INTERNATIONAL HUMANITARIAN LAW RESEARCH INITIATIVE

COMPUTERS AND WAR: THE LEGAL BATTLESPACE

By

Michael N. Schmitt, Professor of International Law, George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany

Heather A. Harrison Dinniss, Ph.D. Candidate, London School of Economics and Political Science

Thomas C. Wingfield Director, Tyranny, Democracy, and Regime Change, Potomac Institute for Policy Studies, Arlington, Virginia

Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June 25-27, 2004

Program on Humanitarian Policy and Conflict Research at Harvard University
1033 Massachusetts Avenue Fourth Floor Cambridge, MA 02138 www.hsph.harvard.edu

HPCR

The use of computers in modern warfare stretches back over decades. Computers have been employed for functions that range from managing materiel and personnel flows into an area of operations to sorting intelligence data and improving the precision capabilities of weapons. In recent conflicts, however, we have witnessed their transformation into a "means of warfare" (weapon) and modern militaries are busily developing information technology "methods of warfare." This article briefly addresses the legal issues surrounding computer use in classic kinetic-based warfare. Attention then turns to the most significant phenomenon for humanitarian law, namely the employment of information technology during network-centric, four-dimensional operations, which increasingly characterize twentieth-first century conflict.[1]

Humanitarian law and the use of computers in classic warfare

Generally speaking, the use of computers to enhance the conduct of traditional military operations poses few novel legal issues. The one exception may be with regard to the "man-out-of-the loop" phenomenon. Information technology has made it increasingly possible for computers to carry out tasks previously performed by humans. Remotely-controlled unmanned Predator aircraft armed with Hellfire missiles have successfully attacked mobile ground targets in Afghanistan and Yemen.[2] In the near future, they may contain sensors that feed onboard computers with data about the characteristics (heat and electronic signatures, speed, and so forth) of potential targets. Those falling within set parameters would be automatically engaged.

A further example is the use of computers in the targeting cycle. Today, computers manage target lists, maintain target data, determine the optimal mission route and weapon, and calculate likely collateral damage and incidental injury. Although human beings remain deeply embedded in the decision process — especially when collateral damage or incidental injury — is likely, computers perform an ever-growing share of targeting functions. The "effects-based" targeting approach that is becoming prevalent in twentieth-first century warfare intensifies the trend, as computer modeling is a powerful tool in determining what to attack and how to achieve particular effects.[3]

Although some observers fear this trend may erode the protection humanitarian law provides civilians, civilian objects, and other specially protected persons and objects, humanitarian law has historically proven quite flexible in adapting to shifts in the methods and means of warfare. So it is likely to in this case. After all, it is not the presence of a human in the loop that is normatively determinative, but rather the extent to which new methods and means expose protected persons and objects to the risk of incidental injury and collateral damage.

Protocol Additional I, Article 57, sets forth the relevant law: "[T]hose who plan or decide upon attack shall…do everything feasible to verify that the objectives to be attacked are

---

[1] The discussion will inevitably be somewhat U.S.-centric, for American capabilities and doctrines in this areas have outpaced those of other states.

[2] In 2002, the CIA used a remotely-controlled Predator to attack a car carrying an alleged Al Qaeda senior operative in the Yemen, Qaed Senyan al Harthi. BBC News World Report, November 5, 2002.

[3] Effects-based targeting attempts to strike only those targets, and only in a way, that can achieve the precise effects that realize the commander's objectives. It is to be distinguished from attrition targeting. See Joint Staff, Joint Doctrine for Targeting, Joint Publication 3-60, January 17, 2002. See also Michael N. Schmitt, *Targeting and Humanitarian Law: Current Issues*, 33 *Israel Yearbook on Human Rights* (2003) at 59-104.

neither civilians nor civilian objects and are not subject to special protection but are military objectives." The article further requires that they "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians, and damage to civilian objects."[4] Although the United States and certain other nations are not Parties to the Protocol, most of its provisions are understood to reflect customary international law and, thus, bind non-Parties.[5]

If a computer-assisted method or means of warfare is more efficient or less costly than that which it replaces, but more likely to affect the civilian population, then the customary principle codified in Article 57 will have been violated. In most cases, however, computers boost the reliability of information feeding the decision and attack processes, thereby fostering humanitarian ends. One could argue that a state with the technological and financial wherewithal to field computer-assisted processes and equipment must do so to comply with the "all feasible" standard. To date, humanitarian law has not been interpreted as requiring states to include particular hardware in their inventory; it only requires use if such equipment is available, practical, and militarily sensible.

International (Humanitarian) Law in the Era of Information Warfare

It is use of computers as a means or method of warfare that is legally challenging. The typology is instructive. At the broadest level are information operations (IO), those "actions taken to affect adversary information and information systems while defending one's own information and information systems."[6] IO can occur during peacetime and at every level of warfare.[7]

"Information warfare" (IW), by contrast, is IO "conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries"[8]; it encompasses "attack and defend" functions. The United States Air Force sub-divides IW into its offensive counterinformation and defensive counterinformation aspects. Offensive IW embraces psychological operations, electronic warfare, military deception, physical attack, and information attack (computer network attack-CNA).[9] Ultimately, the goal of IW is to achieve dominant "information superiority" over the opponent.

---

[4] Protocol Additional (I) to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Article 57.2(a) (i and ii), December 12, 1977, 1125 U.N.T.S. 3, 16 *International Legal Materials* 1391 (1977), (hereinafter Protocol I).

[5] This article will cite points of disagreement when applicable. For a recent delineation of the United States' position, see U.S. Army, The Judge Advocate General's Legal Center and School, Law of War Handbook 23-24 (2004).

[6] Joint Chiefs of Staff, Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, April 12, 2001, at 203.

[7] Chairman, Joint Chiefs of Staff, Instruction 3121.01A, Standing Rules of Engagement, January 15, 2000, at encl. F-1, para. 1a.

[8] Joint Publication 1-02, supra note 6, at 203. The US Air Force usefully distinguishes IW from "information in warfare" (IIW), which extends to the "gain and exploit" functions of information warfare, such as intelligence, surveillance, reconnaissance, precision navigation, weather analysis, information collection and dissemination, and public affairs. U.S. Department of the Air Force, Air Force Doctrine Document 2.5, Information Operations, 5 August 1998, at 2-6.

[9] AFDD 2-5, supra, at 9-15. Defensive counterinformation operations include operations security and information assurance (computer and communications security), counterdeception, counterintelligence, counterpsychological operations, and electronic protection. Ibid. at 15-20.

It is offensive IW, especially CNA, which raises the most perplexing international law questions. The remainder of this article surveys those that military officers and civilian officials are most likely to encounter.

When does an information operation (or group of operations) rise to the level of a "use of force" under international law?

Article 2(4) of the United Nations Charter prohibits "the threat or use of force" in international relations. There are two exceptions in the Charter scheme: a use of force pursuant to a mandate issued by the Security Council in accordance with Article 42; and self-defense consistent with Article 51. The prohibition begs the question of the definition of a use of force. There are three schools of thought.

The first postulates that the use of force prohibition seeks to keep incidents that are below a certain threshold of violence from mushrooming into full-blown wars; it is not the *means* of attack that matters, it is the *amount* of damage done. It should be immaterial whether a power transmission sub-station is destroyed by a 2000-lb bomb or by a line of malicious code inserted into the sub-station's master control program.

The second approach, more popular in academic circles, takes the position that the Charter was meant to favor resolution of conflict by other than military means. Consistent with this approach, only an *armed attack* (a classic attack with traditional military forces) constitutes a use of force. It is the means of attack that matters.

A third approach, embraced by the authors, urges a case-by-case analysis that considers both the qualitative and quantitative aspects of an operation. In this method, the following criteria, albeit not exclusive, act as indicators of the extent to which the international community is likely to judge an information operation a use of force: severity of consequences; immediacy; directness; invasiveness; measurability; presumptive legitimacy; and responsibility.[10]

Holistically considering such factors allows an estimate of whether the operation in question — kinetic, cyber, or hybrid — will be viewed as generally above or below the "use of force" threshold. Furthermore, the approach renders areas of disagreement more transparent, thereby allowing the sharpening of the norm.

When can a state respond with armed force against the originator of an information warfare attack?

Article 51 permits states to engage in individual or collective self-defense in the face of an "armed attack." Most international lawyers accept the International Court of Justice's distinction in the *Nicaragua* case between a "use of force" under Article 2(4) (not all of them armed, e.g., equipping and training rebels) and an "armed attack" which activates the right of self-defense.[11] By this standard, an armed attack is a higher threshold, one that would typically require the direct causation of physical damage to property or injury to human

[10] These factors and the overall approach are described at length in Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 37 *Columbia Journal of Transnational Law* 885, 900-923 (1999) [hereinafter Schmitt, *CNA*].
[11] *Military and Paramilitary Activities* (Nicar. v. U.S.), 1986 I.C.J. 14, 118-19, para. 228 (June 27) (Merits). See generally John Norton Moore, *The Secret War in Central America* (1987).

beings.[12] This does not preclude states from responding to information operations that fall short of this level, but simply excludes the use of military force as a response option.

Naturally, those considering launching an information operation must understand that the meaning of "armed attack" will ultimately be determined by the target state. An attack against a "vital national interest," for example, the national banking system, might well cross that state's threshold even without causing direct damage or injury. In this sense, many of the same factors used to assess whether an operation is a "use of force" may also prove useful in estimating whether a particular operation will be characterized by the victim as a *de facto* armed attack.[13]

Finally, a very contentious international law issue involves acting in anticipation of an imminent attack. Using an information warfare operation to prepare the battlefield for a conventional attack that has been irrevocably decided upon (e.g., bringing down an air defense network) may be sufficient to merit a kinetic response. Beyond such obvious examples, however, the lack of a precise practical standard looms large.

Can information warfare alone initiate an armed conflict in which international humanitarian law applies?

A useful framework for this question is found in the International Committee of the Red Cross' 1949 Geneva Conventions *Commentary*, which defines armed conflict as "any difference arising between two states and leading to the intervention of members of the armed forces…It makes no difference how long the conflict lasts, or how much slaughter takes place."[14] The ICRC *Commentary* to Protocol Additional I adopts the same approach: "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…."[15]

Use of the military, however, is not determinative; if it were, a state could avoid application of humanitarian law simply by using forces other than the military to conduct violent attacks against an adversary. Rather, the reference to the armed forces must refer to the application of force, which in turn implies the causation (or intent to cause) of physical damage or human injury. Thus, to the extent a state-based information warfare attack causes such effects, humanitarian law applies. The one exception would be an operation with minimal, albeit damaging or injurious, results. This assertion is based on an extrapolation of the generally-accepted position that small raids or border incidents do not launch an armed conflict.[16]

---

[12] For an explanation of this analysis, see Schmitt, *CNA*, supra note 10, at 924-933.

[13] See generally Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," 38 *Stanford Journal of International Law* 207, 215-231 (2002).

[14] *Commentary: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* 32-33 (Jean Pictet ed., 1952). See also Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* 60-63 (Aegis Research Corp. 2000).

[15] *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949,* para. 62 (Yves Sandoz, Christophe Swinarki and Bruno Zimmerman eds., 1987) [hereinafter *Protocols Additional Commentary*].

[16] See discussion in Christopher Greenwood, "Historical Development and Legal Basis," in *The Handbook of Humanitarian Law in Armed Conflict* 1, 42 (Dieter Fleck ed., 1995).

Are computers lawful weapons in an armed conflict?

No specific prohibition exists regarding any weapon used in information warfare. Therefore, the legality of such weapons must be judged against the principles of distinction and unnecessary suffering, which have labelled the "cardinal principles" of humanitarian law by the International Court of Justice.[17]

The principle of distinction, codified in Article 51 of Protocol Additional I, prohibits "indiscriminate attacks." Included are attacks by any method or means of combat that "cannot be directed at a specific military objective" or "the effects of which cannot be limited" as required by humanitarian law (for instance, by discriminating between the civilian population and military objectives). An example of the former would be a weapon with a guidance system so rudimentary or unreliable that it could not confidently be targeted at a particular military objective. Biological weapons illustrate the latter because the contagions they release may spread unchecked to the civilian population.

A computer itself is in no way indiscriminate, for it can transmit code very directly. Code can be written, however, that spreads indiscriminately from computer to computer; indeed, most computer viruses are designed to operate in precisely this fashion. Even in a closed network, there is a high risk that malicious code could be transferred into external networks through, for instance, files contained on diskettes.

But when does a computer network attack amount to an "attack" under humanitarian law? The resolution of this issue has implications beyond the parameters of indiscriminate attack, for all humanitarian law targeting prohibitions are framed in terms of prohibitions or limitations on "attacks."

Pursuant to Article 49 of Protocol Additional I, attacks are "acts of violence against the adversary, whether in offence or in defense." The accent on violence, which is repeated elsewhere in the Protocol,[18] cannot be interpreted literally as being limited to acts involving physical force, for, as noted, there is universal acceptance of biological, chemical, and radiological operations as attacks. Rather, "violence" should be characterized as acts having violent *consequences*, specifically injury or death of humans and damage or destruction of physical property. Severe physical or mental suffering would certainly be included in the concept of injury.[19] Arguably, loss of intangible assets (e.g., funds held electronically in a banking system) that are directly transformable into tangible assets (e.g., currency or purchasable objects) could be encompassed in the meaning of property. The Protocol's articulation of the proportionality principle, which weighs military advantage against

---

[17] "Legality of the Threat or Use of Nuclear Weapons" (Advisory Opinion), 1996 I.C.J. 226 (July 8), 35 *International Legal Materials* 809, para. 78.

[18] E.g., Article 51, which provides that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations," and which prohibits "acts or threats of *violence* the primary purpose of which is to spread terror among the civilian population," as well as the commentary to 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." *Protocols Additional Commentary*, supra note 15, para. 1875 (emphasis added).

[19] A point supported by the prohibition on attacks intended to terrorize the civilian population in Protocol Additional I, supra note 4, Article 51.2.

"incidental loss of civilian life, injury to civilians [and] damage to civilian objects," reinforces this approach.[20]

By this interpretation, only information warfare weapons that place the civilian population at risk of such harm would violate the prohibition. Note that humanitarian law requires states to review the legality of new "weapons, means or methods," a requirement echoed in many domestic regulations.[21]

What can information warfare target legitimately during an armed conflict?

Humanitarian law only permits attacks on military objectives.[22] Indeed, the explicit prohibition on attacking civilian objects contained in Article 52 of Protocol Additional I tautologically defines a civilian object as "all objects that are not military objectives."[23]

Military objectives are objects which "by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[24] The resulting question for the commander or other decision-maker is how does a proposed information warfare action further on-going or imminent military operations or hinder those of the opponent. The proposed target will not constitute a legitimate military objective if the reasoning is tortuous or the contribution clearly indirect.

Unfortunately, disparate understandings of the term exist, even though all parties accept the formal articulation set forth in Protocol Additional I. The ICRC, for example, takes a minimalist approach, urging that "effective contribution" is to be understood as objects used or intended for use by the military and locations of "special importance for military operations."[25] It also excludes attacks that offer only a "potential or indeterminate" advantage from the scope of the term "definite military advantage."[26]

By contrast, the United States interprets military objectives expansively by including not only war-supporting targets, but also those that are "war-sustaining," such as economic targets not directly related to military functions. The classic example would be an industry that serves as the dominant source of export income for a country. To the extent that industry can be crippled, the enemy's ability to finance (sustain) its war efforts diminishes. Thus, whereas all would accept the legitimacy of launching computer network attacks against the enemy's military POL (petroleum, oil, lubricants) system, conducting the same attack against oil export assets would be controversial. This disagreement could extend to potential targets ranging from banking systems to broadcast facilities.

The term "military objectives" covers combatants, who therefore may be attacked[27] Combatants include both lawful combatants, such as members of the enemy armed forces,[28] and civilians who

---

[20] Protocol Additional I, supra note 4, Article 51.5(b) and 57.2(a)(iii). See also Rome Statute for the International Criminal Court, Article 8.2(b)(iv), U.N. Doc. A/Conf. 183/9, July 17, 1998, at Annex II, 37 *International Legal Materials* 999 (1998) [hereinafter Rome Statute].
[21] Protocol Additional I, supra note 4, Article 36. Department of Defense, Instruction 5000.2, Operation of the Defense Acquisition System, October 23, 2000, para. 4.7.3.1.4, requires weapons reviews for US forces.
[22] Protocol Additional I, supra note 4, Article 48.
[23] See also Rome Statute, supra note 20, Article 8.2(b)(ii).
[24] Protocol Additional I, supra note 4, Article 52.2.
[25] *Protocols Additional Commentary*, supra note 15, paras. 2020-23.
[26] Ibid., para. 2024.
[27] See discussion in Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* 84-85 (Cambridge, UK: Cambridge University Press, 2004).

take a "direct part in hostilities" (known as either "unlawful combatants" or "unprivileged belligerents").[29] Because combatants are military objectives, CNA could be used lawfully, for instance, to derail a troop train through manipulation of switching signals or cause an aircraft carrying replacements to crash by interfering with navigational guidance.

Finally, many potential information warfare targets are dual-use, i.e., used for both military and civilian purposes. Common examples include airports, rail systems, roads, communications (95 per cent of US Department of Defense communications use commercial sources), satellites, and factories that produce objects for use by both civilians and the military, such as computers. So long as they meet the definition of military objective, and the planned operation complies with the proportionality and precautions in attack requirements (see below), dual-use facilities are legitimate information warfare targets.

As with attack through any means, whether a potential target is a military objective depends not only on the definition (narrow vs. broad), but also on the context of the conflict. For instance, a civilian airfield far from the front in a highly localized conflict may not make an "effective contribution" to military action, while one closer to the battle might by virtue of its actual or potential military use. It should be noted that the facility need not necessarily be currently used for military purposes; the requirement is merely that such use be reasonably likely and that preventing use provides a "definite military advantage" to the attacker.

What objects or individuals enjoy special protection under humanitarian law?

Humanitarian law extends special protection to various objects that would otherwise be likely targets of an information warfare attack. Article 56 of Protocol Additional I forbids attacks on dams, dykes, or nuclear electrical generating stations if attack risks release of "dangerous forces," specifically water or radioactivity (paradoxically, information warfare may make it possible to attack such facilities without risk of release, for example by simply shutting down electrical generation).[30]

Protocol Additional I also proscribes attacks against "objects indispensable to the civilian population"[31] and operations likely to cause "widespread, long-term, and severe damage" to the natural environment.[32] Examples of potential information warfare targets barred by the former include food distribution networks and water treatment plants, whereas causing a massive toxic chemical spill through a CNA illustrates the latter.[33]

---

[28] As well as organized irregular forces under certain conditions. See Geneva Convention Relative to the Treatment of Prisoners of War, August 12, 1949, Article 4A, 6 U.S.T. 3316, 75 U.N. T.S. 135 [hereinafter GC III]; Protocol Additional I, supra note 4, Article 43.

[29] Pursuant to Protocol Additional I, supra note 4, Article 51.3, civilians are only protected 'for such time as they take a direct part in hostilities." See also Rome Statute, supra note 20, Article 8.2(b)(i). On this topic, see generally, Michael N. Schmitt, "Direct Participation in Hostilities and 21st Century Armed Conflict," in *Crisis Management and Humanitarian Protection* (Berlin: Berliner WissenschaftsVerlag, Horst Fischer et al. eds, 2004).

[30] The United States, a non-Party to the Protocol, does not accept this prohibition as customary international law.

[31] Protocol Additional I, supra note 4, Article 54. See also Rome Statute, supra note 20, Article 8.2(b)(xxv).

[32] Protocol Additional I, supra note 4, Articles 35.3 and 55. The articles take a slightly different approach. See generally, Michael N. Schmitt, "Green War: An Assessment of International Armed Conflict," 22 *Yale Journal of International Law* 1 (1977). See also Rome Statute, supra note 20, Article 8.2(b)(iv).

[33] The United States does not accept the Protocol restriction on environmental damage, preferring, instead, the proportionality principle as a means of protecting the environment.

Humanitarian law further restricts (either total prohibition or limitation) attacks against medical facilities, transports, and supplies;[34] cultural objects and places of worship; [35] and humanitarian relief efforts.[36] Moreover, in most cases, reprisals (engaging in a prohibited act in order to compel the other side to desist in such conduct) against protected persons or objects are banned, although the United States and certain other states take a narrow approach to the subject.[37]

What limitations are there on targeting lawful targets with information warfare?

Even if an information warfare operation targets a legitimate military objective, it is forbidden if disproportionate, i.e., "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."[38] This proportionality balancing test is undeniably one of the most difficult tasks for a commander during combat planning. The inherent difficulty derives from the unwieldy comparison of two dissimilar values that shift over time. For instance, what is the civilian suffering equivalent of an information warfare attack that effectively brings down an enemy electrical grid supporting command and control? At the beginning of a conflict, or, alternatively, at its end?

Collateral damage and incidental injury result typically from a lack of sufficient knowledge or understanding of what is being attacked; an inability to meter precisely the amount of force being applied against a target; or an inability to ensure the weapon strikes the intended target with complete accuracy. Although all three impact information warfare, the first is most troublesome. In particular, it occurs in the context of "knock-on effects," i.e., those generated by the initial effects of the attack. As an example, an attack on an electrical grid may disrupt water treatment, which in turn may affect sanitation and result in a health crisis for the affected population. The challenge is unravelling the complex connectivity within and between networks, and thereby estimating what the likely "knock-on" effects might be.

Occasionally, the suggestion is made that "knock-on" effects should be excluded altogether in proportionality calculations. Although treaty law is silent on this issue, most legal scholars assert that they are part of the proportionality analysis to the extent they

---

[34] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, Articles 19-23, 35-37 [hereinafter GCI]; Protocol Additional I, supra note 4, Articles 12-31. See also Rome Statute, supra note 20, Article 8.2(b)(ix).

[35] Protocol Additional I, supra note 4, Articles 53 and 62.3; Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240; Second Protocol to the Hague Convention of 1954 for Protection of Cultural Property in Event of Armed Conflict, 1996, 38 *International Legal Materials* 769 (1999). See also Rome Statute, supra note 20, Article 8.2(b)(ix).

[36] Protocol Additional I, supra note 4, Article 70. See also Rome Statute, supra note 20, Article 8(2)(b)(iii).

[37] GCI, supra note 34, Article 46; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, August 12, 1949, Article 47, 6 U.S.T. 3217, 75 U.N. T.S. 85 [hereinafter GC II]; GC III, supra note 28, Article 13; and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, August 12, 1949, Article 33, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; Protocol Additional I, supra note 4, Articles 20, 51-56. On the U.S. position, see Abraham D. Sofaer, "Agora: The US Decision Not to Ratify Protocol I to the Geneva Conventions on the Protection of War Victims," 82 *American Journal of International Law* 784 (1988).

[38] Protocol Additional I, supra note 4, Articles 51.5(b) and 57. 2(a)(iii). See also Rome Statute, supra note 20, Article 8.2(b)(iv).

"may be expected," that is, are reasonably foreseeable. There is, however, a point where such effects are so remote that they should not be included? One reasonable approach is to ask whether the information warfare operation is the proximate cause of the knock-on effect, i.e., whether the effect would not have occurred "but for" the attack. Beyond that, the effect would nevertheless have to be one that would have been discovered by an attacker complying with humanitarian law's duty to take precautions in attack.

What precautions must be taken by those planning or executing an information warfare attack?

In addition to limiting attacks to military objectives and requiring they be proportionate, humanitarian law obliges attackers to take "constant care …to spare the civilian population, civilians, and civilian objects." In particular, they must "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection…and that it is not prohibited…to attack them." Attackers must further seek to minimize collateral damage and incidental injury when choosing methods and means of warfare. Additionally, when a choice is possible among potential targets to achieve a similar military advantage, they must select that which results in the least damage to civilian objects or injury to civilians.[39]

These requirements bear heavily on information warfare. For instance, to what extent must computer expertise be available during the targeting process to assess possible collateral damage and incidental injury? In traditional kinetic attacks, properly trained mainstream military officers can usually conduct reliable estimates. In information warfare, however, highly specialized expertise would be required. The legal question is whether or not fielding such expertise is "feasible," a contextual and highly subjective assessment. In current operations in Afghanistan, for instance, an Information Operations Working Group plays a central role in identifying targets and planning attacks thereon.[40] Not all armed forces, however, can create such groups. This, in turn, raises the question of the extent to which the inability to assess collateral damage and incidental injury renders an attack indiscriminate in violation of the prohibition on "means of combat the effects of which cannot be limited as required [by humanitarian law]."[41]

On a more positive note, offensive information warfare capabilities, especially computer network attack, make it possible to attack many military objectives that were previously unattainable, either because they were too difficult to feasibly target (location, defenses, and so on) or because an attack thereon risked disproportionate civilian injury and damage to civilian objects. As the universe of potential targets expands, so too do the options for achieving a particular military goal. This, in turn, opens opportunities for minimizing collateral damage and incidental injury. For instance, if the intent is to interrupt rail traffic, it might be possible to simply interfere with the computerized switching net rather than bomb rail facilities. Similarly, information warfare may allow striking a target in a less destructive fashion. As an example, it is far less devastating to disrupt air traffic control communications and data than to bomb an installation.

[39] Protocol Additional I, supra note 4, Article 57.
[40] Pamela M. Stahl and Toby Harryman, "The Judge Advocate's Role in Information Operations," *Army Lawyer*, March 2004, at 30, 34-35.
[41] Protocol Additional I, supra note 4, Article 51.4(c) (one requirement being proportionality).

When is information warfare prohibited as perfidy?

An attack is perfidious, and therefore unlawful, when it involves feigning protected status to take advantage of the enemy.[42] Perfidious acts must be distinguished from lawful ruses, which entail otherwise misleading an enemy.[43] Altering data on friendly force composition, location, and movement in an opponent's database would amount to a lawful CNA ruse. So too would transmitting false orders to enemy forces or changing data on the enemy's forces and activities. It should be noted in this latter regard that the prohibition on using the enemy's military emblem, insignia, and uniforms found in Protocol I does not extend to the use of codes, passwords, and similar communications.[44]

On the other hand, information warfare could also be used to feign protected status, for instance by causing enemy computers to indicate that combat transports are medical aircraft or civilian airliners. Any such use is unambiguously prohibited. Using information warfare to create the impression that an armistice or cease-fire had been signed in order to approach and engage the enemy is also forbidden. Doing so would be the electronic equivalent of treacherously displaying the white flag of truce.[45]

Does the defender bear any obligations?

Humanitarian law requires all parties to the conflict to take "feasible…precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations."[46] Qualifying the requirement with the word "feasible" renders it difficult to judge all but the most egregious cases, such as intentionally using civilians to shield military objectives.

The widespread interconnectedness of military and civilian information and communications systems exacerbates the problem. Arguably, the armed forces should establish separate networks for targets the enemy would find especially attractive in order to minimize the risk of collateral damage or incidental injury. Similarly, it might be argued that the military should avoid using dual-use assets, such as air traffic management systems, that are particularly vulnerable to computer attack. The reality, however, is that the trend is in precisely the opposite direction, as most militaries seek to save money by outsourcing functions performed traditionally by the military and purchasing "off-the-shelf" equipment and services. The extensive use of civilian internet services and commercial software is illustrative. Such state practice weakens the defender's obligation to shelter the civilian population.

---

[42] Protocol Additional I, supra note 4, Article 37.1. See also Rome Statute, supra note 20, Article 8.2(b)(vii) and (xi). Convention (IV) respecting the Laws and Customs of War on Land, Oct. 18, 1907, annexed Regulations, Article 23(b)7, 36 Stat. 2277, 205 Consolidated Treaty Series 277 [hereinafter Hague Regulations], prohibits treacherous killings.

[43] Protocol Additional I, supra note 4, Article 37.2.

[44] Michael Bothe, Karl J. Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts* 207 (1982). Protocol Additional I, Article 38, prohibits the misuse of protective signals.

[45] Protocol Additional I, supra note 4, Article 37.1(a). See also Rome Statute, supra note 20, Article 8.2(b)(vii).

[46] Protocol Additional I, supra note 4, Article 58 (c).

Are commanders or other superiors responsible for the acts of their subordinates in conducting information warfare?

Under the principle of command responsibility, commanders are answerable for failing to prevent or punish war crimes committed by subordinates. Accountability turns on the commander's actual or constructive knowledge of their commission. The standard for imputing knowledge varies. Post-WWII cases applied that of "criminal negligence."[47] More recently, Protocol Additional I holds commanders responsible when they "had information enabling them to conclude in the circumstances at the time,"[48] whereas Article 28 of the Statute of the International Criminal Court (ICC) adopts a "knew, or owing to the circumstances at the time, should have known" standard. The International Criminal Tribunal for the former Yugoslavia has applied a more lenient yardstick to civilian "commanders," requiring that they "knew, or consciously disregarded information which clearly indicated," before they become responsible for criminal acts of subordinates.[49]

The complexity of information warfare makes it difficult to prescribe precisely what it is a commander should know. Is there a requirement, for instance, to have computer operators brief commanders about potential knock-on effects of particular attacks? Along the same lines, does the higher risk of collateral damage when attacking a networked target impose a greater responsibility on the commander to get involved? The various command responsibility standards all refer to the circumstances existing at the time; is complexity such a circumstance? If so, are some information warfare attacks (and the consequent effects thereof) so complex that commanders are effectively free of the command responsibility yoke except in the clearest of cases; or does the law instead impose a greater duty on commanders to get involved because of the complexity of the situation? Unfortunately, there are no clear answers to such questions.

Who may conduct information warfare?

A looming challenge for humanitarian law lies in determining the legal status and treatment of individuals armed with CPUs and keyboards sitting at desks far from the battlefront.[50] How does the basic humanitarian law principle that only combatants have the right to participate in hostilities, while civilians enjoy protection from the dangers arising from military operations, apply to cyber-hostilities?

Yoram Dinstein has usefully identified seven cumulative conditions for lawful combatancy: (i) being under the command of a person responsible for his/her subordinates; (ii) having a fixed distinctive sign recognizable at a distance; (iii) carrying weapons openly; (iv) conducting operations in accordance with the laws and customs of war; (v) organization; (vi) belonging to a Party to the conflict; and (vii) not owing a duty of allegiance to a detaining power.[51]

---

[47] *The High Command Case* (*USA v. von Leeb et al*) (American Military Tribunal, Nuremburg, 1948), 11 NMT 462, 543. "In the latter case [of failure to properly supervise his subordinates] it must be a personal neglect, amounting to a wanton immoral disregard of the action of his subordinates amounting to acquiescence."

[48] Additional Protocol I, supra note 4, Article 86(2).

[49] *Prosecutor v. Delalic et al (Celebici Case)* (2001) ICTY, Appeals Chamber, Case IT-96-21-A, 40 *International Legal Materials* 630, 669 (2001).

[50] Ken W. Watkin, "Combatants, Unprivileged Belligerents and Conflicts in the 21st Century," International Humanitarian Law Research Initiative, HPCR Policy Brief, January 2003, available at www.ihlresearch.org.

[51] Dinstein, supra note 27, at 33-44. The first four derive from Hague Regulations, supra note 42, Article 1; GC I, supra note 34, Article 13; GC II, supra note 37, Article 13; GC IIII, supra note 28 Article 4. The fifth

Although some commentators suggest that the conditions apply only to irregular forces because of the manner in which they are set forth in the relevant conventions, Dinstein correctly rejects this position by noting that a presumption exists that regular forces meet them. Several of the conditions raise particular issues with respect to information warfare.

The second and third, both intended to eliminate confusion when distinguishing combatants from civilians, raise similar questions in the information warfare context. The challenge stems from the difficulty in determining precisely who is conducting a computer network attack. Obviously, the requirements of actually wearing a uniform and holding one's weapon openly do not apply, for CNA is conducted from beyond the sight of the enemy and therefore there is no need for visible indicators of status. Drawing a parallel, however, with the requirement that military equipment such as trucks, tanks or aircraft be marked with a distinctive sign when engaging in hostilities, one could reasonably suggest an analogous obligation during computer network attacks. For instance, might a requirement that CNA emanate from a designated military IP address apply?[52] A form of electronic marking is already in use for medical transports appearing on radar or IFF technology, albeit with the opposite intention of marking a protected object.[53]

On the other hand, it could be argued that there is no practical need for such distinguishers. During a computer network attack against military assets, the originator is either a lawful combatant or a civilian directly participating in hostilities; in either case, he or she may be targeted.

One point bearing on any requirement for distinguishing indicators during CNA is the fact that Protocol Additional I controversially relaxes the fixed distinctive emblem obligation on the grounds that there are situations in which it is impossible (or suicidal) for a combatant to distinguish him or herself.[54] In such cases, the requirement is limited to the pre-engagement deployment and the engagement itself. The provision is aimed primarily at guerrilla fighters, who use covert tactics to compensate for military and logistical inferiority.[55]

Is CNA an example of a type of warfare anticipated by this provision? Computer network attack is by its very nature a covert method of warfare and many authors have cited its possible use as a force multiplier for militarily weaker opponents.[56] This suggests the possibility that CNA preparatory acts from non-military computers (e.g., electronic probing, transmitting a virus with a back-door payload, or recruiting zombie computers) might be

---

and sixth are implied from the terms of GC III, Article 4, while the seventh is inferred from case law, particularly *Public Prosecutor v. Koi et al.* [1968] AC 829 (per Lord Hodson).

[52] Every computer that communicates over the Internet is assigned a four digit numerical address (e.g., 168.212.226.204) that uniquely identifies the device and distinguishes it from other computers. Creating a class of military addresses, or another form of military network designator would be a relatively simple matter.

[53] Protocol Additional I, supra note 4, Annex 1, Article 8.

[54] Ibid., Article 44.3.

[55] *Protocols Additional Commentary*, supra note 15, para. 1702. The United States objects to the provision on the basis that it weakens protection of the civilian population. Other states have argued that this provision is mainly restricted to resistance movements in occupied territories and indeed some countries (for example, the United Kingdom) have stated in their reservations to the convention that their acceptance of this clause is limited to such territories and wars of self-determination. Ibid., para. 1699.

[56] See, e.g., Schmitt, *CNA,* supra note 10, at 897; Michael J. Robbat, "Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum," 6 *Boston University Journal of Science and Technology Law* 10 (2000).

permissible, but that once the CNA proper starts, the attack would need to emanate from a designated "combatant" computer system.

May civilians conduct information warfare operations?

Civilians are entitled to specially protected status under humanitarian law as long as they refrain from taking a "direct part" in hostilities.[57] Those who do directly participate become unlawful combatants and lose civilian status during their involvement. They do not benefit from the prisoner of war status combatants enjoy and may be prosecuted for their actions in domestic or international tribunals.

Despite this proscription, the armed forces widely employ civilians, whether as contractors or as full-time employees.[58] High tech methods of warfare contribute to this practice, as it is far more cost effective to hire civilian contractors to maintain and operate military IT systems than to train military personnel to do so. Further, the systems being used are seldom standard military inventory; they are highly specialized and often still in the throes of research and development.[59] These factors intensify the need for civilian operators.

A vibrant debate exists over the scope of "direct participation."[60] The *Commentary* to Protocol Additional I cites "acts which are intended by their nature or their purpose to hit specifically the personnel and the 'materiel' of the armed forces of the adverse party…." It goes on to note "direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and place where the activity takes place."[61] By this standard, any civilian engaged in proactive, offensive information warfare would undoubtedly be taking a direct part in hostilities.

More problematic is the civilian computer technician who maintains the network from which an attack is launched. While IT support appears ripe for civilian outsourcing, parallels may be drawn with the civilian aircraft maintainer who repairs, loads, and launches aircraft hundreds of miles from a conflict. Regardless of proximity to the battle-space and/or civilian status, maintenance of a weapons system is an act which has a direct causal relationship with the harm done to the enemy.

Even more challenging is the case of the civilian computer technician employed to maintain non-offensive military networks that subsequently come under siege from CNA. At what point does the technician cease to become a protected civilian merely supporting and maintaining a network (including network security measures) and become an active participant defending a military objective? Some scholars have argued that direct participation includes not only activities involving the delivery of violence, but also acts

---

[57] Protocol Additional I, supra note 4, Article 51.3.
[58] Michael Guillory, "Civilianizing the Force: Is the United States Crossing the Rubicon?," 51 *Air Force Law Review* 111 (2001). As an example, there are currently more U.S. civilian government employees and contractors in Iraq, than British military personnel.
[59] Schmitt, *Direct Participation*, supra note 29.
[60] Note that Common Article 3 of the Geneva Conventions employs the term "active" rather than direct. The International Criminal Tribunal for the Rwanda, however, has stated that the terms are so similar that they should be treated as synonymous: *Prosecutor v. Jean-Paul Akayesu*, Case ICTR-96–4-T, Judgment, 2 September 1998, at para. 629.
[61] *Protocols Additional Commentary*, supra note 15, para. 1679.

aimed at protecting personnel, infrastructure, or material.[62] This broader definition appears to extend to those civilians who are engaged in maintaining many military computer networks.

The mounting number of civilian employees and contractors working for the military also raises the issue of mercenaries. Under Protocol Additional I, mercenaries are not combatants and do not become prisoner of war if captured.[63] Individual hackers and professional military companies (PMCs) specializing in information operations have already offered (or are providing) states computer network attack capabilities.[64] In most cases, employees of such companies would not meet the definition of mercenaries because they are either nationals of a Party to the conflict or not recruited for a specific conflict. [65] Where foreign civilians are recruited, however, for their specific offensive information warfare skills in respect of a particular conflict, and the arrangement is purely business (as in the case of a PMC) or otherwise motivated by financial gain in excess of that paid to military counterparts, they may be considered unlawful combatants (who, if captured, would not be entitled to prisoner of war status).[66]

Under what circumstances may computers and computer infrastructure be attacked with traditional weaponry?

There is no question that computers and computer infrastructure used to support military operations are legitimate military objectives that may be attacked so long as the requirements of proportionality and precautions in attack are met. So, too, may the factories that produce computer hardware and software for the war effort. Indeed, even factories that turn out computer components for military use, such as microchips, are valid military objectives if their destruction would yield a definite military advantage.

The problem is practical, not legal. As noted, the military relies increasingly on dual-use information and communications networks, thereby inevitably exposing civilians and civilian property to risk during attacks thereon. Similarly, as the military turns to civilian "off-the-shelf" computer products, the number of potential war-supporting targets grows, again increasing the risk to civilians and civilian property.

---

[62] See, for example, François Quéguiner, "Direct Participation in Hostilities under International Humanitarian Law," International Humanitarian Law Research Initiative Briefing Paper, November 2003, n1. Available at www.ihlresearch.org/ihl/pdfs/briefing3297.pdf.

[63] Protocol Additional I, supra note 4, Article 47(1).

[64] See, for example, "Interview with Hacker," in Frontline *Cyberwar!*, PBS Airdate April 24, 2003. Available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hacker.html (hackers offering services to Serbia in NATO bombardment).

[65] Article 47(2) of Protocol Additional I provides: A mercenary is any person who: (a) is specially recruited locally or abroad in order to fight in an armed conflict; (b) does, in fact, take a direct part in the hostilities; (c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; (d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; (e) is not a member of the armed forces of a Party to the conflict; and (f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

[66] Indeed, under Article 3.1 of the 1989 International Convention against the Recruitment, Use, Financing and Training of Mercenaries, merely being a mercenary is an offense. 29 *International Legal Materials* 89 (1990).

How does the law of neutrality affect information warfare?

Finally, and although an in-depth discussion of neutrality law is beyond the scope of this article,[67] it is worth highlighting the fact that the global community is increasingly connected and interdependent. Communications systems cut across borders, energy production is shared, corporations are increasingly multinational, and markets are often defined regionally and globally. Indeed, international consortia such as INTELSAT, INMARSAT, ARABSAT, EUTELSAT, and EUMETSAT that own and operate communications and weather satellites may have both neutrals and parties to the conflict as members.[68] In the twentieth-first century, it is inevitable that conflict will affect neutral states, citizens, and business entities, often dramatically so.

With regard to information warfare, it is clear that belligerents are forbidden to launch operations from neutral territory, whether using their own assets or the information systems of the neutral.[69] That said, the mere routing of data through the neutral State is allowed as long as the neutral impartially makes its networks available to both sides.[70] Should the neutral violate this obligation or if a belligerent mounts operations from neutral territory that the neutral cannot or will not prevent, the "victim" belligerent may take those measures reasonably necessary and proportionate to put an end to the violations.

It should also be noted that the International Court of Justice, in its Nuclear Weapons Advisory Opinion, opined that the principle of neutrality prohibits cross-border damage caused by a weapon used in belligerent territory.[71] While this is indisputable, the nature and extent of the prohibited damage lacks clarity. For instance, does the principle extend only to physical damage and human injury, or does it include damage to intangibles, such as data, or inconvenience consequences, like interference with access to communications systems? Of course, issues of intent, foreseeability, and precautions would also permeate any analysis of cross-border effects generated by information warfare.

---

[67] George K. Walker, Information Warfare and Neutrality, in *Computer Network Attack and International Law* 233 (Newport R.I.: Naval War College International Law Studies, vol. 76, Michael N. Schmitt and Brian T. O'Donnell eds., 2001).

[68] In some cases, these groups have adopted special provisions for operation during an armed conflict.

[69] Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, October 18, 1907, Article 3, 36 Stat. 2310 (Hague V); Convention Concerning the Rights and Duties of Neutral Powers in Naval Warfare, Oct. 18, 1907, Article 5, 236 Stat. 2415 (Hague XIII).

[70] Hague V, supra note 69, Articles 8 and 9.

[71] *Legality of the Threat or Use of Nuclear Weapons*, supra note 17, paras. 88-90.

Select Bibliography

Government Publications

Department of Defense, Directive S-3600.1, Information Operations, 9 Dec. 1996.

Department of Defense, Office of General Counsel, An Assessment of International Legal Issues in Information Operations, August 2001.

Chairman, Joint Chiefs of Staff Instruction 3210.01A, Joint Information Operations Policy, August 1999.

Chairman, Joint Chiefs of Staff Instruction 6510.01C, Information Assurance and Computer Network Defense, 1 May 2001.

The Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998.

The Joint Chiefs of Staff, Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare, 7 February 1996.

The Joint Chiefs of Staff, Joint Publication 3-51, Joint Doctrine for Electronic Warfare, 7 April 2000.

The Joint Chiefs of Staff, Joint Publication 3-43, Doctrine for Joint Psychological Operations, 10 July 1996.

Chief of Naval Operations, Implementing Instructions for Information Warfare/Command and Control, ONAV Instruction 3430-26, 18 January 1995.

U.S. Department of the Air Force, Air Force Doctrine Document 2.5, Information Operations, 5 August 1998.

U.S. Department of the Air Force, Air Force Pamphlet 14-210, Intelligence Targeting Guide, 1 February 1998, chapter 11.

U.S. Department of the Army, Field Manual 100-6, Information Operations, 27 August 1996.

U.S. Army, International and Operational Law Handbook (Charlottesville, Va.: The Judge Advocate General's Legal Center and School, 2004), chapter 19.

Scholarly Publications

Aldrich Richard W., "How Do You Know You Are at War in the Information Age?, 22 *Houston Journal of International Law*, 223 (2000).

Arquilla, John, "The Great Cyberwar of 2002," *Wired Magazine*, February 1998, available at http://hotwired.wired.com/collections/future_of_war/6.02_cyberwar_20021.html.

Barkham, Jason, "Information Warfare and International Law on the Use of Force," 34 *New York University Journal of International Law and Politics* 57 (2001).

Greenberg, Lawrence T., et al., *Information Warfare and International Law* (Washington D.C.: National Defense University, 1997)

Haslam, Emily, "Information Warfare: Technological Changes and International Law," 5 *Journal of Conflict and Security law* 157 (2000).

Jensen, Eric T., "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," 38 *Stanford Journal of International Law* 207 (2002).

Jensen, Eric T., "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations," 18 *American University International Law Review* 1145 (2003).

Joyner, Christopher C. and Lotrionte, Catherine, "Information Warfare as International Coercion: Elements of a Legal Framework," 12 *European Journal of International Law* 825 (2002).

Sharp, Walter Gary, Sr., *CyberSpace and the Use of Force* (Falls Church, VA: Aegis Research Corp., 1999).

Schmitt, Michael N. and O'Donnell, Brian T., eds., *Computer Network Attack and International Law* (Newport, R.I.: Naval War College International Law Studies, vol. 76, 2002).

Schmitt, Michael N., "Wired Warfare: Computer Network Attack and International Law," 84 (No. 846) *International Review of the Red Cross* 365-399 (June 2002)

Schmitt, Michael N., "Computer Network Attack: The Normative Software;" 4 *Yearbook of International Humanitarian Law* 53-85 (2001).

Schmitt, Michael N., "Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework," 37 *Columbia Journal of Transnational Law* 885-937 (1999).

Shulman, Mark R., "Discrimination in the Laws of Information Warfare," 37 *Columbia Journal of Transnational Law* 939 (1999).

Stahl Pamela M. and Harryman, Toby, "The Judge Advocate's Role in Information Operations," *Army Lawyer*, March 2004, at 30.

Wingfield, Thomas C., *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, VA: Aegis Research Corp., 2000).

Wingfield, Thomas C., "Legal Aspects of Offensive Information Operations in Space," 9 *USAF Academy Journal of Legal Studies* 121 (1998/99).