COMMUNICATIONS TECHNOLOGY, WARFARE, AND THE LAW: IS THE NETWORK A WEAPON SYSTEM?

*Gregory F. Intoccia**
*Joe Wesley Moore***

* *Gregory F. Intoccia (B.S. United States Air Force Academy; J.D. University of Denver; M.A. Wichita State University; Ph.D. University of Missouri-St. Louis) is a lieutenant colonel in the Air Force Reserve Judge Advocate General's Corps attached to Headquarters Air Force Operations Law Division, Washington, D.C. He also is Associate Chief-Legal, Public Safety and Critical Infrastructure Division, Wireless Telecommunications Bureau, Federal Communications Commission.*

** *Joe Wesley Moore (B.A. Texas Tech; J.D. Baylor Law School; L.L.M. Institute of Air & Space Law, McGill University) is an active duty lieutenant colonel in the Air Force Judge Advocate General's Corps assigned to Headquarters Air Force Operations Law Division, Washington, D.C., where he is Chief, Air and Space Law Branch. The views expressed in this Article are those of the* Authors *and do not necessarily reflect those of the U.S. Air Force, the Federal Communications Commission or any other government agency.*

Communications networks have had a transformational effect on virtually every aspect of modern American life, and modern American warfare is certainly no exception. Currently, what has been referred to by some as the "Information Technology Revolution in Military Affairs"[1] has greatly increased the effectiveness of military command and control and has increased the efficiency and accuracy with which many weapons and weapon systems can be employed. In fact, the importance of networks to developing concepts such as "network-centric warfare"[2] has led some U.S. military communicators to believe that the network is, or will become, in effect, a weapon system unto itself. This reference to the "network as a weapon system" has become a virtual mantra among some of the nation's military professionals. Whether motivated by the desire for a bigger slice of a finite federal budgetary pie, by the allure of a more prominent seat at the "warfighter" table in a military culture that highly values those who directly contribute to the ability to more effectively wage war, or simply by a desire to more forcefully articulate the need

1. *E.g.*, Christopher D. Kolenda, *Transforming How We Fight: A Conceptual Approach*, 55 NAVAL WAR C. REV. 100, 101 (2003), *available at* http://www.nwc.navy.mil/press/Review/2003/Spring/pdfs/art6-sp3.pdf.

2. *See infra* notes 7–10.

to focus greater attention on fundamental infrastructure issues that should be addressed as new technology in warfighting is developed, the reference to the network as a weapon system has become increasingly in vogue. This practice has evolved without significant analysis of the legal implications, especially with regard to those provisions of the law of armed conflict dealing with the development and employment of weapons.

This Article will examine the following questions: (a) Does the network constitute a weapon system? (b) What legal implications follow from continued use of the "network as a weapon system" terminology with respect to (i) targeting, (ii) military manning, (iii) contractors and other civilian portions of the network, and (iv) U.S. policy relating to weapons in outer space? These and related issues are addressed in this Article, which examines the subject primarily from a law of armed conflict (LOAC) perspective. After defining relevant terms, this Article will examine and apply the LOAC principle that combatants be distinguished from noncombatants and the principles of military necessity, proportionality, and neutrality.[3]

This Article concludes that it is currently inaccurate to refer to the network as a "weapon system" and that continuing this practice could potentially influence a developing area of the law inconsistent with U.S. interests. Given that LOAC is unsettled

---

3. An analysis of whether an attack by a computer network constitutes an "act of war" or "armed attack" is beyond the scope of this discussion. This subject is addressed elsewhere. *See* LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 30–33 (Daniel T. Kuehl ed., 1998), *available at* http://www.dodccrp.org/publications/pdf/Greenberg_Law.pdf; *see also* Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F. L. REV. 173, 183–84 (1997) ("[O]ne should not assume that because LOAC predates information warfare, it is not applicable. Many classes of weapons have been developed in the last century which could not have been conceived of when LOAC was being developed . . . ."); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 919–23 (1999) ("[W]hen does a computer network attack amount to . . . [an] act of aggression such that the [UN Security] Council may authorize a response by armed force? The answer can only be provided by the Security Council . . . ."). The Department of Defense (DOD) has determined, for policy reasons, that it will comply with LOAC "during all armed conflicts, however such conflicts are characterized, and . . . with the principles and spirit of the law of war during all other operations." JOINT CHIEFS OF STAFF, IMPLEMENTATION OF THE DOD LAW OF WAR PROGRAM § 4 (2002). Thus, LOAC fully applies—whether by law or by policy—to all U.S. military operations.

with respect to electronic applications, the practice could lead one to conclude that the restrictions applicable to use of weapon systems—such as the prohibition on direct involvement by civilians in using these systems for their ultimate purpose—should be applied to any network operations. Such continued reference could also foreseeably result in enemy attempts to justify intentional targeting of nonmilitary personnel and assets that are not in fact contributing to the war effort.

I. BACKGROUND

The "network as a weapon system" terminology, as used by the Air Force and the other Services, can be traced back to at least the year 2000, when that phrase was used by Lieutenant General William J. Donahue (USAF) in a January 2000 *Intercom* article.[4] Since that time, the phrase has been more frequently used by military communicators both in their respective Services and in joint environments.[5] Moreover, companies in the defense contracting community now are frequently referring to the "network" and "information warfare" in the same manner.[6]

Consistent with this development in terminology, there has been further development in the concept of network-centric warfare, a concept that has been the cornerstone of an ongoing

---

4. William J. Donahue, *Information Assurance in the New Millennium*, INTERCOM, Jan. 2000, at 3 ("The network is a weapons system and we need to treat it as such.").

5. *See* Doug Mohney, *U.S. Navy Dumps Microsoft, Makes the Network the Weapon*, INQUIRER, July 21, 2003, *available at* http://www.theinquirer.net/?article=10581; *see also* Press Release, U.S. Air Force, Cyber Warriors Protect Air Force Computer Network (Oct. 10, 2002), http://www.findarticles.com/p/articles/mi_prfr/is_200210/ai_3964551162 ("Because the Air Force computer network is a weapons system and is under constant attack by viruses and illegal entry attempts by adversaries, defending that weapons system has become an ongoing war, said the director of operations for the 33rd Information Operations Squadron . . . .").

6. *See* David A. Fulghum, *Network Wars*, AVIATION WK. & SPACE TECH., Oct. 25, 2004, at 90. One reporter states that "[a]dvocates say networked computers will be the *most powerful weapon in the American arsenal*." Tim Weiner, *Pentagon Envisioning a Costly Internet for War*, N.Y. TIMES, Nov. 13, 2004, at A1 (emphasis added). *See also* David Wichner, *Raytheon Changes the Battlefield*, ARIZ. DAILY STAR, Nov. 10, 2004, at A1 ("Scientists and engineers at Tucson's Raytheon Missile Systems—the world's biggest missile-making operation—are shaping the future of warfare.").

DOD transformational effort[7] dating back at least a decade. The concept posits that "information superiority is [the] essential ingredient of success" in warfare[8] and emphasizes that combat power can be generated from the "effective linking or networking of the warfighting enterprise."[9] Network-centric warfare is "characterized by the ability of geographically dispersed forces . . . to create a high level of shared battlespace awareness that can be exploited . . . to achieve commanders'" intentions.[10] The concept includes a "future for remote-control combat, where land battles may be fought with . . . unmanned aircraft and missiles that 'talk' amongst themselves to coordinate attacks on fast-moving enemy forces."[11] It is hoped that use of the network-centric approach will reduce dependence on "stove-piped" legacy systems and will improve upon the sharing of critical intelligence information among warfighters.[12]

DOD expects that network-centric warfare capabilities will "enhance the capability of the Joint force commander to understand the [battlefield] situation, determine the effects desired, select a course of action and the forces to execute it, accurately assess the effects of that action, and reengage as necessary while minimizing collateral damage."[13] It is fully expected that "net-centric warfare" will increase in importance

---

7. Weiner, *supra* note 6, at A1 (noting that in July 2004, the GAO indicated that "the Pentagon is depending on the GIG [Global Information Grid] to enable a fundamental transformation in the way military operations are conducted."); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, DEFENSE ACQUISITIONS: THE GLOBAL INFORMATION GRID AND CHALLENGES FACING ITS IMPLEMENTATION (2004) [hereinafter DEFENSE ACQUISITIONS], http://www.gao.gov/new.items/d04858.pdf ("DOD is looking to the GIG to form the basis of a network-centric or 'netcentric' way of fighting wars and to create a decisive advantage over adversaries.").

8. Brian Nichiporuk, *U.S. Military Opportunities: Information-Warfare Concepts of Operation*, *in* STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION WARFARE 182 (Zalmay Khalilzad et al. eds., 1999), *available at* http://www.rand.org/publications/MR/MR1016.chap7.pdf.

9. DAVID S. ALBERTS, JOHN J. GARSTKA & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY 88 (2d ed. 1999).

10. *Id.*

11. Wichner, *supra* note 6, at A1.

12. *See* Mohney, *supra* note 5.

13. DOD COMMAND AND CONTROL RESEARCH PROGRAM, U.S. DEP'T OF DEF., NETWORK CENTRIC WARFARE 2–9 (2001).

in the immediate years ahead.[14] Major General Dale Meyrose (USAF) stated that he believes "net-centricity is the future;" he believes that it "will play a major role in how U.S. armed forces fight abroad as well as protect themselves at home," and it will help to "replace the existing satellite constellation with an [Internet Protocol]-based network."[15] Twenty-eight companies, including Lockheed Martin, Boeing and Northrop Grumman, have recently formed the Network Centric Industry Consortium, which will provide recommendations on which technical standards and architectures will best allow participation in a global network environment.[16]

Major efforts are already underway to develop specific systems that will upgrade battlefield capability. For example, a large effort is underway to build a secure network based on Internet protocol, called the "Global Information Grid" (GIG), that could send classified intelligence and stratagems instantly to the U.S. military in the battlefield, making them a faster, fiercer force against the enemy.[17] Such a network would allow,

---

14. *See id.*

15. Rodney L. Pringle, *Net Centric Operations to be Key 'Change Agent' for U.S. Forces*, *NORTHCOM Commander Says*, AVIATION NOW, Oct. 14, 2004, *available at* http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/NETCENT10144.xml.

16. *Id.*

17. Weiner, *supra* note 6, at A1. The GIG is defined as follows:

> Globally interconnected, end-to-end set of information capabilities, associated, processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information.

U.S. DEP'T OF THE AIR FORCE, AIR FORCE INSTRUCTION 33–302, NETWORK AND COMPUTER SECURITY 61 (2004). The GIG has also been described in the following way:

> The GIG . . . is intended to integrate virtually all of DOD's informational systems, services, and applications into one seamless, reliable, and secure network. DOD's overall concept is to enable data access for a variety of systems and users in the network no matter which military service owns a weapon system or where a user might be located in the world. DOD is looking to the GIG to form the basis of a network-centric or "netcentric" way of fighting wars and to create a decisive advantage over adversaries.

DEFENSE ACQUISITIONS, *supra* note 7.

for example, "marines in a Humvee, in a faraway land, in the middle of a rainstorm, to open up their laptops, request imagery" from a reconnaissance satellite, and "get it downloaded within seconds."[18] Numerous efforts at building other specific systems are also underway. For example, in May 2004, "a Raytheon-Lockheed Martin joint venture was awarded a $1 billion contract to develop the Non Line-of-Sight Launch System . . . a system [consisting] of two types of small missiles" that could be fired remotely.[19] Data links would provide two-way communications between the missiles and military commanders in the battlefield, while satellite technology combined with advanced guidance and targeting systems would allow quick retargeting.[20]

Despite such ambitious programs, most of the U.S. military's communications today are highly integrated with and dependent upon the nation's commercial communications infrastructure.[21] Approximately "[ninety-five percent] of the telecommunications of the [DOD] travel through the Public Switched Network," and a significant amount of both the operation and maintenance of military-owned network segments is currently handled by civilians on a contracted-out basis.[22] Further, the military community is becoming increasingly electronically interconnected. In recent years, the armed forces and civilian users have become increasingly dependent upon the same commercial space systems.[23] Because the U.S. military's own dedicated satellite communications systems cannot handle its increasing demands, the military has leased, and plans to continue leasing, commercial satellite communications capacity.[24] For instance, "DOD uses leased Intelsat circuits to

---

18. Weiner, *supra* note 6, at A1 (quoting Peter Teets, Undersecretary of the Air Force, before Congress).

19. Wichner, *supra* note 6, at A1.

20. *Id.*

21. *See* GREENBERG, GOODMAN & SOO HOO, *supra* note 3, at 12.

22. *See id.*; *see also* Hanseman, *supra* note 3, at 194.

23. Elizabeth Seebode Waldrop, *Integration of Military and Civilian Assets: Legal and National Security Implications*, 55 A.F. L. REV. 157, 157 (2004).

24. *Id.;* COMM'N TO ASSESS U.S. NAT'L SEC. SPACE MGMT. & ORG., REPORT OF THE COMMISSION TO ASSESS UNITED STATES NATIONAL SECURITY SPACE MANAGEMENT AND ORGINZATION (2001), *available at* http://www.space.gov/docs/fullreport.pdf.

supplement its capabilities; in fact, some DOD satellite command and control facilities routinely use Intelsat to relay data from its satellites."[25] Moreover, approximately "[sixty percent] of the satellite communications [requirements] of the U.S. military are provided by commercial entities."[26]

II. LOAC CONSIDERATIONS

LOAC is comprised of treaties, other international agreements, and customary international law.[27] The key principles of LOAC, found primarily in the four Geneva Conventions of 1949[28] and various Hague Conventions,[29] may be

25. Waldrop, *supra* note 23, at 169.

26. *Id.* at 200.

27. Hanseman, *supra* note 3, at 180. Whether the United States accepts a particular LOAC principle as binding U.S. law can be a controversial topic beyond the scope of this discussion. The principles discussed here are either recognized by the United States as customary international law or are applicable as a matter of DOD policy.

28. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of the War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Convention Relative to Prisoners of War]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Convention Relative to Protection of Civilian Persons]. Two protocols additional to the Geneva Conventions of 1949 were negotiated between 1974–1977. Protocol Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), *adopted on* June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Relating to the Protections of Victims of Non-International Armed Conflicts (Additional Protocol II), *adopted on* Dec. 7, 1978, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]. Although the United States signed Additional Protocol II in December 1977, it did not ratify either of them. On January 29, 1987, President Reagan informed the Senate that the United States did not intend to become party to Additional Protocol I and that he, therefore, would not submit it for advice and consent. President Reagan's Message to the Senate Transmitting a Protocol to the 1949 Geneva Conventions (Jan. 29, 1987), *reprinted in* 133 CONG. REC. S1428 (daily ed. Jan. 29, 1987). Although Additional Protocol II was submitted, the Senate has not offered its advice and consent. *Id.* Accordingly, the provisions of Additional Protocol I and Additional Protocol II are not binding on the United States. However, to the extent that the United States accepts certain of the protocols' provisions as reflective of customary international law or existing law under the Geneva Conventions of 1949, the United States adheres to those provisions. *See* MARIAN NASH, OFFICE OF THE LEGAL ADVISER, U.S. DEP'T OF STATE,

summarized as follows:

A. Distinction Between Combatants and Noncombatants[30]

With limited exceptions, only members of a state's regular armed forces are entitled to use force against the enemy.[31] Combatants must be trained in the law of war, serve under effective discipline, and be under the command of officers responsible for their conduct.[32] Combatants must distinguish themselves from noncombatants, must further distinguish between civilian objects and military ones, and must direct their operations against military objectives.[33]

Civilians enjoy a protected status and may not be the direct

CUMULATIVE DIGEST OF THE UNITED STATES PRACTICE IN INTERNATIONAL LAW 1981–1988, at 3434–35 (1995).

29. *See, e.g.*, Convention Respecting the Laws and Customs of War on Land, 36 Stat. 2277 (1908) [hereinafter Hague Convention IV]. Various other conventions, regulations, and rules were also adopted by the international Diplomatic Conferences at the Hague in 1899 and 1907. *See, e.g.*, Convention—War on Land, July 29, 1899, 32 Stat. 1803; Convention—War on Land, Oct. 18, 1907, 37 Stat. 2277.

30. *See id.* Annex, art. 3.

31. *See, e.g.*, William H. Ferrell, III, *No Shirt, No Shoes, No Status: Uniforms, Distinction, and Special Operations in International Armed Conflict*, 178 MIL. L. REV. 94, 104 (2003). The right to use force is limited to "lawful combatants" who have "combatant immunity" for their lawful uses of force. *See id.* While the term "combatant immunity," as such, cannot be found in either the Hague or Geneva Conventions, the concept is inherent in their structure and meaning. *Id.* In fact, commentators generally suggest that the protection of lawful combatants is a fundamental aspect of the Hague and Geneva regimes. *See id.*

32. *See* Hague Convention IV, *supra* note 29, Annex, art. 1. Moreover, these requirements are reflected in Article 4(A) of the Geneva Convention Relative to the Treatment of Prisoners of War. Convention Relative to Prisoners of War, *supra* note 28, art. 4(A). Article 4(A) recognizes prisoner of war status for certain members of the armed forces and persons accompanying the armed forces without further inquiry, but certain militia, volunteer corps, and resistance movements receive prisoner of war status only in the following situations: (a) they are commanded by a person responsible for his subordinates; (b) they have a fixed distinctive sign recognizable at a distance; (c) they carry arms openly; and (d) they conduct their operations in accordance with the laws and customs of war. *Id.*

33. Additional Protocol I, *supra* note 28, arts. 48, 52. "Military objective" means any object that by its "nature, location, purpose or use make[s] an effective contribution to military action and whose total or partial destruction, capture or neutralization, in circumstances ruling at the time, offers a definite military advantage." *Id.* art. 52(2). "Civilian objects" are "all objects that are not military objectives." *Id.* art. 52(1).

object of military attacks as long as they are not taking an active part in hostilities.[34] Taking an active or direct part in hostilities means engaging in acts likely to cause actual harm to the personnel or equipment of the adversary.[35] The latter rule may

34. Additional Protocol II, *supra* note 28, art. 13.

35. CLAUDE PILLOUD ET AL., INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 619 (1987). Article 3 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War provides, "[p]ersons taking no *active* part in the hostilities . . . shall in all circumstances be treated humanely." Convention Relative to Protection of Civilian Persons, *supra* note 28, art. 3 (emphasis added). However, the Commentaries to the four Geneva Conventions of 1949, International Committee of the Red Cross (1960), do not include any discussion of which activities constitute taking an *active* part in hostilities. Article 51, paragraph 3, of Additional Protocol I provides, "[c]ivilians shall enjoy the protection afforded by this Section, unless and for such time as they take a *direct* part in hostilities." Additional Protocol I, *supra* note 28, art. 51 (emphasis added). Thus, Additional Protocol I uses the word "direct" instead of "active" in describing involvement in hostilities. The terms are often treated as synonymous. The Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 discussing Article 51 states the following:

> In general the immunity afforded civilians is subject to a very stringent condition: that they do not participate directly in hostilities, *i.e*., that they do not become combatants, on pain of losing their protection. *Thus "direct" participation means acts of war, which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces* . . . .
>
> There should be a clear distinction between direct participation in hostilities and participation in the war effort. The latter is often required from the population as a whole to varying degrees . . . . In fact, in modern conflicts, many activities of the nation contribute to the conduct of hostilities, directly or indirectly . . . .

PILLOUD ET AL., *supra*, at 619 (emphasis added). The United States has, on one occasion, taken a position on the meaning of "direct part in hostilities" as "immediate and actual action on the battlefield likely to cause harm to the enemy because there is a direct casual relationship between the activity engaged in and the harm done to the enemy." Optional Protocol No. 1 to the Convention on the Rights of the Child, S. TREATY DOC. NO. 106-37(A) (2000). The Optional Protocol was transmitted to the U.S. Senate on July 25, 2000, for advice and consent to ratification. OFFICE OF COMMUNICATIONS, THE WHITE HOUSE, MESSAGE FROM THE PRESIDENT TO THE SENATE ON CHILDREN'S RIGHTS (2000). The Senate granted its advice and consent, and the instruments of ratification were deposited at the United Nations on December 23, 2002. OFFICE OF THE SPOKESMAN, U.S. DEP'T OF STATE, RATIFICATION OF OPTIONAL PROTOCOLS TO THE CONVENTION ON THE RIGHTS OF THE CHILD (2002). This understanding did not, however, purport to address the meaning of the phrase outside of the context of the so-called "Child Soldier Protocol." Thus, this analysis will rely on the more widely accepted standard enunciated in the Commentary to Additional Protocol I.

encompass more than just firing a weapon, since harm may be caused by a variety of activities. If civilians take an active, direct part in hostilities or engage in acts likely to cause actual harm to the personnel or equipment of an adversary, they lose their protected status. [36] Civilians could lose their protected status not only if they fired a weapon, but also for other activities likely to cause harm to the enemy.[37]

B. Military Necessity

Acts that are indispensable for securing the prompt submission of the enemy with the least possible expenditures of resources, and that are not otherwise forbidden by international law, are permitted by reason of military necessity.[38] Enemy forces are deemed to be hostile and "attacks are to be directed solely toward military objectives."[39] Thus, enemy forces may be attacked at will, along with their equipment and stores. Additionally, civilians and civilian property that make a direct contribution to the war effort may also be attacked, along with objects whose damage or destruction would produce a military

---

36. *See* Additional Protocol I, *supra* note 28, art. 51(3).

37. *See* PILLOUD ET AL., *supra* note 35, at 619.

38. *See United States v. List*, 11 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 757, 1253 (1949). In 1863, Francis Lieber defined the term as follows: "Military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war." Francis Lieber, *Instructions for the Government of the Armies of the United States in the Field*, *in* THE LAWS OF ARMED CONFLICTS, A COLLECTION OF CONVENTIONS, RESOLUTIONS, AND OTHER DOCUMENTS 6 (Dietrich Schindler & Jiri Toman eds., 1981). In *List*, the Nuernberg War Tribunal that prosecuted Nazi war crimes stated the following: "Military necessity permits a belligerent, subject to the laws of war, to apply any amount and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life and money." *List*, 11 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 1253.

39. Int'l Comm. of the Red Cross, *Fundamental Rules of Humanitarian Law Applicable in Armed Conflicts*, *in* INT'L REV. OF THE RED CROSS 248–49 (1978); Additional Protocol I, *supra* note 28, arts. 48, 52; THE LAWS OF WAR: CONSTRAINTS ON WARFARE IN THE WESTERN WORLD 3, 8 (Michael Howard et al. eds., 1995); Nathan A. Canestaro, *Legal and Policy Constraints on the Conduct of Aerial Precision Warfare*, 37 VAND. J. TRANSNAT'L L. 431, 455 (2004).

advantage because of their nature, location, purpose, or use.[40] Conversely, noncombatants making no direct contribution to the war effort and civilian objects whose destruction would provide no significant military advantage to the attacker are immune from deliberate attack.[41]

C. Proportionality

When an attack is made against a lawful military target, collateral injury and damage to noncombatants and civilian property may be unavoidable. Attacks may be carried out against lawful military targets even if some amount of collateral damage is foreseeable, unless the foreseeable collateral damage is disproportionate to the military advantage likely to be attained.[42]

D. Neutrality

States not engaged in a conflict that declare themselves to be neutral and act accordingly are entitled to immunity from attack by belligerents.[43]

---

40. Additional Protocol I, *supra* note 28, arts. 51(3), 52.

41. *E.g.*, *id*. art. 51(3); *see also* Burrus M. Carnahan, *Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity*, 92 AM. J. INT'L. L. 213 (1998) (discussing the historical underpinnings of military necessity); Lieber, *supra* note 38, at 8.

42. Additional Protocol I, *supra* note 28, arts. 515(b), 572(a)(iii); Thomas M. McDonnell, *Cluster Bombs Over Kosovo: A Violation of International Law?*, 44 ARIZ. L. REV. 31, 75 (2002). Other basic LOAC principles, not relevant for this discussion, include the following: (1) Superfluous injury: States have agreed to ban certain weapons because they cause superfluous injury; (2) Indiscriminate weapons: States have agreed to ban certain other weapons because they cannot be directed with any precision against combatants; and (3) Perfidy: LOAC provides certain visual and electronic symbols to identify persons and property protected from attack.

43. Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, arts. 1–3, Oct. 18, 1907, 36 Stat. 2310 (1908) [hereinafter Hague Convention V]; Waldrop, *supra* note 23, at 227.

III. ANALYSIS

A. Legally, Does the Network Constitute a Weapon System?

The treaties that form the core of LOAC were largely drafted at a time when today's electronic technologies were scarcely dreamed of. Thus, the DOD Office of the General Counsel's statement regarding information operations techniques is equally applicable to network-enabled operations: "It is by no means clear what . . . techniques will end up being considered to be 'weapons' . . . ."[44] At this time, however—given the existing role that network-enabled operations play in the overall picture, and the application of regulatory, doctrinal, and traditional law of war principles—it is inaccurate to refer to the entire network as a "weapon system" for the reasons that will be explored.

"Network" defined. Rendering it difficult for LOAC analysis, the term "network" has been used in many different ways and has acquired different meanings. Sometimes, the "network" has been used to describe strictly military-only communications systems.[45] The "network" also has been used to

---

44. OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 6 (2d ed. 1999). It should be noted that from an Air Force doctrinal standpoint, the evolutions in network technology that form the basis for the "network as a weapon system" rhetoric would be categorized as the Network Operations (NetOps) component of Integrated Control Enablers (ICE), which "are not IO [Information Operations], but rather the 'gain and exploit' capabilities that are critical to all air, space, and information operations." John P. Jumper, *Forward* to U.S. DEP'T OF THE AIR FORCE, AIR FORCE DOCTRINE 2-5, INFORMATION OPERATIONS (2005). In defining ICE and its relationship to IO, Air Force Doctrine 2-5 provides as follows:

> ICE includes intelligence, surveillance, and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and precision navigation and timing (PNT). Information operations are highly dynamic and maneuverable. The transition between the find, fix, track, target, engage, and assess (F2T2EA) phases can be nearly instantaneous. The ICE components support this interactive relationship and strive to provide commanders continuous decision-quality information to successfully employ information operations.

Id. at 6.

45. In an armed conflict, the LOAC principle of "military necessity" certainly would allow military-only communications networks to be attacked, and would allow other

describe national and international communications infrastructures, including local networks, telecommunications switches, wireless networks, and Internet-linking technologies.[46] Indeed, the hallmark of our networked society is the inter-connectedness and convergence of numerous communication systems, including radio broadcast, land-based wireline, fiber optic, and satellite systems. As the latter, broader meaning appears to be the more prevalent meaning, we will employ it for purposes of this analysis, bearing in mind the potential for misunderstanding flowing from the lack of a single, widely agreed-upon definition.

"Weapon System" defined. Further rendering it difficult for LOAC analysis, what has been referred to as a "weapon system" has varied in meaning. Generally, a weapon is defined as an instrument of offensive or defensive combat.[47] The most authoritative Air Force guidance can be found in AFPD 51-4, which addresses Air Force regulatory compliance with LOAC and defines "weapons" as "[d]evices designed to kill, injure, or disable people, or to damage or destroy property."[48] It seems clear that a network, by itself, neither kills, injures, disables, damages nor destroys; it can only enable other devices, to which it is connected, in bringing about those ends. Networks will increasingly contribute to this effort, but, to reiterate, because networks are not designed to be the implements for the application of force unless they are linked to another technology system that can kill, injure, disable people or damage or destroy property, the networks themselves cannot credibly be referred to as "weapons."[49]

---

networks to be attacked if they made a direct contribution to the war effort. *See supra* notes 38–39 and accompanying text; *see also infra* note 63.

46. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 251, 833 (11th ed. 2003) (defining network and communication generally).

47. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 2589 (1981).

48. U.S. DEP'T OF THE AIR FORCE, AIR FORCE POLICY DIRECTIVE 51-4, COMPLIANCE WITH THE LAW OF ARMED CONFLICT 2 (1993).

49. Perhaps the type of use in which the network comes closest to being a weapon is in the area of Computer Network Attack (CNA). CNA refers to "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." JOINT CHIEFS OF STAFF, JOINT PUB 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS GL-5 (1998). However, even in the case

The analysis of whether a network can credibly be referred to as a "weapon system" builds on the above analysis. An examination of the DOD Dictionary of Military and Associated Terms[50] shows that "weapon system" is a more complex definition than "weapon." A weapon system is a "combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency."[51]

Applying the DOD definition, it appears that a weapon system, at a minimum, consists of a weapon or weapons and those supporting capabilities required to make it function. *Having already concluded that the network is not a weapon, it follows that the network does not meet the more encompassing definition of a weapon system.* Although communications networks are integral to some current weapon systems, references to the network *by itself* as a weapon system ignore the fact that the network is functioning as one of those supporting capabilities, and further ignore other elements of the weapon system such as personnel or materials. To the extent the net-centric warfare concept is realized, communications networks (or more specifically, the GIG) will become increasingly vital to virtually every networked weapon. Still, the net-centric warfare concept's end goal is providing timely, more useful information to the warfighter, who will remain as an important component of the weapon system. So, from a semantic point of view, even as the network becomes increasingly vital, it

---

of CNA, the network is more analogous to a medium through which a specific tool or weapon would be employed. Furthermore, the contexts in which networks are referred to as "weapon systems" generally are not speaking of CNA, but rather of the increasing importance of the networks under the net-centric concept. *See* ALBERTS, GARSTKA & STEIN, *supra* note 9, at 88. The legalities inherent in CNA operations have been broadly discussed and are beyond the scope of this discussion.

50. *See generally* JOINT CHIEFS OF STAFF, JOINT PUB 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS (1994) [hereinafter DOD DICTIONARY) (This publication contains definitions according to current military usage).

51. *Id*. at 413. It should be noted that manpower management regulations require DOD Components to determine which defense systems qualify as weapon systems for purposes of preventing DOD civilians and contract personnel from participating in military combat. *See* U.S. DEP'T OF DEF., MANPOWER MIX CRITERIA E2.2.5.1, http://www.defenselink.mil/prhome/docs/criteria_mix_04.doc [hereinafter MANPOWER MIX].

does not transcend its position as an enabler of various weapon systems.[52]

Somewhat complicating this analysis is the prevalent use of the term "weapon system" to describe the Air Operations Center (AOC). Under the Air Force's current Concept of Operations (CONOPs), the AOC is the "weapon system (personnel, capabilities and equipment) through which the JFACC [Joint Forces Air Component Commander] exercises command and control of aerospace forces."[53] Significantly, the reference to personnel, capabilities, and equipment as the elements of the weapon system seems to ignore Joint Publication 1-02's requirement that a weapon system contain a weapon. Although one could argue that weapons fit within the term "capabilities," it is clear that none of the capabilities inherent within the AOC are the implements through which harm is directly inflicted upon the enemy.

Since the AOC is not a weapon system in the traditional sense, or according to the definition, one must question whether this CONOP represents an expansion of the scope of the term "weapon system," or, alternatively, whether this represents a scenario where policy concerns have driven the use of the term even though it is not precisely correct. In the absence of other expansive uses of the term, the latter conclusion seems more apt. Further, continued use of the term "weapon system" to describe communications networks and other systems that are not weapon systems in the traditional sense could eventually fuel an argument that the term itself has expanded to include

---

52. While one could argue that as weapon systems become increasingly dependent on the network, it could at some point fit within the definition as "services" that are "required for self-sufficiency," such a conclusion would only make the network a *part* of various weapon systems. DOD DICTIONARY, *supra* note 50, at 413. A contrary argument could be made that the network is not a part of any particular weapon system, but rather is the conduit through which various weapon systems can gain information. Indeed, the net-centric concept may challenge the very idea of the weapon system as a discrete, self-sufficient unit, as has been the case historically. To the extent this results in the expansion of the weapon system concept to include every system on which it relies, the definition may lose its utility as an effective discriminator.

53. U.S. DEP'T OF THE AIR FORCE, SECTION L: INSTRUCTIONS, CONDITIONS AND NOTICES TO OFFERORS § 1.0 (2005), http://herbb.hanscom.af.mil/dowload.asp?rfp=R495&FileName=AOC_Section_L_7_Sep_05_Final_05.doc.

such systems.

B. What Legal Implications Follow from Continued Use of the "Network as a Weapon System" Terminology with Respect to (1) Targeting, (2) Military Manning, (3) Contractors and Other Civilian Portions of the Network, and (4) U.S. Policy on Weapons in Outer Space?

This subpart of the discussion will identify some of the requirements and ramifications that generally are associated with the fielding, operation, and military application of weapons or weapon systems. While merely calling something a "weapon system" may not mean that it indeed is one for the purposes of these requirements, it may complicate the military's ability to credibly explain the failure to accomplish these requirements. In viewing these requirements, one must ask to what extent the advantages of referring to networks as "weapon systems" outweigh the potential disadvantages in terms of imposing unnecessary requirements, or in terms of the effort and possible loss of credibility associated with justifying the failure to fulfill those requirements.

1. Targeting Implications

Lawful targeting is generally a function of the principles of necessity and proportionality.[54] There is little doubt that as networks become increasingly important parts of various weapon systems, they will likewise become increasingly important targets for U.S. adversaries, irrespective of what we call them. Furthermore, those networks providing an effective contribution to ongoing operations will doubtless be viewed under LOAC targeting principles as legitimate targets. The key factor in assessing LOAC implications here lies in how networks will actually be deployed and intended for use against a potential enemy. However, as this area of the law relating to modern communications technology is not settled, the "network as a weapon system" terminology could be one factor used in assessing LOAC implications of network use during warfare.

---

54. *See generally* Rebecca Grant, *In Search of Lawful Targets*, AIR FORCE MAGAZINE, Feb. 2003, at 38 (detailing evolution of the concept of lawful targets).

A danger of continued use of the terminology lies in the possible targeting of networks or network segments not making an effective contribution to the war effort. This danger is especially evident, as it is by no means abundantly clear which networks or network segments lack connections to weapon systems. It might later be difficult for the United States to gain international support in condemning an attack on portions of the Internet or financial networks if the statements of the nation's public officials could be construed, rightly or wrongly, as characterizing them as our weapon system(s) or part(s) thereof. Notwithstanding the fact that this discussion has concluded that the network is not a weapon system, there is no international legal precedent from which to draw in reaching this conclusion, and certainly LOAC is unsettled with respect to electronic applications. Therefore, it is possible that an international court could look at continued reference by U.S. military communicators to the "network as a weapon system" as one factor, among others, in evaluating whether the network is in fact a weapon system. Recognizing this possibility, continued use of this terminology, which infers the existence of a weapon system, could serve to potentially label a communications system as a weapon system when it is not reasonable to do so, thereby potentially risking the possibility that a tribunal could later impose obligations that would not otherwise exist.

2. Military Manning Implications

Continued reference to the network as a "weapon system" could also cause difficulties from a military manning standpoint. Generally, the manpower mix of military versus civilian positions is viewed as a policy issue, and weapon systems are to be manned by military personnel.[55] Yet against that backdrop, with limited exceptions, LOAC requires that only members of regular armed forces be entitled to employ use of force against the enemy in an international conflict. Contractors and other civilians cannot exercise such force because they are not subject to an effective disciplinary system, are not under the command of officers responsible for their conduct, and generally may not

55. MANPOWER MIX, *supra* note 51, at E1.1.1.2.

have been trained in the law of war.[56] Thus, at some point it becomes incumbent upon the military to either man the "network weapon system" with military personnel, or make a convincing explanation of the reasons not to do so. Additionally, DOD manpower standards require manpower authorities to designate manpower as "military" if "the incumbents operate weapon systems against the enemy."[57]

If contractors or other civilians employ a weapon system in a manner viewed as taking an active, direct part in hostilities by engaging in acts likely to cause actual harm to the personnel or equipment of an adversary, they lose their protected status.[58] The precise point at which civilians providing combat support services become "active" participants in the conflict, and in so doing forfeit their protected status, is not defined with clarity in international law; there is no bright line.[59] For example, there is no general consensus about whether the "gathering and dissemination of intelligence" (often a key military purpose of sophisticated communications systems) constitutes direct participation in hostilities.[60] As the line is not a clear one, one must consider whether calling a network operated at least in part by civilians a "weapon system" promotes or detracts from the desired perception of the United States as a nation that scrupulously honors its obligations under LOAC.[61]

---

56. *See supra* notes 30–33 and accompanying text. Also, while contractors historically have not been trained in LOAC, this is changing. Recently enacted federal law requires that all federal employees and civilian contractors engaged in the handling or interrogation of individuals detained by the DOD now complete such training annually. *See* Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, §§ 1091–1093, 118 Stat. 1811, 2070.

57. *See* MANPOWER MIX, *supra* note 51, at E1.1.1.2.

58. *See supra* notes 30–37 and accompanying text.

59. *See* Waldrop, *supra* note 23, at 229–30. Nonetheless, it is generally agreed that noncombatant participation in activities such as weapons production, military engineering, and military troop transport is not prohibited, even though these acts ultimately harm an enemy. *See id*.

60. *Id*.

61. As the line is not a clear one, one legal writer has argued that caution should be exercised in assigning contractors or other civilians to positions in which information can be used offensively against the enemy and in devising contract specifications for offensive information capabilities. *See id*.

3. Implications for Contractor and Other Civilian Portions of the Network

Currently, contractors and other civilians operate portions of the network used by the military, and significant portions of DOD's network communications travel over civilian pathways.[62] These pathways may include facilities ranging from landlines leased from U.S. telecommunications providers, to transponders on orbiting satellites owned by international consortia. This fact could implicate the subjects of targeting[63] and manning[64] mentioned above, and, in the case of assets acquired from foreign or international consortium concerns, raises an issue of neutrality in armed conflict. This "neutrality issue" will be examined next in more detail.

As noted previously, armed forces and civilian users increasingly depend upon the same commercial space systems.[65] Under LOAC principles, legitimate military targets—a category

---

62. *See supra* notes 21–26 and accompanying text.

63. Under LOAC, civilian objects cannot generally be the subject of an intentional direct attack. *See supra* notes 34–35, 39, 43 and accompanying text. Given that ninety-five percent of U.S. military telecommunications currently takes place via the public switched network, it could be argued that military use of the network results in the network being a potentially legitimate target under LOAC, perhaps placing innocent civilians in undue danger of collateral injury. GREENBERG, GOODMAN & SOO HOO, *supra* note 3, at 194. It would be difficult for the United States to argue that its telecommunications system, as a shared infrastructure, cannot be considered a military target when it could have developed parallel systems for purely military use, like the Defense Switched Network. *See* DEF. INFO. SYS. AGENCY, U.S. DEP'T OF DEF., THE DEFENSE SWITCHED NETWORK (DSN): A BRIEF HISTORY OF THE DSN, http://www.disa.mil/gs/dsn/dsn_history.html (last visited Jan. 29, 2005) (defining DSN as "a primary system of communication during peacetime, periods of crisis, preattack, non-nuclear, and post-attack phases of war").

64. Under LOAC, only members of regular armed forces are entitled to employ military measures against the enemy; DOD regulatory manpower standards require the designation as "military" those positions whose incumbents would operate weapon systems against an enemy. *See supra* notes 30–33 and accompanying text. Again, given that ninety-five percent of U.S. military telecommunications takes place via the public switched network and that the U.S. military admits to using the network—which includes the national telecommunication infrastructure—as a "weapon system," it could be argued that at least that portion of the infrastructure being used as a weapon system must be manned by military personnel. *See* Greenberg, Goodman & Soo Hoo, *supra* note 3, at 194; Donahue, *supra* note 4.

65. *See supra* notes 21–26 and accompanying text.

that most assuredly includes weapons and weapon systems—must be distinguished from protected civilian objects, anticipated collateral damage must be weighed against expected military damage, and excessive civilian damage must be avoided.[66] However, force may lawfully be used against objects that an adversary is using for a military purpose if neutralization of the object would offer a military advantage.[67] Applying these principles to neutral states, if a neutral state permits its space systems to be used by a belligerent's military, the opposing belligerent would have the right to demand that the neutral state stop doing so. If the neutral state is unwilling or unable to prevent use by one belligerent, it could be permissible for the other belligerent to prevent the offending use.

In the context of space systems used in a time of conflict, before resorting to force, a belligerent could demand that a neutral state not provide satellite services, such as imagery, navigation, and weather information, to the belligerent's adversary. Articles VIII and IX of the Hague Convention V provide that a neutral state is not required to restrict a belligerent's use of "telegraph or telephone cables or of wireless telegraphy apparatus" belonging to it or to companies or private individuals, as long as these facilities are provided impartially to both belligerents.[68] On the other hand, Article III forbids belligerents from erecting or using previously erected devices on the territory of a neutral for communications with belligerent forces or for "military purposes."[69] Article V obligates neutral states not to allow those actions prohibited by Article III to take place on its territory.[70]

The extent to which either of these provisions—adopted when satellite communications were scarcely dreamed of—apply to information traveling across satellites registered to neutral states is unclear. Continued reference to the network as a "weapon system" could, however, influence the development of

66. *See supra* notes 33, 42 and accompanying text.

67. *See supra* notes 38–41 and accompanying text.

68. Hague Convention V, *supra* note 43, ch. 5, arts. 8–9.

69. *Id*. ch. 5, art. 3.

70. *Id*. ch. 5, art. 5.

this area in a manner inconsistent with U.S. interests, as few would dispute that operation of a weapon system from or through the territory of a state would jeopardize that state's claims to neutrality. Thus, foreign concerns may be less likely to provide communications services if the U.S. government is referring to them as weapon systems.

4. Implications for Weapons in Outer Space

Existing international treaty restrictions on weapons in outer space are in fact very limited—prohibiting placement of weapons of mass destruction into orbit, and requiring any use of the moon and other celestial bodies "exclusively for peaceful purposes."[71] In light of the longstanding use—with virtually no international objection—of satellites for military purposes by the United States, the former Soviet Union, and numerous other states, international debate has largely shifted to the question of the weaponization of outer space.[72] Although the United States has not foreclosed the idea of placing weapons in space, it has not yet expended the political capital to do so.[73] Given that satellite communications are integral to present and future military networks, the "weapon system" terminology could serve as the basis for a conclusion that the United States has already crossed the space weapons threshold, possibly emboldening near-peer states to more aggressively pursue their own space weapon programs.[74]

---

71. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27. 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205. While a review of the law of outer space is beyond the scope of this discussion, it is clear that international legal and policy issues remain over military applications in outer space. The predominant view is that outer space remains open to military use. *See* Christopher M. Petras, "*Space Force Alpha:" Military Use of the International Space Station and the Concept of "Peaceful Purposes*," 53 A.F. L. REV. 135, 159 (2002).

72. *See generally* Petras, *supra* note 71 ("examin[ing] the permissibility of military activity . . . onboard the [International Space Station]); Robert A. Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 A.F. L. REV. 1 (2000).

73. *See* Ramey, *supra* note 72, at 130–31 (noting that United States weaponization of space is inevitable).

74. Taking the position that certain satellite systems—as part of the network—are also weapon systems raises questions of the need of "dual target" protocols in circumstances in which there is military use of commercial or other civilian satellite

IV. CONCLUSION

In the final analysis, while there is no legal rule or principle violated by calling the network a "weapon system," such practice appears to be inconsistent with current DOD regulatory definitions. More importantly, continued use of the terminology could work at cross purposes to important U.S. policy goals, and could negatively influence the evolution of the LOAC as it adapts to new means and methods of warfare. Based on our understanding of the term, it is difficult to conclude that the network is, or reasonably will become, a weapon system unto itself. With legal precedent lacking, continued inaccurate use of the term could serve to potentially undermine the U.S. military's efforts to flexibly use the network to enhance its capabilities by providing additional rationale for the nation's adversaries to target the network, and by raising unnecessary questions regarding its network manning decisions and its decisions to utilize civilian, foreign, and international consortium network elements.

---

systems. As noted previously, armed forces and civilian users increasingly depend upon the same space systems. *See supra* notes 23–26 and accompanying text. Under principles of LOAC, satellites used for both commercial and military purposes could become legitimate military targets. Accordingly, the United States could be criticized if it does not pursue developing protocols that separate commercial and or civilian use from military use for targeting purposes.