Wired warfare: Computer network attack and *jus in bello*

by
MICHAEL N. SCHMITT

Despite ongoing debates about the existence, or lack thereof, of a "revolution in military affairs", it is undeniable that twenty-first century warfare will differ dramatically from that which characterized the twentieth century. The tragic terrorist attacks of 11 September 2001 and their aftermath are dominating the headlines at the beginning of the new century. Perhaps equally remarkable will be the maturing of "information warfare" as a tool of combat.[1] It will challenge existing doctrine on the waging of war, necessitate a revised concept of battle space and expand the available methods and means of warfare. Of particular note will be the impact of information warfare on the principles of international humanitarian law — and vice versa.

In brief, information warfare is a subset of information operations, i.e. "actions taken to affect adversary information and information systems while defending one's own information and information systems".[2] Such operations encompass virtually any non-consensual measures intended to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer. They can occur in peacetime, during

Professor of International Law, and Director, Executive Program in International and Security Affairs at George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany.

crises, or at the strategic, operational or tactical levels of armed conflict.[3] Information operations are distinguished by that which is affected or protected — information.

Information warfare is narrower. It consists of "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries".[4] Thus information warfare is differentiated from other operations by the context in which it occurs — crisis or conflict. Routine

1 The United States National Military Strategy cites information superiority as a key element of its strategy for this century. "Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting and denying an adversary's ability to do the same." Joint Chiefs of Staff, National Military Strategy (1997), ‹http://www.dtic.mil/jcs/nms/strategy.htm›, at n.p. For an excellent collection of essays on the nature of war in the 21st century, see Robert H. Scales (ed.), *Future War Anthology*, Carlisle Barracks, Pa., US Army College, 2000. On the specific issue of information and conflict, see Stephan Metz, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare*, Carlisle Barracks, Pa., US Army College, 2000; William A. Owens and Edward Offley, *Lifting the Fog of War*, John Hopkins University Press, Baltimore, 2000; Thomas E. Copeland (ed.), *The Information Revolution and National Security*, Carlisle Barracks, Pa., US Army College, 2000; David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 44ISR Cooperative Research Program, Washington D.C., 1999; Dan Kuehl, *Strategic Information Warfare: A Concept*, Working Paper 322, Strategic & Defence Studies Centre, Australian National University, Canberra, 1999; Zalmay Khalilzad and John White (eds), *Strategic Appraisal: The Changing Role of Information Warfare*, RAND, Santa Monica, 1999; Dorothy E. Denning, *Information Warfare and Security*, ACM Press, New York, 1999; James Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere*, Simon & Schuster, New York, 1998.

2 Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 12 April 2001, p. 203 (hereinafter JP 1-02). Operations that might constitute information operations include operations security, psychological operations, military deception, electronic warfare, physical attack and computer network attack. See Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13, 9 October 1998, at I-9 (hereinafter JP 3-13).

3 At the strategic level, information operations can be employed to "achieve national objectives by influencing or affecting all elements (political, military, economic, or informational) of an adversary's or potential adversary's national power while protecting similar friendly elements". At the operational level, the focus of information operations is "on affecting adversary lines of communication (LOCs), logistics, command and control (C2), and related capabilities and activities while protecting similar friendly capabilities and activities". Finally, at the tactical level the objective is to affect adversary "information and information systems relating to C2, intelligence, and other information-based processes directly relating to the conduct of military operations...". JP 3-13, *op. cit.* (note 2), at I-2 – I-3.

4 JP 1-02, *op. cit.* (note 2), p. 203.

peacetime espionage is, for example, an information operation that does not constitute information warfare unless conducted during a crisis or hostilities.

Computer network attacks (CNA), which may amount to information warfare or merely information operations, are "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves".[5] The essence of CNA is that, regardless of the context in which it occurs, a data stream is relied on to execute the attack.[6] Thus, the *means* used set CNA apart from other forms of information operations. These means vary widely. They include, *inter alia*, gaining access to a computer system so as to acquire control over it, transmitting viruses to destroy or alter data, using logic bombs that sit idle in a system until triggered on the occasion of a particular occurrence or at a set time, inserting worms that reproduce themselves upon entry into a system and thereby overloading the network, and employing sniffers to monitor and/or seize data.

This article addresses the use of CNA during *international* armed conflict and is limited to consideration of *jus in bello*, that body

5 *Ibid.*, p. 88. *The USAF Intelligence Targeting Guide*, AF Pamphlet 14-210, 1 February 1998, para. 11.4.3, notes the following information warfare employment concepts:

Corruption – The alteration of information content; the manipulation of data to make it either nonsensical or inaccurate. Destroying existing knowledge.

Deception – A specific type of corruption; the alteration of, or adding to, information to portray a situation different from reality. Creating false knowledge to include masquerading.

Delay – The reversible slowing of the flow of information through the system, and the slowing of the acquisition and dissemination of new knowledge.

Denial – The reversible stopping of the flow of information for a period of time; although the information may be transmitted and used within friendly territory, the adversary is denied access to it. The prevention of the acquisition and dissemination of new knowledge.

Disruption – The reduction of the capacity to provide and/or process information (reversible). This is a combination of delay and corruption. The delay of the acquisition and dissemination of new knowledge and the destruction of existing knowledge.

Degradation – The permanent reduction in the capacity to provide and/or process information.

Destruction – The destruction of information before it can be transmitted; the permanent elimination of the capacity to provide and/or process information.

6 Thus electronic attack (EA) would not fall within this category. For instance, using an electromagnetic pulse to destroy a computer's electronics would be EA, whereas transmitting a code or instruction to a system's central processing unit to cause the power supply to short out would be CNA. *Ibid.*

of law concerned with what is permissible, or not, during hostilities, irrespective of the legality of the initial resort to force by the belligerents.[7] Discussion therefore centres on the use of CNA in the context of "State-on-State" armed conflict. Moreover, the article is an effort to explore *lex lata*, rather than an exercise in considering *lex ferenda*. While setting forth *lex ferenda* is an especially worthy project as the nature of warfare evolves,[8] the goal here is simply to analyse the applicability of existing humanitarian law to computer network attack, and identify any prescriptive lacunae that may exist therein.

Applicability of humanitarian law to computer network attacks

The threshold question is whether computer network attack is even subject to humanitarian law. To begin with, there is no provision in any humanitarian law instrument that directly addresses CNA, or, for that matter, information warfare or information operations; this might suggest that CNA is as yet unregulated during armed conflict. Additionally, it could be argued that the development and employment of CNA postdates existing treaty law and thus, having not been within the contemplation of the parties to those instruments, is exempt from the coverage thereof. A third possible argument for inapplicability is that humanitarian law is designed for methods and means that are kinetic in nature; since there is little that is "physical" in CNA, attacks by computers fall outside the scope of humanitarian law.[9]

7 On CNA and *jus ad bellum*, that body of international law governing the legality of the resort to force by States, see Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Colombia Journal of Transnational Law*, Vol. 37, 1999, p. 885; Richard Aldrich, "How Do You Know You are at War in the Information Age?", *Houston Journal of International Law*, Vol. 22, 2000, p. 223.

8 For a discussion of CNA in the context of both law and ethics that conclude a new convention is required, see William J. Bayles, "The Ethics of Computer Network Attack", *Parameters*, Spring 2001, p. 44.

9 On this point see Emily Haslam, "Information Warfare: Technological Changes and International Law", *Journal of Conflict and Security Law*, Vol. 5, 2000, p. 157. See particularly her discussion of points made in Richard Aldrich, "The International Legal Implications of Information Warfare", *Airpower Journal*, Fall 1996, p. 99; and Mark Shulman, "Discrimination in the Laws of Information Warfare", *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 939.

In other words, humanitarian law applies to armed conflict, and computer network attack is not "armed".

The first two possibilities are easily dispensed with. The fact that existing conventions are silent on CNA is of little significance. First, the Martens Clause, a well-accepted principle of humanitarian law, provides that whenever a situation is not covered by an international agreement, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity, and from the dictates of public conscience."[10] By this norm, all occurrences during armed conflict are subject to application of humanitarian law principles; there is no lawless void. The acceptance of "international custom" as a source of law in Article 38 of the Statute of the International Court of Justice also demonstrates the fallacy of any contention of inapplicability based on the absence of specific *lex scripta*.[11]

10 Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 1(2), 12 December 1977, 1125 U.N.T.S. 3 (hereinafter Additional Protocol I). The original formulation of the Martens Clause in the preamble of the Hague Convention IV respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2295, I Bevans 634, states "the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations as they result from the usages established amoung civilized peoples, from the laws of humanity, and the dictates of the public conscience", reprinted in Adam Roberts and Richard Guelff, *Documents on the Laws of War*, 3rd ed., Oxford University Press, Oxford, 2000, p. 67.

11 The Statute of the International Court of Justice defines custom as "a general practice accepted by law". Statute of the International Court of Justice, 26 June 1977, Art. 38(1)(b), 59 Stat. 1031, T.S. No. 933, 3 Bevans 1153, 1976 Y.B.U.N. 1052. The United States Restatement notes that custom "results from a general and consistent practice of states followed by them from a sense of legal obligation". Restatement (Third), Foreign Relations Law of the United States, sec. 102(2) (1987). See also *North Sea Continental Shelf Cases*, 3 ICJ Reports 1969, p. 44 ("Not only must the acts concerned amount to settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule requiring it."); *The Paquete Habana*, 175 US 677, 20 S.Ct. 290, 44 L.Ed 320 (1900); *The S.S. Lotus (France v. Turkey)*, PCIJ (ser. A) No. 10, 1927; *Asylum Case (Colombia v. Peru)*, 5 ICJ Reports, 1950, p. 266; *Case Concerning Right of Passage over Indian Territory (Portugal v. India)*, ICJ Reports, 1960, p. 6. For academic comment on customary international law, see Jack L. Goldsmith and Eric A. Posner, "Understanding the Resemblance Between Modern and Traditional Customary International Law", *Virginia Journal of International Law*, Vol. 40, 2000, p. 639; Patrick Kelly, "The Twilight of Customary International Law", *Virginia Journal of International Law*, Vol. 40, 2000, p. 449; Anthony A. D'Amato, *The Concept of Custom in International Law*, Cornell University Press, Ithaca, 1971.

Arguments focusing on the fact that CNA postdates present prescriptive instruments are similarly fallacious. Precisely this line of reasoning was presented to the International Court of Justice in *Legality of the Threat or Use of Nuclear Weapons*. In its advisory opinion, the Court summarily rejected the assertion that because humanitarian "principles and rules had evolved prior to the invention of nuclear weapons", humanitarian law was inapplicable to them. As the Court noted, "[i]n the view of the vast majority of States as well as writers there can be no doubt as to the applicability of humanitarian law to nuclear weapons".[12] There being no reason to distinguish nuclear from computer weapons, at least on the basis of when they were developed vis-à-vis the entry into force of relevant humanitarian law norms, the same conclusion applies to CNA. Furthermore, a review of new weapons and weapon systems for compliance with humanitarian law is a legal, and often a policy, requirement.[13] Obviously, this would not be so if pre-existing law were inapplicable, *ab initio*, to nascent methods and means of warfare.

This analysis leaves only the third argument for inapplicability of humanitarian law to computer network attack — that it is not *armed* conflict, at least not in the absence of conventional hostilities. In fact, armed conflict is the condition that activates *jus in bello*. Article 2 common to the four 1949 Geneva Conventions provides that they apply, aside from specific provisions that pertain in peacetime, "to all cases of declared war or of any other *armed conflict* which may arise

12 *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Reports, 1996, p. 226 (July 8), 35 *International Legal Materials*, p. 809, para. 85.

13 Additional Protocol I, *op. cit.* (note 10), Art. 36: "In the study, development, acquisition or adoption of new weapons, means or methods of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party." For the United States, the weapon review is required by Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, 23 October 2000, para. 4.7.3.1.4. It provides, in relevant part, that "DoD acquisition and procurement of weapons and weapon systems shall be consistent with all applicable domestic law and all applicable treaties, customary international law, and the law of armed conflict (also known as the laws and customs of war)... Additionally, legal reviews of new, advanced or emerging technologies that may lead to development of weapons or weapon systems are encouraged."

between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them".[14] The 1977 Additional Protocol I, which, like the Conventions pertains to international armed conflict, adopts the same "armed conflict" standard, one that has become an accepted customary law threshold for humanitarian law.[15] The fact that the 1977 Additional Protocol II also embraces the term "armed conflict",[16] albeit in the context of non-international armed conflict, demonstrates that armed conflict is a condition determined by its nature rather than its participants,[17] by its location[18] or, as was formerly the case with "war", by the belligerents' declaration thereof.[19]

It seems relatively clear, then, that humanitarian law is activated through the commencement of armed conflict. But what is armed conflict? Commentaries published by the International Committee of the Red Cross on the 1949 Geneva Conventions and the 1977 Additional Protocols take a very expansive approach towards

14 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949, Art. 2 , 6 U.S.T. 3114, 75 U.N. T.S. 31 (hereinafter GC I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, 12 August 1949, Art. 2, 6 U.S.T. 3217, 75 U.N. T.S. 85 (hereinafter GC II); Geneva Convention Relative to the Treatment of Prisoners of War, 12 August 1949, Art. 2, 6 U.S.T. 3316, 75 U.N. T.S. 135 (hereinafter GC III); and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, Art. 2, 6 U.S.T. 3516, 75 U.N.T.S. 287 (hereinafter GC IV) (emphasis added). The Conventions are reprinted in Roberts and Guelff, *op. cit.* (note 10), at 195, 221, 243 and 249 respectively.

15 Additional Protocol I, *op. cit.* (note 10), Art. 1.

16 Additional Protocol II to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609, 16 *International Legal Materials*, p. 1442 (1977), reprinted in Roberts and Guelff, *op. cit.* (note 10), p. 481.

17 Additional Protocol I deals with conflict between States, whereas Additional Protocol II is concerned with conflict between a State and a rebel group (or groups).

18 Non-international armed conflict occurs solely within the confines of a single State.

19 Hague Convention III relative to the Opening of Hostilities, 18 October 1907, Art. 1, I Bevans 619, 2 *American Journal of International Law*, Vol. 2 (Supp.), 1908, p. 85, reprinted in Dietrich Schindler and Jiri Toman, *The Law of Armed Conflict*, M. Nijhoff, Dordrecht, 1988, p. 57. According to the Commentary on the 1949 Geneva Conventions, "[t]here is no longer any need for a formal declaration or war, or for recognition of the state of war, as preliminaries to the application of the Convention. The Convention becomes applicable as from the actual opening of hostilities." Jean Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32 (hereinafter GC I Commentary).

the meaning of the term. The former define armed conflict as "[a]ny difference arising between two States and leading to the *intervention of armed forces*... even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place."[20] Similarly, the Commentary on Additional Protocol I specifies that "humanitarian law... covers any dispute between two States involving the *use of their armed forces*. Neither the duration of the conflict, nor its intensity, play a role...".[21] That on Additional Protocol II describes armed conflict as "the existence of open *hostilities between armed forces* which are organized to a greater or lesser degree".[22] The *sine qua non* in all three cases is commitment of armed forces.

But a dispute or difference resulting in the engagement of armed forces cannot be the sole criterion. Military forces are used on a regular basis against adversaries without necessarily producing a state of armed conflict — consider aerial reconnaissance/surveillance operations as just one example. Furthermore, it is now generally accepted that isolated incidents such as border clashes or small-scale raids do not reach the level of armed conflict as that term is employed in humanitarian law.[23] Accordingly, State practice, supplemented by the writings of publicists, illustrates that Additional Protocol I's dismissal of intensity and duration has proven slightly overstated.

Instead, the reference to armed forces is more logically understood as a form of prescriptive shorthand for activity of a particular nature and intensity. At the time when the relevant instruments were drafted, *armed* forces were the entities that conducted the

20 GC I Commentary, *op. cit.* (note 19), pp. 32-33 (emphasis added).

21 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987, para. 62 (emphasis added) (hereinafter Additional Protocols: Commentary). The Commentary on Additional Protocol II refers back to the commentary on common Article 3 of the 1949 Conventions and to that on Additional Protocol I. *Ibid.*, para. 4448, fn 2.

22 Additional Protocols: Commentary, *op. cit.* (note 21), para. 4341 (emphasis added).

23 See, for example, discussion in Ingrid Detter De Lupis, *The Law of War*, 2nd ed., Cambridge University Press, Cambridge, 2000, pp. 20-21; Christopher Greenwood, "Historical Develop-ment and Legal Basis", in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflict*, Oxford University Press, Oxford, 1995, p. 42.

contemplated activity at the requisite level of intensity; by focusing on the armed forces, the intended ends were achieved. Restated, the relevant provisions of the Conventions and their commentaries were actor-based because citing the actors engaged in the undesirable conduct — armed forces — was, at the time, a convenient and reliable method for regulating it.

And what was that conduct? The logical answer is found in the underlying purposes of humanitarian law. A review of its instruments and principles makes clear that protecting individuals who are not involved in the hostilities directly, as well as their property, lies at their core.[24] Most notably, protected entities include civilians and civilian objects, as well as those who are *hors de combat* (e.g. wounded or captured personnel) or provide humanitarian services (e.g. medical personnel). As for the protection they are entitled to, it is usually framed in terms of injury or death or, in the case of property, damage or destruction. These Geneva Law purposes are complemented by Hague Law norms intended to limit suffering generally through restrictions on certain weaponry and methods of warfare.[25]

This excessively abbreviated summary of humanitarian law's fundamental purposes elucidates the term armed conflict. Armed conflict occurs when a group takes measures that injure, kill, damage or destroy. The term also includes actions intended to cause such results or which are the foreseeable consequences thereof. Because the issue is *jus in bello* rather than *ad bellum*, the motivation underlying the actions is irrelevant. So too is their wrongfulness or legitimacy. Thus, for example, the party that commences the armed conflict by committing such acts may be acting in legitimate anticipatory (or interceptive)

24 For instance, the Preamble to Additional Protocol I notes that "it [is] necessary... to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application...". Additional Protocol I, *op. cit.* (note 10).

25 The designation "Geneva Law" refers to that portion of the law of armed conflict addressing protected categories of persons: civilians, prisoners of war, the sick or shipwrecked, and medical personnel. It is distinguished from "Hague Law", which governs methods and means of combat, occupation, and neutrality. For a discussion of the international instruments which fall into each body of law, and of those which display elements of both, see Frederic DeMulinen, *Handbook on the Law of War for Armed Forces*, ICRC, Geneva, 1987, pp. 3-4.

self-defence; nevertheless, as long as the actions were intended to injure, kill, damage or destroy, humanitarian law governs them. It should be noted that given the current weight of opinion, actions that are sporadic or isolated in nature would not suffice. Additionally, because the issue is the law applicable to international armed conflict, the relevant actions must be attributable to a State.[26]

Returning to the topic at hand, and quite aside from *ad bellum* issues, humanitarian law principles apply whenever computer network attacks can be ascribed to a State are more than merely sporadic and isolated incidents and are either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable. This is so even though classic *armed* force is not being employed. By this standard, a computer network attack on a large airport's air traffic control system by agents of another State would implicate humanitarian law. So too would an attack intended to destroy oil pipelines by surging oil through them after taking control of computers governing flow,[27] causing the meltdown of a nuclear reactor by manipulation of its computerized nerve centre, or using computers to trigger a release of toxic chemicals from production and storage facilities. On the other hand, humanitarian law would not pertain to disrupting a university intranet, downloading financial records, shutting down Internet access temporarily or conducting cyber espionage, because, even if part of a regular campaign of similar acts, the foreseeable consequences would not include injury, death, damage or destruction.

It should be apparent that, given advances in methods and means of warfare, especially information warfare, it is not sufficient to apply an actor-based threshold for application of humanitarian law; instead, a consequence-based one is more appropriate. This is hardly a jurisprudential epiphany. No one would deny, for instance, that biological or chemical warfare (which does not involve delivery by a kinetic

26 On the topic of attribution of an act to a State, see the Draft Articles on Responsibility of States for internationally wrongful acts, adopted by the International Law Commission at its fifty-third session (2001), *Official Records of the General Assembly, Fifty-sixth session, Supplement No. 10* (A/56/10), chp. IV.E.1.

27 This possibility was described in *President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures*, October 1997, at A-46.

weapon) is subject to humanitarian law. A consequence-based threshold is also supported by the fact that once armed conflict has commenced (and except for prohibitions relevant to particular weapons), the means by which injury, death, damage or destruction are produced have no bearing on the legality of the causal act. Intentionally targeting a civilian or other protected persons or objects is unlawful irrespective of the method or means used. Starvation, suffocation, beating, shooting, bombing, even cyber attack — all are subject to humanitarian law owing to the fact that a particular consequence results. That this is so counters any assertion that, standing alone, cyber attacks are not subject to humanitarian law because they are not "armed" force. On the contrary, they may or may not be, depending on their nature and likely consequences.

Computer network attack targets

As has been discussed, computer network attacks are subject to humanitarian law if they are part and parcel of either a classic conflict or a "cyber war" in which injury, death, damage or destruction are intended or foreseeable. This being so, it is necessary to consider the targets against which computer network attacks may be directed.

A useful starting point is to frame the conduct that is subject to the prescriptive norms governing targeting. Because most relevant Additional Protocol I provisions articulate standards applicable to Parties and non-Parties (as a restatement of binding customary law) alike, that instrument serves as an apt point of departure.[28] Article 48, the basic rule governing the protection of the civilian population, provides that "Parties to the conflict... shall direct their operations only

28 Although not party to Protocol I, the United States considers many of its provisions to be declaratory of customary international law. For a non-official, but generally considered authoritative, delineation of those viewed as declaratory, see Michael J. Matheson, "Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions", *American University Journal of International Law and Policy*, Vol. 2, 1987, p. 419. See also International & Operational Law Division, Office of the Judge Advocate General, Department of the Air Force, *Operations Law Deployment Deskbook*, tab 12, no date, and comments by the then State Department Legal Advisor Abraham D. Soafer in "Agora: The US Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims", *American Journal of International Law*, Vol. 82, 1988, p. 784.

against military objectives".[29] At face value, Article 48 would seem to rule out *any* military operation, including CNA, directed against other than purely military objectives. In fact, it does not. In subsequent articles, proscriptions are routinely expressed in terms of "attacks". Thus, "the civilian population as such, as well as individual civilians, shall not be the object of attack";[30] "civilian objects shall not be the object of attack";[31] "indiscriminate attacks are forbidden";[32] "attacks shall be limited strictly to military objectives";[33] and so forth. The term is expressly defined in Article 49: "'Attacks' means acts of violence against the adversary, whether in offence or in defence." As a general matter then, the prohibition is not so much on targeting non-military objectives as it is on *attacking* them, specifically through the use of violence. This interpretation is supported by the text of Article 51, which sets forth the general principle that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations" and prohibits "acts or threats of *violence* the primary purpose of which is to spread terror among the civilian

29 Additional Protocol I, *op. cit.* (note 10), Art. 48. The centrality of the principle to humanitarian law is noted in the ICRC Commentary thereon:

> "The basic rule of protection and distinction is confirmed in this article. It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule of customary law. It was already implicitly recognized in the St. Petersburg Declaration of 1868 renouncing the use of certain projectiles, which had stated that 'the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy'. Admittedly this was concerned with preventing superfluous injury or unnecessary suffering to combatants by prohibiting the use of all explosive projectiles under 400 grammes in weight, and was not aimed at specifically protecting the civilian population. However, in this instrument the immunity of the population was confirmed indirectly... In the Hague Conventions of 1899 and 1907, like the Geneva Conventions of 1929 and 1949, the rule of protection is deemed to be generally accepted as a rule of law, though at that time it was not considered necessary to formulate it word for word in the texts themselves. The rule is included in this Protocol to verify the distinction required and the limitation of attacks on military objectives."

Additional Protocols: Commentary, *op. cit.* (note 21), paras 1863-64.

30 Additional Protocol I, *op. cit.* (note 10), Art. 51(2).

31 *Ibid.* Art. 52(1).

32 *Ibid.*, Art. 51(4).

33 *Ibid.*, Art. 52(2).

population",[34] as well as the Commentary on Article 48, which notes that "the word 'operation' should be understood in the context of the whole of the Section; it refers to military operations during which *violence* is used."[35]

In light of this interpretation, does computer network attack fall outside the ambit of "attacks" because it does not employ violence? No, and for precisely the same reason that armed attacks can include cyber attacks. "Attacks" is a term of prescriptive shorthand intended to address specific consequences. It is clear that what the relevant provisions hope to accomplish is shielding protected individuals from injury or death and protected objects from damage or destruction. To the extent that the term "violence" is explicative, it must be considered in the sense of violent *consequences* rather than violent *acts*. Significant human physical or mental suffering[36] is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise constitutes damage or destruction. The point is that inconvenience, harassment or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion. As an example, a major disruption of the stock market or banking system might effectively collapse the economy and result in widespread unemployment, hunger, mental anguish, etc., a reality tragically demonstrated during the Depression of the 1930s. If it did cause this level of suffering, the CNA would constitute an attack within the meaning of that term in humanitarian law.

Other articles within the section sustain this reading. For instance, the rules of proportionality speak of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof",[37] those relating to protection of the environment refer to "widespread, long-term, and severe damage",[38] and the protection of dams, dykes and nuclear electrical generating stations is framed in

34 *Ibid.*, Arts 51(1) and 51(2) (emphasis added).

35 Additional Protocols: Commentary, *op. cit.* (note 21), para. 1875 (emphasis added).

36 It is reasonable to include human suffering in the connotation, since the Protocol prohibits causing terror, which is also a psychological condition. Additional Protocol I, *op. cit.* (note 10), Art. 51(2).

37 *Ibid.*, Arts 51(5)(b); 57(2)(a)(iii); 57(2)(b).

38 *Ibid.*, Arts 35(3) and 55(1).

terms of "severe losses among the civilian population"[39] which "would be excessive in relation to the concrete and direct military advantage anticipated". Furthermore, during negotiations on Additional Protocol I, the issue of whether laying landmines constituted an attack arose. Most agreed that it did because "there is an attack whenever a person is directly endangered by a mine laid".[40] By analogy, a computer network attack which foreseeably endangers protected persons or property would amount to an attack.

Let us return now to Article 48. In the context of computer network attack, and as a general rule (various other specific prohibitions are discussed below), the article would ban those CNA operations directed against non-military objectives that are intended to, or would foreseeably, cause injury, death, damage or destruction. Unless otherwise prohibited by specific provisions of humanitarian law, CNA operations unlikely to result in the aforementioned consequences are permissible against non-military objectives, such as the population.[41] As a result of this distinction, the need to carefully assess whether or not an information warfare operation is or is not an "attack" is greatly heightened. In the past, analysis of this matter approximated to a *res ipsa loquitor* approach. However, CNA is much more ambiguous than traditional military operations, thereby demanding a more challenging consequence-based consideration.

While CNA does dramatically expand the possibilities for "targeting" (but not attacking) non-military objectives, it is unfair to characterize this as a weakening of the prescriptive architecture. Instead, it simply represents an expansion of permissible methods and means resulting from advances in technology; existing norms remain intact. Recall, for example, that psychological operations directed against the civilian population that cause no physical harm are entirely permissible, so long as they are not intended to terrorize.[42] This is so

39 *Ibid.*, Art. 56(1).

40 Additional Protocols: Commentary, *op. cit.* (note 21), para. 1881.

41 But see Haslam, *op. cit.* (note 9), p. 173.

42 Indeed, the United States has even developed doctrine for the conduct of psychological operations. Joint Chiefs of Staff, Joint Doctrine for Psychological Operations, Joint Publication 3-53, 10 July 1996. Actions intended to terrorize the civilian population are prohibited by Additional Protocol I, *op. cit.* (note 10), Art. 51(2).

whether the motivation for the operations is military in nature or not. Nevertheless, although the objective regime is a constant, the advent of CNA reveals a normative lacuna that, unless filled, will inevitably result in an expansion of war's impact on the civilian population.

Assuming that a CNA operation is an "attack," what can be targeted? Analytically, potential targets can be classified into three broad categories: 1) combatants and military objectives; 2) civilians and civilian objects; and 3) dual-use objects. Moreover, particular types of potential targets enjoy specific protection. It is useful to address each grouping separately.

Combatants and military objectives

Combatants and military objectives are by nature valid targets and may be directly attacked as long as the method and means used, as discussed in the next section, are consistent with humanitarian law restrictions. Those who plan or decide on attacks have an affirmative duty to "do everything feasible" to verify that intended targets are legitimate, i.e. that they do not enjoy immunity from attack under humanitarian law.[43]

A combatant is a member of the armed forces other than medical personnel and chaplains; armed forces include "all organized

43 Additional Protocol I, *op. cit.* (note 10), Art. 57(2)(a)(i). The commentary on this provision further explains the obligation.

"Admittedly, those who plan or decide upon such an attack will base their decision on information given them, and they cannot be expected to have personal knowledge of the objective to be attacked and of its exact nature. However, this does not detract from their responsibility, and in case of doubt, even if there is only slight doubt, they must call for additional information and if need be give orders for further reconnaissance to those of their subordinates and those responsible for supportive weapons (particularly artillery and air force) whose business this is, and who are answerable to them. In the case of long-distance attacks, information will be obtained in particular from aerial reconnaissance and from intelligence units, which will of course attempt to gather information about enemy military objectives by various means. The evaluation of the information obtained must include a serious check of its accuracy, particularly as there is nothing to prevent the enemy from setting up fake military objectives or camouflaging the true ones. In fact it is clear that no responsible military commander would wish to attack objectives which were of no military interest. In this respect humanitarian interests and military interests coincide."

Additional Protocols: Commentary, *op. cit.* (note 21), para. 2195.

armed forces, groups and units which are under a command responsible to [a Party to the conflict] for the conduct of its subordinates... [They must] be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict".[44] Directing computer network attacks against combatants, for instance by causing a military air traffic control system to transmit false navigational information in order to cause a military troop transport to crash, is clearly permissible.

Military objectives are defined in Article 52 of Additional Protocol I as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite advantage".[45] Military equipment and facilities, other than medical and religious items, are clearly military objectives, and thereby subject to direct computer network attack. However, determining which objects are military objectives beyond these obvious exemplars is often difficult.[46] The problem lies in ascertaining the required nexus between the object to be attacked and military operations.

The crux of the dilemma is interpretation of the terms "effective" and "definite". Some, such as the International Committee of the Red Cross (ICRC), define them very narrowly. According to the ICRC Commentary on the Protocol, effective contribution includes objects "directly used by the armed forces" (e.g. weapons and equipment), locations of "special importance for military operations" (e.g. bridges), and objects intended for use or being used for military purposes.[47] As to "definite military advantage". the Commentary excludes attacks that offer only a "potential or indeterminate" advantage.[48] By contrast, the United States, which does not dispute the

44 Additional Protocol I, *op. cit.* (note 10), Art. 43(1)-(2).

45 *Ibid.*, Art. 52(2).

46 Indeed, the Commentary states that: "The text of this paragraph certainly constitutes a valuable guide, but it will not always be easy to interpret, particularly for those who have to decide about an attack and on the means and methods to be used". Additional Protocols: Commentary, *op. cit.* (note 21), para. 2016.

47 *Ibid.*, paras 2020-23.

48 *Ibid.*, para. 2024.

wording of the definition, would include economic targets that "indirectly but effectively support and sustain the enemy's war-fighting capability", a particularly expansive interpretation.[49]

This difference has interesting implications for computer network attack. Can a banking system be attacked because wealth underpins a military's sustainability? What about the ministry responsible for taxation? The stock market? Are attacks on brokerage firms acceptable because they will undermine willingness to invest in the economy? If a country disproportionately relies on a particular industry to provide export income (e.g. oil), can computer network attack be used to disrupt production and distribution? The issue of striking economic targets is a particularly acute one because the operation of most is computer-intense in nature and hence very appealing to information warfare targeteers.

The threshold issue, to revert to the discussion above, is whether or not the attack would cause injury, death, damage or destruction. Once this determination is made, the differing interpretations of military objective would come into play, in all likelihood leading to disparate results on the legitimacy of striking the target. On the other hand, if the operation were designed to cause, for example, mere incon-venience, it would not rise to the level of an attack and would thus be permissible regardless of the target's nexus, or lack thereof, to military operations. For instance, if the Serbian State television station had been targeted by CNA rather than kinetic weapons during NATO strikes on Belgrade in April 1999, there might well have been no consequent injury, death, damage or destruction. In that circumstance, criticism on the basis that a civilian target had been hit would probably have fallen on deaf ears and thereby avoided the resulting

49 US Navy/Marine Corps/Coast Guard, *The Commander's Handbook on the Law of Naval Operations* (NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7), para 8.1.1 (1995), reprinted as an annotated version in *US Naval War College's International Law Studies series*, Vol. 73 (hereinafter Handbook). This assertion is labelled a "statement of customary international law". The Handbook cites General Counsel, Department of Defense, Letter of 22 September 1972, *reprinted in American Journal of International Law*, Vol. 67, 1973, p. 123, as the basis for this characterization.

negative publicity, as well as the litigation in the European Court of Human Rights.[50]

Civilians and civilian objects

Civilians are those persons who are not considered combatants,[51] whereas a civilian object is one that is not a military objective.[52] The prohibition on attacking civilians and civilian objects is nearly absolute. Specifically, Additional Protocol I stipulates:

> Article 51(2) "The civilian population as such, as well as individual civilians shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."
>
> Article 52 "Civilian objects shall not be the object of attack or of reprisals."[53]

Doubts as to the character of an object or individual are to be resolved in favour of a finding of civilian status.[54] Again, in the case of computer network attack, the threshold question is whether or not the attack is intended to, or foreseeably will, cause injury, death, damage or destruction; if so, the prohibitions set forth earlier, which undeniably restate existing customary law, apply.

Unfortunately, the norms, albeit clear at first sight, are subject to interpretative difficulties. The differing standards for distinguishing civilian objects from military objectives have already been highlighted. Similar disparities exist with regard to when a civilian may be attacked. Additional Protocol I allows for this possibility only

50 *Bankovic & Others v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom*, ECHR, App. No. 52207/99 (2001). In its decision of 12 December 2001, the Court found the application inadmissible.

51 Additional Protocol I, *op. cit.* (note 10), Art. 50(1).

52 *Ibid.*, Art. 52(1).

53 *Ibid.*, Art. 51(2) and 52. The Statute for the International Criminal Court also prohibits the direct targeting of civilians or civilian objects. Rome Statute for the International Criminal Court, Art. 8(2)(b)(i) and (ii), UN Doc. A/Conf. 183/9, July 17, 1998, at Annex II (hereinafter Rome Statute), reprinted in *International Legal Materials*, Vol. 37, p. 999 (1998) and M. Cherif Bassiouni, *The Statute of the International Criminal Court: A Documentary History*, Transnational Publishers, New York, 1999, p. 39.

54 *Ibid.*, Arts 50(1) (for civilians) and 52(3) (for civilian objects).

in the case of a civilian taking a "direct part in hostilities", a standard described in the Commentary as "acts of war which by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces".[55] This is the illegal combatant problem. Some would limit civilian immunity even more severely by, for instance, characterizing mission-essential civilians working at a base during hostilities, though not engaged directly in acts of war, as legitimate targets.[56]

In the context of information operations, the civilian issue is an important one. Some countries have elected to contract out information warfare functions, whether those functions involve the maintenance of assets or the conduct of operations. Moreover, computer network attack is a function that may be tasked to government agencies other than the military. In the event of civilian contractors or non-military personnel being in a support role that is essential to the conduct of operations, for instance maintaining CNA equipment, by the latter interpretation they would be directly targetable. Further, because they are valid targets, any injury caused them would not be calculated when assessing whether an attack is proportional (see discussion above). On the other hand, narrowly applying the "direct part in hostilities" standard would preserve the protection they enjoy as civilians, though if captured they would be entitled to prisoner-of-war status as persons "accompanying the armed forces".[57]

Should civilians engage in a computer network attack themselves, the problem becomes more complex. If the CNA results, or foreseeably could result, in injury, death, damage or destruction, then the "perpetrators" would be illegal combatants. This status attaches because they have taken a direct part in hostilities without complying with the criteria for characterization as a combatant. As illegal combatants, they may be directly attacked, any injury suffered by them would be irrelevant in a proportionality calculation, and in

55 *Ibid.*, Art. 51(3); Additional Protocols: Commentary, *op. cit.* (note 21), para. 1944.

56 Letter from DAJA-IA to Counselor for Defense Research and Engineering (Economics), Embassy of the Federal Republic of Germany (22 January 1988), cited in W.H. Parks, "Air War and the Law of War", *Air Force Law Review*, Vol. 32, 1992, p. 1.

57 GC III, *op. cit.* (note 14), Art. 4(4).

the event of their capture they would not be entitled to prisoner-of-war status.

Conversely, if the civilians involved were conducting computer network operations that did not reach the level of "attacks", they would not be illegal combatants because they would have committed no "acts of war that by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces". Their civilian status and its corresponding protections would remain intact. Nevertheless, as with support personnel, if attached to a military unit and accompanying that unit these civilians would be classed as prisoners of war.[58] Of course, the facility and equipment being used to conduct the operations might well be valid military objectives and, as a result, be subject to attack; but the operators themselves could not be directly attacked.

As should be apparent, the use of civilians, whether contractors or government employees, is fraught with legal pitfalls. Clearly, a prudent approach would be to employ military personnel for information warfare purposes.

Dual-use objects

A dual-use object is one that serves both civilian and military purposes. Examples of common dual-use objects (or objectives) include airports, rail lines, electrical systems, communications systems, factories that produce items for both the military and the civilian population and satellites such as INTELSAT, EUROSAT and ARABSAT, etc. If an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack. This is true even if the military purposes are secondary to the civilian ones.

Several caveats are in order. First, whether or not an object is a military objective may turn on whether the narrow or broad definition of the term, a matter discussed above, is used. Second, whether an object is dual-use, and therefore a military objective, will depend on the nature of the specific conflict. An airfield may be utilized for logistics purposes in one conflict, but serve no military function in another.

58 *Ibid.*

Third, an object that has the potential for military usage, but is currently used solely for civilian purposes, is a military objective if the likelihood of military use is reasonable and not remote in the context of the particular conflict under way. Finally, dual-use objects must be carefully measured against the requirements of discrimination and proportionality, discussed above, because by definition an attack thereon risks collateral damage and incidental injury to civilians or civilian objects.

Specifically protected objects

In addition to the general rules regarding the protection of the civilian population, certain objects enjoy specific protection. A controversial category of specially protected objects is dams, dykes and nuclear electrical generating stations. Because of their reliance on computers and computer networks, such facilities are especially vulnerable to CNA. Article 56 of Additional Protocol I, a provision opposed by the United States, forbids an attack on these facilities if the attack might "cause the release of dangerous forces [e.g. water or radioactivity] and consequent severe losses among the civilian population".[59] This prohibition applies even if they are military objectives. Interestingly, CNA offers a fairly reliable means of neutralizing such facilities without risking the release of dangerous forces, a difficult task when using kinetic weapons.

Conducting attacks that starve the civilian population or otherwise deny it "indispensable objects",[60] even if enemy armed

59 Additional Protocol I, *op. cit.* (note 10), Art. 56(1). This prohibition extends to attacks on other military objectives in their vicinity if the attack might cause such a release. There are exceptions to the general prohibition of the article.

"2. The special protection against attack provided by paragraph 1 shall cease:

(a) for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;

(b) for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;

(c) for other military objectives located at or in the vicinity of these works or installations 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."

Ibid., Art. 56(2).

60 *Ibid.*, Art. 54(2). See also Rome Statute, *op. cit.* (note 53), Art. 8(2)(b)(xxv).

forces are the intended "victims", is prohibited.[61] Indispensable objects include such items as foodstuffs, crops, livestock or drinking water. Under this restriction, computer network attacks against, for instance, a food storage and distribution system or a water treatment plant serving the civilian population would not be permissible even if military forces also rely on them.

Additional Protocol I furthermore prohibits military operations likely to cause widespread, long-term and severe damage to the environment,[62] although the United States does not recognize the provision as a restatement of customary law. Computer network attacks might conceivably cause such devastation. An attack on a nuclear reactor could result in a meltdown of its core and consequent release of radioactivity. Similarly, CNA could be used to release chemicals from a storage or production facility or rupture a major oil pipeline. Many other possibilities for causing environmental damage through CNA exist. It is important to note that the prohibition applies regardless of whether or not the attack is targeted against a valid military objective and even if it complies with the principle of proportionality. Once the requisite quantum of damage is expected to occur, the operation is prohibited.

Finally, it must be noted that there are a number of other objects, persons and activities that enjoy special protected status and are susceptible to computer network attack, but do not present unique CNA opportunities or challenges. These should be handled during the targeting cycle in the same manner as they would be in the planning

61 Additional Protocols: Commentary, *op. cit.* (note 21), para. 2110. However, the prohibition does not apply to objects used solely for the sustenance of enemy forces or "in direct support of military action". Additional Protocol I, *op. cit.* (note 10), Art. 54(3). An example of the latter would be an agricultural area used for cover by military forces.

62 *Ibid.*, Arts 35(3) and 55. See also Rome Statute, *op. cit.* (note 53), Art. 8(2)(b)(iv). On the issue of environmental damage during armed conflict, see Jay E. Austin and Carl E. Bruch (eds), *The Environmental Consequences of War: Legal, Economic, and Scientific Perspectives*, Cambridge University Press, Cambridge, 2000; Michael N. Schmitt, "Green War: An Assessment of the Environmental Law of International Armed Conflict", *Yale Journal of International Law*, Vol. 22, 1997, pp. 1-109; Richard J. Grunawalt, John E. King and Ronald S. McClains (eds), *Protection of the Environment during Armed Conflict and other Military Operations*, US Naval War College International Law Studies, Vol. 69, 1996.

of kinetic attacks.[63] In addition, there are limitations on striking certain objects or individuals in reprisal, including reprisals by computer network attack.[64]

63 For example, military and civilian medical units and supplies are exempt from attack unless being used for military purposes. Additional Protocol I, *op. cit.* (note 10), Art. 12. There are specific criteria for the extension of protection to civilian facilities. *Ibid.*, Art. 12(2). See also Rome Statute, *op. cit.* (note 53), Art. 8(2)(b)(ix) and (xxv). Medical transport enjoys similar protection. Additional Protocol I, *op. cit.*, Arts 21-31. The extent of the protection varies, depending on the category of transportation and its location. Other objects enjoying protection include cultural objects, places of worship and civil defence shelters, facilities and material. *Ibid.*, Arts 53 and 62(3). In addition, humanitarian relief activities must not be interfered with. *Ibid.*, Art. 70. Special provisions as to when such operations are entitled to the protection apply. Rome Statute, *op. cit.* (note 53), Art. 8(2)(b)(iii). By these prohibitions, for example, a computer network attack to alter blood type information in a hospital's data bank, deny power to a bomb shelter or œmisroute humanitarian relief supplies would all be unlawful. Of course, misuse of protected items or locations for military purposes renders them valid military objectives that may be attacked.

64 Reprisals are otherwise unlawful actions taken during armed conflict in response to an adversary's own unlawful conduct. They must be designed solely to cause the adversary to act lawfully, be preceded by a warning (if feasible), be proportionate to the adversary's violation, and cease as soon as the other side complies with the legal limitations on its conduct. The right to conduct reprisals has been severely restricted in treaty law, much of which expresses customary law. There are specific prohibitions on reprisals conducted against civilians; prisoners of war; the wounded, sick and shipwrecked; medical and religious personnel and their equipment; protected buildings, equipment and vessels; civilian objects; cultural objects; objects indispensable for the survival of the civilian population; works containing dangerous forces; and the environment. GC I, *op. cit.* (note 14), Art. 46; GC II, *op. cit.* (note 14), Art. 47; GC III, *op. cit.* (note 14), Art. 13; GC IV, *op. cit.* (note 14), Art. 33; Additional Protocol I, *op. cit.* (note 10), Arts 20, 51-56. In fairness, it should be acknowledged that certain countries argue that the Additional Protocol I restrictions on reprisals fail to reflect customary law. The United States, while accepting that most reprisals against civilians would be inappropriate (and illegitimate), asserts that the absolute prohibition thereon "removes a significant deterrent that presently protects civilians and other war victims on all sides of the conflict". Soafer, *op. cit.* (note 28), p. 470. For the official US position on reprisals against civilians, see Handbook, *op. cit.* (note 49), paras 6.2.3 and 6.2.3.1-3. The United Kingdom issued a reservation on precisely the same point when it became party to the Protocol. Reprinted on the International Committee of the Red Cross Treaty Database website, ‹http://www.icrc.org/ihl›. For these and other countries that have adopted this position, reprisatory computer network attacks are issues of policy, not law.

Limits on striking legitimate targets

The core prescriptions on striking legitimate targets are based on the principle of discrimination.[65] It is this principle which most clearly expresses humanitarian law's balancing of State-centric interests in resorting to force against the more broadly based human interest in shielding non-participants from the effects of what is, at best, an unfortunate necessity.

The discrimination requirement is twofold. Applied to weapons, it prohibits the use of those that are incapable of distinguishing between combatants and military objectives on the one hand and civilians, civilian objects and other protected entities on the other. Applied to tactics and the use of weapons, it requires that an effort be made to distinguish between these two categories, civilian and military, when conducting military operations. Additional Protocol I articulates this difference in Article 51(4):

> "Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction."

Subparagraph (a) refers to indiscriminate use, whereas (b) and (c) describe indiscriminate weapons or tactics. The indiscriminate use aspect of discrimination consists of three related components — distinction, proportionality, and minimizing collateral damage and incidental injury.[66]

65 For a comprehensive review of the principle, see Esbjörn Rosenblad, *International Humanitarian Law of Armed Conflict: Some Aspects of the Principle of Distinction and Related Problems*, Henry Dunant Institute, Geneva, 1979.

66 This typology is adopted from Christopher Greenwood, "The Law of Weaponry at the Start of the New Millennium", in Michael N. Schmitt and Leslie C. Green (eds), *The Law of Armed Conflict: Into the Next Millenium*, Naval War College, Newport, RI, 1998, p. 185; also published in *US Naval War College International Law Studies*, Vol. 71, 1998. By contrast, the US Air Force employs the categories of military necessity, humanity and chivalry, with proportionality folded into necessity, whereas the US Navy uses

Indiscriminate weapons

Computer network attacks are mounted by a weapon system consisting of a computer, a computer code and a means by which that code is transmitted. Obviously, the computer itself is not indiscriminate for it can very discreetly send code to particular computers and networks. The sending of e-mail is an apt example. By contrast, code can be written that is very, perhaps intentionally, indiscriminate. The classic example is a virus that passes, free of any control by its originator, from computer to computer. Because the code, even if it is an uncontrollable virus, can be targeted at particular military objectives, it is not indiscriminate on the ground that it cannot be directed. However, such code may be indiscriminate in that its *effects* cannot be limited. In many cases, once a viral code is launched against a target computer or network, the attacker will have no way to limit its subsequent retransmission. This may be true even in a closed network, for the virus could, for instance, be transferred into it by diskette. Simply put, a malicious code likely to be uncontrollably spread throughout civilian systems is prohibited as an indiscriminate weapon.

Care must be taken not to overstate the restriction. Note that Article 51(4) cites "methods and means of combat". A means of combat is defined in the Commentary on Additional Protocol I as a "weapon", whereas a method of combat is the way in which a weapon is used.[67] The plain meaning of "weapon" is something that can be used to *attack* an adversary. From the above analysis of the humanitarian law term "attacks" it follows that computer code is part of a weapon system only when it can cause the effects encompassed by that term — injury, death, damage and destruction (including related effects such as severe mental suffering, terror, etc.). In the event it cannot, it is not part of a weapon system, and thus would not be prohibited, at least not on the ground that it is indiscriminate.

necessity, humanity and chivalry. Compare Department of the Air Force, *International Law: The Conduct of Armed Conflict and Air Operations*, AF Pamphlet 110-31, 1976, at 1-5 – 1-6 with Handbook, *op. cit.* (note 49), para. 5-1.

67 Additional Protocols: A Commentary, *op. cit.* (note 21), para. 1957.

Distinction

The principle of distinction, unquestionably part of customary humanitarian law, is set forth in Additional Protocol I, Article 48: "[T]he Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives". Whereas the prohibition of direct attacks on civilians rendered a specific category of potential targets off-limits, the distinction requirement extends protection to cases in which an attack may not be directed against civilian or civilian objectives specifically, but in which there is a high likelihood of striking them nonetheless. An example would be firing a weapon blindly, although that weapon is capable of being aimed.

This is a particularly relevant prohibition in the context of computer network attack. For example, it would embrace situations where it is possible to discreetly target a military objective through a particular means of CNA, but instead a broad attack likely to affect civilian systems is launched. Such an attack would be analogous to the Iraqi SCUD missile attacks against Saudi and Israeli population centres during the 1990-91 Gulf War.[68] The SCUD is not an inherently indiscriminate weapon. Indeed, it is easily capable of being aimed with sufficient accuracy against, for instance, military formations in the desert. However, the use of SCUDS against population centres was indiscriminate even if the Iraqi intent was to strike military objectives situated therein; the likelihood of striking protected persons and objects so outweighed that of hitting legitimate targets that the use was inadmissible. Given the interconnection of computer systems today, computer network attacks could readily be launched in an analogous fashion.

Proportionality

Scienter distinguishes the principle of proportionality from that of distinction. Distinction limits direct attacks on protected persons or objects and those in which there is culpable disregard for

68 On the attacks, see US Department of Defense, "Conduct of the Persian Gulf War", Title V Report to Congress, 1992, p. 63, reprinted in 31 *International Legal Materials*, 1992, p. 612.

civilian consequences. Conversely, proportionality governs those situations in which harm to protected persons or objects is the foreseeable consequence of an attack, but not its intended purpose. The principle is most often violated (sometimes in an unintended but culpably negligent fashion) as a result of: 1) lack of sufficient knowledge or understanding of what is being attacked; 2) an inability to surgically craft the amount of "force" being applied against a target; and 3) the inability to ensure the weapon strikes the intended target with complete accuracy.[69] All three pitfalls could be encountered in the context of computer network attack.

As set forth in Additional Protocol I, an attack is indiscriminate as violating the principle of proportionality when it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[70] A concrete and direct advantage is "substantial and relatively close[;] ... advantages which are hardly perceptible and those which would only appear in the long term should be disregarded".[71] Moreover, the advantage calculated is that resulting from the overall operation, not the individual attack itself.[72]

Basically, the principle of proportionality calls for striking a balance — a task that is especially difficult to accomplish because differing entities (suffering and damage v. military advantage) are being

69 An expanded discussion is in Michael N. Schmitt, "Bellum Americanum: The US View of Twenty-First Century War and its Possible Implications for the Law of Armed Conflict", *Michigan Journal of International Law*, Vol. 19, 1998, p. 1051, pp. 1080-81.

70 Additional Protocol I, *op. cit.* (note 10), Arts 51(5)(a) and 57(2)(a)(iii) and (b). On proportionality, see William J. Fenrick, "The Rule of Proportionality and Protocol Additional I in Conventional Warfare", *Military Law Review*, Vol. 98, 1982, p. 91; Judith G. Gardam, "Proportionality and Force in International Law", *American Journal of International Law*, Vol. 87, 1993, p. 391.

71 Additional Protocols: A Commentary, *op. cit.* (note 21), para. 2209.

72 A number of understandings/declarations/reservations have been issued on this point by parties to the Protocol. For instance, the United Kingdom made the following reservation when ratifying Additional Protocol I in 1998: "In the view of the United Kingdom, the military advantage anticipated from an attack is intended to refer to the advantage anticipated from the attack considered as a whole and not only from isolated or particular parts of the attack". ICRC website, *op. cit.* (note 64).

weighed against each other without a common system of valuation.[73] Complicating matters is the fact that the answers to these and similar questions, assuming that there are any "right" answers, are contextual because the military advantage resulting from an attack always depends on the state of hostilities at the time.[74] Acknowledging the difficulty of putting principle into practice, the Commentary on Additional Protocol I notes that "[p]utting these provisions into practice... will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population".[75]

Further complicating matters is the issue of knock-on effects, i.e. those effects not directly and immediately caused by the attack, but nevertheless the product thereof — it is the problem of the effects caused by the effects of an attack. The most cited example is that of the attack on the Iraqi electrical grid during the 1990-91 Gulf War. Although it successfully disrupted Iraqi command and control, the attack also denied electricity to the civilian population (a "first-tier" effect), thereby affecting hospitals, refrigeration, emergency response, etc. Similarly, when NATO struck at Yugoslavia's electrical supply network during Operation "Allied Force", one consequence was to shut down drinking water pumping stations.[76] Such attacks gave rise, as a knock-on effect, to "second-tier" suffering of the population. Obviously, precisely the same effects could have resulted had the attacks been conducted through CNA. Indeed, the problem of knock-

73 For instance, how should civilian passenger lives be weighed against military aircraft in a computer network attack on an air traffic control system? How much human suffering is acceptable when shutting down an electrical grid that serves both military and civilian purposes? Can computer network attacks be conducted against telecommunications if they result in degrading emergency response services for the civilian population?

74 An additional problem is that the valuation process itself is complex. For instance, culture may determine the value placed on an item or the value of an item may shift over time. The issue of valuation paradigms is explored, in the context of environmental damage during armed conflict, more fully in Michael N. Schmitt, "War and the Environment: Fault Lines in the Prescriptive Landscape", *Archiv des Völkerrechts*, Vol. 37, 1999, p. 25.

75 Additional Protocols: Commentary, *op. cit.* (note 21), para. 1978.

76 "NATO Denies Targeting Water Supplies", BBC World Online Network, 24 May 1999, ‹http://www.news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm›.

on effects looms much larger in computer network attacks than in kinetic attacks owing to the interconnectivity of computers, particularly between military and civilian systems.

Knock-on effects have a bearing on proportionality analysis because they must be considered when balancing collateral damage and incidental injury against military advantage. Unfortunately, when caused by computer network attack such damage and injury, whether direct or indirect, are difficult to assess without knowing how the computer systems involved function and to which other systems they are linked. Despite this obstacle, planners and decision-makers have an affirmative duty to attempt to avoid collateral damage and incidental injury whenever feasible, a duty that necessarily implies an effort to ascertain the damage or injury likely to result from an attack.[77] Given the complexity of computer network attack, the high probability of an impact on civilian systems and the relatively low understanding of its nature and effects on the part of those charged with ordering the attacks, computer experts will have to be available to assess potential collateral and incidental effects throughout the mission-planning process.[78] Additionally, modelling and simulation, like those already conducted for nuclear weapons, would prove invaluable in identifying possible knock-on effects; to conduct them prior to the outbreak of hostilities — free from the fog, friction and pace of war — would be well advised.

Minimizing collateral damage and incidental injury

The determination of proportionality establishes whether a military objective may be attacked at all. However, even if the selected target is legitimate and the planned attack thereon would be proportional, the attacker has an obligation to select that method or means of warfare likely to cause the least collateral damage and incidental injury, all other things being equal (such as risk to the forces conducting the attack, likelihood of success, weapons

77 See generally Additional Protocol I, *op. cit.* (note 10), Art. 57.

78 The US Joint Warfare Analysis Center, headquartered at Naval Surface warfare Center, Dahlgren, Va., is currently engaged in modelling foreign infrastructures and contingent outcomes.

inventory, etc.).[79] Furthermore, whenever a choice is possible between military objectives that can be attacked to achieve a desired result, the attack which carries the lowest risk of collateral damage and incidental injury must be chosen.[80]

The availability of computer network attack actually increases the options for minimizing collateral damage and incidental injury. Whereas in the past physical destruction may have been necessary to neutralize a target's contribution to the enemy's efforts, now it may be possible to simply "turn it off". For instance, rather than bombing an airfield, air traffic control can be interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth. Those who plan and execute such operations must still be concerned about collateral damage, incidental injury and knock-on effects (consider the Iraqi electric grid example above), but the risks associated with conducting classic kinetic warfare are mitigated significantly through CNA. Also, depending on the desired result, it may be possible to simply interrupt operation of the target facility. This tactic would be particularly attractive in the case of dual-use objectives. Consider an electrical grid. It might only be militarily necessary to shut the system down for a short period, for example immediately preceding and during an assault. The system could be brought back on track as soon as the pressing need for its suspension is over, thereby limiting the negative effects on the civilian population. Similarly, because targets are not physically damaged and thus do not need to be repaired or rebuilt, the civilian population's return to normalcy at the end of the conflict would be facilitated.

Perfidy

Although the core normative constraints on computer network attack derive from the principle of discrimination, several other related aspects of humanitarian law are brought into play by this new means of warfare. One is the prohibition on perfidy. Perfidy is the feigning of protected status in order to take advantage of an adversary. Examples include pretending to be wounded or sick or have non-

79 *Ibid.*, Art. 57(2)(a).

80 Ibid., Art. 57(3).

combatant status, or surrendering and improperly displaying symbols that signify protected status, such as the red cross or red crescent. Perfidy is distinguished from ruses, which are acts intended to mislead an adversary and cause him to act recklessly, but which do not involve false claims of protected status. Ruses are lawful.

Information warfare, including computer network attack, offers many opportunities for ruses and perfidy. This is because both techniques are intended to convey false... information. For instance, lawful ruses might include transmitting false data, meant to be intercepted by an adversary, about troop deployment or movements. Alternatively, it might involve altering data in an adversary's intelligence databases, sending messages to enemy headquarters purporting to be from subordinate units, or passing instructions to subordinate units that appear to be from their headquarters.[81] All such activities would be perfectly legitimate.

On the other hand, any action intended to mislead the enemy into believing that one's forces enjoy protected status and thereby enable them to kill, injure or capture the enemy would be illegitimate.[82] For instance, medical units and transports may use codes and signals established by the International Telecommunications Union, the International Civil Aviation Organization, and the International Maritime Consultative Organization to identify themselves.[83] Falsely transmitting such codes/signals or, a more likely prospect in the computer network attack context, causing adversary systems to reflect receipt of such signals would be clear examples of perfidy. The US Department of Defense has also opined that using

81 Article 39 prohibits the use of the enemy's military emblems, insignia or uniforms. This prohibition, which the United States disagrees with except when it occurs during the actual engagement (see Handbook, *op. cit.* [note 49], para 12.1.1, fn 2), does not extend to the use of codes, passwords and the like. Micheal Bothe, Karl J. Partsch and Waldermar A. Solf, *New Rules for Victims of Armed Conflicts*, M. Nijhoff, The Hague, 1982. However, Article 38 prohibits the misuse of protective signals.

82 Additional Protocol I, *op. cit.* (note 10), Art. 37. See also Rome Statute, *op. cit.* (note 53), Art. 8(2)(b)(vii) and (xi). Convention (IV) respecting the Laws and Customs of War on Land, October 18, 1907, annexed Regulations, Art. 23(b)7, 36 Stat. 2277, 205 Consolidated Treaty Series 277, reprinted in Roberts and Guelff, *op. cit.* (note 10), p. 73, prohibits treacherous killing.

83 Additional Protocol I, *op. cit.* (note 10), Annex, Art. 11.

"computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed" would be a war crime if false.

Conclusion

By and large, existing humanitarian prescriptive norms suffice to maintain the protection civilians, civilian objects and other protected entities enjoy. However, certain novel aspects of CNA do pose new and sometimes troubling quandaries. The unease over the use of cyber warfare during NATO's campaign against Yugoslavia in 1999 is compelling evidence that the question of how humanitarian law bears on CNA remains unsettled.[84]

First, in order to apply extant norms to CNA, it is necessary to accept various interpretative premises. Most important are the consequence-based interpretations of "armed conflict" and "attack". In the absence of such understandings, the applicability, and therefore adequacy, of present-day humanitarian law principles would come into question. Interestingly, consideration of computer network attack in the context of *jus ad bellum* also leads to consequence-based interpretation.[85]

Second, even if the parameters resulting from the suggested interpretations are accepted, normative lacunae exist. Most notably, attacks against civilians and civilian objects that do not injure, kill, damage or destroy (or otherwise produce the requisite level of suffering) are on the whole permissible. Given that kinetic attacks usually have such effects, civilians and civilian objects enjoy broad protection during conventional military operations. However, computer network attack, because it may not amount to an *attack*, opens up many possibilities for targeting otherwise protected persons and objects. The incentive for conducting such operations grows in relation to the extent to which the "war aims" of the party conducting the CNA are coercive in nature; the desire, for instance, to "turn out the lights" for a

84 For a description of hesitancy to use CNA during Operation "Allied Force", see Bradley Graham, "Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia", *Washington Post*, 8 November 1999, p. A1.

85 See Schmitt, "Computer Network Attack", *op. cit.* (note 7).

civilian population in order to motivate it to pressure its leadership to take, or desist from taking, a particular course of conduct (a step suggested by NATO's air commander during Operation "Allied Force") will grow as the means for doing so expand.[86] The absence of kinetic effects almost invites usage.

In humanitarian terms, this is to a great extent a negative reality. Some computer network attacks may not amount to an "attack" — but some surely will. The mere fact that a target can be "attacked" in other than a kinetic fashion does not mean that humanitarian law norms are inapplicable. Civilians and civilian objects continue to enjoy protected status vis-à-vis those aspects of CNA that cause human suffering and physical damage. Moreover, even when conducting computer network attacks against military objectives, the principle of proportionality continues to safeguard civilians and civilian objects from injury and damage that is excessive in relation to the military advantage. For instance, turning off the electricity to a city to disrupt enemy command, control and communications may be acceptable if doing so does not cause excessive civilian suffering. However, if the operation is directed at other than a military objective, the sole issue is whether any harm caused reaches the level of an "attack". If so, the CNA is prohibited.

Third, and more encouraging, is the fact that CNA may make it possible to achieve desired military aims with less collateral damage and incidental injury than in traditional kinetic attacks. Indeed, military commanders will in certain cases be obligated to employ their cyber assets in lieu of kinetic weapons when collateral

86 Consider the comment of Lieutenant General Michael Short, USAF, who commanded the air war during Operation "Allied Force":

> "I felt that on the first night, the power should have gone off, and major bridges around Belgrade should have gone into the Danube, and the water should be cut off so that the next morning the leading citizens of Belgrade would have got up and asked, 'Why are we doing this?' and asked Milosevic the same question."

Craig R. Whitney, "The Commander: Air Wars Won't Stay Risk-Free, General Says", *The New York Times*, 18 June 1999, p. A1.

and incidental effects can be limited.[87] That said, it will be critically important to carefully analyse the effects of such operations, particularly their knock-on effects, when assessing an attack's compliance with the principle of proportionality. This will require planning, legal and computer experts to operate in concert throughout the targeting cycle.[88]

Finally, much as CNA challenges existing notions of "attack", it will also test traditional understanding of combatant status because of the use of typically civilian technology and know-how to conduct military operations via computer. Failure to strictly comply with the limitations on the participation of civilians in hostilities will inevitably lead to heightened endangerment of the civilian population and weaken humanitarian law norms.

So the jury remains out. While humanitarian law in its present form generally suffices to safeguard those it seeks to protect from the effects of computer network attack, and even though it offers the promise of periodically enhancing such protection, significant prescriptive faultlines do exist. Therefore, as capabilities to conduct computer network attacks increase in terms of both sophistication and availability, continued normative monitoring is absolutely essential. We must avoid losing sight of humanitarian principles, lest the possible in warfare supplant the permissible.

●

87 Additional Protocols: Commentary, *op. cit.* (note 21), para. 1871, notes that "it is the duty of Parties to the conflict to have the means available to respect the rules of the Protocol. In any case, it is reprehensible for a Party possessing such means not to use them, and thus consciously prevent itself from making the required distinction."

88 A typical Information Operations cell is illustrated in JP 3-13, *op. cit.* (note 2), at figure IV-4 and accompanying text. It includes an IO officer from J-3; representatives from J-2, 4, 5, 6, 7, supporting combatant commands, and service and functional components; a judge advocate; and public affairs, counterintelligence, civil affairs, targeting, special operations, special technical operations, electronic warfare, psychological operations, military deception and operations security experts.

Résumé

La guerre par le biais des réseaux de communication : les attaques contre les réseaux informatiques et le *jus in bello*

by MICHAEL N. SCHMITT

*La guerre de l'information s'annonce comme le nouvel outil révolutionnaire qui sera utilisé pour se battre dans les conflits armés. Une attaque contre les réseaux informatiques (*Computer Network Attack, *CNA) désigne toute opération visant à perturber, refuser, dégrader ou détruire l'information résidente dans les ordinateurs ou les réseaux informatiques. Dans les conflits armés internationaux, les ramifications de ce genre d'attaque peuvent se révéler considérables. Cet article examine le recours aux attaques contre les réseaux informatiques dans les conflits armés internationaux. Il analyse d'abord l'applicabilité du droit international humanitaire à ces attaques, puis les effets juridiques de cette branche du droit sur le recours à telles attaques comme moyens de combat. Certains estiment que, bien qu'il n'y ait pas en droit international humanitaire de règles explicites relatives aux attaques contre les réseaux informatiques et que ces attaques n'aient pas un caractère cinétique (en d'autres termes, ces attaques ne sont pas des attaques «armées»), le droit humanitaire s'applique néanmoins si l'on tient compte de ses objectifs sous-jacents, à savoir protéger les personnes qui ne participent pas directement aux hostilités et leurs biens. Quand les attaques contre les réseaux informatiques ont pour but ou risquent de mettre en danger des personnes ou des biens protégés, le droit humanitaire devient applicable, et ces attaques relèvent du* jus in bello. *En analysant la licéité du recours aux attaques contre les réseaux informatiques sous l'angle du droit international humanitaire, l'auteur met non seulement en lumière les questions juridiques fondamentales (et non résolues) relatives à ce type de guerre, mais il soulève aussi des questions essentielles telles que la définition d'un conflit armé et la capacité du droit international humanitaire de réglementer des méthodes et moyens de guerre nouveaux et intéressants d'un point de vue conceptuel.*