A Proposal for an International Convention
To Regulate the Use of
Information Systems in Armed Conflict

Davis Brown

It seems one has to accept as inevitable that when something useful for
the improvement of man’s life has been invented, thoughts will either
turn into how to weaponize or destroy it, or, in the case of computer
network technology, both.

—Louise Doswald-Beck¹

INTRODUCTION

One of the greatest challenges of law is keeping up with the advancement
of technology. In this respect, international law is no different. Indeed, the
process of creating international law is hampered by constraints that do not
affect the making of domestic law. In an autocratic state, the rule of law is
the will of the ruler and is enforced by the ruler. In a democratic state, the
rule of law is a composite of the diverse opinions of legislators who have
come together to forge a principle that carries the support of the majority.
That norm is then applied to the entire state and enforced by the government
on its people. The law of nations, however, is enforceable only by the nations
themselves, making the creation of norm-creating law more difficult.

In responding to the advancement of weaponry, the international commu-
nity has struggled to promulgate standards of conduct in a timely manner
that carry nearly universal support and adherence. On the heels of the first
use of poison gas during World War I came the 1925 Geneva Gas Protocol,
regulating the use of gas and “bacteriological” warfare.² However, the Hague
Rules of Aerial Warfare, crafted in the aftermath of the first use of aircraft in
armed conflict, is a dead letter.³ It took nearly fifty years to formulate a total
ban on biological weapons in the form of the 1972 Biological Weapons Conven-

¹ Visiting Scholar, George Washington University Law School; former Deputy Staff Judge Advocate,
U.S. Defense Information Systems Agency. The author’s conclusions are his alone and are not the official
position of the U.S. Government.

² Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of

tion⁴ and an additional twenty years to devise a comprehensive treaty outlawing the use of chemical weapons with the passage of the 1993 Chemical Weapons Convention.⁵ On the other hand, some rules of warfare have been rather ahead of their time, such as the treaty banning the use of environmental modification techniques in warfare;⁶ the protocol banning weapons whose fragments cannot be detected by X-ray;⁷ and the protocol banning the use of blinding lasers.⁸

Overall, the body of jus in bello has been able to adapt to the development of new means of warfare remarkably well. For example, armed forces have applied the rules set forth in the Hague Regulations on Land Warfare⁹ to air warfare with relative ease. The basic principles of military necessity, proportionality, humanity, chivalry, and distinction are not situation-specific; they govern all use of force everywhere. Therein lies the problem inherent in the emergence of cyberspace as a medium of warfare: Cyberspace is nowhere.

Computer technology has advanced to the point where military forces now have the capability to inflict injury, death, and destruction via cyberspace. Not all of the injury is physical. Using techniques that disrupt automated systems or destroy or alter data, computers that fall into the wrong hands are capable of doing long-lasting personal and economic damage to military and civilians alike. The highly destructive scenarios that various authors on cyberwar have theorized,¹⁰ as well as the potential use of cyberwar techniques

---

¹⁰. See, e.g., DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 65 (1999) (presenting a scenario in which trained military hackers target and disable commercial information systems such as banking and finance, telecommunications, air traffic control, and power); MICHAEL ERSCHLOE, INFORMATION WARFARE: HOW TO SURVIVE CYBERATTACKS 65–96 (2001) (inventing an “electronic doomsday scenario” in which ten people cause one trillion dollars in economic disruption by launching computer viruses and denial-of-service attacks against Wall Street and major companies and transferring money from bank accounts); John Arquilla, The Great CyberWar of 2002, Wired, Feb. 1998, at 122 (imagining a terrorist group demanding that the United States close all of its military bases overseas and, in the face of U.S. noncompliance, launching cyberattacks against the civilian infrastructure of the United States).
in asymmetrical warfare, underscore the need for an unambiguous standard of conduct for information warfare that will be universally recognized and respected—a cyber-*jus in bello*.

This Article will examine the principles and specific areas that a comprehensive body of international law regulating information warfare must cover. It will explore the tension between the needs of military forces to engage in information warfare and the rights of non-participants to safety and security. In doing so, the Article attempts to fashion a legal standard that is palatable to the major participants in information warfare. To that end, a hypothetical convention, Regulating the Use of Information Systems in Armed Conflict, is presented at the end of this work.

I. SCOPE OF THE CONVENTION

A. Understanding the Need

Why is a separate convention necessary at all? The existence of a substantial body of literature already produced on this topic, as well as the present work, suggest that the law of armed conflict ("LOAC") as applied to information warfare derives from the law as it applies to conventional warfare. By this logic, a separate legal instrument to regulate information warfare would be extraneous. Yet such logic erroneously assumes that warfare by computer

---


12. This work is not intended to recommend any principles concerning when the use of information warfare constitutes aggression or an armed attack within the meaning of article 51 of the U.N. Charter, thus justifying the use of force by states in their defense. Such a standard would be counter-productive; a "Definition of Cyber-Aggression" is very likely to be abused by aggressor states. This *jus ad bellum* of information warfare can be derived with little difficulty, and the more vague the principles, the stronger a deterrent to aggression they will be. For discussion of the ramifications of information warfare on *jus ad bellum*, see generally WALTER GARY SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* (1999); Barkham, supra note 11; Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 Int'l L. Stud. 99 (2002); Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, 76 Int'l L. Stud. 73 (2002); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 58 Stan. J. Int'l L. 207 (2002); Horace B. Robertson, Jr., *Self-Defense against Computer Network Attack under International Law*, 76 Int'l L. Stud. 121 (2002); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999); James P. Terry, *The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?*, 169 Mil. L. Rev. 70 (2001).

13. Major David DiCenso surveys the applicability of several fields of law to information warfare. See David J. DiCenso, *IW Cyberlaw: The Legal Issues of Information Warfare*, 33:2 L./Tech. 1 (2000). He argues persuasively that space law is not helpful in resolving the issues and his coverage of telecommunications law and domestic criminal law suggests the same. See id. at 6–10.

14. In the twenty-first century, the terms "armed conflict," "war," and "use of force" are used virtually interchangeably. Similarly, the terms "law of armed conflict," "law of war," and "international humanitarian law" all refer to the same body of Geneva and Hague law that regulates the conduct of parties to an armed conflict by way of the principles of distinction, military necessity, proportionality, humanity, and chivalry. The precise manner of division and nomenclature of these principles varies from source to source. See LESLIE C. GREEN, *THE CONTEMPORARY LAW OF ARMED CONFLICT* 17–18, 52–53 (2d ed. 2000).
is not significantly different from warfare with kinetic weapons such as bombs and bullets. It therefore assumes that conventional LOAC will resolve all of the new issues raised by the use of malicious code, denial-of-service attacks, and control of vital systems when used against an enemy. In actuality, information warfare carries significant differences.

The advent of information warfare is the latest in a series of developments in warfighting capabilities that Professor Michael Schmitt calls Revolutions in Military Affairs ("RMAs"). The information warfare RMA spawns two paradigm shifts that could fundamentally alter the conduct of war itself. One is a shift in favored weaponry from kinetic weapons toward information weapons. By accessing or interfering with the enemy’s weapons or targeting systems, one can effectively disable the enemy’s means of fighting without the need for kinetic weapons and its attendant damage, injury, and death. Control over the enemy’s infrastructure can enable one to deprive the enemy of basic services, such as electricity, fuel, and transportation, thus weakening the enemy’s ability and will to fight. Moreover, collateral damage and the cost of post-conflict reconstruction are greatly reduced by information warfare. O’Donnell and Kraska even go so far as to suggest that in the future, information weapons will displace kinetic weapons as the preferred means of warfare.

The other paradigm shift occurs in what Schmitt calls the “Militarization of Civilians and Civilian Activities.” He posits a “growing military dependency on civilians, and on civilian objects and activities.” This is an innocuous way of saying that the logistics of modern warfare impose burdens on a state that blur the distinction between the military and civilians. Successful modern warfare requires the mobilization of not only military personnel and equipment, but also industry, transportation, energy, and communications.

"[I]n modern warfare," writes Ruth Wedgwood, “the mobilization of national economies and war production makes industrial plants and infrastructure into a second battlefield." In addition, many functions and services previously fulfilled by military personnel have now been outsourced to private contractors.
Information warfare is affected by this outsourcing trend. Attacks are launched by well-fed persons sitting in air-conditioned office buildings, creating a great temptation for the military to simply rent space in office complexes rather than incur the expense of building new facilities on overcrowded bases. The relative comfort also makes the field more attractive to civilians. As demand for skilled information warriors increases, military forces will be tempted to hire contractors to handle the additional workload. This, in turn, may create a greater incentive for low-paid military personnel to join the ranks of those contractors, further blurring the distinction between civilians and military personnel. The emergence of cyberspace as a theater of operations has far-reaching repercussions for the law of armed conflict.

The square peg of conventional LOAC thus does not fit neatly into the round hole of information warfare. Nonetheless, LOAC can and must serve as a model for devising rules. Indeed, if the rules of information warfare are to elicit compliance, they must adhere to more general legal principles and conform to the pre-existing legal structure for armed conflict. Accordingly, the newly devised rules should draw from conventional LOAC, but not to the point at which rigid conformity would impose unreasonable burdens on the use of information warfare. The discussion of malicious code and perfidy in Part III.D.2 exemplifies this point. The value of a separate legal instrument addressing the law of information warfare lies in memorializing the rules. This is particularly true for areas in which conventional LOAC does not fit neatly—some problems are better settled not by scholars but by the states that will themselves be governed by the solution. In areas where conventional LOAC does provide a ready-made solution, a separate instrument would strengthen the rules by clarifying and codifying them. This, indeed, is the role of most treaty-based international law. Finally, a settled, codified statement of the law of information warfare would go far in alleviating military commanders’ apprehension of the consequences of violating such law. In the United States, for example, commanders tend to be quite wary of innovative but relatively untested means of warfare, particularly when the rules of conduct are so arcane and ill-defined.

B. Defining the Weapon

The term “information warfare” is quite broad. U.S. military doctrine defines it as “actions taken to use information and information systems to access or affect foreign information and information systems and defend one’s own infor-


23. For example, the first three Geneva Conventions of 1949 (on wounded and sick; wounded, sick, and shipwrecked at sea; and prisoners of war) were drawn to replace the Geneva Conventions of 1929, and as such did not introduce any new concepts or approaches to the law of armed conflict. Green, supra note 14, at 43. The Biological Weapons Convention outlawing the use of toxins in warfare also fits within this category, as poisons have long been banned in customary international law. Id. at 142.

While LOAC applies to all “hostilities” carried out by the armed forces of a state, it does not directly govern all aspects of information warfare. Captain Robert Hanseman classified information warfare into three categories: (1) maintaining information superiority while protecting against counter-information warfare; (2) using information as a weapon against the enemy; and (3) using information systems to enhance force effectiveness. LOAC has little direct application to the first and third categories, other than the prohibition against perfidy. However, it directly governs operations of the second category: using information systems as weapons.

A legal regime governing the use of information systems as weapons must first define the weapons in order to have practical application. In the absence of such a definition, defensive or counter-offensive attacks on information weapons would be indiscriminate, a situation that any legal regime on warfare seeks to avoid. The U.S. Air Force, which is the lead agency for information warfare within the U.S. Department of Defense, defines the term “weapon” as a “device[] designed to kill, injure, or disable people, or to damage or destroy property.” In the information age, armed forces need not always deploy bombers and artillery to accomplish these objectives. In other words, the use of computer technology to wage war necessitates a reevaluation of the definition of the term “weapon.”

In defining the information weapon, it is useful to draw an analogy to the firearm. When a gun is fired, the bullet travels through space and hits a target, damaging it. The firearm by itself cannot do damage (unless used as a bludgeon); its role is to propel the bullet to its target. The bullet itself cannot do damage (unless it explodes or is ingested); it becomes deadly only by virtue of being propelled at high velocity by the gun. Finally, neither the gun nor the bullet is effective unless a combatant is present to load the bullet.


27. Hanseman, supra note 25, at 176. Hanseman worded the first category as “control[ling] the realm.” Id.


29. Air Force Instruction 51-402, *Weapons Review*, para. 1 (May 13, 1994), available at http://www.e-publishing.af.mil/publishes/af/51/a51-402/a51-402.pdf (last visited Nov. 27, 2005). The regulation is intended to set forth procedures for the review of the legality under the law of armed conflict of weapons that do physical damage, and for that reason, it goes on to specifically exclude “electronic warfare devices” from the definition. *Id.* With the advent of an international standard of conduct for use of computers and the Internet in armed conflict, the Air Force will no doubt have to reconsider its position.
into the gun and shoot it. In offensive information warfare, the malicious code, the damaging instructions, or the data is the bullet. The code does not write itself, nor does it enter its target by apparition. A computer system is necessary for writing the code or instructions, transmitting them to other systems, and altering the data. The diligence of the computer operator is essential to the processes of creating the code and instructing the computer to transmit it.

Thus, three information weapons are identified: the code, the computer system, and the operator. Each of these weapons becomes subject to the international law regulating armed conflict. The use of these weapons is constrained by the principles of distinction, military necessity, proportionality, humanity, and chivalry, and the weapons themselves become legitimate targets.

The weaponization of computer code and computer systems does not imply the weaponization of all aspects of information infrastructure. The medium through which the malicious code travels—the physical wires—is not a weapon in itself, any more than the space through which the bullet travels between the gun and the target is a weapon. The computer systems used to generate the malicious code may be classified as weapons, but the other computer systems, telephone relay stations, satellites, and other communications hardware that innocently and automatically transmit any signal they receive probably should not be classified as weapons. However, they are not immune from attack: As conduits of attack, communication systems contribute to the military warfighting capability and their destruction or neutralization does confer a definite military advantage. This attribute puts a state’s information infrastructure on the same plane as those for energy, transportation, and food and water distribution. Military and civilian facilities alike are dependent on these basic services, and as Professor Wedgwood notes, dedicated infrastructures for exclusive military use rarely exist. Accordingly, an attack on enemy communication systems used or usable in information attacks cannot be summarily considered unlawful.

C. When Are Computers Used in Armed Conflict?

1. Definitions

A legal standard governing the use of computers in armed conflict must specify what the phrase “used in armed conflict” means, otherwise the standard is too vague to carry much meaning. A distinction must also be made between the use of computer systems in furtherance of the conflict and the use of computer systems by combatant forces generally. The former denotes the

---

30. The approach of the U.S. Marine Corps is to not treat a satellite used as a conduit for an information attack as a weapon. DiCenso, supra note 13, at 4.
31. Wedgwood, supra note 21, at 224.
use of computers for the purpose of attack, or for inflicting damage or degrading the enemy's abilities. The latter covers all other uses, such as communications, logistical support, intelligence, or passive computer network defense. Essentially, the former refers to using computer systems as **weapons**, as opposed to mere **tools**.

At this point it is necessary to declare a standard label to denote the use of computers to carry out offensive operations. The military and legal lexicon appears to contain no standard terminology to describe the offensive conduct that the proposed convention would regulate. The term “information warfare,” as the U.S. military uses it, is too broad because in addition to offensive uses, it covers non-offensive uses such as operational security, deception, electronic counter-measures, psychological operations, and computer network defense.

Dorothy Denning uses the term “offensive information warfare” to describe an operation that “targets or exploits a particular information resource with the objective of increasing its value to the offensive player and decreasing its value to the defensive player.” Charles Dunlap uses the term “electronic attack” and “cyberassault” interchangeably. Michael Erbschloe, whose recent book on the subject uses the term “cyberattack” in its title, introduces the term “offensive ruinous information warfare” as “an organized deliberate military effort to totally destroy the military information capabilities, industrial and manufacturing information infrastructure, and information technology-based civilian and government economic activities of a target nation, region, or population.” He also introduces the term “defensive ruinous information warfare,” a term synonymous with “cyberattack,” except that the former is used against an aggressor whose actions provoked the attack. Eric Jensen, relying upon military doctrine, uses the term “computer network attack,” defined as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” Jensen’s term, while the most precise, is also one of the most unwieldy for frequent use. Denning’s term is not precise enough because it would cover espionage, which is not an “attack” that LOAC is intended to regulate.

33. Joint Chiefs of Staff, Joint Publ’n No. 3-13, Joint Doctrine for Information Operations I-9 to -10 (Oct. 9, 1998).
34. Denning, supra note 10, at 28.
36. Erbschloe, supra note 10, at 125.
37. Id.
38. Jensen, supra note 12, at 208 n.3 (citing Joint Chiefs of Staff, Joint Publ’n No. 3-13, supra note 33, at I-9). The Naval War College has adopted this appellation. See Computer Network Attack and International Law Symposium, 76 INT’L L. STUD. 1 (2002).
with the prefix “cyber” imply the use of cyberspace, which is accessible by computers, but not by less sophisticated devices, such as telephones and fax machines, which could be used to conduct denial-of-service attacks or transmit propaganda. Because the activities regulated in the proposed convention cover information or information systems as the object, means, or medium of attack, this Article proposes the term “information attack.”

2. Casus Belli

Because information warfare lies at the intersection of war, crime, and tort, some means must be devised to distinguish them. This distinction is key in determining whether the law of armed conflict applies at all to any given situation. The threshold of computer activity constituting armed conflict can be defined using two different approaches. One is a results-oriented approach. In his seminal 1963 work *International Law and the Use of Force by States*, Ian Brownlie used this approach in defining whether a certain act is a “use of force” in international law by looking beyond whether death or injury results from the “force” of impact. Brownlie observed that chemical and biological weapons achieve the same result as conventional munitions that kill people. Similarly, it is sometimes possible to inflict physical damage on objects via information attack, such as releasing flood waters by remotely opening a dam, causing a meltdown at a nuclear power plant, or rupturing an oil pipeline. In each case, a computer is used to cause physical damage that could not otherwise be accomplished without conventional munitions. Physical damage may include damage by electromagnetic pulse (“EMP”), which disables electronic systems not by the kinetic force of explosives, but by overloading them with electromagnetic radiation and burning out their components. The electronic system is thus rendered inoperable, which is the same objective and result that a kinetic attack would achieve. Under Brownlie’s approach, if an information attack achieves the same result that could have been achieved with bombs or bullets, then it has been conducted in the course of armed conflict.

contrast, no provision of international law prohibits espionage.

40. A published report by the Center for Strategic and International Studies classifies “information warfare attacks” into four categories: (1) data attack, such as propaganda, disinformation, data overload, spam, and do-loop triggers; (2) software attack, using computer viruses, Trojan horses, or trapdoors; (3) hacking, i.e., the penetration, unauthorized use, and/or snooping in other computer systems; and (4) physical attack, in which an information system is physically attacked by way of electromagnetic pulse (EMP), electronic countermeasures (ECM), or conventional military strike. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, CYBERCRIME, CYBERTERRORISM, CYBERWARFARE: AVERTING AN ELECTRONIC WATERLOO 9–11 (1998) [hereinafter CSIS Report]. While these distinctions are useful in military science, they are less useful in defining standards under the law of armed conflict, which is more results-oriented than means-oriented.


42. An oil pipeline may be ruptured remotely by regulating the pressure in a way that creates a “hammering” effect in the pipe, causing it to burst. Jensen, *supra* note 12, at 222.
A denial-of-service attack is another example of an information attack under the results-oriented approach. A denial-of-service attack directs massive amounts of artificially generated traffic to another computer or communication system in order to overwhelm the target system and impede its ability to properly handle the legitimate traffic. The result of a successful denial-of-service attack is to neutralize the system by forcing it to shut down, thereby rendering it useless to the enemy. But for the ability of information or communications systems to shut down another system in this manner, that other system could only be neutralized by kinetic force. While no physical damage is inflicted on the system by a denial-of-service attack, the result is the same.

The second approach to determining whether computer activity constitutes an armed attack is the effects-oriented approach. The information attack may not necessarily cause physical damage, but it may have some other effect on the civilian population, protected sites, or the ability of the enemy to fight. For example, an information attack might be used to misdirect shipments of medical supplies, disrupt air traffic control, or crash financial markets by altering prices or flooding the system with false orders. Hacking into a system to alter data does not inflict physical damage, nor does it neutralize a system in the way that a denial-of-service attack does, but it may have an adverse effect on civilians if the altered data consists of, for example, personal or financial records of individuals. Although such actions do not accomplish the work of explosives, they do inflict harm on the class of people that LOAC is meant to protect, regardless of whether the harm is intentional or simply a collateral effect of an attack on some other target. International law should therefore govern the use of computers for these purposes as well.

A basic principle of information warfare may be distilled from these two approaches: An act that violates LOAC if carried out by conventional means also violates LOAC if carried out by an information attack. Obversely, an act that is not a war crime if carried out by conventional means cannot be converted to one if accomplished electronically. However, certain criminal activities could conceivably be converted to war crimes if conducted in the furtherance of an armed conflict. For example, an individual act of murder motivated by ethnic hatred is a common crime; an organized campaign of such murders is a war crime. Similarly, the illicit or fraudulent transfer of funds from another’s bank account is not a war crime, even if accomplished using the same techniques used in prosecuting information warfare. However, it might become

---

43. Thus Schmitt ties the appellation “attack” to the “level of suffering” resulting from it. Schmitt, Wired, supra note 17, at 194.

44. Daniel Silver makes an excellent point in showing that inflicting economic damage, such as in crashing a national stock exchange, cannot be squared with the kind of force contemplated in Article 2(4) of the U.N. Charter. Silver, supra note 12, at 87. It is, however, the effect on the civilian population that is the bailiwick of the law of armed conflict and such an act, when committed in the course of inter-state hostilities, is appropriate for discussion under this topic. Schmitt similarly warns against viewing information attacks in such a way that confuses jus ad bellum and jus in bello. Schmitt, Wired, supra note 17, at 190.
a war crime if accomplished by a state or other entity in the course of armed conflict.

This latter scenario forces the long-running debate of when LOAC applies into new territory. Before the information age, a state wishing to steal from another state had to forcefully violate its territorial integrity to do so. Now, it is possible to carry out such an act without force. Such acts should be considered violations of LOAC. The proposed convention is drafted accordingly.

Ultimately, however, for a state to apply LOAC to any given military operation, it must first acknowledge that its adversary is a party to an armed conflict as opposed to a riot or other civil disturbance. States are often reluctant to do so in internal conflicts because such acknowledgement tends to confer a quasi-international legal personality on their adversaries, thus legitimizing rebel movements, for example. Existing legal instruments on conventional armed conflict do not speak to this issue (otherwise they would carry little support from states), and it is therefore appropriate that the proposed convention not speak to it either.

3. Espionage and Sabotage

Certain types of computer activities do not fall within either of the categories outlined above, in that they do not result in physical damage or directly affect the civilian population, protected persons, or protected sites. Hacking into an enemy’s computer systems in order to obtain information or to alter data of a strictly military nature is not an information attack; rather, it is more appropriately classified as espionage or sabotage. The application of the law of armed conflict to espionage and sabotage is limited, speaking only to the treatment of spies and saboteurs captured by the enemy.\(^{45}\) It seems highly unlikely that remote intelligence gathering and data alteration could be charged as espionage under existing international law. The Hague Regulations define “spy” as one who, “acting clandestinely or on false pretences . . . obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.”\(^{46}\) Modern Geneva law provides that “[a] member of the armed forces . . . who, on [its] behalf . . . and in territory controlled by an adverse Party, gathers or attempts to gather information shall not be considered as engaging in espionage if, while so acting, he is in the uniform of his armed forces.”\(^{47}\) A computer specialist on a military base hacking into an enemy computer system to extract classified information does not commit espionage under this definition, since he or she does not operate clandestinely or under false pretense, or inside the enemy state. The law of armed conflict does not outlaw spies or saboteurs; it only regulates their treatment once they are caught and protects uniformed service-

---

\(^{45}\) Additional Protocol I, supra note 32, art. 46.

\(^{46}\) Hague Regulations, supra note 9, art. 29.

\(^{47}\) Additional Protocol I, supra note 32, art. 46, para. 2 (emphasis added).
men from espionage or sabotage charges that might be used as a pretext for executing them. The proposed convention is intended only to cover information attacks in armed conflict and therefore omits discussion of espionage or sabotage.

D. Conclusion

The lesson to be drawn from the above analysis is that information warfare has made it possible for states, as well as nonstate actors, to engage in armed conflict by way of bits and bytes instead of bullets and bombs. Cyberspace is the new frontier of armed conflict and information warfare has become an integral component of modern armed forces. It is both necessary and appropriate that the same principles of international law intended to regulate conventional armed conflict and reduce its adverse effects apply to information warfare. The next several sections will analyze in greater detail the various principles of the law of armed conflict, the law of neutrality, and their application to information warfare.

II. The Principle of Distinction

Customary international law places considerable emphasis on the distinction between combatants and noncombatants in warfare. The principle of distinction takes two forms: (1) a strict, formal distinction between combatants and noncombatants; and (2) the duty to conduct warfare in a manner that minimizes harm to civilians and other noncombatants. Each of these principles shall be applied to information warfare below.

A. Status of Information Warriors

Only lawful combatants have the legal right to participate directly in hostilities. Lawful combatants are immunized from criminal liability for certain acts which otherwise would be unlawful, as long as the act itself does not violate LOAC. Thus a lawful combatant has the right to kill enemy forces in battle or drop a bomb on a legitimate military target, but not to kill an unarmed civilian, engage in looting or rape, or firebomb an undefended civilian population center. Information attacks also achieve results or effects that may be considered criminal acts if carried out by unlawful combatants. Therefore, when the objective of an information attack is to achieve a result or effect that would otherwise require a conventional attack, the information attack should be conducted only by lawful combatants.

49. See id. at 51.
50. Additional Protocol I, supra note 32, art. 43, para. 2.
Lawful combatants include the uniformed regular armed forces of a state (except medical personnel and chaplains) and any irregular forces that satisfy all of the following four conditions: (1) They are commanded by a person responsible for his subordinates; (2) they wear a fixed emblem recognizable at a distance; (3) they carry their arms openly; and (4) they conduct their operations in accordance with the laws and customs of war. The Third Geneva Convention recognizes the right of civilians accompanying armed forces to be treated as prisoners of war if captured, just like the armed forces themselves. These include civilian members of air crews, supply contractors, or service personnel. Nothing in the Geneva Conventions or other sources of international law, however, grants these accompanying civilians the legal right to engage the enemy. Similarly, civilian employees and contract personnel accompanying the armed forces may use computer technology for force enhancement, such as in logistics and communication, and to defend against information attacks, but should be prohibited from engaging in information attacks themselves. That function should lie exclusively with the armed forces, who are lawful combatants.

International law recognizes the right of a civilian population of a non-occupied country to spontaneously take up arms to resist the invading forces (levée en masse). Participants of a levée en masse are entitled to prisoner of war status if captured and are similarly immunized from criminal liability for acts committed in armed conflict with the invading force. Theoretically, an attack on a state, and not even necessarily an information attack, could lead to angry civilian computer users launching a counter-attack on the attacking state’s systems, without any prompting or sanction by the governmental authorities. However, the right of civilians to engage in a cyber-levée en masse should be explicitly extinguished for three reasons. First, combatants are required to distinguish themselves from the civilian population while engaging in an attack or preparing to attack. To confer on civilians the right to engage in information attacks would further erode the already tenuous barrier between combatants and noncombatants in a levée en masse setting. Second, if the civilian population, acting in what it perceives as the defense of its country, commits an information attack that warrants a forceful response, the civilian popula-

52. Hague Regulations, supra note 9, art. 1; GPW, supra note 51, art. 4(A)(2).
53. GPW, supra note 51, art. 4(A)(4).
55. Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 13, para. 6 [hereinafter GWS]; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, art. 13, para. 6; GPW, supra note 51, art. 4(A)(6).
57. Additional Protocol I, supra note 52, art. 44, para. 5.
tion and its infrastructure become legitimate objectives of a direct, conventional attack. Thus, the civilian population loses the protection that LOAC is supposed to give them. Third, the only reasonably conceivable targets of a cyber—levée en masse are the military and civilian information infrastructures of and within the attacking state. Such operations go beyond the purpose and purview of the levée en masse, which is intended to provide for spontaneous civilian defense of their homeland. There is no legal precedent for a levée en masse bringing the fight to the attacker’s homeland. For these reasons, the distinction between combatants and noncombatants in information warfare must be scrupulously maintained.

International law also states that armed forces must carefully observe and maintain the distinction between combatant and noncombatant facilities. As pointed out in Part I.B of this Article, the computer systems and operators engaged in information attacks may be classified as weapons, and thus may become legitimate objects of conventional attack. States have a duty not to use the civilian population to shield legitimate military targets from attack. The application of this duty requires that personnel and equipment directly engaged in information warfare be located in facilities whose attack by kinetic weapons would not result in excessive collateral damage. Any information warfare facility located on a military base or other separate, distinct place is probably sufficiently removed from the civilian population for the principle of distinction to be maintained. A hypothetical information warfare facility located on Wall Street, however, is almost certainly not, and if an attack on such a facility destroyed the entire fifty-floor building and killed thousands of civilians working in it, the responsibility for that excessive destruction would rest with the state that put the facility there. The same policy weighing against allowing a civilian population to engage in information attacks also warrants a norm providing that combatants engaged in those activities separate themselves from noncombatants in order to minimize the effects of warfare on the civilian population.

58. See generally Henckaerts & Doswald-Beck, supra note 48, at 35.

59. The problem of defending against attacks by nonstate actors is addressed at the end of Part III.C of this Article.

60. The exception to this proposition is when the civilian effort is directed toward enemy information systems within their own state. This can only happen if enemy forces are actually in that state, such as when the enemy is an occupying force. A civilian cyber-uprising, however, would be hard-pressed to identify which information systems are in-country and which are not.

61. See Hoffman, supra note 56, at 423.

62. Of course, such precedent does exist when military forces defend the homeland against invasion. John Warden advocates forcing complete submission of the enemy by attacking its leadership targets in order to facilitate a subsequent attack on the military forces themselves. Examples of such targets are command centers and communications headquarters. Schmitt, Bellum Americanum, supra note 8, at 1063–64 (citing Colonel John A. Warden III, The Enemy as a System, AIRPOWER J., Spring 1995, at 41). This tactic was used with extraordinary success against Iraq during the Gulf War of 1990–1991. See U.S. DEP’T OF DEFENSE, CONDUCT OF THE PERSIAN GULF WAR 73–75, 95–101 (1992).

63. Additional Protocol I, supra note 32, art. 51, para. 7.
B. Principle of Distinction Applied to Information Attack

This Article will now turn to the effects of information attacks on the civilian population itself. The basic rule in protecting civilians against the effects of war is that the warring parties "shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." 64 Three types of information attacks will be analyzed under this principle: (1) inflicting physical damage; (2) inflicting economic damage; and (3) propagating malicious code.

1. Physical Damage

In the law of armed conflict, civilians and the civilian population may not be the objects of attack, and attacks or threats of attack whose main purpose is to terrorize the civilian population are forbidden. 65 LOAC also prohibits indiscriminate attacks, which are attacks "of a nature to strike military objectives and civilians or civilian objects without distinction." 66 Indiscriminate attacks include those that are not directed at a specific military objective and those carried out with weapons that cannot be directed at a specific military objective, such as the Iraqi Scud missile attacks during the Gulf War. Direct attacks on civilians are prohibited.

Although the rules of international law prohibiting direct attacks on non-combatants do not specify any particular weapon, it is commonly understood among the armed forces that the rules are meant to govern the infliction of physical damage on targets. If both kinetic and information weapons are capable of causing physical damage, then LOAC should make no distinction between them. To do so might defeat one of the benefits of information warfare, which is the lessening of collateral damage and reconstruction cost. There is no reason to exempt physical destruction carried out by information attack from the rules of LOAC.

As the experiences of the United States in the Gulf War and Operation Allied Force in Yugoslavia 68 have demonstrated, the modern concept of warfare does not exclude targets whose destruction or neutralization do not directly advance the overall objective of the war, but do nonetheless degrade the enemy's ability and will to fight. 69 The destruction of bridges, railroads, communications centers, and fuel supplies thus offers a definite military advantage, and

64. Id. art. 48.
65. Id. art. 51, para. 2.
66. Id. art. 51, para. 4.
67. Id.
68. “Operation Allied Force” was the operational code-name for the NATO bombing of Yugoslavia to stop ethnic cleansing of Kosovo Albanians. See Sean D. Murphy, Contemporary Practice of the United States Relating to International Law, 94 AM. J. INT’L L. 677, 691 (2000).
such facilities are lawful targets if they are part of the infrastructure used by
the military or are necessary for military mobilization. But frequently, such
facilities (especially communications centers) are also part of the civilian infra-
structure. For example, ninety-five percent of communications traffic of the
U.S. Defense Information Systems Agency, the lead defense agency operating
communications and computer systems serving the entire Department of
Defense ("DOD"), travels on civilian lines available to the public.\textsuperscript{70} The law-
fulness of any attack on such dual-use facilities will turn on whether the
military advantage gained by attacking the target outweighs the adverse
effect on civilians and the civilian population.\textsuperscript{71} This principle should apply
to attacking infrastructural targets by information attack as well.

Two additional principles govern the destruction or neutralization of a lawful
target. One is that warfare should not cause long-term environmental dam-
age. The law of armed conflict prohibits "methods or means of warfare which
are intended or may be expected to cause [widespread, long-term and severe]
damage to the natural environment and thereby prejudice the health or sur-
vival of the population."\textsuperscript{72} The other principle is that installations containing
dangerous forces, such as dams, dikes, and nuclear facilities, whose attack
may cause severe losses among the civilian population, warrant additional pro-
tection. Such facilities should only be attacked if they are used in "regular,
significant and direct support of military operations and if such attack is the
only feasible way to terminate such support."\textsuperscript{73} No aspect of information war-
fare warrants exemption from these two principles.

2. Economic Damage

Physical damage to the civilian infrastructure can exact a heavy toll on the
economy of the target state. When the damaged facilities are lawful military
targets, or targets whose neutralization confers a military advantage that out-
weighs the adverse effect on the civilian population, the economic damage is
collateral. Information warfare is also capable of attacking civilian facilities,
not for the purpose of doing physical damage, but to disable them in some
fashion. Examples include shutting down the computer system that manages
the national stock market, disabling the computer systems of major banks,
or shutting down telephone lines in areas in which military forces have no
interest. Such targets have no military use and their neutralization confers no
definite military advantage. Attacks on such facilities using conventional
methods would likely be condemned as violating LOAC, and since informa-

\textsuperscript{70} CSIS Report, \textit{supra} note 40, at xiii.
\textsuperscript{71} \textit{See generally Henckaerts \& Doswald-Beck, supra note 48, at 58.}
\textsuperscript{72} Additional Protocol I, \textit{supra} note 32, art. 55. In addition, the ENMOD Convention addresses
techniques of modifying the environment as a means of warfare. It prohibits "military or any other hos-
tile use of environmental modification techniques having widespread, long-lasting or severe effects as the
means of destruction, damage or injury to any other State Party." ENMOD Convention, \textit{supra} note 6, art.
1, para. 1.
\textsuperscript{73} Additional Protocol I, \textit{supra} note 32, art. 56, para. 2.
tion attacks on these same targets seem to serve no legitimate military purpose, such attacks should likewise be prohibited.

3. Malicious Code

As noted above, the law of armed conflict requires belligerents to distinguish between military and civilian targets and further prohibits them from making civilians, civilian objects, or the civilian population the object of a direct attack.\(^{74}\) LOAC also proscribes methods of warfare that cannot be directed at a specific military objective, or methods of warfare the effect of which cannot be limited to military objectives.\(^{75}\) In information warfare, the type of weapon that poses the greatest danger of eroding this principle is self-propagating malicious code.

An analogy of the effects of computer viruses may be drawn from those of biological and chemical weapons. Biological and chemical weapons can be highly effective in neutralizing the combatant forces against whom they are directed. However, they kill over a wide area and while their targets may be specific, their effects are widespread. In that respect chemical and biological weapons are indiscriminate, for they have the potential to kill far more non-combatants than the combatants against whom they are directed, as was the case with Iraq’s use of chemical weapons against Iranian forces and Kurdish separatists during the Iran-Iraq War.\(^{76}\) Biological and chemical weapons also inflict unnecessary suffering on (successfully) targeted combatants. Bullets and shrapnel injure at least as often as they kill, thus having the same effect—neutralizing enemy forces—without resulting in as many deaths. Biological and chemical weapons, on the other hand, kill far more often than they injure, and the long-term effects of injuries caused by chemical weapons, such as blister agents, are far more painful than any long-term injuries caused by conventional weapons. Use of such weapons violates the rule of proportionality, in that it causes collateral damage “which would be excessive in relation

\(^{74}\) See Henckaerts & Doswald-Beck, supra note 48, at 26.

\(^{75}\) See, e.g., Additional Protocol I, supra note 32, art. 54, para. 4.

Chemical and biological weapons also pose as great a risk to the attacker as to the victim. The same may be said of computer viruses. Computer viruses affect all unprotected computer systems they reach, without distinction between combatant and noncombatant systems. An attack on enemy military computer systems using malicious code cannot be considered unlawful per se. However, malicious code such as viruses, worms, Trojan horses, logic bombs, and trap doors, tends to spread to systems used by civilians as well as to protected sites such as medical facilities. Malicious code that makes no distinction between lawful and unlawful targets should be prohibited. At first glance, such a task might appear Herculean at best, and unenforceable at worst. However, military forces already have the obligation to distinguish themselves from civilians, and it is common practice for many states to further distinguish protected persons and sites within their military forces. One potential method of making military computer systems similarly identifiable may be to create universally recognized electronic identifiers to correspond with the status of persons and sites under the Geneva Conventions (combatants, medical, chaplain, etc.), much as the red cross and red crescent serve as universal visual identifiers for medical personnel and sites. As a further protective measure, states could require manufacturers of information systems within their jurisdictions to install a similar identifier for civilian systems. The use of electronic identifiers is susceptible to abuse, of course, but the same is true of the visual identifiers used now. In addition, it is conceivable that the malicious code itself can be made smarter, that is, able to identify the likely uses of information systems according to the type of software and hardware they contain or by the type of networks to which they are connected. For example, networks associated with the U.S. military use the Internet extension “.mil,” and hard drives containing medical records or medical laboratory software are likely to be used by protected facilities.

Logic bombs pose a problem of distinction akin to that of landmines. Landmines have the legitimate purpose of deterring enemy forces from approaching via certain routes. However, abandoned, non-self-neutralizing mines inflict far greater harm to the civilian population in the decades following the termi-

77. Additional Protocol I, supra note 32, art. 51, para. 5(b).
78. Barkham defines the foregoing technical terms as follows: A *virus* is “a code fragment that attaches itself to a program and only operates when its host program begins to run”; a *worm* is “an independent program that copies itself onto other computers but usually does not change other programs”; *Trojan horses* are “code fragments that disguise worms or viruses and allow attackers to gain access to systems”; a *logic bomb* is a variety of Trojan horse that “activates only when a certain condition is met. It can lie dormant in a system for long periods of time before activating”; a *trap door* is a “mechanism[ ] that allow[s] a programmer to access software at any time without the owner's knowledge.” Barkham, supra note 11, at 62–63.
nation of hostilities. The harm is both physical, due to accidental injuries and deaths to unwitting victims, and economic, in that their presence renders unusable land that could otherwise be used for agriculture or industry. Geneva law regulates the use of mines and booby traps by prohibiting their use near concentrations of civilians when no ground combat between military forces is taking place, and by requiring either that their positions be recorded (presumably for later removal) or that they be equipped with self-destruction or self-neutralizing mechanisms that activate when they are no longer reasonably anticipated to serve any useful military purpose. Logic bombs lie dormant in a system until certain conditions are met for their activation—for example, when a certain targeting system is run or the software records some other event. When activated, the logic bombs disable part or all of the system. The danger of logic bombs to the civilian population is twofold. First, unless they have been designed to distinguish between civilian and military systems, logic bombs affect civilian information systems as well. Second, older, excess computer systems may eventually find their way into civilian use and any dormant logic bombs could be triggered inadvertently. For these reasons, logic bombs should also be designed to distinguish between lawful and unlawful targets. Since the danger of such bombs is very similar to that posed by landmines, precautionary measures taken against logic bombs should also be similar to those taken against mines. The proposed convention therefore requires that logic bombs distinguish between military and civilian systems, and that they be programmed to self-neutralize once they are reasonably anticipated to no longer serve a legitimate military purpose.

C. Conclusion

The principle of distinction has the objective of separating the participants of warfare from the non-participants in order to minimize harm to noncombatants. Because information warfare has emerged as a method of armed conflict, the principle of distinction applies to it as well. Information attacks calculated to cause physical damage must, like any other offensive operation, balance the importance of the military objective against deaths and injuries to civilians and damage to civilian property. This balancing is especially crucial to decisions to attack dual-use facilities, where harm to the civilian population is certain to result. Information attacks on objects that do not support military operations or whose destruction or neutralization confers no definite military advantage should be prohibited. Malicious code must discriminate between

80. United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II), art. 4, para. 2, Oct. 10, 1980, 1342 U.N.T.S. 168. This prohibition has two exceptions: (a) The mines are placed at or near an enemy facility, e.g., to impede access to it; or (b) measures are taken to warn the civilian population of the mines’ existence.
81. Id. art. 5, para. 1.
lawful and unlawful targets; any malicious code that cannot do so should also be prohibited.

III. METHODS AND MEANS OF WARFARE

Whereas the previous Part focused on the application of “Geneva” law—the protection of non-participants in an armed conflict, the following Part will be devoted to the application of “Hague” law—the legal constraints on the methods and means of warfare. The right of belligerents to select methods and means of warfare is not unlimited. That right is governed by the four basic principles of Hague law: (1) military necessity; (2) humanity; (3) proportionality; and (4) chivalry.

A. Military Necessity

The principle of military necessity is closely related to that of distinction—so closely, in fact, that future treaties on the law of armed conflict may do well to combine the two. Under the principle of military necessity, an attack on a particular target is lawful only if its destruction, damage, or neutralization furthers a legitimate military objective or confers a definite military advantage. When this principle is applied to information attacks, attacks on most of the enemy’s military computer systems are permitted.

The same cannot be said of information attacks against purely civilian computer systems, such as a systematic campaign to damage the enemy’s economy. It seems unlikely that military necessity could justify attacks on stock markets or other financial systems. It is also conceivable that a state could mount an information attack by making numerous fraudulent transactions to drain capital from the target state and undermine consumer confidence in the financial system. While such activities may have an adverse effect on the morale of the enemy, thereby degrading its will to fight, the connection between such economic damage and a definite military advantage is too remote to justify such attacks on the grounds of military necessity. Information attacks on a state’s financial system, or any information attack involving financial transactions carried out under false pretense, should therefore be prohibited.

Information attacks calculated to cause widespread environmental damage offend the principle of military necessity as well. Information attacks on the enemy’s oil or other fuel supplies undoubtedly confer a military advantage, but the attacks must be carried out so as to avoid widespread environmental damage such as the massive oil spills and oil well fires set by Iraq in Kuwait at the end of the Gulf War. Similarly, using information attacks to release flood waters from dams should be permitted only if the civilian water supply

82. Hague Regulations, supra note 9, art. 22; Additional Protocol I, supra note 32, art. 35, para. 1.
83. Additional Protocol I, supra note 32, art. 52, para. 2.
84. See Additional Protocol I, supra note 32, art. 35, para. 3.
would not be adversely affected and the flood would not be reasonably expected to cause damage to civilian population centers.

Additionally, the law of armed conflict confers a protected status on certain kinds of sites. These sites include medical units 85 which should be identified by using distinctive emblems, 86 religious establishments, 87 and specially marked cultural property. 88 Conventional attacks on these protected sites are prohibited. Information attacks on the computer systems of protected sites should be treated similarly.

Occasionally, the protected status of a site may conflict with the right to engage legitimate targets. In conventional terms, if a state uses a protected (or civilian) site to shield a legitimate target, such as putting a command post under a hospital or parking fighter aircraft next to a cultural shrine, the protected site loses its protection to the extent that attacking it is necessary to destroy the military target. 89 Similarly, if a state deliberately makes it impossible to attack its military computer systems, for example with malicious code, without also attacking the computer systems associated with protected sites, the protected systems lose their protection. Just as it is possible to use protected sites as shields against bombs, it is also possible to use protected servers as shields against malicious code. States should be required to separate computer systems with a protected status from those without one. States also should be specifically prohibited from embedding medical systems in other military systems that are lawful objects of attack.

B. Humanity

The second fundamental principle governing the methods and means of warfare is humanity. Modern international law articulates the principle as follows: “It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.”90 It is this principle that drives the bans on, for example, exploding and expanding bullets, 91 poison, 92 fragments undetectable by X-ray, 93 and laser

85. Id. art. 12, para. 1.
86. Id. art. 18, para. 4.
87. Hague Regulations, supra note 9, art. 27.
89. The legality of striking a target in such circumstances is still contingent on the military necessity of attacking the target outweighing the resulting death, injury, and damage to civilians and civilian property.
90. Additional Protocol I, supra note 32, art. 35, para. 2; see also Hague Regulations, supra note 9, art. 23(e).
92. Hague Regulations, supra note 9, art. 23(a).
weapons whose combat function is to cause permanent blindness.\textsuperscript{94} Whereas the principle of distinction protects noncombatants from needless suffering, the principle of humanity protects combatants from the same.

Computers and the Internet can be used in ways that target military personnel but cause excessive injury in the process, particularly in a form of psychological warfare known as "personal information warfare."\textsuperscript{95} An information attack could be used to interfere with the military payroll system or otherwise disrupt the personal finances of individual military members. If members' personal information such as the social security numbers of U.S. personnel, were widely broadcast, military members would become much easier targets for identity theft by criminal elements, or worse, the attacking state itself. Information attacks of this nature offend the principle of humanity, in that they cause superfluous injury and unnecessary suffering to their targets. As combatants, military members assume the risk of injury or death from attacks carried out by guns or bombs. However, military members also reasonably expect to be able to make a living, enter into personal relationships, and raise and support families. Disrupting the personal finances or invading the personal privacy of military members assaults them not in their combatant capacities, but in their personal capacities. Just as international law protects noncombatants and persons who are hors de combat from "outrages upon personal dignity,"\textsuperscript{96} international law should protect combatants from the same.

A related form of information attack is harassing military members by contacting them at their residences by phone or by e-mail. It is difficult to justify an outright prohibition on such activity, as military members are a legitimate target for psychological operations,\textsuperscript{97} and intruding into their homes in this manner does further the legitimate military objective of degrading their morale. However, international law forbids "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."\textsuperscript{98} While harassing the military member at home may be permissible, terrorizing his or her family should not be. States that engage in psychological operations of this nature must take care to focus such operations on only legitimate targets.

\section*{C. Proportionality}

The principle of proportionality acts as the arbiter between the two conflicting principles of military necessity and humanity. The principle of military necessity is \textit{permissive}: Military forces are free to strike any target using any force
that is necessary to achieve a legitimate military objective. The principle of humanity is restrictive: Military forces are prohibited from inflicting foreseeable harm, even to combatants, that is not necessary to achieve their legitimate military objective. Proportionality is the tool by which military necessity and humanity are balanced: If the necessity of decisively and expeditiously disabling the target outweighs the foreseeable harm, that is death, injury, and property damage, that will be inflicted, then the operation is permitted. If not, it is prohibited.\footnote{Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict 120–23 (2004) [hereinafter Dinstein, Hostilities].}

The applicability of the principle of proportionality to information warfare is most evident in the context of responding to malicious code and denial-of-service attacks. With today’s technology, it can be difficult to trace the source of such an attack if, as most are, the attack is carried out clandestinely. As Ruth Wedgwood notes:

If . . . [a country] were the victim of an attack on vital computer systems, the temptation to respond in kind would be considerable. Yet the ultimate source of a computer attack can be acutely difficult to determine—a problem magnified by the deliberate use of “looping” or “weaving”—using another’s server to disguise the origination of the attack. An attack is likely to be sent through an unrelated server in order to mask its authorship, and a response in kind may end up damaging or disabling the “looped” server.\footnote{Wedgwood, supra note 21, at 227.}

This restatement of the problem assumes that the “looped” servers belong to innocent parties whose systems have been taken over by malicious code without their knowledge and/or consent, as is usually the case with malicious code propagation. It also assumes that passive defensive measures, such as antivirus software and firewalls, are insufficient to protect the intended targets from the code, requiring an information counter-attack to restore those systems. That being the case, Professor Wedgwood looks to the law of state responsibility to resolve this conflict—in the absence of evidence linking the attack to another state, a counter-attack “may be disputed.”\footnote{Id.}

A better approach, however, would be to apply the principle of proportionality as explained above. Under such an approach, military forces would first have to determine whether passive defensive measures are adequate to defend against the attack or a counter-attack against the attacking servers is necessary. If the latter, leaders must then consider the importance of the attacked systems as well as the harm that would result if the attack were successful in disabling those systems.\footnote{For example, will vital information such as bank records, criminal records, medical records, etc., be lost, corrupted, or compromised? Will a successful attack enable the enemy to remotely control works or facilities containing dangerous forces? Would the attack disable targeting or logistics systems essential}
able to take into account the likelihood that an offensive counter-attack may serve to deter attacks in the future. These three considerations together would determine the necessity of launching an information counter-attack. That necessity would then have to be weighed against the consequence of the counter-attacked system’s being disabled. If the necessity of the counter-attack were to outweigh the harm resulting from it, then the possibility—even likelihood—that innocent parties’ systems may be affected would figure little in the equation. LOAC does not protect noncombatants from being inconvenienced; it protects them only from life-threatening conditions caused by the armed conflict. If innocent parties are harmed in the counter-attack, the responsibility for that harm would lie with the original attacking party who co-opted the innocent systems in the first place.

Finally, in response to Professor Wedgwood’s prerequisite of state involvement, it should be noted that not all threats to states’ security come from other states. For example, some scholars assert that the Chinese government encourages its citizens to engage in private cyberwars,103 and Professor Wedgwood herself alleges that private hackers in Europe offered their services to Iraq during the Gulf War.104 It is but a small step from private cyberwar with explicit state support to private cyberwar without it.105

D. Chivalry

1. Prohibition of Perfidy

International law prohibits perfidy, defined as an act “inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.”106 The classic example of perfidy is feigning surrender in order to draw the enemy closer, and then firing on the enemy at close range, thereby gaining a tactical advantage.107 Other examples include feigning wounded status, misusing protective emblems such as the red cross or red crescent, and feigning noncombatant or neutral status. These kinds of activities lead the enemy to believe that certain forces have a protected status, and thus should not be attacked, when in fact they have no protected status and are not immune to attack.

---


104. Wedgwood, supra note 21, at 230. Professor Wedgwood does not cite any support for this proposition, but it must be remembered that much information, as well as regulation, in the area of information warfare is classified.

105. See Hoffman, supra note 56, at 421. Hoffman takes note of instances of information attacks by supporters of both sides of the Israeli-Palestinian conflict who have attacked each others’ cyberspace, as well as supporters of the Sri Lankan insurgent movement. Id. at 416.

106. Additional Protocol I, supra note 32, art. 37.

Developments in information technology have greatly expanded the methods and effectiveness of committing perfidy in the areas of imaging, spoofing and psychological operations. Images of military facilities or encampments, for example, could be intercepted and morphed to disguise them. Morphing an image to make it appear that nothing is there would be a legitimate ruse and would not amount to perfidy. However, morphing the image to make a military facility appear to be a protected site, when in fact it is not, would amount to perfidy. Sending false communications to mislead the enemy into believing that the sender’s forces are in a different location, of a different strength or are in possession of a different intent are permissible ruses of war.\textsuperscript{108} However, false communications intended to make the enemy wrongly believe that a certain target has a protected status when it does not, or falsely declaring the intent to surrender, could constitute perfidy.

2. **Perfidy and Malicious Code**

The anonymous nature of much e-mail traffic presents a special problem. Malicious code is most often propagated by sending e-mail attachments to unsuspecting victims. In order not to arouse the suspicion of the unwitting recipient, the e-mail must appear innocuous; otherwise, any military member who has been properly indoctrinated in communications security is likely to delete such an e-mail without first opening it. An attacking state obviously has little chance of success if its viruses are attached to e-mails from “[attacking state] Information Warfare Center.” To be successful, a malicious code attack by e-mail must misrepresent the origin of the e-mail. In a sense, this practice violates the requirement that combatants be easily identifiable. Even worse, it may violate the prohibition against feigning civilian or noncombatant status, or feigning a protected status.\textsuperscript{109} Mark Shulman concludes that disguising an e-mail containing malicious code as originating from the International Committee of the Red Cross or from Microsoft Software Support is perfidious.\textsuperscript{110} Thus, a literal interpretation of LOAC could create legal impediments that would almost totally negate the effectiveness of an information attack by malicious code. Such an \textit{a priori} restrictive construction however, is both unreasonable and unrealistic, and it oversteps the purpose of LOAC. As long as reasonable care is taken to discriminate between combatant and noncombatant targets, information attacks using malicious code would be valid methods of warfare and thus deserving of regulation, but they should not be regulated out of existence.

The rules of identifiability and open arms in clandestine operations present themselves as a potential solution to this problem. The United States

\textsuperscript{108} \textit{Army Field Manual}, supra note 107, para. 51.


\textsuperscript{110} \textit{Id.}
interprets customary international law as applicable to clandestine operations in the following manner:

Commando forces and airborne troops, although operating by highly trained methods of surprise and violent combat, are entitled, as long as they are members of the organized armed forces of the enemy and wear uniform [sic], to be treated as prisoners of war upon capture, even if they operate singly.\textsuperscript{111}

The 1977 First Geneva Protocol fudges the rules as follows:

Recognizing, however, that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly:

(a) during each military engagement, and

(b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.

Acts which comply with the requirements of this paragraph shall not be considered as perfidious . . . .\textsuperscript{112}

Thus, special forces, whose success depends on the element of surprise, may be indistinguishable as such until they are irrevocably committed to hostilities. As applied to information warfare, however, this approach raises additional questions in defining the point at which the malicious code is being “deployed.” Indeed, for a malicious code attack to be successful, it must be “deployed” to its target computer system by stealth.

In order to achieve a balance between the legitimate utility of malicious code in military operations and the prohibition against perfidy, the proposed convention offers a compromise by carving out a narrow exception to the requirements of identifiability and open arms for the deployment of malicious code. Under the convention, the transmission of malicious code disguised as harmless message traffic, and not readily identifiable as from the hostile state, would be permitted under certain conditions. First, the transmission may not be disguised as originating from an official in the government or armed forces of the target state, or of any third state.\textsuperscript{113} Second, the transmission may be disguised as originating from somewhere in the target state (or from the originating state), but not from any third state.\textsuperscript{114} Identifying the transmis-

\textsuperscript{111} Army Field Manual, supra note 107, para. 63.
\textsuperscript{112} Additional Protocol I, supra note 32, art. 44, para. 3.
\textsuperscript{113} Such use is akin to the “improper use . . . of the national flag or of the military insignia and uniform of the enemy” and is prohibited. Hague Regulations, supra note 9, art. 23(f).
\textsuperscript{114} To do so could violate the neutrality rights of the third state.
sion as coming from some non-government or non-military source in the attacking state would also not be prohibited. Though the question of whether disguising malicious code as originating from a civilian source constitutes perfidy has generated some disagreement among scholars, this author believes that the answer is in the negative. Finally, the transmission may not be disguised as a message from any medical or religious establishment in any location. Adhering to these restrictions should enable states to engage in information warfare using discriminating malicious code without eroding the principle of chivalry in any significant way.

3. Morphing

The principle of chivalry also does not directly speak to morphing images for propagandistic purposes. This Article has already assessed the legality of morphing second-hand images of individual military members in order to inflict injury on those individuals in their personal capacities. This section addresses the use of computers to alter reality. During the Gulf War, Iraqi officials broadcast pictures to the news media of a mosque with its dome missing, accusing the United States of having attacked the mosque and blown off the dome. However, analysts concluded that the Iraqi forces had themselves removed the dome in order to make it appear, falsely, that U.S. forces had committed an atrocity. In a short fictional piece written several years after the war, Charles Dunlap wrote of tactics that might be used by a “Holy Leader” in an asymmetrical fight against the United States in 2007. Dunlap conceived of a scenario in which an enemy state detonates a nuclear bomb in one of its own cities just as U.S. planes are dropping conventional ordnance on a lawful target, in order to make it appear that the United States has committed a nuclear attack.

115. Mark Shulman, for one, asserted that disguising malicious code as an e-mail from “Microsoft Software Support” is no less perfidious than disguising it as an e-mail from the ICRC. Shulman, supra note 109, at 959. The following year, Thomas Wingfield claimed the opposite, arguing that Microsoft is not a protected entity in the sense that medical sites are. Thomas C. Wingfield, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 169 (2000). An e-mail invites the recipient’s confidence that the message originates from a noncombatant source. Despite intent to betray that confidence, the e-mail does not lead the recipient to accord any special protection to the affected originator, that is, by refraining from attacking an entity that it would otherwise attack. For this reason, it is not perfidious. In addition, it should be noted that civilian sources, especially large corporations such as Microsoft, are spoofed very frequently. The harm to Microsoft in such a scenario would be more akin to inconvenience than to a threat to its survival. Finally, a reasonably knowledgeable and prudent Internet user, especially in the military, would treat any unsolicited e-mail with care, regardless of the claim of origin, and especially if the e-mail invites the user to open an attachment.

116. See Jefferson D. Reynolds, COLLATERAL DAMAGE ON THE 21ST CENTURY BATTLEFIELD: ENEMY EXPLOITATION OF THE LAW OF ARMED CONFLICT, AND THE STRUGGLE FOR A MORAL HIGH GROUND, 56 A.F. L. REV. 1 (2005) (“For example, chivalry distinguishes acts of deception from those that undermine the goodwill of the enemy. Acts of perfidy are prohibited pursuant to Protocol I, Article 37. In contrast, camouflage, decoys, mock operations, and misinformation used to deceive an adversary are not prohibited.”).

The advent of morphing technology makes it easier for states to fabricate evidence. Video images of a state’s forces committing atrocities on their own people could be altered to change their uniforms to those of the enemy state. Computer technology could be used to splice voice recordings of an enemy head of state to create a false recording of that head of state issuing an order to commit a war crime.118 Such tactics may advance the short-term political interests of the deceiving state, but in the long-term they risk prolonging and widening the war, increase casualties, and hamper the restoration of peace. These results strike at the heart of the rationale behind the principle of chivalry: “Treachery or perjured conduct in war is forbidden because it destroys the basis for a restoration of peace short of the complete annihilation of one belligerent by the other.”119

These scenarios illustrate the need to supplement the definition of perfidy so as to reinforce the necessity of “[a]bsolute good faith with the enemy.”120 Perfidy should include the creation or alteration of images or recordings for the purpose of advancing a claim that another state committed an attack against protected persons or sites, or that it is about to do so, when the state advancing such a claim knows or reasonably should know that its claim is false. The commission of such an act should be considered a war crime. Two uses of computer morphing would be exempt from this prohibition. First, a state is not prohibited from making it appear that it is about to attack another state at a particular time and place, or using a particular means, when in fact it intends to attack using different means or at a different time and place. Such an act is properly characterized as a ruse, and is well-recognized as lawful.121 Second, this supplemental provision for perfidy would not affect a state’s use of computer morphing to make it appear that that state is preparing to attack another state, when in fact it does not intend to do so, or that another state is preparing to attack the deceiving state when that other state in fact does not so intend. These two activities are not calculated to falsely accuse another state of atrocities or to widen an ongoing war. They may, however, be calculated to start a war and could very well constitute aggression if the propaganda is successful in doing so.122 Such aggression is not perfidy, however, and its lawfulness is defined in the body of international law constituting *jus ad bellum*, therefore putting the question beyond the scope of the proposed convention. The proposed convention does, however, prohibit a state from making it falsely appear that another state has committed (or is about to commit) an attack

---

118. Shulman theorizes the ability of a state to broadcast morphed images of a religious leader committing a sacrilegious act on another state’s television systems. Shulman, *supra* note 109, at 942.
119. *Army Field Manual*, *supra* note 107, para. 50.
120. *Id. para. 49.*
121. *Additional Protocol I, supra* note 32, art. 37, para. 2; *Hague Regulations*, *supra* note 9, art. 24.
122. The imagined scenario is of a state using its own false claim that another state is preparing to attack it as an excuse to mobilize its own forces in a manner that threatens the other state. A large mobilization of military forces in such a manner may justify the other state in striking first, as an act of anticipatory self-defense. The other state may have struck the first blow, but it is the propagandizing state that started the war.
on a third state. Such conduct does not fit neatly into the definition of perfidy, nor does it amount to a direct act of aggression. The conduct is treacherous, however, and should be outlawed as a matter of policy. To the extent that the proposed treaty regime would regulate the use of morphing to alter reality, it would serve as a convenient vehicle for prohibiting such conduct.

E. Conclusion

Information warfare now makes it possible to degrade the enemy’s capability and will to fight in ways that were almost unimaginable when the means of warfare was limited to explosives and projectiles. As this Part has shown, computers and the Internet can be used to inflict harm of a nature that offends the fundamental principles of military necessity, humanity and chivalry. Certain kinds of information attacks do more harm than is justifiable, when, for example, the military benefit conferred as a result of the attack does not outweigh the resultant injuries inflicted on combatants and non-combatants alike. International law cannot permit states to resort to dishonorable means of warfare and must therefore regulate information warfare in accordance with the foregoing principles and hold accountable those who violate them. International law also strives to protect the states that are not parties to the conflict, the subject of the next Part.

IV. Neutrality

States that are not parties to an armed conflict have certain rights under international law, as well as responsibilities if they wish to retain their neutral status. The specific rights of neutral states include the inviolability of their territory and airspace to entry by belligerent forces and the right not to have their territory used for the movement of troops or supplies of belligerents. Duties of neutral states include not forming organizations of combatants to assist any of the belligerents and preventing and punishing any violations of the rights enumerated above. Should a neutral state fail or be unable to discharge its duties in maintaining its neutrality, the state may forfeit the rights associated with that status or even its neutrality altogether. For example, should a neutral state not prevent the troops of one belligerent from entering its territory, “the other belligerent may be justified in attacking the enemy forces on this territory.” Belligerents’ obligations in their

125. Id. art. 1.
126. Id. art. 2.
127. Id. art. 4.
128. Id. art. 5.
129. Army Field Manual, supra note 107, para. 520.
relations with neutral states are correspondingly converse to the rights of the neutral states with respect to the belligerents. Essentially, whereas neutral states are required to remain officially impartial to the belligerents, the belligerents are obligated to respect neutral states’ impartiality.

With special regard to communications, customary international law is based on the principle that “neutral territory must not become the basis of activities directly connected with the war operations.” Treaty law in force applies this principle according to the following rule:

Belligerents are . . . forbidden to:

(a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;

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

The foregoing passage applies only to direct communications by belligerents to their forces, communications that neutral states are obligated to prohibit. It does not, however, impose on neutral states the duty to restrict belligerents from using the neutral states’ own communications systems or privately owned systems. "A neutral power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals." However, neutral states must be impartial in allowing belligerents to communicate over systems within their jurisdiction and must require privately owned systems also to be impartial. Thus, a neutral state cannot grant communications rights to one belligerent but not another and still remain neutral.

Because information systems can now be weaponized, it is useful also to examine international treaty law with respect to arms exports by neutral states to belligerent states: "A neutral power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet." The requirement of impartiality applies equally to this provision.

---

131. Id. § 356a.
132. Hague Convention V, supra note 124, art. 3. It is presumed that the prohibition in article 3(a) extends to belligerent forces in the air and space as well.
133. Id. art. 3. Oppenheim opined that this principle also prohibits states from laying hard-wired communication lines, e.g., submarine telegraph cables through neutral states for the same purpose. 2 Oppenheim, supra note 130, § 356, at 749.
135. Id. art. 9.
136. Id. art. 7.
137. Id. art. 9.
Bearing the foregoing principles in mind, this Part will explore three issues relating to information warfare and neutrality: (1) information attacks by or against neutral states; (2) misuse of a neutral state’s cyberspace by a belligerent; and (3) the use of a neutral state’s computer or communication systems as a conduit for an information attack.

**A. Information Attacks by or Against Neutral States**

As long as a neutral state maintains its neutrality, belligerent states have an obligation to refrain from engaging in information attacks against it, for such acts would be tantamount to aggression. Likewise, a neutral state is under an obligation to refrain from information attacks against the belligerents, lest the neutral state be considered to have abandoned its neutrality. Without relinquishing its neutral status, a neutral state is, however, entitled to resist attempts to violate its neutrality by force.\(^{138}\) In the realm of information warfare, this principle gives neutral states the right to defend against information attacks by resorting to information warfare itself or launching physical attacks if necessary.

**B. Misuse of a Neutral State’s Cyberspace**

While cyberspace is often considered not to lie within the “territory” of any state, states do retain jurisdiction, and subsequently the right and responsibility, to regulate the use of computer systems located on its territory or within its control as well as parts of the Internet under its control. Many Internet domain name extensions are specific to particular states and may be controlled by them.\(^{139}\) It is possible for states, acting individually or in collusion, clandestinely to register domain names in other states and use those sites to store information or host force enhancement systems, such as supply control systems. This ability conceivably makes the sites more difficult for a hostile state to locate and neutralize. Such activities would not only constitute perfidy,\(^{140}\) but also would violate the neutrality of the other state if the other state is neutral or does not consent to false registration. It is also conceivable that a state may host such information systems on computer systems physically located in other states. If those computer systems become lawful targets, whether physically or by information attack, then the neutrality of the state having jurisdiction over the computer systems has been violated.

Determining which of the belligerents has violated the neutral state’s neutrality, however, would be more difficult than it might appear at first glance. On the one hand, the placement of a target within the neutral state’s jurisdiction violates the neutral state’s rights. On the other hand, other belligerents have a duty not to attack a target within the neutral state unless the neutral

---

\(^{138}\) Id. art. 10.

\(^{139}\) For example, the extension `.fr` denotes websites in France and `.ch` denotes sites in Switzerland.

\(^{140}\) See supra Part III.D.1.
C. Use of Neutral States’ Systems as Conduits for Information Attacks

As discussed in Part I.B of this Article, the weapons of information attack include the computer systems from which the attacks originate and the information packets which travel along lines of communications and through other computer systems. The physical communication lines and conduit systems are not weapons themselves, but they do become lawful objects of attack and their destruction or neutralization confers a definite military advantage to the attacker. When an information packet containing malicious code travels through computer systems under the jurisdiction of a neutral state, a strict construction of the law of neutrality would result in that state’s neutrality being violated. In addition, the computer systems and communication lines of that neutral state would become objects of attack.

The problem with this approach is that, on the Internet, information travels along routes that cannot always be predicted. When one server goes down, for example, Internet traffic is automatically rerouted via another. Under such circumstances, a state may not be able to prevent information attacks from leaving its jurisdiction unless it severs all connections with computer systems in other states. To impose such a duty on any and all states neutral to an armed conflict would be unreasonable, for doing so would likely grind the Internet to a halt. The law of neutrality in information warfare must be fashioned so as to preserve the obligation of belligerents to respect the principle of neutrality, and to preserve the obligation of neutral states to maintain that neutrality, while taking into consideration the realities of the Internet.

The proposed convention offers an approach to neutrality based on intent and restraint. States would be prohibited from launching information attacks from computer systems in neutral states, or from taking control of neutral systems in furtherance of information attacks. While it would remain possible that information attacks would be unintentionally routed through neutral states, states would not be allowed to do so intentionally. Computer sys-
tems and communications lines in neutral states would not be objects of attack, physical or otherwise, even if used as conduits for information attack, unless the neutral state were abandoning its neutrality by actively assisting a belligerent state in committing an attack. Deliberate violation of a state’s neutrality would be cause for the neutral state to sever communications and Internet links with the violator, without requiring the neutral state to sever the same links with the other belligerents. However, if a neutral state were to choose to sever communications and Internet links with belligerent states without cause, the neutral state would have to do likewise with all participants in that conflict.

D. Conclusion

Treaty-based international law on neutrality was formulated nearly a century ago, even before the rise of airpower. The principles underlying the law, however, remain strong enough to apply to warfare in the information age, as long as they are crafted in a balanced manner. Neutral states have rights in information warfare, as in any other branch of warfare, and consequently have the responsibility of even-handedness in exercising those rights. At the same time, belligerent states have an obligation to respect that neutrality. International law must be adapted to preserve these rights and obligations in the information age.

V. Enforcement of the Law of Information Warfare

Neither Geneva law nor Hague law provides for the enforcement of LOAC against states. Customary international law provides for states to respond to violations with reprisals. In the *jus in bello* context, customary international law defined reprisals as “acts of retaliation in the form of conduct which would otherwise be unlawful, resorted to by one belligerent against enemy personnel or property for acts of warfare committed by the other belligerent in violation of the law of war, for the purpose of enforcing future compliance with [it].” The lawful objects of reprisals, however, are now quite limited, and the practice of belligerent reprisal, and as a result the law thereof, is currently in decline.

In the age of the U.N. Charter, the means for enforcing the law of armed conflict against individuals have slowly evolved into positive law. In the aftermath of World War II, compliance with LOAC were enforced via the Nuremberg and Tokyo war crimes tribunals, but without any positivist legal basis

141. See, e.g., Hague Convention V, supra note 124.
143. Army Field Manual, supra note 107, para. 497(a).
apart from treaties among the victors.\footnote{147} In the post–Cold War era, the U.N. Security Council has provided for the prosecution of war crimes in the former Yugoslavia\footnote{148} and Rwanda.\footnote{149} The renewed interest of the international community of states in individual accountability for violations of LOAC culminated in the 1998 Rome Statute of the International Criminal Court ("ICC"),\footnote{150} whose function is to institutionalize the prosecution of individuals for genocide, crimes against humanity, and war crimes.

An international convention on the use of information systems in armed conflict would be weakened if it lacked provisions for its enforcement. Mark Shulman has urged that such a convention automatically confer jurisdiction for the prosecution of information war crimes to the ICC.\footnote{151} That approach, however, has two fundamental flaws. The first flaw is that information war crimes are not included among the offenses enumerated in the Rome Statute. Article 8 of the Statute contains an extensive list of specific acts considered "war crimes" under the Statute. All listed acts have been lifted from the Geneva Conventions and Protocols and the Hague Regulations. War crimes will be prosecuted under the Rome Statute in accordance with specific elements of each crime.\footnote{152} Under the Statute, the principle of \textit{nullum crimen sine lege} (that there must be pre-existing law for punishment of crime) strictly applies. Article 22 of the Statute reads as follows:

1. A person shall not be criminally responsible under this Statute unless the conduct in question constitutes, at the time it takes place, a crime within the jurisdiction of the Court.

2. The definition of a crime shall be strictly construed and \textit{shall not be extended by analogy}.\footnote{153}

The plain language of this provision raises serious questions as to whether the ICC would have the necessary jurisdiction to prosecute acts of information warfare which should constitute war crimes, but do not fit neatly under the specific crimes enumerated in article 8 of the Statute. Furthermore, the Statute restricts the jurisdiction of the ICC over persons in such a way as to render prosecution of individuals in some major information warfare states

\begin{footnotes}
\item[151] Shulman, \textit{supra} note 109, at 965.
\item[152] Rome Statute, \textit{supra} note 150, art. 9.
\item[153] Id. art. 22 (emphasis added).
\end{footnotes}
virtually impossible. The ICC can exercise personal jurisdiction over only individuals who are nationals of states party to the Statute or individuals who commit a war crime on the territory of a state party, specifically “[t]he State on the territory of which the conduct in question occurred or, if the crime was committed on board a vessel or aircraft, the State of registration of that vessel or aircraft.” An information attack or war crime launched from a non-party state by a national of a non-party state would thus be immune from ICC jurisdiction. Neither the United States nor China, two major powers in information warfare, is a party to the ICC Statute. The virtually complete inability of the ICC to prosecute individuals of these two states, as well as its apparent lack of jurisdiction over the crimes themselves, renders a provision for the enforcement of the proposed convention by the ICC so weak that it would be considered a dead letter almost immediately upon passage.

The second flaw undermining a possible treaty provision conferring jurisdiction over information war crimes on the ICC is that it would make ratification of the convention by the parties most affected by it virtually impossible. Ratifying a convention containing such a provision is tantamount to consenting to the jurisdiction of the ICC, even if the ratifying state is not a party to the Rome Statute. Even if such consent were limited to crimes committed incident to information warfare, to expect non-party states, especially the United States, to reverse their position regarding the ICC is politically unrealistic, given for example the painstaking effort of the United States to immunize its forces abroad from the ICC’s jurisdiction by securing agreements with the forces’ host countries. For political reasons alone, a convention expressly granting ICC jurisdiction over information war crimes would probably lose the signatures of the United States and China. Without the support of all the major powers of information warfare, any set of rules governing it would be significantly weaker. Simply put, a treaty norm lacking the support of states most affected by it necessarily loses its normative legitimacy.

A more practical approach to the enforcement of a convention on information warfare would be to include a compromissory clause in which states agree that disputes and claims arising under the convention would be referred to the International Court of Justice (“ICJ”). Under the Statute of the ICJ, such

154. Id. art. 12(2)(b).
155. Id. art. 12(2)(a) (emphasis added).
156. A list of states party to the Rome Statute may be found at http://www.icc-cpi.int/asp/Statesparties.html (last visited Nov. 1, 2005).
157. The ICC would be able to prosecute information war criminals in two narrow circumstances: (1) the information war crime is launched from the territory of a state party to the Statute, or (2) the Security Council refers a war crime to the Prosecutor acting under Chapter VII of the U.N. Charter, thus conferring jurisdiction under article 13(b). Two practical problems arise, however, in prosecutions of U.S. or Chinese nationals under these exceptions. The first is that both the United States and China are permanent members of the Security Council and are thus likely to veto any referral of an information war crime involving one of their own nationals. The second is that an extraordinary amount of luck would be required to identify and detain a suspected information war criminal before he or she is repatriated; once repatriation occurs, the responsible state would not easily give up its national for prosecution.
158. Rome Statute, supra note 150, art. 12(3).
a provision would confer jurisdiction on the Court to adjudicate such cases.\textsuperscript{159} The ICJ would then have the power to adjudicate not only questions regarding the interpretation and application of the proposed convention, but also claims for injury to states that are victims of information war crimes. While individuals would not be held accountable under this means of enforcement,\textsuperscript{160} the delinquent state would be held liable to the injured state in law for the actions of both its employees and agents under the theory of original responsibility, and possibly also for those of noncombatants under its jurisdiction, depending on the degree to which the delinquent state endorsed the acts\textsuperscript{161} or failed to take reasonable measures to prevent and punish the acts.\textsuperscript{162} The value of this admittedly weaker enforcement mechanism lies in the greater likelihood that the major information warfare powers would agree to it, especially since they would also be able to state a reservation to that particular provision without violating the object and purpose of the proposed convention.\textsuperscript{163} The conclusion here is that weak enforcement mechanism carrying the support of all of the states most affected by the convention is better than a strong mechanism carrying no such support.

\section*{VI. Conclusion}

The international community has adopted standards of conduct for the use of many varieties of weapons. As cyberspace emerges as a medium of warfare, a standard of conduct on the use of information systems in armed conflict is essential to the preservation of the rule of law in those very situations that place the greatest strain on it. This Article has discussed the various principles that will likely influence the drafting of positive international law in this developing area, and has provided a proposal for what form that law should assume. The following appendix contains a draft of the actual text of the proposed convention. States are invited to consider this draft as a point of departure for adopting a comprehensive and meaningful standard of conduct for information warfare.

\begin{footnotesize}
\begin{enumerate}
\item Only states may be parties in cases before the ICJ. Id. art. 34(1).
\end{enumerate}
\end{footnotesize}
Appendix

Draft Convention Regulating the Use of Information Systems in Armed Conflict

The High Contracting Parties,

[preambular paragraphs]

have agreed to the following:

I. General

Article 1

a. The term “information attack” means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial-of-service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target, for the purpose of inflicting injury or degrading the enemy’s ability or will to fight.

b. The term “use of information systems in armed conflict” means the use of computers and/or other information and communications systems in an information attack, as opposed to use for the sole purpose of communication, intelligence gathering, logistical support, passive computer network defense, or other force enhancements.

c. The term “State” includes all organs and instrumentalities of any administration purporting to govern the territory and population of an area, whether or not that area is recognized as a State, and whether or not the government is recognized as legitimate.

d. The term “law of armed conflict” means the body of law that regulates the conduct of persons in armed conflict, and encompasses the terms “international humanitarian law,” “law of war,” and “jus in bello.”

Article 2

This Convention regulates the use of information systems in armed conflict, applying and upholding the generally accepted principles of distinction, military necessity, humanity, proportionality, and chivalry.

Article 3

An act that violates the law of armed conflict if carried out by conventional means also violates the law of armed conflict if carried out by an information attack. An attack that does not violate the law of armed conflict if carried out by conventional means also does not violate the law of armed conflict if carried out using information systems. A common crime that is committed using information systems, such as larceny, violates the law of armed conflict if
it is committed by lawful or unlawful combatants in furtherance of an armed conflict.

II. Distinction

Article 4
The term “combatant” shall designate any member of the regular, uniformed armed services of a State, including reserves and national guard, and uniformed internal security and law enforcement services as Parties shall designate; and other armed forces and organized resistance movements meeting all of the following conditions:

a. they are commanded by a person responsible for his or her subordinates;

b. they wear uniforms or other fixed distinctive signs recognizable at a distance;

c. they carry their arms openly; and

d. they conduct their operations in accordance with the laws and customs of war.

The term “combatant” shall not include medical or religious personnel.

Article 5
The term “noncombatant” shall designate any person who is not a combatant as defined in Article 4 above.

Article 6
For the purpose of this Convention, civilians engaged in a dévée en masse shall not be considered lawful combatants.

Article 7
Only lawful combatants shall be permitted to engage in information attacks on other States. This Convention shall not restrict the capacity of noncombatants to use information systems for communications, logistical support, or other force enhancement systems, provided such uses do not otherwise violate the prohibitions set forth in this Convention or the principles of the law of armed conflict.

Article 8
States shall engage in information attacks in only facilities located a safe distance away from facilities used by noncombatants.
Article 9
States shall separate information systems used by combatants from those used by noncombatants. States shall not use information systems used by noncombatants to shield information systems used by combatants from attack, and shall not embed medical information systems in other military information systems that are lawful objects of attack.

Article 10
States shall launch information attacks from only information systems operated by lawful combatants. States shall not use the information systems of noncombatants or nonparties to the conflict as proxies for such attacks. States shall take reasonable measures to prohibit and prevent such attacks by private persons.

Article 11
States engaging in information attacks shall make best efforts to minimize the adverse effects of information warfare on noncombatants.

Article 12
Information attacks calculated to cause physical damage shall be directed against only targets whose destruction, damage or neutralization confers a definite military advantage, provided that military advantage outweighs the adverse effect on civilians or the civilian population.

Article 13
Information attacks which are intended or may be reasonably expected to cause widespread, long-term, and severe damage to the natural environment, and thereby to prejudice the health or survival of the population, are prohibited.

Article 14
In addition to the prohibitions set forth in Articles 12 and 13 of this Convention, information attacks directed against works and installations containing dangerous forces, such as dams, dikes, and nuclear facilities, whose attack may cause severe losses among the civilian population, shall be attacked only if they are used in regular, significant and direct support of military operations, and if such attack is the only feasible way to terminate such support.

Article 15
Information attacks directed against any of the following facilities shall be prohibited:

a. Medical and religious facilities.
b. Banks; stock, bond and commodities markets; and any other financial institutions.

c. Supplies and distribution systems for food and water, unless the supply or distribution system is used exclusively for providing food and water to lawful combatants.

d. Supplies and distribution systems for electricity and other energy sources for the civilian population, unless the systems are used to supply energy to military installations, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population.

e. Communications systems used by the civilian population, unless the systems are also used by combatant forces, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population.

f. Sites protected as cultural property.

This Convention shall not prejudice the right to attack the above facilities if they are being used to shield other, lawful targets from attack.

Article 16
States shall use all reasonable means to ensure that information attacks involving malicious code, including logic bombs, discriminate between information systems used by combatants and those used by noncombatants and neutral States.

Article 17
States shall program logic bombs to neutralize themselves automatically once they are no longer reasonably anticipated to serve a legitimate military purpose.

III. Rules of Warfare

Article 18
States shall conduct information warfare according to customary international law principles of military necessity, proportionality, humanity, and chivalry. States shall not conduct information attacks in a manner so as to cause superfluous injury or unnecessary suffering.

Article 19
States shall not conduct commercial or financial transactions that are fraudulent or under false pretense as a means of warfare.
Article 20
States shall not interfere with the personal finances of any individuals, including combatants and public officials, as a means of warfare. Violations of this article include, but are not limited to, interfering with payroll systems, transferring money or other capital assets without authorization, and altering or erasing records of ownership of money or assets.

Article 21
States shall not engage in identity theft against individuals as a means of warfare, nor shall States obtain and display personal identifiers of individuals, whose display would facilitate identity theft from such individuals by other States or non-State actors.

Article 22
The practice of contacting military members at their residences, for example, by electronic mail, shall not be prohibited. However, States shall engage in such practices in a manner so as not to terrorize noncombatants, including the family members of military members.

Article 23
The use of information systems to invite the confidence of an adversary to lead it to believe that an individual, location, or facility is entitled to protection under the law of armed conflict, with intent to betray that confidence, constitutes perfidy, and States shall be forbidden from engaging in such acts.

Article 24
States shall not transmit malicious code disguised as harmless electronic message traffic if:

a. The message is disguised as originating from an official in the government or armed forces of any State other than the attacking State;

b. The message is disguised as originating from any State other than the attacking State or the target State; or

c. The message is disguised as originating from any medical or religious establishment of or within any State, or any other person or institution of or within any State that is accorded protected status.

Article 25
The alteration of images or recordings shall be prohibited if:
a. The alteration falsely depicts any individual engaged in an unlawful, lewd or lascivious, or sacrilegious act, with the intent to induce others to believe that the individual actually committed the act, when the individual in fact did not commit the act;

b. The alteration falsely depicts a war crime, whether actual or imminent, particularly but not limited to an atrocity or attack on a protected site, with the intent to induce others to believe that another State actually committed the war crime, atrocity, or attack, or is about to do so, when that State in fact did not do so and is not about to do so; or

c. The alteration falsely depicts an attack by another State against any third State with the intent to induce others to believe that such an attack has actually taken place or is imminent, when such an attack in fact has not taken place and is not imminent.

IV. RIGHTS OF STATES NOT PARTY TO AN ARMED CONFLICT

Article 26

a. Belligerent States shall not engage in information attacks against neutral States.

b. Neutral States shall not actively assist or facilitate information attacks against belligerent States.

Article 27

A State shall not use domain names or information systems for military purposes, or conduct any information warfare activities, within the jurisdiction of any other State, unless it does so with the consent of that other State.

Article 28

Belligerent States shall not launch information attacks from computer systems in neutral States, or take control of such systems in furtherance of information attacks. Belligerent States shall not intentionally route information attacks through neutral States.

Article 29

Computer systems and communications lines in neutral States shall not be the object of attack, physical or otherwise, even if they are used as conduits for an information attack, unless the neutral State is actively assisting an attacking State in committing the attack.

Article 30

A neutral State is not required to sever communications or Internet links with belligerent States. If a belligerent State deliberately violates a neutral
State’s rights of neutrality, the neutral State shall be permitted to sever communications and Internet links with the violating State, but shall not be required to sever the same links with the other belligerent States. However, if several belligerent States violate the neutral State’s neutrality, the neutral State may sever links with the belligerent States in a manner proportional to the severity of the violations, provided that the neutral State treat equivalent violations equally. If the neutral State chooses to sever communications and/or Internet links with any belligerent States without cause, the neutral State must sever the same links with all the belligerent States.

V. ENFORCEMENT

Article 31

States shall enact legislation to prohibit noncombatants within its jurisdiction from engaging in information attacks against other States and shall prescribe criminal penalties for the same. States shall take all reasonable and appropriate measures to prevent and punish noncombatants within its jurisdiction from engaging in information attacks against other States.

Article 32

States shall submit disputes and claims arising under this Convention to the International Court of Justice or other adjudicatory bodies as established by the Parties.

VI. MISCELLANEOUS

[amendments, ratification, deposit, entry into force, authentic texts, etc.]

[signatures]