they were the initial stages of a computer-generated attack by a hostile government. The incident galvanized US Government agencies with foreign and domestic missions alike to coordinate their efforts in response, which required a massive cooperative effort by the FBI, the Justice Department's Computer Crimes Section, the Air Force Office of Special Investigations, NASA, the Defense Information Systems Agency, the National Security Agency, the CIA and various computer emergency response teams from the military services and government agencies. See Drogin, 'Yearlong Hacker Attacks Net Sensitive US Data: Technology: The Systematic Assault on Pentagon Computers Originates in Russia, Officials Say', *Los Angeles Times*, 7 October 1999.

[55] The NIPC is the FBI unit responsible for coordinating the federal response to computer threats. President Clinton made the FBI the lead agency for protecting the nation's computer systems when he signed Presidential Decision Directive 63 on 22 May 1998. See PDD-63, *supra* note 26.

[56] Testifying before a Senate subcommittee on technology and terrorism, Michael A. Vatis, Director of the FBI's NIPC, stated that 'the intrusions appear to have originated in Russia', and that the intruders stole 'unclassified but still sensitive information about essentially defence technical research matters'. See generally the discussion about Moonlight Maze in Drogin, *supra* note 54, at A1.

state-sponsored Russian intelligence campaign to secure US technology,[57] which targeted not just DOD, but also the Department of Energy, NASA, military contractors and military-linked civilian universities.[58]

The Moonlight Maze intrusions were 'distributed coordinated attacks', a style of penetration that is particularly effective at compromising existing defences. Distributed coordinated attacks can employ thousands of servers to attack and overwhelm a single server. Because so many servers are used, each attack can be camouflaged as a legitimate connection attempt, making it difficult for the victim's intrusion software to know that it is under attack, and disguising the identity of who is attacking.[59] The lesson learned from Moonlight Maze is that the United States and Western societies have become 'extraordinarily vulnerable' to penetration and sabotage of critical computer systems.[60] Left unattended is what lawful recourse government officials may take in response to state-sponsored attacks such as that by Moonlight Maze.

[57] Kimery, 'The Russians Are Coming', in 3 *Military Information Technology*, which is available online at www.MIT-kmi.com.

[58] No classified computers were reported to have been breached and no networks were reported destroyed or damaged. Notwithstanding that no classified databases were compromised, the US Government's unclassified networks contain significant amounts of confidential and sensitive data that might be valuable to foreign governments. DOD computer databases, for example, contain information about military logistics, planning, purchases, payroll and personnel, as well as routine e-mails between Pentagon personnel. Pentagon officials reportedly said that this was the first time Russia made a 'sophisticated, patient, and persistent' attempt to penetrate US computer networks. As the NASA Inspector General Roberta Gross said in an interview: 'It's difficult to tell what the damage is … They weren't shutting down systems. They were taking file listings, looking to see what's in people's directories.' *Ibid.* Kimery, *supra* note 57. Gross said that the intruders also installed 'parking tools that they can use to get back in later'. Such electronic 'trapdoors' may be used to evade detection devices and to secretly regain access to a computer system.

[59] Kimery, 'Moonlight Maze', in 3 *Military Information Technology*, online at www.MIT-kmi.com. A number of commentators have publicly acknowledged the gravity of these incidents. 'The kids [responsible for the Solar Sunrise attack last year into DISA and other DOD computer networks] essentially found a well-known vulnerability of the operation system and came in that way', Arthur L. Money, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, disclosed in October 1999 at the National Information Systems Security Conference in Arlington, VA. But Moonlight Maze brings 'a whole different, much more sophisticated approach … it also brings another dimension — no longer with hackers, but with the problem of a state-sponsored attack'. Drogin, *Los Angeles Times*, 7 October 1999, at A1. According to Money: 'It's the magnitude of the extraction that is alarming to us.' *Ibid.* In the same vein, Vatis opined that: 'The greatest potential threat comes from foreign state actors who might choose to engage in information warfare against the United States, because they realize that they can't take us on in conventional military terms and would seek to go after what they perceive as our Achilles heel … which is our reliance on information technology, more than any other country to control our critical operations.' Vatis testimony, *supra* note 56.

[60] As Richard Clark posited on *60 Minutes* in April 2000: 'An enemy could systematically disrupt banking, transportation, utilities, finance, government functions and defense. We know other countries that are developing information technology and are doing reconnaissance of our computer networks.' Clark sees the Moonlight Maze intrusions as 'pre-war reconnaissance' where half a dozen nations are busy scanning each other's networks to get a good map of where the key things are and what the key vulnerabilities are of those networks. He describes these circumstances as ones where, for the first time, the US has a 'potential foreign threat … where the military can't save us'. *Ibid.*

The Kosovo Crisis

Experiments with the use of IW occurred during the Kosovo crisis. On 30 March 1999, three days after NATO began its bombing missions over Serbia and Kosovo, hackers initiated a coordinated programme to disrupt NATO's e-mail communications system by overloading it.[61] While the hackers' identities were not determined, Western authorities suspect they were members of the *Crna Ruka* (Black Hand) that attacked the Kosovo Information website earlier in October 1998.[62]

According to US officials, the United States also resorted to cyber-attacks during the Kosovo conflict. President Clinton reportedly approved a top secret plan to destabilize Yugoslavian leader Slobodan Milosevic by using computer hackers to infiltrate and attack foreign bank accounts held by Yugoslavia in order to siphon off funds that might be used for military purposes.[63] Public reports also suggest that the United States instigated a coordinated attack to disrupt the Yugoslav command and control network in order to protect NATO warplanes from being targeted by the air defence command and to confuse Yugoslav military messages.[64] The degree of success stemming from these US efforts at cyber-war against the Milosevic regime remains unclear, however.

4 The Legal Setting: Understanding the Implications

A *Sovereignty Considerations*

The realistic threat of cyber-attacks resurrects the need to consider fundamental international legal rules. Contemporary international law gives to each state a right to liberty within the international arena — that is, a certain right to be free, independent and unfettered from foreign control and forcible influence. This general principle of exclusive sovereignty over national territory is firmly fixed in customary international law.[65] This principle implies that each state is autonomous, free from coercion, and able to preserve the corporate integrity of its territory. Each state exercises control

[61] See Vizard, *supra* note 6, at 80.

[62] *Ibid.*

[63] See Vistica, 'Cyberwar and Sabotage', *Newsweek*, 31 May 1999, at 38; and Sullivan, 'Cyberwar? The US Stands to Lose', 28 May 1999, www.msnbc.com/news/274526.asp.

[64] Hoffmann, 'US Opens the Door to Cyberwar Technology: The Kosovo Conflict Saw the First Electronic Attacks on Enemy Computer and Communications Systems', *Orange Reg.*, 24 October 1999, at A35.

[65] See *Restatement (Third) of the Foreign Relations Law of the United States* (1987) para. 102; see also the Statute of the ICJ, 26 June 1945, Article 38(1)(b), 832 USTS 993, *Yearbook of the United Nations* (1978) 1197 (customary law is a 'general practice accepted as law'). See *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. US)*, ICJ Reports (1986) 1, at 93–99, para. 202 (noting '[t]he principle of non-intervention right of every sovereign State to conduct its affairs without outside interference . . . [I]t is part and parcel of customary international law'.). See also the 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty', General Assembly Resolution 2131, UN GAOR, 20th Session, Supp. No. 14, at 12, UN Doc. A/6220 (1965) 26; the 'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations', General Assembly Resolution 2625 (XXV), UN GAOR, 25th Session, Supp. No. 28, at 121, UN Doc. A1 8082

over its national territory to the exclusion of all other states, and any limitation of this authority is subject to the consent of the territorial state. In particular, no state may use armed force to invade the territory of another state, no state may conduct a physical assault against another state by land, sea or air, and no state may carry out strategic observation in or over the national territory of another state. The territorial scope of sovereignty covers all national spaces. International law establishes qualifications of state jurisdiction on the high seas, in outer space, and through national airspace.[66] Critical is whether these same principles of territorial sovereignty apply as legal rules for governing the international use of cyberspace. Consider the following scenarios.

Suppose a foreign government, in an attempt to influence the political process in a target state, sends thousands of random e-mail messages to the citizens of that target state, criticizing the policies of the party in power. Would this form of e-mail propaganda violate the sovereignty of the foreign state? Or, what if a government launches an IW attack against another state by routing a corrupted e-mail message containing a computer virus through an Internet service provider that is located in a third state. Has the sovereignty of the target state been violated? Has that of the third state been violated? Does it matter that there was no physical damage done to the third state? What if, unintentionally, the computer virus does harm to the computer systems of the third state? Does it matter that the attacking state did not intend to cause harm to the third state? Such questions strike at core issues compounding the lawfulness of IW transborder data flow as it relates to the sovereignty of states.

The new technological capability of governments to employ IW instruments across international networks or through the atmosphere as electromagnetic waves challenges the viability of territorial sovereignty as a legal construct.[67] Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each state retains exclusive authority over activities within its borders. Under this principle, so long as physical boundaries of jurisdiction exist and objects and activities can be precisely located, the legal concepts of possession, sovereignty and inviolability make sense. Each new medium that is accessed through technological advancement can be possessed, divided and held as sovereign territory (e.g. land and airspace) or shared in common (e.g. the high seas and outer space).

To punctuate these precepts, such customary rules of territorial sovereignty are

---

(1970). For a discussion of what customary international law is, see Anthony Clark Arend, *Legal Rules and International Society* (1999) 47–48 (customary international law consists of two elements: it must reflect consistent state practice over time by a significant group of states and there must be a belief on behalf of the state that the practice is required by law (*opinio juris*)).

[66] See United Nations Convention on the Law of the Sea, 10 December 1982, UN Doc. A/CONF.62/122, 21 ILM 1261; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 18 UST 2410; TIAS No. 6347; 610 UNTS 205; Convention on International Civil Aviation, Chicago, 7 December 1944, 59 Stat. 1693, 84 UNTS 289 ('The contracting States recognize that every state has complete and exclusive sovereignty over the airspace above its territory.').

[67] See Kanuck, *supra* note 45, at 275–276 (discussing the challenges that IW presents to an international paradigm based on territorial sovereignty).

codified by modern conventional law.[68] UN Charter law in Article 2(4) uses the term 'territorial integrity' to substantiate these modern legal concerns, which makes immanent legal sense. The meaning of these terms appears plain and simple: 'Territorial' means limited to a specific territory. 'Integrity' means an unimpaired or unmarred condition, original perfect state, entireness, completeness, undivided or unbroken.[69] However, as tested by state practice and legal interpretation over the past half-century, the parameters of the terms are less clear and may suggest wider latitude in meaning. Such seems the case for what interpretation best suits these terms within the modern purposes of Article 2(4). The traditional concept of sovereignty may not be suitable for an increasingly interdependent and globalized world. This seems especially true for a world that is becoming electronically interconnected as billions of signals travel between national networks, as electromagnetic waves cross national borders instantaneously, unsupervised and with impunity, thereby creating conditions that allow individuals or groups in one place to affect systems transglobally, while the legal authority of the state to regulate those activities generally stops at its national borders.

In an international technological milieu where the globe is shrinking and cooperation and interaction across national boundaries are increasingly essential, the isolation of any state or its society becomes impractical. New rules to govern technological advancements and their international deployment may be required to keep interstate co-existence peaceful. Every day, more individuals, societies and governments plug into the global electronic, digital network simply because they have determined that for their activities to be successful, they must be 'connected'. Thus, the concept of sovereignty no longer is static. It appears to be evolving into a construct made more porous by the twin forces of interdependence and globalization. Similarly, the intangible penetration of borders carried by electronic signals might not be the sort of violation traditionally thought to constitute an 'attack' under UN Charter law. These features in post-industrial technological society complicate the development of international legal rules that might deal more effectively with transnational activities in cyberspace.

Rigid notions of Westphalian sovereignty and territorial integrity yield to a more porous, dynamic set of technological realities. For a legal regime to account for pervasive activities within the realm of cyberspace, where massive amounts of data flow unchecked as electronic signals across national borders, the legal paradigm must reach beyond the dimension of local events. Interactions and consequences, not mere physical territory, must be treated more as legal bases of a new legal system. It is reasonable to surmise, therefore, that, if the notion of sovereignty is becoming

[68] The first step to codify this principle of territorial sovereignty was taken in 1919 in the Covenant of the League of Nations, Article 10 of which provides for the protection of territorial integrity: 'The Members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all members of the League.' Covenant of the League of Nations, Article 10, Versailles, 28 June 1919 (Treaty Series, 1919/4, 25). The Charter of the United Nations reaffirms the principle of territorial integrity in its Article 2(4).

[69] *Webster's Third New International Dictionary*, vol. II (1966) at 1174 and 1148.

antiquated, so too might be traditional interpretations of 'use of force' and 'armed attack' under contemporary UN Charter law as they relate to IW. We now turn to address this point.

Cyber-Force as an Armed Attack

The United Nations was founded 'to save succeeding generations from the scourge of war' and 'to suppress acts of aggression or other breaches of the peace'.[70] At the heart of the UN Charter lies Article 2(4), which asserts the key prescription under modern international law regarding the 'use of force' and reaffirms the principle of 'territorial sovereignty'.[71] The provision simply declares that: 'All members [of the United Nations] 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.' The choice of using the term 'force', as opposed to 'war', 'aggression' or 'military conflict', is significant in that it encompasses situations which include hostile acts that fall short of the technical state of belligerency. This fundamental proscription against the use of interstate force is traditionally regarded as being confined to the use or threat of 'armed' force, meaning the possible resort to a violent weapon that inflicts human injury.[72] Obviously, computers are neither troops nor tanks. In the case of cyber-force, fundamental questions arise over what weapons might be covered within the legal scope of Article 2(4). Indeed, it is not off the mark to assert that modern technologies defy attempts to set out as exhaustive a list of which weapons may or may not be used within the legal meaning of UN Charter law. Even so, an international consensus admits that such a prohibition on the use force extends to conventional weapons, as well as to bacteriological, biological and chemical devices and nuclear and thermonuclear weapons. The issue remains, however, as to whether instruments of IW such as 'Trojan horses', 'viruses', 'worms' or 'sniffers' qualify as weapons of 'force' as construed under contemporary international legal rules.

While the 'threat or use of force' may be interpreted broadly to mean both armed

[70] UN Charter, Preamble. See also Schachter, 'International Law: The Right of States to Use Armed Force', 82 *Michigan Law Review* (1984) 1620 ('When the UN Charter was adopted it was generally considered to have outlawed war.'). The drafters of the Charter intended that instrument to resolve shortcomings in the Kellogg–Briand Pact regarding the prohibition on war. See Pact of Paris, 26 August 1928, Stat. 46:2343, TS No. 796, UNTS 94:57 (signatories condemned recourse to war and agreed to resolve all disputes by peaceful means); see also Yoran Dinstein, *War, Aggression and Self-Defence* (2nd ed., 1994) 83–84. The Kellogg–Briand Pact was an attempt to prohibit the use of war as an instrument of national policy.

[71] See Ian Brownlie, *Principles of Public International Law* (4th ed., 1990) 58–59 and 112; Ingrid Detter De Lupis, *The Law of War* (1987) 56; and Dinstein, *supra* note 70, at 84 (explaining that the expression 'use of force' includes war, measures short of war, and even threats of force).

[72] D.W. Bowett, *Self-Defence in International Law* (1958) 148; and Ian Brownlie, *International Law and the Use of Force by States* (1963) 361.

and non-armed force,[73] pragmatism tends to restrict this interpretation to armed interventions.[74] Indeed, the primary purpose promoting the formation and function of the United Nations is to prevent war. Seen from this vantage point, UN Charter law clearly prohibits international intervention through the use of *armed* force, but withholds comment on other, more subtle forms of 'subversive' coercion that do not involve, at the very least, a perceived threat of armed force.[75] The Age of Information Warfare invites reconsideration of the restrictive scope of this prohibition. The fact that one government today can use IW instruments transnationally through cyberspace to inflict damage on cyber-based facilities in another state suggests the need to consider a broader interpretation of the prohibition on the use of force.

Article 2(4) stipulates a clear prohibition on a state's right to use force, which presumably would include cyber-force. Yet, exceptions to this proscription are evident, two of which find explicit mention in Charter language, although others have also evolved into acceptance through state practice. First, there is the well-known self-defence exception to the proscription on use of force contained in Article 51 of the Charter.[76] Secondly, the Security Council retains the authority to authorize the use of force to respond to 'any threat to the peace, breach of the peace or act of aggression'.[77]

Coupled with these Charter-based exceptions are certain UN resolutions that maintain the permissibility to use force in support of self-determination movements.[78] Similar consideration accrues to the possibility that a norm of humanitarian intervention exists within the realm of the customary right of self-defence.[79] Nonetheless, disagreement persists over what these challenges to the scope and application of Articles 2(4) and 51 mean for the UN Charter and contemporary

[73] See, e.g. Kelsen, 'General International Law and the Law of the United Nations', in Gesina H.J. Van Der Molen *et al.* (eds), *The United Nations: Ten Years Legal Process* (1956) 4–5; see also Ahmed M. Rifaat, *International Aggression: A Study of the Legal Concept, Its Development and Definition in International Law* (1979) 120, at 234.

[74] Wright, 'Subversive Intervention', 54 *AJIL* (1960) 521, at 529.

[75] While some have attempted to classify covert action as a form of aggression, see Report of the International Law Commission to the General Assembly, 2 *Yearbook of the International Law Commission* (1950) 123, at 123–133, UN Doc. A/CN.4/SER.A.

[76] UN Charter, Article 51. See *infra* note 94.

[77] UN Charter, Articles 39 and 42.

[78] See Brownlie, *supra* note 71 (describing how it may be lawful for a self-determination movement to seize territory and for other states to use force in support of it). See also Reisman, 'Criteria for the Lawful Use of Force in International Law', 10 *Yale Journal of International Law* (1985) 279, at 281; and Reisman, 'Article 2(4): The Use of Force in Contemporary International Law', 78–79 *American Society of International Law Proceedings* (1984–1985) 74, at 79–84.

[79] See Joyner and Arend, 'Anticipatory Humanitarian Intervention: An Emerging Legal Norm?', 10 *Journal of Legal Studies* (2000) 27; see also Bowett, *supra* note 72; Lillich, 'Forcible Self-Help by States to Protect Human Rights', 53 *Iowa Law Review* (1967) 325; Moore, 'The Control of Foreign Intervention in International Conflict', 9 *Virginia Journal of International Law* (1969) 205, at 261–264; W. O'Brien, *The Law of Limited International Conflict* (1965) 29–30; Reisman, 'Humanitarian Intervention to Protect the Ibos', in R. Lillich (ed.), *Humanitarian Intervention and the United Nations* (1973) 167, at 177 (Reisman notes that a 'close reading of [Article 2(4)] will indicate that the prohibition is not against the use of coercion per se, but rather the use of force for specified unlawful means').

international legal rules.[80] Even so, the lack of agreement on the precise formulation of obligations contained in Article 2(4) and the principle of non-intervention is not cause for them to be rejected as irrelevant. To do so jettisons the modern basis upon which legal restraints on forcible interstate violence rest.

Other instruments vehemently confirm the prohibition against intervention by one state into the affairs of other states, and make relevant the need to devise legal restrictions on the use of cyber-force. Pre-eminent among these, the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States[81] avers that:

> No state has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other state. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the state or against its political, economic and cultural elements, are condemned.

This prohibition was reaffirmed in the 1970 Declaration on Principles in International Law,[82] with the proviso that not only were such interferences condemned, but they were held to be in breach of international legal rules.[83] Intervention is prohibited when it interferes in matters in which each state is permitted to decide freely by virtue of the principle of state sovereignty. Respect for the principle of the sovereignty of states closely allies to legal rules that prohibit the use of force and interstate intervention.[84] At first blush, then, the unmistakable inference is that any transnational cyberspace activities that affect the internal affairs of a state might well breach general legal principles upholding respect for sovereignty and non-intervention. Other considerations, however, call for caution in reaching that conclusion.

Widespread international agreement upholds the prohibition on intervention by

[80] At least three major schools of thought assert disparate views on the efficacy of Articles 2(4) and 51. One group, which has been labelled the 'legalists', argues that Article 2(4) is still good law. The reasoning here rests upon the fact that the UN Charter is a treaty and, until the parties have withdrawn from the treaty, the treaty terms are still binding. The second and most accepted view is espoused by so-called 'core-interpretationists', who argue that, while the core of Article 2(4) is still good law, state practice has gone beyond a literal interpretation of Article 2(4). According to this approach, Article 2(4) does not prohibit all forms of force; for instance, force is allowed to rescue nationals and for humanitarian intervention. Finally, a third group of commentators, called the 'rejectionists', contend that, because states have chosen to ignore Article 2(4) when it suits their policy objectives, the inescapable conclusion is that Article 2(4) is not controlling of state behaviour. For this group, if a norm fails to reflect state behaviour and a state's belief that it has a legal obligation to follow the norm, then the norm is less than law. See Arend and Beck, *Use of Force* (1993) 82–92.

[81] General Assembly Resolution 2131 (XX).

[82] General Assembly Resolution 2625 (XXV).

[83] More than two decades earlier, the International Court of Justice in the *Corfu Channel Case* had declared specifically that 'the alleged right of intervention [was] the manifestation of a policy of force, such as has, in the past, given rise to serious abuses and as such cannot . . . find a place in international law'. The Court noted that to allow such a right as a derogation from a state's territorial sovereignty would be even less admissible. The Court concluded that the essence of international relations lay in the respect by independent states of each other's territorial sovereignty. ICJ Reports (1949) 4, at 35; 16 ILR 155, at 167. See also Brownlie, *supra* note 72, at 283–289.

[84] ICJ Reports (1986) 111; 76 ILR 445.

one state into the sovereign affairs of another.[85] However, legal opinion diverges over the scope of the non-intervention rule. Indeed, few topics prompt greater legal controversy than the duty not to intervene, or the alleged right under certain circumstances of states to intervene. The debate is compounded in the quest to define which types of intervention by which actors might be acceptable under what particular circumstances.[86]

The line separating unlawful intervention from legitimate interference is often difficult to draw. It is easy to argue that incursions by military forces across national borders violate international norms, and that mere economic and diplomatic forms of coercion are more likely to fall within the realm of permissive behaviour. The dilemma becomes apparent, however, when attempts are made to distinguish between more subtle kinds of intervention, such as naval interdiction, massive economic sanctions, humanitarian intervention, and computer-directed forms of cyber-assault. Legal logic suggests that a government-sponsored computer attack involving transnational networks and telecommunications might trigger legal implications arising from the prohibitions in Article 2(4). So it becomes necessary to ascertain what activities involving use of the Internet constitute 'force' or 'the use of force' as prohibited by

[85] See Emerich de Vattel, *The Laws of Nations or the Principles of Natural Law* (1758) Book I, chapter III, section 37 (testifying to the universal consensus against 'intermeddl[ing] in the domestic affairs of another Nation'); and *Restatement (Third) of the Foreign Relations Law of the United States* (1987) para. 102.

[86] Various views on intervention tend to fall into four rules, over which there is still debate. First, there is the 'neutral non-intervention' rule, which holds that aid from a foreign state is permissible when requested and when there exists a low level of civil strife. According to this rule, aid is not permissible in the event of an insurgency or belligerency, and should never be given to the rebel forces. Secondly, a 'self-determination' rule permits a foreign state to provide aid to any group seeking self-determination, the government or the rebels. Thirdly, the 'proportionate counter-intervention' rule permits offsetting assistance to the government of a state if a third state has already given aid to the rebels. Aid is limited to the territory involved in the civil strife; and, if the aid to the rebels is equivalent to an armed attack, the outside state providing assistance to the government can respond against the third state. And, finally, the 'limited counter-intervention' rule permits offsetting assistance to the government of a state if a third state has already given aid to the rebels, aid must be limited to the territory experiencing the conflict, and the aiding state can never take action against the third intervening state giving aid to the rebels. See Arend and Beck, *supra* note 80, at 82–92. Cf. Jackamo, 'From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention', 32 *Virginia Journal of International Law* (1991) 929 (discussing the contemporary customary law of non-intervention). The International Court of Justice recently flushed out one factor that distinguishes between permissible and impermissible intervention. In *Military and Paramilitary Activities In and Against Nicaragua*, the ICJ found that the United States violated the customary international law of non-intervention by training, encouraging and arming the Contra forces in Nicaragua. See *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. US)*, ICJ Reports (1986) 1, at 93–99 (noting that the United States recognized Article 2(4) as both a 'universal norm' and a 'universal international law'). The Court in this case determined that Article 2(4)'s prohibition of the use of force was a principle of customary international law, 'to be thenceforth treated separately from the provisions, especially those of an institutional kind, to which it is subject to the treaty-law plane of the Charter'. *Ibid.*, at 100. The ICJ also held that overflights by US aircraft violated customary international law regarding the violation of the territorial sovereignty of states. *Ibid.*, at 147.

Article 2(4). Arguably, this provision applies only to 'armed force'.[87] Yet, a use of force implies unlawful violence threatened or committed against persons or property, and, if cyber-force qualifies as a form of violence, it involves swift, injurious impacts on a targeted facility.

The critical point is this: though perhaps not 'armed force' in the literal sense, resort to cyber-force may be viewed as a form of intervention that can produce certain harmful or coercive effects in other states. Serious legal questions thus arise: does a denial-of-service attack against a foreign Internet site breach the legal rule prohibiting use of transnational force? Is the denial of service an act of coercion that fits within the legal ambit of acts prohibited by relevant UN declaratory instruments? Does a government's intentional interference with or interruption of another state's Internet service violate international legal rules? Or, should it be regarded as more legally akin to the lawful domestic decision of a government to instigate a legal economic embargo of another state? Would such interference be sufficiently 'coercive' so as to construe breach of the international legal rule that prohibits the use of force? Suppose a government 'attacks' another state's computer systems. Would such an attack against a bank or defence industry in another state constitute an unlawful 'use of force' or an 'armed attack' against that latter state? What form or repercussions must that cyber-generated assault take before the target state can respond? What degrees or kinds of cyber-force would be permissible? Clear answers to these quandaries are provided neither by UN Charter law nor by contemporary international legal rules.

Similar difficulties arise in defining what should constitute a 'use of force' with regard to biological and chemical weapons.[88] Chemical and biological weapons, it can be argued, should be viewed as forms of force because, if used, such weapons can destroy life and property.[89] Certain, though not all, weapons of IW also present real threats of widespread destruction. If, for example, a 'worm' were released and it incapacitates a hospital's computer network or an emergency 911 computer system, hundreds of lives might be put at risk. Equally plausible are circumstances that involve the cyber-instigated downing of computers that control chemical and nuclear power plants or oil refineries, which could cause massive releases of deadly gases or toxic effluents.[90] Such attacks could produce social impacts as devastating as those caused

[87] See Brownlie, *supra* note 72, at 265–278. Brownlie concludes that Article 2(4) includes force besides 'armed force', but he does not indicate the nature of these other uses of force.

[88] See Brownlie, *supra* note 72, at 362. Much like information operations, chemical and biological weapons do not have to involve the physical explosions and violence associated with traditional conceptions of armed force.

[89] *Ibid.*, at 362.

[90] See Constantini, 'Information Warriors Form New Army', International Press Service, 9 August 1996, available in 1996 WL 10768646. See also Lake, *supra* note 6 (examining six real scenarios that threaten the US, including cyber-terrorism).

by chemical weapons.[91] Using similar technologies, some computer attacks could destroy property, but spare harm to people. For example, a computer virus might be used to compromise Wall Street's electronic power supply and telecommunication infrastructures, thereby shutting down the financial markets. Chaos and panic could ensue, perhaps cascading even into dramatic repercussions for the economic stability of the United States and other Western financial markets. In the event, however, no human lives likely would be lost. Still, the real possibility that computer-based information operations in one state could destroy lives and damage property in other states points up the legal rationale for concluding that such activities should be prohibited as a 'use of force' under UN Charter law.

The argument seems persuasive that cyber-based activities that directly and intentionally result in non-combatant deaths and destruction — such as the premeditated disruption of an air traffic control system that results in the crash of a civilian airliner or the corruption of a medical database that causes civilians or wounded soldiers to receive transfusions of the wrong blood type — breach modern prohibitions on the use of force. Less clear is the case of other cyber-based activities, for example the disruption of a financial or social security system or the disclosure of confidential personal information, which produces no human injuries or property damage. These activities clearly intrude into the internal affairs of another state, but do not exceed any visible threshold of harm against which customary international law protects civilians. While certainly impermissible, one might argue whether such acts of subversive intervention are legally sufficient for automatically triggering forms of retaliation involving use of armed force by the targeted state.

B *Resort to Self-defence*

Contemporary international legal rules prohibit the threat or use of force except when authorized by the Security Council, or when undertaken by individual states in self-defence and in response to 'an armed attack'.[92] At least two important exceptions apply to these prohibitions on the use of force. First, in accordance with Chapter VII provisions of the Charter, the United Nations may use force, including military force, as a means to enforce decisions of the Security Council.[93] Secondly, individual

[91] See Laqueur, *supra* note 14, at 14 (arguing that a computerized, information warfare-based attack initiated against the Federal Reserve's main switching terminal in Culpepper, Virginia, would be disastrous to the United States); see also Schwartau, *supra* note 5, at 308–310 (describing the spiralling confusion and panic a concerted series of information-warfare attacks could cause); see also Wilson, 'The Precipice Problem: A Guide to the Destabilization of Western Civilization', www.infowar.com/class3/class3.html-ssi (visited on 17 March 1997). Wilson describes a concerted campaign which is geared towards catastrophically disrupting critical functions of society controlled by technology such as phone, power, financial, transportation, communication and law enforcement information networks. Wilson concludes that, after such an attack, 'some things are clear — there will be immediate chaos. The amount of damage that will be done will total into the trillions; this does not take into account the long-term economic effects, which will not be correctable. The West will be suffering from near-fatal internal strife.'

[92] See UN Charter, Articles 2(4) and 51.

[93] Under Article 39 of the UN Charter, the Security Council can determine whether there has been a 'breach of the peace' and can authorize the use of force under Article 42.

governments may take forcible action, including the use of military measures, in self-defence.[94]

In the world of cyberspace, however, serious issues of law and policy concerning self-defence persist. Suppose a state is the targeted victim of a computer network attack from a private terrorist organization located within another country. The IW attack takes the form of sophisticated intrusions into top-secret military databases of the victim state. Classified military information is stolen, destroyed and altered. When the victim state's intrusion-detection mechanisms fail to give warning of these intrusions, the victim state erroneously relies on false data in making foreign policy and military decisions. The goal of the attack is successful. The result is the death of 20 servicemen who perish when a military unit conducting training operations launches a missile into their military unit, rather than the vacant training grounds because they relied on the compromised data.

Under this scenario, does the victim state have any recourse against the state from which the IW attack originated, or just the private terrorist organization? Could the victim state launch an attack in self-defence in order to stop the computer intrusions into its computer systems? Is the victim limited to destroying the computer virus that has penetrated its system, or can the victim state attack back in self-defence with conventional forces, destroying the structural facilities from where the computer viruses were launched? Does the victim state have first to gain permission from the government of the state where the terrorists are located before acting in self-defence using armed force?

Finally, does the victim state's inability to detect the compromise of its computer system in some way detract from its right to act in self-defence? What if the victim state did not have any intrusion-detection system in place? And would the victim state's right of self-defence under international law be different if the result of the attack was not loss of life, but only the theft of classified information?

Contemporary international legal rules provide few definitive answers to these considerations. In instances where a state can link cyber-attack to a foreign government, a forcible response may be necessary, either to defend that state against an ongoing attack or to prevent future attacks. Provided that the attack is actual or the threat is imminent and without any alternative choice of means, the victim state may lawfully invoke self-defence to justify reasonable, necessary and proportional measures to safeguard its security. This, in essence, embodies the right of self-defence.[95] The victim state would justify its response as part of its right of self-defence as set out in contemporary UN Charter law. Less obvious, however, is that these UN Charter rules provide legal support for taking military action against a state or its agents that conduct cyber-based information attacks against another state.

The exercise of self-defence, clearly a right of states, remains subject to legal

[94] As provided for in Article 51: '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.'

[95] Bowett, *supra* note 72, at 269; O'Brien, *supra* note 79, at 23–32, a comprehensive summary of various views on the meaning of self-defence.

restrictions, even in cases of cyber-attack. On the one hand, only actions taken in self-defence are permitted; reprisals and retaliation are proscribed under contemporary UN Charter law.[96] This being the case, a government can respond to an IW attack by using some kind of force.[97] Once the cyber-attack ends, however, it is questionable whether international legal rules allow the target state to retaliate forcibly against the attacker. If a state is under a continuous, foreign-instigated IW attack and is suffering physical, financial and potentially mortal harm, that government is not expected to tolerate events that are destroying its national infrastructure. It seems reasonable that a government subjected to such a cyber-attack would be permitted to respond immediately by taking action in self-defence to thwart the attack. But suppose a government discovers several weeks afterwards that it has been victimized by a cyber-assault on its computer systems. Is that government granted any right of subsequent retaliation? The rules of modern international law generally suggest that this should not be the case, and instances of cyber-assault should be treated no differently than an act of foreign espionage. Forcible retaliation as retribution is not permitted. Compensation or reparations may be sought through diplomatic channels from the offending government, but acts of reprisal are not lawfully acceptable, largely because they could perpetrate a circle of persistent violence.[98] Retaliation by means of IW should be treated no differently.

A second limitation on the right to self-defence mandates that not all uses of force, inclusive of cyber-force, necessarily qualify as 'armed' attacks. As the International Court of Justice concluded in *Nicaragua v. United States*, governments do not perforce have the right of armed response to acts that fall short of constituting an 'armed attack'. Only military attacks, and not every isolated armed incident, rise to the level of an 'armed attack'.[99] The point to be made here is that certain acts of intrusion may be unlawful, but that fact does not necessarily give a state the right to respond by using armed force in self-defence. Simply put, some illegal actions taken by a government against another state rise to the level of violating prohibitions of the use of force, but not every act of intervention rises to the level of an 'armed attack', nor necessarily triggers a state's right to respond in self-defence, resorting to military force.

The traditional limitation on armed force to measures taken strictly in self-defence upholds world community standards contributing to a more stable international

[96] Brownlie, *supra* note 72, at 281–283; Schachter, *supra* note 70, at 1620.

[97] See Arend, 'International Law and the Recourse to Force: A Shift in Paradigms', 27 *Stanford Journal of International Law* (1990) 1, at 14 (referring to the 'typical action taken in self-defense' as one in which the state must immediately act to protect itself from an ongoing attack).

[98] See, e.g. Security Council Resolution 188, UN SCOR, 19th Session, 188th Meeting, UN Doc. AA/5751 (1964); *Restatement (Third) of the Foreign Relations Law of the United States* (1987) para. 905. For a review of the legality of reprisals in the context of the US missile raid on Baghdad in 1993 in response to the alleged assassination attempt on President Bush, see Reisman, 'Self-Defence or Reprisal? The Raid on Baghdad: Some Reflections on Its Lawfulness and Implications', 5 *European Journal of International Law* (1994) 120, at 125; and Ratner and Lobel, 'Bombing Baghdad: Illegal Reprisal or Self-Defense?', *Legal Times*, 5 July 1993, at 24.

[99] See *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. US)*, ICJ Reports (1986) 1, at 93–99.

order. First, the restriction tends to dissuade the scenario of the vicious cycle of escalating violence from occurring. Secondly, it ensures that force is used only as an emergency measure — as a necessary last resort. Thirdly, it functions as a restraint against uses of force that are based on pretext, misunderstanding and erroneous factual determinations. Professor Louis Henkin put it well when he observed that the United Nations 'recognize[s] the exception of self-defense in emergency, but limit[s] [it] to actual armed attack, which is clear, unambiguous, subject to proof, and not easily open to misinterpretation or fabrication'.[100] In the post-Second World War era of conventional military weapons and international war, such considerations were particularly apt.

The legal and technological situations have changed radically today. When one state attacks another state with tanks, air strikes or missiles, the factual predicate for self-defence stands clear and manifest. Such is hardly the present case. In a time earmarked by pervasive unchecked transnational electronic interactions, techniques of cyber-based IW can be used by a government to disrupt (or 'attack') facilities in another state. A computer-network-based attack involving software weapons such as viruses or 'Trojan horses' is far less apparent than Professor Henkin's observation suggests. It seems untenable that international rules require a government that is being subjected to an electronic attack — the results of which may inflict catastrophic social and economic damage on its society — to delay responding until the factual predicate or the intent of the perpetrators are made clear. Similarly untenable is the case for a government to launch an armed attack on another state, merely because it suspects that the latter state is using the Internet subversively. Irrefutable evidence must exist to support that suspicion or justify a retaliatory response. Such a licence eviscerates legal prohibitions against the use of force, and invites unsubstantiated accusations of 'cyber-aggression' as a new legal predicate for states to retaliate forcibly. These undesirable scenarios suggest the need to construct new international rules that hold factual predicates to a less ambiguous legal standard.

A first step towards shaping new rules is to clarify what constitutes an 'armed attack' in the context of cyber-generated IW. As noted earlier, the right of self-defence may be permissible against an armed attack or its imminent threat. But neither contemporary UN Charter law nor general international legal rules furnish adequate answers for what actions constitute an 'armed attack' or its imminent threat. Moreover, the issue of whether 'armed attack' is legally synonymous with 'aggression' has never been satisfactory resolved.[101] This conundrum remains no less conflicted in cases of cyber-attack that disrupt vital military, industrial or public healthcare facilities.

Certain misconceptions surround contemporary interpretations of self-defence.

[100] Louis Henkin, *How Nations Behave* (2nd ed., 1979) 142 (emphasis added).

[101] The definition of 'aggression' put forward by the UN General Assembly in 1974 contributes little to clarifying the legal status of cyber-based acts by one state against facilities in another state: 'Aggression is the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.' United Nations Press Release, GA/5194, 20 December 1974.

One surmises that UN Charter law restricts the right of self-defence to a delict committed by one state, which constitutes an 'actual' armed attack.[102] While sometimes true, considerable legal support resides in the proposition that a state has an inherent right to use force in self-defence against acts that do not constitute a classic armed attack.[103] Another misconception about self-defence is the supposition that an 'armed attack' can only occur if the military forces of a state carry it out. That may not always be the case. Paramilitary forces, irregular forces, border security forces, police forces or even armed civilians might take actions that amount to such an attack. Moreover, an armed attack may take either direct or indirect forms. It assumes a direct character if a state employs armed forces straight away against another state. Armed attack can take an indirect form if a state launches an attack from a third state, or uses irregular or foreign forces as its surrogates. Finally, the misconception persists that a state must be attacked before the right to defend its territorial integrity can be exercised. The notion of pre-emptive or anticipatory self-defence permits a state to defend itself in the event of imminent danger or an actual threat of armed attack. The legal caveat is that the threat must be real and credible and create an imminent need to act, with a genuine probability of attack. As succinctly expressed in the well-known *Caroline* doctrine, the threat must be 'instant, overwhelming, leaving no choice of means, and no moment for deliberation'.[104] The reasonable conclusion is that

[102] See Brownlie, *supra* note 72, at 265–278. For more detailed argument rejecting this view, see Bowett, *supra* note 72, at 187–193; J. Brierly, *The Law of Nations: An Introduction to the International Law of Peace* (6th ed., 1963) 417–418; and O'Brien, *supra* note 79, at 23–32.

[103] This view is supported by the inclusion in the General Assembly's definition of aggression of acts that do not entail armed attacks by a nation's armed forces, such as the unlawful extension of the presence of visiting forces, or allowing a nation's territory to be used by another state 'for perpetrating an act of aggression against a third State'. See United Nations Press Release, GA/5194, 20 December 1974, Article 3, which states that the following qualify as acts of aggression: '(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof; (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State; (c) The blockade of the ports or coasts of a State by the armed forces of another State; (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State; (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement; (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.' Definition of Aggression, General Assembly Resolution 3314, UN GAOR, 29th Session, Supp. No. 19, 2319th Plenary Meeting, at 392, UN Doc. A/9890 (1974).

[104] See *The Caroline Case*, in J.B. Moore, *Digest of International Law*, vol. 2 (1906) 409. Bowett, *supra* note 72, at 59; R.Y. Jennings, 'The Caroline and McLeod Cases', 32 *AJIL* (1938) 89.

international law is not a suicide pact among states, and thus a society does not have to wait until it is physically harmed to defend itself.[105]

Computer-generated intrusions and cyber-communication disruptions elude easy classification as being 'attacks'. In evaluating the propriety of taking defensive action, it seems more useful to consider the legal consequences of such a computer-generated action rather then the mechanism used to launch the attack. That is, computer intrusions committed to steal data or disrupt air traffic control may be equally intrusive, but the more extensive destruction and death caused by disruption of a public air traffic control system render that action more susceptible to the equivalent of an 'armed attack' than an attempt at data theft. It seems reasonable to qualify cyber-assaults that are sufficiently destructive as 'armed attacks', regardless of the level of intrusion. Difficulty persists in asserting that an unauthorized cyber-based intrusion into an unclassified information system *ipso facto* always meets the legal threshold of being an armed attack. If, however, the same act resulted in shutting down a state's air traffic control system, as well as in collapsing banking institutions, financial systems and public utilities, and opened the floodgates of dams that caused deaths and property damage, considerable merit would reside in alleging that such an attack inflicted damage equivalent to that caused by an 'armed attack'. Although those information systems do not contain classified information, such computer-generated acts would obviously imperil that state's society and threaten its national security.

The nature of the information stolen or compromised also contributes to determination of whether an action rises to the level of legally being considered 'an attack'. If certain data are considered vital to national security (i.e. information that is 'classified'), that information may be afforded special protections under the regime of self-defence. For instance, if a foreign government attacks the computer databases of another state's department or ministry of defence, and steals classified information related to troop locations during a time of armed conflict, or the codes to nuclear weapons' launch instruments, such actions could qualify as being tantamount to 'armed attacks', even though no immediate loss of life or destruction results. If a state's government discovers that these computer attacks against its defence ministry's classified databases were continuous, and evidence exists to support that the perpetrators are planning future cyber-attacks (and the government's claims are accepted as true and accurate), a reasonable deduction is that the computer intruders were engaged in an ongoing attack against the defence establishment of that state.

The government's assertions, if in fact true, could thus give rise to a right of

[105] Whether an imminent danger of an armed attack actually exists depends on the individual circumstances of each case. For an armed attack to occur, some level of actual or potential physical destruction, combined with some level of intrusion into a target state's borders or violation of its sovereignty rights, should be evident. Some actions, such as aerial bombardment of a state's military command and control centres, will clearly constitute 'armed attacks', as they inflict high levels of both forcible intrusion and destruction. Other acts, such as radio and television propaganda broadcasts, are not considered 'armed attacks' and are usually relegated to forms of subversive intervention.

self-defence against the cyber-intruders and the government intentionally sponsoring those IW activities. Such a right permits the target state to take necessary and proportionate countermeasures, including the use of force intended to halt those actions and to prevent similar future assaults.[106] Perhaps the targeted computers are unclassified military logistics systems containing information about the management of spare parts, troop mobilization and medical supplies, the corruption of which would seriously interfere with a state's ability to conduct military operations and defend its national security. Such a cyber-attack on unclassified systems may still give rise to a right of self-defence. As suggested earlier, the consequences of the cyber-attack on the targeted programs may be more important than the means used to implement it.

Discussion of deterrence often arises from advocates of strong and swift military responses to terrorist attacks. They argue that force is necessary as 'an effective counterweight to extremism'.[107] Even so, some experts question the deterrent value of military responses to attacks.[108] They identify the risks of error and lack of a prompt military response in military self-defence attacks as not justifying any gains in deterrence value. They are also concerned with provoking the original attackers, thereby causing an escalation of violence and a cycle of retaliation.[109]

Under these circumstances, IW may actually serve as an effective tool for dissuading self-defence, as well as deterring military responses. In using IW a government could react immediately through use of computers that can be accessed instantaneously. Once an intrusion is detected, only minutes are needed for a state to collect enough computer-generated evidence to meet the predicate factual threshold for lawfully initiating a response. The time to respond is thus significantly less than that required for military equipment and personnel to be readied and deployed abroad for a conventional strike. Targeting the attackers, moreover, can be more precise and is less likely to inflict human casualties. Finally, cyber-based actions taken in self-defence can be prosecuted instantaneously and covertly, thus avoiding public acts that expose a state to a breach of international legal rules and to any action taken in self-defence by the targeted government. This covert process allows the opportunity for an offending state, once it realizes that it has been found out, to halt its aggressive

[106] See *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. US)*, ICJ Reports (1986) 1. However, the target state would not have the right to launch a computer attack through a third state's territory in order to react in self-defence without that third state's permission.

[107] See Schultz, 'Low Intensity Warfare: The Challenge of Ambiguity', 25 ILM (1986) 204, at 205.

[108] As former CIA Director James Woolsey testified, an effective military response is often 'at odds with its being prompt'. Hearings on Counterterrorism Policy Before the Judiciary Committee of the Senate, 105th Cong. (1998) (testimony of James Woolsey, former Director of the CIA), 1998 WL 564420.

[109] See Scherman, 'US Fury on 2 Continents: Pros and Cons', *New York Times*, 21 August 1998, at A11 ('Experts say, it is most likely that the targets of the action and their supporters will lash back'). Some believe that the bombing of Pan Am Flight 103 over Lockerbie, Scotland in 1988 was Libya's response to the US air strike against Libya in 1986 after the Libyans allegedly ordered the bombing of a nightclub in West Berlin that killed a US Army sergeant and injured 50 American military personnel. Newman *et al.*, 'Clinton Raises the Stakes in the War Against Terrorism', *US News and World Report*, 31 August 1998, at 38 ('The bombing of Pan Am Flight 103 in 1988 is widely believed to have been an act of revenge for the US bombing of Libya in 1986').

actions without being subjected to international criticism. This avoids humiliating the attacking state. At the same time, this process might persuade the perpetrator not to retaliate, thus alleviating that government from its felt need to escalate its response on account of national security or national interests, which probably would avoid exacerbating the level of violence.[110]

C *Implications for Anticipatory Self-defence*

Some contemporary legal theories support the premise that customary international law does not limit a state simply to reacting to traditional armed attack,[111] and that cyber-force might be used lawfully as an instrument of pre-emptive self-defence. According to general legal rules for self-defence, not only may a government respond to an attack launched against its territory, but a government can also take self-defensive military action in anticipation of such an armed attack.[112] This principle of 'anticipatory self-defence' asserts that the use of force by one state against another is permissible as self-defence if the force used to respond is both really necessary and not excessive in relation to the perceived threat. Even so, such a principle of 'pre-emptive' self-protection does not sanction acts of self-defence under any and all circumstances. To do so might invite committing acts in circumstances that actually constitute aggression. Moreover, while the right of self-defence may at times seem ambiguous, accepted legal criteria have evolved under customary international law that set limits for determining the legitimacy of action taken in self-defence.

These concerns directly relate to cyber-warfare. For instance, suppose a government's military officials locate a 'trapdoor' within their computers that control that

[110] We would like to thank Phillip Johnson for his helpful insights on this point.

[111] For a discussion of the various views of international scholars regarding the legitimacy of anticipatory self-defence under Article 51, see Arend and Beck, *supra* note 80, at 73 and the accompanying footnotes. According to Arend and Beck, most international legal scholars can be divided into two schools of thought regarding the legitimacy of anticipatory self-defence: the 'restrictionists', who take the position that anticipatory self-defence violates Article 51; and the 'counter restrictionists', who argue that, for various reasons, anticipatory self-defence does not violate Article 51.

[112] See Dinstein, *supra* note 70, at 172 (explaining the customary right of self-defence as a preventive measure and not only as a responsive measure). The *Caroline Case* of 1837 is often cited as legitimizing the right of anticipatory self-defensive action taken in response to an imminent armed attack by another state or other entity. See *The Caroline Case*, in J.B. Moore, *Digest of International Law*, vol. 2 (906) 412. In 1837, British forces took action against an insurgency by Canadian rebels who had mounted several attacks from islands in the Niagara River. The British sought to capture the US steamboat *Caroline* that the rebels had chartered to maintain their supply lines. The British seized the *Caroline* while it was moored in US territory, burned the vessel and sent it downstream where it plunged over the Falls. During the incursion the British killed several US citizens. The US Government complained that the British had violated US sovereignty while the British countered that they had simply acted 'in self-defence'. In a letter to Henry Fox, the British minister in Washington, DC, Secretary of State Daniel Webster wrote that the British could only justify the use of force in self-defence so long as the British could prove 'a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation'. Letter from Secretary Webster to Mr Fox, 24 April 1981, *British and Foreign State Papers* (1857) 1129, at 1138. The traditional principle of anticipatory self-defence was first enunciated by Secretary of State Daniel Webster in his response to a Canadian attack on the American ship *Caroline*, which had been assisting Canadian rebels in their efforts against the Canadian Government. See Jennings, *supra* note 104.

state's missile defence systems. They identify the source of a computer intrusion to be the ministry of defence of a foreign government. The victim state is able to verify the theft of at least a dozen passwords, and undertakes the necessary action to have the entire missile launch passwords immediately changed. However, because of the nature of the trapdoor, the targeted government cannot know for sure what sensitive information was stolen, including whether the codes to deactivate the defence system were compromised. Without sufficient time to change the codes, the victim government must decide whether to react in a pre-emptive fashion, i.e. to act against the foreign state that intruded into the victim state's missile defence computer systems. Would the victim state be justified in attacking the foreign state to pre-empt an IW attack that would deactivate their missile defensive system?

Contemporary international law supports the possibility of such a response. As a traditional international rule, however, for recourse to anticipatory self-defence to be lawful, it must be limited by specific considerations. First, such action must be necessary. In this respect, necessity requires that a state undertake self-defence only as a last resort. At the same time, the law requires that a state demonstrate that actions taken in response are proportional to the threat being directed against its territory. Plainly put, cyber-force used in anticipatory self-defence must be neither unreasonable nor excessive. This notion of proportionality implies that the degree of cyber-force employed be limited in magnitude, intensity and duration to that which is reasonably necessary to counter the threat actually posed against the target state. Proportionality applies both to whether a given level of cyber-force is appropriate as a response to a particular grievance (as part of the law of the use of force, *jus ad bellum*) and whether a given cyber-action is appropriate in light of its objectives and the damages/casualties that will result (as part of the law of armed conflict, *jus in bello*).[113] In short, the level of forcible response by a victim state must be proportionate to the force applied by the aggressor state in the initial attack. For example, a full-scale blitzkrieg across a broad front, accompanied by massive aerial bombardment, would obviously be disproportionate as a response to a patrol's border raid. Nor would a cyber-generated effort to bring down a society's financial or banking infrastructure be appropriate as a response to a computer intrusion that temporarily disrupted public telecommunications in the victim state.

Secondly, the cyber-generated response must strive to balance the damage it inflicts, especially to civilians, against the military objectives it aims to accomplish. In this regard, a cyber-attack directed against civilian healthcare facilities would not be permissible as an act of self-defence. For over 150 years these precepts drawn from the *Caroline* incident have influenced the interpretation of international legal rules. While an international consensus is still lacking to substantiate the applicability of anticipatory self-defence as a universally accepted principle of international law, no consensus actively opposes the concept either. It thus appears that no strict prohibition precludes a government using cyber-force pre-emptively as long as the perceived threat is demonstrated to be real and immediate, and the criteria of

[113] *Restatement (Third) of the Foreign Relations Law of the United States* (1987) para. 905.

proportionality and necessity as general legal rules are adhered to in the application of computer-generated coercion.

5 Rethinking Legal Thresholds for Information Warfare

We live in an era in which many countries possess instruments of IW and the peacekeeping function of the UN Security Council is less than fully effective. Many IW weapons are capable of instantaneous mass destruction with no forewarning of the impending destruction. Other IW tools, such as preset 'logic bombs' and 'Trojan horses', operate like mines floating in territorial waters as their cyber-programs lie in wait until activated. In this context, governments must ponder not only whether the UN Security Council will act on their behalf, but also whether any assistance if offered will be too little, too late. In the absence of genuine guarantees of collective security against conventional military threats, governments will have to weigh whether launching a pre-emptive cyber-based attack is warranted against another state's computer assets in order to preserve their own national security from a perceived threat of IW.[114] Given such circumstances, a broader reading of self-defence would permit cyber-generated forms of anticipatory self-defence to be conducted lawfully, presumably with fewer human casualties and less property damage.[115]

As a source of customary international law, state practice seems to sympathize with permitting some IW activities. For instance, espionage, universally criminal under domestic laws, does not *ipso facto* violate international law.[116] In this context, IW conducted as espionage activity might be considered lawful. Furthermore, ruses have long been part of warfare and their legitimacy is explicitly recognized in the laws of war.[117] Just as the original ancient Trojan Horse was legal, so too would the use of some 'Trojan Horse' pieces of software be permissible in times of armed conflict between two states.

If a target state cannot substantiate that a foreign-generated computer attack against its information systems meets the threshold of force necessary for an 'armed attack', then that government may not respond with conventional, kinetic military force, unless it is willing to risk that response being labelled the form of aggressive 'armed attack' prohibited under UN Charter law. International legal rules and customary state practice presently support a state's acting in self-defence against attacks on its national information infrastructure. However, a government's response

[114] One useful approach to the concept of self-defence in the context of IW is Michael Walzer's restatement of the *Caroline* principle. According to Walzer, a state has the right to self-defence when a nation perceives the following on the part of an aggressor: (1) an intent to injure; (2) active preparation making intent a positive danger; and (3) a general situation in which waiting or doing anything other than fighting greatly magnifies the risk. Michael Walzer, *Just and Unjust War: A Moral Argument with Historical Illustrations* (2nd ed., 1992) 81.

[115] See Walter G. Sharp Sr, *CyberSpace and the Use of Force* (1999) 43.

[116] See Kanuck, *supra* note 45; and Abram N. Shulsky, *Silent Warfare: Understanding the World of Intelligence* (2nd ed., 1993) 103.

[117] Protocol Additional to the Geneva Conventions of 12 August 1949; and Relating to the Protection of Victims of International Armed Conflicts, 12 December 1977, 1125 UNTS 3.

to a cyber-attack, like that to any force, must comply with the prescribed legal principles set down in the concepts of necessity, imminence and proportionality. Moreover, the perceived 'intent' behind a cyber-attack should be taken into account in making any decision to anticipate or respond to an offensive act. In this regard, certain factors serve as useful guidelines when considering whether to act in self-defence, among them the following: (1) a clear indication of intent by the offending state; (2) the availability and sufficiency of evidence to demonstrate that preparations for the attack have advanced to the point where it is imminent; and (3) the ability to make the advantage of a pre-emptive attack proportional to the risks of precipitating a war that might otherwise be avoided.[118] In any event, deciding whether a particular form of cyber-based attack meets the conditions of necessity and imminence depends on the particular perceptions of the threatened state. A targeted government's decision to respond also depends on that state's vulnerabilities and the potential for damage by a particular cyber-attack. Similarly, the perceived intent of the offending government may determine the level of response by a target state. If the government of a targeted state believes that another state's assault on its information systems merely serves as a prelude to a larger conventional attack, then it might view the 'non-armed' assault as the first phase in a war-making process. Similarly, a state victimized by cyber-assaults might absorb some degree of damage while reserving the right to act later in accordance with the doctrine of self-defence. Whether a government considers cyber-based danger 'imminent' depends on the intensity of the attack, the target of the attack, the reaction time required in order to successfully pre-empt the attack, and the speed with which the damage may move throughout the computer networks.

Just as it is not clear that an attack on information systems amounts to an 'armed attack' against a state's territorial integrity or political independence, neither is it obvious what types of action would be proportionate to such an attack, especially in cases where the attack inflicts little or no physical damage or loss of life. Where a computer intrusion disrupts or corrupts a database, or denies service for vital elements of a society's electronic infrastructure, thereby inflicting great hardship on the target country, that state must decide what form of response qualifies as being proportionate to the cyber-attack. In the absence of real physical destruction or human deaths — such as the crash of a passenger aircraft through manipulation of the air traffic control system — it remains polemical as to whether a conventional military attack would be proportionate. However, if a conventional response is deemed disproportionate to an IW attack, a response in kind may be an option as long as its effects remain proportionate to the offending state's 'armed attack'.

The dual-use quality of most telecommunications networks further complicates the feasibility of applying traditional international legal rules as constraints on the use of IW. These dual uses blur the distinctions between military and civilian systems. By doing so, confusion is introduced between military targets, which are legitimate to attack during conflict, and civilian facilities, which are protected under humanitarian

[118] William V. O'Brien, *The Conduct of Just and Limited War* (1981) 132–133.

rules of armed conflict. Some IW tools do not always allow their users to distinguish between military and civilian facilities. Additionally, Western military forces are particularly dependent on non-military systems for deployment and logistics.[119] Attacks having military objectives might be directed predominantly at civilian systems, with resultant collateral damage and injury to the civilians who operate and depend upon them.[120]

Cyber-attacks on military targets may cause civilian systems connected to those military systems to fail. Alternatively, a virus fed into an adversary's military computer might inadvertently or otherwise enter into civilian systems. In a related vein, electronic assaults on computer systems that otherwise might be considered legitimate targets may be impermissible also on account of the danger caused to civilians by malfunction of those systems. A cyber-attack on military power facilities, defence-related munitions factories, pharmaceutical plants or nuclear power plants could pose problems for society in general if the computer-generated failure of a facility leads to the release of toxic substances into the atmosphere. In this regard, the issue remains as to whether a state necessarily waives its rights to protection against cyber-attacks on civilian targets if it purposefully integrates military facilities into its civilian systems. Given the current rules of armed conflict, one would think that, yes, the rights to protection of civilian facilities are given up when those facilities are used for military purposes. A state may leave its civilian computer-based communications systems vulnerable to a legitimate attack if that government allows both military and civilian systems to run on the same networks.

As warfare capability evolves through fast, accurate and covert information weaponry, the requirement under the UN Charter of an 'armed attack' occurring before a government may act in self-defence becomes less pragmatic. Given the capabilities of IW techniques, this approach may prove too restrictive. In circumstances involving the possible use of IW weapons, a government simply may not be able to afford to wait until the necessity to act is so dire. Within this context, a more appropriate approach may be reliance upon the customary international rule of anticipatory self-defence, which would permit resort to force if the threat is instant and overwhelming, and leaves no choice of means or no moment for deliberation. In an age when many states possess instruments that can be employed transnationally to conduct IW, the instantaneous need to interpret other governments' intentions can mean the difference between peace and conflict. The potential for pervasive societal disruptions caused by a premeditated IW attack renders such a 'wait and see' approach overly risky for most technologically advanced states.

The instant quality of cyber-force suggests the need for a more practical approach to dealing with IW, one which would tolerate the pre-emptive use of cyber-force under the doctrine of anticipatory self-defence when a government perceives that there exists a significant and real threat to its national security, and responds to pre-empt

[119] See Sterner, 'Digital Pearl Harbor, National Security in the Information Age', 2 *National Security Studies Quarterly* (Summer 1996) 33, at 43.

[120] See Kanuck, *supra* note 45, at 284.

that threat in a reasonable and responsible manner. To be lawful, this modern theory of anticipatory self-defence to counter IW threats would rest upon the ability to determine the reality of the perceived threat and the reasonableness of the response in self-defence. The standard of reasonableness would have to meet both a subjective and an objective test. On the one hand, the subjective test would ascertain whether the purported target state has reasonable grounds for believing that a real threat exists. On the other hand, the objective test would determine whether third party states view the threat in the same light.[121] The objective test would also consider whether the cyber-force used to counter the perceived threat was reasonable relative to the threat posed.[122] When applied to the transnational use of cyber-force, anticipatory self-defence would allow governments to meet their minimum national security requirements and at the same time ensure that the use of force is necessary and proportional under the circumstances.

6 Legal Rules and Information Warfare Reconsidered

International legal rules provide the framework for organizing and processing political and military interaction among nation-states. Today, the Internet performs a critical role in this regard, as it provides a vast web of interlinked channels for instantaneous intergovernmental communication. More profoundly, the Internet makes possible new types of legal regimes. The Internet and international law thus can become partners in shaping new considerations and forms of sovereignty. International law can crystallize norms of behaviour in cyberspace. The Internet can provide the mechanism for giving these ideas form and substance through human activities.

At the same time, cyber-based activities can be used for unlawful purposes, in particular the pursuit of IW as examined in this study. No provision of modern international law explicitly prohibits IW.[123] This is significant because, as usually regarded under international law, that which international law does not prohibit it generally permits.[124] However, the absence of a prohibition against IW is not dispositive, since under international law general principles may apply to the use of

[121] In August 1998, US cruise missiles struck a terrorist training camp in Afghanistan and a chemical plant in Sudan. The rationale articulated for this action was self-defence.

[122] See generally Myers S. McDougal and Florentino Feliciano, *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (1961).

[123] Because of the nature of certain IW activities such as jamming and spoofing, orbital assets are necessary to carry out IW activity, thus implicating rules and principles of outer space law. Yet no public law convention dealing with outer space prohibits the use of IW activities that make use of satellite assets. See the 1967 Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 18 UST 2410; TIAS No. 6347; 610 UNTS 205; the 1971 Agreement Related to the International Telecommunications Satellite Organization, 23 UST 3813; TIAS No. 7532; and the 1976 Convention on the International Maritime Satellite Organization, 31 UST 1; TIAS No. 9605.

[124] See *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), at para. 21.

IW.[125] International law may pose constraints on the conduct of IW, just as it does on modes of warfare that use traditional forms of attack. Alternatively, international law may leave wiggle room for using many types of IW techniques in many circumstances. In some situations, international law might find that certain cyber-actions do not rise to the level of acts that count as indicators of hostile intent, nor of a use of force. It is neither possible nor necessary to create a comprehensive list of what cyber-techniques lay definitively beyond the bounds of acceptable acts under international law. State actions, like human behaviour generally, assume significance from their own particular context, not as generic stereotypes classified into a specific legal category.

The major legal issues for the future turn on whether and to what extent a state should be authorized to use information operations and whether a state can act in self-defence using information operations. The most important task confronting international lawyers is to clarify various criteria by which the legitimacy of a state's use of forcible measures in information operations situations can be appraised, with the ultimate goal of bringing the international system closer to a more orderly, predictable environment for interstate intercourse. To this end, certain criteria might be useful for designing a framework of legal rules affecting the use of force applicable to IW. For one, determination must be made as to what constitutes lawful force when information operations are used transnationally. A state could use information operations to defend itself from an imminent armed attack, or actions deemed equivalent to an armed attack (i.e. indirect aggression that rose to the level of an armed attack).

Secondly, a determination must be made as to what actions in information operations amount to an 'armed attack'. Such an assessment of the character of the information operations could be done based upon a critical evaluation of various interrelated factors, in particular the nature of the activities, the severity of the effect of the activities, and how long the activities persist. Gauging these factors would contribute much towards gauging the quality and quantity of a particular act of cyber-force, as well as its lawful character.

For a computer assault to qualify as an 'armed attack', its intensity and effects should be equivalent in severity to those inflicted by a traditional 'armed attack'. That is, a foreign-instigated computer action that temporarily interrupts service of another state's local phone company and causes a few hundred people to be without a phone service would not amount to an 'armed attack'. Conversely, a computer attack that intentionally compromises the control system of a chemical or biological plant, and, as a result, causes the release of toxic gases over large population centres, is more likely to be considered the legal equivalent of an armed attack.

A third factor to be weighed in determining whether a computer attack rises to the level of an 'armed attack' is the duration of the action. A one-time computer attack against the financial markets of Wall Street, causing a crash, or the penetration and theft of classified top-secret information from defence department databases, might by

[125] *Ibid.*, at para. 86.

itself be sufficient to constitute an armed attack. Yet, even a low intensity attack against a state's financial markets that produces intermittent interruptions or causes the theft of sensitive, albeit not top-secret information, could conceivably constitute an armed attack if done as part of an ongoing continuous attack. While the theft of secrets from one database may in and of itself not qualify as an armed attack, the persistent, premeditated theft of sensitive information may do so.

In addition, other standards can be applied to the process of evaluating the responsive use of information operations, particularly in self-defence. These would include: the degree to which a cyber-attack caused an immediate and extensive threat to human lives; an assurance that a proportional use of force will not threaten a greater destruction of values than those at stake; a demonstration that the action taken in response causes only minimal effects on authority structures; evidence that a prompt disengagement occurs consistent with the purpose of the action; and in the aftermath of the cyber-attack and its response, an assurance that the government of a targeted state furnish immediate and full reporting to the Security Council and any appropriate regional organizations.[126]

7 Conclusion

Western societies have invested trillions of dollars in building information infrastructures that are interpretable, easy to access and easy to use. Attributes like openness and the ease of systems' interconnectivity, which promote efficiency and expeditious customer service, are the same factors that make these systems vulnerable to attacks. Recent cyber-attacks in the United States underscore this point. Information warriors have taken the threat out of the realm of the abstract and made it real. Thus, a major challenge for national governments during the next decade will be to find ways to defend cyber-based infrastructure and to protect telecommunications commerce while maintaining an open society, all carried out through lawful means.[127]

To be relevant today, the rules of modern international law must define more sharply the criteria used to distinguish between which state actions are permissible as normal computer-generated transborder data flows for international communications, trade and financial assistance from those cyber-activities that might qualify as an 'armed attack', against which the use of force is permissible. Even with new forms of computer-generated weapons and changing concepts of sovereignty and territory, international law will continue to rely upon UN Charter principles and rules to define the legal boundaries of 'cyberspace'. Modern state practice is grounded in those norms, and they remain the foundation for guiding interstate behaviour in the Information Age. Yet, at the same time, international law must evolve and adapt.

[126] Moore, *supra* note 79, at 264.

[127] In the recent words of President Clinton, in the context of meeting the challenges of terrorism, the challenge of IW 'requires the confident will of the American people to retain our convictions for freedom and peace and to remain the indispensable force in creating a better world at the dawn of a new century'. 'Remarks by the President on American Security in a Changing World' at George Washington University, Washington, DC, Office of the Press Secretary, The White House, 5 August 1996.

Clearer rules for what kinds of IW action constitute an 'armed attack', what responses are permissible as self-defence by a state targeted in an IW situation, and how international institutions can facilitate processes aimed at reaching these objectives should be re-examined and re-evaluated. This ambition cannot help but remain a constant challenge, as international law struggles to keep pace with the all-too-rapid advancements in technology in general, but especially as more people in more societies add to the burgeoning worldwide use of cyber-technologies.