1-1-1999

Discrimination in the Laws of Information Warfare

Mark R. Shulman
Pace Law School

Notes

Discrimination In the Laws of Information Warfare

As societies and economies increasingly rely on electronic telecommunications, they grow more vulnerable to threats from other computer systems. At the same time, states' military and intelligence organizations are increasingly developing the capability to attack and defend these assets. As with the introduction of earlier weapons systems, would-be users express the belief that the laws restraining warfare no longer apply. This Note seeks to explain the emerging relationship between electronic telecommunications and the laws of war. In particular, this Note seeks to show how the norm requiring the discrimination between military and civilian objectives may be retained in an era of long-distance warfare. Finally, it presents a model protocol to guide warriors and lawyers in planning or judging the legitimacy of information operations.

I. INTRODUCTION[1]

War is thus an act of force to compel our enemy to do our will . . . . Attached to force are certain self-imposed, imperceptible limitations hardly worth mentioning, known as international law and custom, but they scarcely weaken it.[2]

—Carl von Clausewitz

1. In 1995-1996, I served as a professor at the Air War College, United States Air Force's senior service school. However, this Note is not directly informed by any classified information, nor does it represent anyone's opinions but my own.

2. CARL VON CLAUSEWITZ, ON WAR 75 (Michael Howard & Peter Paret eds. & transs., 1976) (1832). Likewise, centuries before, Cicero claimed that *inter arma silent leges* (in war the law is silent).

> *War consists largely of acts that would be criminal if performed in time of peace—killing, wounding, kidnapping, destroying or carrying off other peoples' property. Such conduct is not regarded as criminal if it takes place in the course of war, because the state of war lays a blanket of immunity over the warriors. But the area of immunity is not unlimited, and its boundaries are marked by the laws of war.*[3]
>
> —Telford Taylor

As Telford Taylor noted, the laws of war distinguish soldiers, sailors, marines, airmen, and even spies from murderers, kidnappers, and arsonists. The distinction Taylor describes is inextricable from legal notions of war, a conclusion down-played or possibly misconstrued by strategist Carl von Clausewitz in the cited excerpt from his seminal treatise, *On War*.[4] In reality, the laws of war have long restrained its legitimate conduct. These constraints include distinctions between campaign and non-campaign seasons,[5] and they guide "the selection of methods, of weaponry and of targets."[6] They provide specific immunities for certain persons and places. They distinguish between combatants and noncombatants, between legitimate and illegitimate targets.[7] Over the millennia and particularly the past half-century, these rules have expanded and been codified in international law. Despite these remarkable advances, discrimination between legitimate and illegitimate weapons, methods, and targets has also eroded over the past half-century, as warfare expanded from limited set-piece encounters into virtually unlimited wars between multi-state alliances.[8] Even so, this critical norm of humanitarian law has survived. As the laws improved, the breaches became more stark.

---

3. TELFORD TAYLOR, NUREMBERG AND VIETNAM: AN AMERICAN TRAGEDY 19 (1970).

4. *See* Michael Howard, *Introduction* to THE LAWS OF WAR: CONSTRAINTS ON WARFARE IN THE WESTERN WORLD 2 (Michael Howard et al. eds., 1994) [hereinafter LAWS OF WAR]. While the formal laws of war were less developed in the Napoleonic era than they are today, Howard notes that Clausewitz "knew very well . . . that the conduct of war was subject to considerably greater and more perceptible limitations in his own time than it had been in the days of, say, Genghis Khan." *Id.*

5. Josiah Ober, *Classical Greek Times*, *in* LAWS OF WAR, *supra* note 4, at 13-26.

6. DOCUMENTS ON THE LAWS OF WAR 5 (Adam Roberts & Richard Guelff eds., 2d ed. 1989) [hereinafter Roberts & Guelff].

7. For an introduction to the notion of the immunity of non-combatants, see Howard, *Constraints on Warfare*, *in* LAWS OF WAR, *supra* note 4, at 3-11. Examples of this principle abound in history. *See* Robert Stacey, *Age of Chivalry*, *in* LAWS OF WAR, *supra* note 4, at 29-31; Geoffrey Parker, *Early Modern Europe*, *in* LAWS OF WAR, *supra* note 4, at 41, 46; Gunther Rothenberg, *The Age of Napoleon*, *in* LAWS OF WAR, *supra* note 4, at 87-97.

8. For a description and analysis of the most horrifying example of the expansion of war, see David Alan Rosenberg, *Nuclear War Planning*, *in* LAWS OF WAR, *supra* note 4, at 160; *see also* David Alan Rosenberg, *The Origins of Overkill: Nuclear Weapons and American Strategy, 1945-1960*, 7 INT'L SECURITY (Spring 1983) at 3-71.

This Note analyzes some of the problems and suggests some guidelines for retaining the critical norm of discrimination in the era of long-distance, impersonal, and undeclared war in the information age. Part I introduces discrimination—the long-standing norm requiring that military planners and operators distinguish between legitimate military objectives and non-combatants. Part II grapples with the fast-changing subject of warfare in the information age. Part III tackles the problems of applying discrimination today. Discrimination faces many new challenges, but the traditional means for formulating solutions still offer valuable tools for finding legal and ethical constraints on the application of force via electronic media. Part IV provides a model protocol that acknowledges these international norms, formalizing them in international law. Finally, Part V offers a few concluding remarks.

While states frequently engage in armed conflict,[9] aggressive international war has been outlawed—first by the Kellogg-Briand Treaty (1928)[10] and more efficaciously by the UN Charter (1945).[11] Nonetheless, "[t]he application of the laws of war does not depend upon the recognition of the existence of a formal state of 'war,' but (with certain qualifications) comprehends situations of armed conflict and military occupation in general, whether formally recognized as 'war' or not."[12]

Thus the tradition of the laws of war has evolved into the law of armed conflict (LOAC).[13] Moreover, because the laws limiting a state's

---

9. The most interesting inquiry into the end of formal war may be MARTIN VAN CREVELD, TRANSFORMATION OF WAR (1991). *See also* Paul Kennedy & George J. Andreopoulos, *The Laws of War: Some Concluding Reflections*, *in* LAWS OF WAR, *supra* note 4, at 214-25.

10. General Treaty For the Renunciation of War as an Instrument of National Policy ("Kellogg-Briand Pact"), Aug. 27, 1928, T.S. No. 796.

11. U.N. CHARTER arts. 2(4) ("All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."), 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations . . . .").

12. Roberts & Guelff, *supra* note 6, at 1.

13. For the transition from laws of war to LOAC, see Lt. Col. Marc L. Warren, *Operational Law—A Concept Matures*, 152 MIL. L. REV. 33, 35 (1996) ("Military operations other than war present numerous and diverse legal issues."). The U.S. codification of LOAC began with the field manual Columbia Law School professor Francis Lieber wrote for the Union Army during the Civil War. *See* U.S. Army General Order No. 100, Instructions for the Government of Armies of the United States in the Field (1863) (addressing legal issues about the treatment of the enemy without a declaration of war), *available in* THE AVALON PROJECT AT THE YALE LAW SCHOOL: DOCUMENTS IN LAW, HISTORY, AND DIPLOMACY, <http://www.yale.edu/lawweb/avalon/lieber.htm> [hereinafter Lieber Code]. *See* LAWS OF WAR, *supra* note 4, at 6. General Order No. 100 has undergone significant revisions but remains the basic Field Manual of the U.S. Army. *See* Lieber Code, *supra*, at 100-05. "Although such national manuals also have a function in providing evidence of the law, they

entry into hostility are now governed by a variety of international laws that have replaced the just war tradition (*jus ad bellum*), this Note will concentrate on the *jus in bello*—restraints on the conduct of warfare.[14]

II. INFORMATION WARFARE

One of the most dynamic types of "armed conflict" is Information Warfare ("IW").[15] Ironically, IW is neither 'armed' in the traditional sense, nor does it necessarily involve 'conflict.' Dramatic hypothetical accounts of IW abound and best serve to introduce this apparent paradox. Consider a few hypothetical situations. Special forces detonate a small non-nuclear electromagnetic pulse weapon (EMP) near an enemy nation's central bank computer storage facility, burning out the electronics that transact, communicate, and store the nation's financial information. Or, an intelligence operator hacks from his own country into another nation's telecommunications network, planting computer code that destroys the software running that system. Or, a military operator feeds into another state's television broadcast "morphed" images of that state's religious leader engaged in sacrilegious acts. Or, another operator hacks into a target nation's computer network coordinating air or rail traffic to reprogram the systems to shut down without warning.[16] At the extreme, each of these hypothetical situations would lead to dramatic results: economies

---

are in general bound to be viewed with some caution." Roberts & Guelff, *supra* note 6, at 7.

Today, the applicable law might preferably be called "international humanitarian law applicable in armed conflicts" or "Operational Law." For the former term, see International Committee of the Red Cross (ICRC), *Final Act of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict* (1977). The ICRC was founded at the 1863 Geneva International Conference "with the express purpose of reducing the horror of warfare." Roberts & Guelff, *supra* note 6, at 8.

For the latter term, "Operational Law," see Lt. Col. David E. Graham, *Operational Law: A Concept Comes of Age*, ARMY LAW., July 1987, at 9 ("that body of law, both domestic and international, impacting upon legal issues associated with the planning for and deployment of US Forces overseas in both peacetime and combat environments."); *see also* Warren, *supra*, at 36.

14. Roberts and Guelff note the "cardinal principle that *jus in bello* applies in cases of armed conflict whether the conflict is lawful or unlawful in its inception under *jus ad bellum*." Roberts & Guelff, *supra* note 6, at 1.

15. Douglas Waller, *Onward Cyber Soldiers*, TIME, Aug. 21, 1995, at 39 ("'information warfare'—now the hottest concept in the halls of the Pentagon").

16. These hypothetical situations are based directly on those in Waller, *supra* note 15, 39-44. *See also* Lt. Col. Kurt C. Reitinger, *New Tools for New Jobs,* 124 PROC. U.S. NAVAL INST. 37 (Apr. 1998) (discussing the need for new doctrine to successfully employ new non-lethal military technology). *See also* Elaine Scarry, *The Fall of TWA 800: The Possibility of Electromagnetic Interference*, N. Y. REV. BOOKS, Apr. 9, 1998.

would be destroyed; societies would disintegrate; planes and trains would crash. As a result, governments might fall. Thousands of people would likely perish. As dramatic as these hypotheticals are, IW may prove complicated and possibly even more devastating than these examples suggest.[17] If subtle or carefully played, attacks might go undetected, and the target countries or organizations would not even know to protect themselves against follow-on attacks. For example, an air-traffic controller would wonder why his system crashed at such an inopportune moment. A banker would wonder about a million dollar discrepancy in a large transaction. IW's potential impact ranges from the cataclysmic to the trivial. And yet, we have only begun to consider what it is and how it may be pursued.

Definitions of this fast-changing and mostly classified set of capabilities and operations—IW—vary. Each of the U.S. military services is currently engaged in studying IW. Each has considerable experience and expertise in information operations of one variety or another.[18] While their definitions do not vary significantly, this Note adopts that of the Air Force (USAF), which appears to be the lead agency. IW is any "action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against

---

17. For context on *jus ad bellum* [just war theory], *see* MICHAEL WALZER, JUST AND UNJUST WARS, pt. 2, at 51-124 (1977). The most critical and difficult *jus ad bellum* issues for IW include: 1) problems of proof when a party suspects an information assault; and 2) deciding when such an assault attains the level of an "armed attack" as required under U.N. CHARTER art. 51, or "aggression" as defined by the U.N. General Assembly, G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., Supp. No. 31, art. 1, U.N. Doc. 1/9631 (1974). For a start, see George I. Seffers & Mark Walsh, *Does a Cyber Attack Constitute War?*, DEFENSE NEWS, Sept. 8, 1997, at 1.

A recent article does address some of the larger international legal implications. *See* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272 (1996) (arguing that successful resolution of international conflicts in the information age will require a new theoretical structure of law).

18. For instance, the U.S. Army has long had the standing capability to engage in psychological operations such as those relying on broadcast reports or distributing pamphlets to encourage an enemy to retire from the field. *See* Army Chief of Staff, Gen. Gordon R. Sullivan & Col. James M. Dubik, *War in the Information Age*, 74 MIL. REV. 46 (July 1993), *reprinted in* 94-4 LANDPOWER ESSAYS SERIES (May, 1994). The Navy also has considerable expertise. *See* Vice Admiral Arthur K. Cebrowski & John J. Gartska, *Network-Centric Warfare: Its Origin and Future*, 124 PROC. U.S. NAVAL INST. 88 (Jan. 1998). The Air Force has an Information Warfare squadron at Shaw AFB, North Carolina. *See* Col Phillip A. Johnson, USAF, Associate Deputy General Counsel (IA), Office of the General Counsel, DOD, *in Opening Shots: Information Warfare and the Law*, brief to FY 98, US Air Force Judge Advocate General School, Legal Aspects of Information Operations Symposium, Maxwell AFB, Ala., app. F, *Principal DoD Information Warfare Organizations*, at F-33-34. The USAF also has an Information Warfare Center at Kelly, AFB, Texas. Information superiority is an official Air Force core competency, alongside such traditional concerns as rapid global mobility and precision engagement. *See Global Engagement* (visited Mar. 8, 1999) <www.af.mil/current/global/>.

those actions; and exploiting our own military information functions."[19] It includes electronic warfare, military deception, physical destruction, security measures, and information attack.[20] The Air Force defines information in this context as "data and instructions" and distinguishes IW from warfare in the information age generally, including in the former only those attempts to influence the information directly.[21] In

---

19. DEP'T OF THE AIR FORCE (USAF), CORNERSTONES OF INFORMATION WARFARE 3-4 (1995) [hereinafter CORNERSTONES]. *See also* OFFICE OF THE CHIEF OF NAVAL OPERATIONS, DEP'T OF THE NAVY, OPNAVINST 3430.26, at 1 (Jan. 18., 1995) ("Information warfare is the action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.").

The literature on IW is small but growing and includes: THE INFORMATION REVOLUTION AND NATIONAL SECURITY (Stuart J.D. Schwartzstein ed., 1996); WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY (1994); NATIONAL RESEARCH COUNCIL (NRC)'S SYSTEM SECURITY COMMITTEE, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE (1991); THE FIRST INFORMATION WAR (Alan D. Campen ed., 1992); MANUEL DELANDA, WAR IN THE AGE OF INTELLIGENT MACHINES (1991); KENNETH C. ALLARD, COMMAND, CONTROL, AND THE COMMON DEFENSE (1996); PAUL STRASSMANN, THE POLITICS OF INFORMATION MANAGEMENT (1995); MARTIN C. LIBICKI, THE MESH AND THE NET: SPECULATIONS ON ARMED CONFLICT IN A TIME OF FREE SILICON (1995); DAVID F. RONFELDT, CYBEROCRACY, CYBERSPACE, AND CYBEROLOGY: POLITICAL EFFECTS OF THE INFORMATION REVOLUTION (1991); GERALD HUST, TAKING DOWN TELECOMMUNICATIONS (1994); BATTLEFIELD OF THE FUTURE: 21ST CENTURY WARFARE ISSUES (Barry R. Schneider & Lawrence E. Grinter eds., 1995); MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE (1995).

The periodical literature includes: John Arquilla & David Ronfeldt, *Cyberwar is Coming*, 12 COMP. STRATEGY 141 (Apr.-June 1993); Martin C. Libicki & James A. Hazlett, *Do We Need an Information Corps?*, JOINT FORCE Q. (Autumn 1993); P.C. Emmett, *Software Warfare: The Emerging Future*, ROYAL UNITED SERVICES INST. J. (Dec. 1992); Mary Fitzgerald, *Russian Views of Electronic Signals and Information Warfare*, AM. INTELLIGENCE J. (Spring-Summer 1994); John Rothrock, *Information Warfare: Time for some Constructive Skepticism*, AM. INTELLIGENCE J. (Spring-Summer 1994); Craig Johnson, *Information War—Not a Paper War*, J. ELECTRONIC DEF. (Aug. 1994); Chet Morris et al., *Weapons of Mass Protection: Nonlethality, Information, Warfare, and Airpower in the Age of Chaos, in* AIRPOWER J. (Spring 1995); George J. Stein, *Information Warfare, in* AIRPOWER J. (Spring 1995); Richard Szafranski, *A Theory of Information Warfare: Preparing for 2020, in* AIRPOWER J. 77 (Spring 1995); Richard Szafranski, *When Waves Collide: Future Conflict*, JOINT FORCE Q. (Spring 1995); Jim Anderson, *Chugging up the Onramp of the Info Interstate*, FOR. SERVICE J. (Mar. 1995); *Defense Technology*, ECONOMIST, June 10, 1995, supp. 5-20; Donald E. Ryan, *Implications of Information-Based Warfare*, JOINT FORCE Q. (Autumn-Winter 1994-95); H.D. Arnold et al., *Targeting Financial Systems as Centers of Gravity: 'Low Intensity' to 'No Intensity' Conflict*, 10 DEF. ANALYSIS (1994); Spacecast 2020, *Leveraging the Infosphere: Surveillance and Reconnaissance in 2020*, AIRPOWER J. (Summer 1995).

20. The USAF defines information attack as "[d]irectly corrupting information without visibly changing the physical entity within which it resides." CORNERSTONES, *supra* note 19, at 6.

21. The information age is most famously explained by the Tofflers. *See* ALVIN TOFFLER & HEIDI TOFFLER, WAR AND ANTI-WAR: SURVIVAL AT THE DAWN OF THE 21ST CENTURY (1993) (the emerging knowledge-based society will use knowledge-based systems to conduct warfare). *See also* Mark R. Shulman, *War and Anti-War*, 121 PROC. U.S. NAVAL INST. 84 (Oct. 1994) (book review).

For an overview of information superiority, see Cebrowski & Gartska, *supra* note 18, at 28-35; and Col. Owen D. Ryan & John J. Gartska, *The Emerging Joint Strategy for Information*

addition to being defined, IW also needs to be placed within the broader context of military operations.

IW operations potentially range across the entire spectrum of military capabilities. The traditional state-sponsored uses of force define the categories of conflict. Because the international system has effectively outlawed aggressive war, most cross-border conflicts are styled "self-defense" or "defensive."[22] At the most basic level, I distinguish between a military operation based on an "offensive defense" and one based on a "defensive defense."[23] For example, the defensive can be offensive, as it was when the Allied Forces landed at Normandy in 1944 or in Kuwait and Iraq in 1991.[24] These are offensive measures undertaken in collective self-defense. The defense was defensive when the Anglo-French forces attempted to keep the *Wehrmacht* from pushing them out of France in 1940 or when the UN Forces sent USAF F-15s to Saudi Arabia fifty years later to deter the Iraqi invasion. Strictly defensive or security operations include camp or perimeter defenses like sentries firing sidearms when they detect a perimeter breach.

In IW, these distinctions also apply. Offensive defense IW operations might include: 1) active collection of intelligence about

---

Superiority, US DOD, Joint Staff J-6, information briefing (visited Mar. 4, 1999) <http://www.dtic.mil/JCS/J6/edu_tr.html>.

22. U.N. CHARTER art. 51 (nothing "shall impair the inherent right of individual or collective self-defense").

23. Throughout most of the nineteenth century, coastal defense boats and fortresses provided the United States with defensive defense. As they evolved in the 1880s and 1890s, battleships provided a new offensive defense, defending the nation instead by threatening to bring the battle to the enemy. Strictly defensive measures were never abandoned; if a spy attempted to destroy a naval vessel in a U.S. harbor, he would have been arrested or killed. *See* MARK RUSSELL SHULMAN, NAVALISM AND THE EMERGENCE OF AMERICAN SEA POWER, 1882-1893, at 1-2 (1995). For a graphic explanation of these types of warfare, see *id.*; see also *infra*, Appendix II.

24. There are potential military applications for information operations that are neither offensive nor defensive. Consider, for instance, the use of radio jamming when Hutu extremists are broadcasting "lists of enemies to be hunted down and butchered." Jamie Frederic Metzl, *Information Intervention*, FOREIGN AFF. 15-20 (Nov./Dec. 1997). For more extensive treatment, see also Jamie Frederic Metzl, *Rwandan Genocide and the International Law of Radio Jamming*, 91 AM. J. INT'L L. 628 (1997) (proposing "a narrow exception to the general international standard supporting the free flow of information . . . for clear cases of incitement to genocide where the occurrence of that genocide appears imminent" or for cases of mass human rights abuse). For a comprehensive program, see CARNEGIE COMMISSION ON PREVENTING DEADLY CONFLICT, FINAL REPORT: PREVENTING DEADLY CONFLICT (1997). *See also* Warren, *supra* note 13, at 34-37; *Joint Doctrine for Military Operations Other Than War*, Joint Chiefs of Staff Publication 3-07 (1995) (visited Mar. 24, 1999) <www.dtic.mil/doctrine/jel/C_pubs2.htm>.

information systems;[25] 2) unauthorized intrusions into information systems; 3) introduction of vulnerabilities into information systems; 4) corruption or denial of data; and 5) disabling or destroying information systems.[26] These are sometimes referred to as "information operations." United States law requires that the armed forces and intelligence services of the United States undertake this type of operation only against particular foreign opponents under executive order, presumably as part of a coordinated national policy to implement unilateral or multilateral defensive operations.[27]

The legal issues of offensive information operations have never been brought before U.S. courts. The military and intelligence agencies, however, would likely be authorized to undertake them when ordered by the Executive. This law has not yet been pled or decided, but it seems like a small step from traditional forms of covert action to the types of net-centric IW considered in this Note.[28] The Central Intelligence Agency (CIA) and the Department of Defense (DOD) are granted general authority to undertake covert action at the direction of the National Security Council.[29] The breadth of this authority was clarified by Executive Order No. 12,333, which provides in part:

> No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period

---

25. Active collection includes such measures as infiltrating another country's computer systems, either by sitting down in front of its dedicated terminals or via telecommunications systems from a distance. Compare this with passive gathering, which includes such measures as intercepting broadcasted communications.

26. This list is suggested by Col Phillip A. Johnson. *See* Johnson, *supra* note 18. Another more comprehensive list proposes that offensive defense operations could include: "psychological operations, military deception, jamming of enemy information systems, signal intelligence (SIGINT), and attacks on enemy information systems by physical destruction or by electronic means." OFFICE OF THE JUDGE ADVOCATE GENERAL, HEADQUARTERS UNITED STATES AIR FORCE, PRIMER ON LEGAL ISSUES IN INFORMATION OPERATIONS 13-14 (3d ed., draft, Oct. 1997) [hereinafter PRIMER]. Note that both lists come from the USAF indicating an ever-changing reality.

27. For a more complete discussion of the war powers, see Louis Henkin, *The Use of Force: Law and U.S. Policy, in* LOUIS HENKIN ET AL., RIGHT V. MIGHT: INTERNATIONAL LAW AND THE USE OF FORCE 37-69 (2d ed. 1991). For operations conducted by intelligence services, see ROY GODSON, DIRTY TRICKS OR TRUMP CARDS: U.S. COVERT ACTION AND COUNTERINTELLIGENCE (1995); W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW (1992); Robert F. Turner, *Coercive Court Action and the Law Regulating Covert Action*, 20 YALE J. INT'L L. 427 (1995) (book review).

28. For more in this volume on this concept and its legal implications, see Michael N. Schmitt, *Computer Network Attach and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

29. National Security Act of 1947, 50 U.S.C. §§ 403, 413 (1982); Foreign Assistance Act of 1961 § 662, 22 U.S.C. § 2422 (1988).

> covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any special activity *unless the President determines that another agency is more likely to achieve a particular objective.*[30]

Michael Reisman and James Baker conclude that the "unless" clause "effectively leaves the matter up to the President."[31]

As with the more traditional forms of covert action, particular IW operations are constrained by LOAC as well as the requirement for executive authorization.[32] As with all operations, the choice of tool or weapon is critical for the legality of the operation. While the effects of many of these operations could be achieved with conventional arms, this Note concentrates on those undertaken via the electronic telecommunications media. Dropping an explosive on a computer server or a hydroelectric dam, using a laser to destroy a telephone line, or using a directed electro-magnetic pulse (EMP) to disrupt a satellite's operations have enough similarity to conventional warfare that the traditional LOAC would still apply. While not simple, these scenarios do not present new categories of challenges like the type under analysis here. This Note concentrates on information attacks, those that seek to alter "information without visibly changing the physical entity within which it arises."[33] Rather than explosives, lasers, or directed EMP's, it

---

30. Exec. Order No. 12,333, § 1.8(e), 46 Fed. Reg. 59941 (1981) (emphasis added). Section 1.11(c) also provides that the secretary of defense shall "[c]onduct programs and missions necessary to fulfill national, departmental, and tactical foreign intelligence requirements."

31. REISMAN & BAKER, *supra* note 27, at 119. At the time of publication, Baker was an Attorney Advisor in the Office of Legal Counsel, Department of State. He should not be confused with then Secretary of State James A. Baker III.

32. These restraints now include, most famously and substantively, a ban on assassination. This ban presents an irony by barring excessive discrimination. President Gerald Ford issued an executive order to ban U.S. intelligence officers from "engag[ing] in, or conspir[ing] to engage in, political assassination." United States Foreign Intelligence Activities, Exec. Order No. 11,905, § 5(g), 41 Fed. Reg. 7,733 (1976). President Jimmy Carter issued Executive Order No. 12,036, § 2-305, 43 Fed. Reg. 3687 (1978); and President Ronald Reagan issued Executive Order No. 12,333, § 2.11, 48 Fed. Reg. 59,947 (1981). *See* ABRAM N. SHULSKY, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 100-101 (Gary J. Schmitt ed., 2d ed. 1993).

The debate, however, is not over. *See* REISMAN & BAKER, *supra* note 27, at 71; Robert F. Turner, Commentary & Opinion, *Killing Saddam: Would it Be A Crime?*, WASH. POST, Oct. 7, 1990, at D1; Lt. Cmdr. Bruce A. Ross, *The Case for Targeting Leadership in War*, 46 NAVAL WAR C. REV. 73 (Winter 1993); George Stephanopoulos, *Why We Should Kill Saddam*, NEWSWEEK, Dec. 1, 1997, at 34. Turner, Ross, and Stephanopoulos argue that the ban forces the U.S. to invade a country like Panama (or potentially Iraq) at great risk and cost rather than effecting a more efficient solution.

33. PRIMER, *supra* note 26, at 14.

analyzes the use of such weapons as electronic viruses, worms, and logic bombs. They can be inserted remotely via various media of electronic communications: telephone, radio, or Internet. Alternatively, like a clipper chip, they can be embedded in the software of electronic machinery manufactured in the United States and sold abroad.[34] Then they could be triggered remotely by telephone, radio, or other electronic means. These weapons might also be used against the United States, its resources, people, or infrastructure.

If a non-U.S. party (whether state, group, or individual) assaults or attempts to assault a U.S. information system, numerous possible responses exist. As with other armed conflict, defensive IW operations are subject to the restraints of LOAC and its principle of proportionality. The traditional laws of armed conflict provide a starting point for the application of proportionality. Any U.S. response to an attack should be intended to have an effect of inflicting roughly the same scale of harm as was intended in the initial assault. Under general LOAC principles, the defender should attempt to focus the retaliation against only the source of the initial assault (or attempt). Application of this general rule is relatively simple when air defense interceptors or missiles simply shoot down intruder reconnaissance planes after a failed attempt to warn them off. The defender does not destroy the intruder's air force. It is equally straightforward when a navy destroyer returns fire and sinks an attacking gunboat but not its entire, far-off fleet. IW complicates the equation, because the attacker may not be a single, readily identified individual.

In a conventional assault, the defender knows precisely who is attacking, *e.g.*, the reconnaissance plane or the gunboat. He may not know its nationality, but he will usually know which people are directly engaged in the assault. In IW, an assault will likely be camouflaged. The assailant will probably route her assault through an innocent intermediary telecommunications systems. For example, a hacker would first route her communications through various servers around the world before attempting to gain access to a DOD computer system. In such a situation, too hasty a defender might destroy the innocent intermediate system(s) in his effort to thwart and punish the attacker.

---

34. A clipper chip is the proposed electronic processor that would allow authorized key-holders to decrypt an encrypted transmission, one in which mathematical algorithms are used to "scramble data to protect its confidentiality." Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L. J. 931, 957 n.27 (1996). In theory the chip could be added to a machine built almost anywhere by anyone, but it would likely be simpler to add to machines manufactured in the United States.

A second major distinction between IW and conventional warfare is that in a conventional assault, the gravity of the threat is relatively unambiguous. Thus, we know that a reconnaissance plane could collect sensitive information and that a gunboat could sink a cruiser. An electronic assault, however, might merely amount to the hapless intrusion of an American teen-age hacker,[35] for example, or it might be part of a *Hezbollah* strategy to degrade CENTCOM's[36] command and control functions in preparation for a coordinated large-scale terrorist attack upon Israel. In fact, during the months leading up to the Gulf War, private Dutch hackers actually pillaged DOD computer sites and subsequently offered information about UN troops' strength, capabilities, and positions to Iraqi leaders.[37] Had Iraqi president Saddam Hussein availed himself of this information, thousands more people on both sides might have died.

The DOD's computers will be subject to approximately 14,000 hack attacks this year.[38] Despite the potential gravity of the threat, active responses must be made carefully—not automatically. An operator should evaluate the situation, decide if there has indeed been an attack and what the appropriate response should be. He assures some level of protection for harmless trespassers (children or those entering by mistake). "Any decision to use active defense system ought to be based, among other factors, on available information about the intruder's skill, status, and apparent intentions."[39] These active defense systems can destroy the computers or systems used to launch the assault, or they may

---

35. Some American teenagers pose relatively serious threats, but they are subject to criminal law and retain constitutional protections. *See, e.g.*, United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (young American hacker inserted a worm—a self-contained computer program—into various computers via the Internet that crippled 6,200 computers and caused nearly 100 million dollars in damage). Alternatively, an apparently harmless hacker might be in the employ of an unfriendly foreign intelligence service and capable of inflicting serious harm. *See* CLIFFORD STOLL, THE CUCKOO'S EGG (1989) (young German in employ of KGB hacked into US defense-related computers). *See also* Charney & Alexander, *supra* note 34, at 931; M.E. Bowman, *Is International Law Ready for the Information Age?*, 19 FORDHAM INT'L L.J. 1935 (1996) (author as Associate General Counsel of the FBI is concerned with attacks on National Information Infrastructure (NII)). Naturally, the gravity of a conventional threat can also be miscalculated, as when Korean Air Lines 007 entered Soviet air space.

36. CENTCOM is the unified operational command responsible for U.S. military forces in the Middle East and the Indian Ocean basin.

37. *See* Graeme Browning, *Hack Attacks*, GOV'T EXECUTIVE 23 (Aug. 1997).

38. *See* Schmitt, *supra* note 28, at 893 & nn.25-26. As a test of 9,000 DOD computer networks, the Defense Information Systems Agency (DISA) hacked into and took control of 88 percent of the networks. Only 4 percent of systems operators recognized that they had lost control and only 0.2 percent reported the events. *See* Greg Rattray, *The Emerging Global Information Infrastructure and National* Security, 21-FALL FLETCHER F. WORLD AFF. 83-84. *See also* John Elvin, *Insight*, WASH. TIMES, Mar. 23, 1998, at 32.

39. PRIMER, *supra* note 26, at 8.

go further and destroy the assailant's infrastructure, *e.g.*, the power and telecommunications grids in her city. Removing the human being from this decision (*i.e.*, leaving it to a computer's automated response mechanisms) would likely result in faster but less responsible decisions.

International law traditionally distinguishes between retorsion and reprisal—a valuable distinction that should be retained in the context of information operations. Retorsion consists of an unfriendly but legal act of force undertaken with retaliatory or coercive purpose.[40] Reprisals are more complicated. They involve acts that are illegal unless they follow three steps. First, there must be an illegal act by another state. Second, the state intending to effect the reprisal must give the original assailant the opportunity to "make right their international wrong."[41] Finally, if this demand goes unsatisfied, then the attacked party may respond in a manner proportional to the original attack.[42]

In the context of IW, the decision to adopt a policy of retorsion or reprisal presents serious but not necessarily fatal evidence problems.[43] The likelihood of a camouflaged assault means that the responding party has no reasonable expectation that he will be punishing the perpetrator, unless he can first trace the assault back to a suspect nation, group, or individual. He might limit these forceful responses to those occasions when he does trace the assault back to groups or actors already suspected of being terrorists. Even then, he may only know that he has traced the attack back to a suspect group. He will likely not know for sure that he has identified the true assailant. So, he must proceed with caution. On-screen warnings are important to put intruders on effective notice, although they may be ineffective when intruders gain access through back doors, *i.e.*, bypassing entry procedures and access protocols available to legitimate Internet traffic.[44] Moreover, reliance

---

40. *See* Richard B. Lillich, *Forcible Self-Help Under International Law*, *in* NATIONAL SECURITY LAW 131, 132-33 (John Norton Moore et al. eds., 1990). *See also* LOUIS HENKIN ET AL., INTERNATIONAL LAW: CASES AND MATERIALS 579 (3d ed. 1993) ("Retorsion is often an 'equivalent' act of retaliation in response to an unfriendly act.").

41. Lillich, *supra* note 40, at 133.

42. *See id.*

43. Moreover, a vast literature debates whether the U.N. Charter bans retorsion and reprisals as impermissible uses of force. *See* U.N. CHARTER art. 2(4). Lillich summarizes the debate. *See* Lillich, *supra* note 40, at 133-36. As long as the response is limited to non-forceful measures such as using computer code to neutralize the offending machinery, this issue should be avoidable. Lillich concludes the discussion by summarizing a speech by Professor Myres McDougal on how to read Article 2(4), "in the absence of collective machinery to protect people against attack and deprivation . . . the principle of major purposes requires an interpretation which would honor self-help against a prior unlawfulness." *Id.* at 136.

44. *See* PRIMER, *supra* note 26, at 8. An intruder might enter through a "trap door" of his own creation. He could gain initial entry through a Trojan Horse—a program which on its face has a legitimate purpose but has a hidden, illicit purpose. Note the term's origins in a ruse of

upon on-screen warnings could result in an attack upon the innocent intermediary. Given these problems, retorsion should be limited to shutting down (either temporarily or permanently) the computer system believed to be generating the original attack. Retorsion would not extend to destroying the power and telecommunications grids in the city of the suspected assailant. This would probably exceed the limits of action deemed defensive defense.

Much like retorsion, strictly defensive operations like computer security (COMPUSEC) also apply to both military and non-military systems. Stock exchanges, corporations, travel and communication systems, and educational institutions all rely on the integrity and smooth running of their own information systems, much as the military does, although the failure would rarely be a matter of life and death. Security measures include virus checks, fire-walls, passwords, or simply locking the building's front door. U.S. domestic losses to hack attacks were estimated at $100,000,000 in 1995.[45] Estimates for computer fraud of all varieties in the United States run to ten billion dollars a year.[46] Strictly defensive measures must always be applied when protecting critical infrastructure. If not, the society risks losing use of its military, transportation, communications, or other instrumentalities vital to its continued security and well-being.

In terms of national security, infrastructure is both military and civilian. "Infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continuous flow of goods and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole."[47] Furthermore "[c]ertain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[48] These include telecommunications, electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply,

---

war.

45. Browning, *supra* note 37, at 23.

46. Charney & Alexander, *supra* note 34, at 936-37. See NRC, COMPUTERS AT RISK, *supra* note 19; Emilio Jaksetic, *Computer Security and Government Lawyers*, 43 FED. LAW. 26 (Jul. 1996).

47. President's Commission on Critical Infrastructure Protection (PCCIP), *Overview Briefing*, F-3 (June 1997) (visited Mar. 24, 1999) <http://www/pccip.gov/>. *See also* Rattray, *supra* note 38, at 81. *But see* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465 (1997).

48. Exec. Order No. 13,010, 61 Fed. Reg. 138 (1996).

emergency services and government services.[49] Protecting them is vital to the well-being of the nation.

Myriad federal laws and enforcement systems support and encourage a strictly defensive defense. Foremost among these laws are the Computer Fraud and Abuse Act and the Wiretap Act, each of which defines felonies and misdemeanors.[50] U.S. law against hacking is broad-ranging and appears comprehensive. Section 1029 of Title 18 generally prohibits fraud and related activity with telecommunications access devices. The Computer Fraud and Abuse Act[51] is the main hacker law, enumerating the types of computer espionage. The act prohibits unauthorized access to computer-based financial records, unauthorized access to nonpublic computers of a department or agency of the United States, unauthorized access to a computer with intent to defraud, criminal trespass that results in damage, and trafficking in a password. The Wiretap Act makes it unlawful for "any person" to intentionally intercept, use, or disclose or endeavor to intercept, use, or disclose any wire, oral, or electronic communication.[52] The Wiretap Act is subject to several exceptions, most importantly for systems administrators,[53] with consent of a party to the communication,[54] or if intercepted under a court order.[55] The agencies charged with enforcement responsibility are criminal investigative units of the military services, the intelligence community, and the FBI.[56] Aside from tightening some loopholes, these laws do not appear to need any significant modifications at this point—at least insofar as they seek to protect U.S. infrastructure from IW attacks. In stark contrast, international law is vague and has considerable room for improvement.

---

49. *See id.*

50. For these citations, the author is indebted to Major Stanley R. Smith's briefing on hacker law, before the Legal Aspects of Information Warfare Symposium, Air Force Judge Advocate General School, Maxwell AFB, Alabama (Nov. 1-3, 1995). For a more complete listing of relevant U.S. law, see SCIENCE APPLICATIONS INTERNATIONAL CORPORATION (SAIC) TELECOMMUNICATIONS AND NETWORKING SYSTEMS OPERATION, INFORMATION WARFARE: LEGAL, REGULATORY, POLICY AND ORGANIZATIONAL CONSIDERATIONS FOR ASSURANCE, app. B (1995) (United States Code: Annotated Bibliography and Index). Table 2-2-1 of this report enumerates the various state computer crime statutes.

51. 18 U.S.C. § 1030 (1998).

52. 18 U.S.C. § 2511 (1998).

53. *See* 18 U.S.C. §2511(2)(a)(i).

54. *See* 18 U.S.C. § 2511(2)(c).

55. *See* 18 U.S.C. § 2511(2)(a)(ii).

56. *See* SAIC, *supra* note 49, tbl. 2-2-2 (indicating the various jurisdictions for computer crimes that occur in this country). When an intruder penetrates a Federal system in the U.S. with criminal intent, the act falls under the jurisdiction of the FBI and the U.S. Secret Service. When the intruder's intent is espionage, then the FBI shares jurisdiction with the National Security Agency. *See id.*

III. DISCRIMINATION AND THE LAWS OF WAR

Despite the challenges in applying it, discrimination between military and civilian targets remains imperative in the age of IW—notwithstanding the new difficulties of distinguishing legitimate targets within the critical infrastructure. The Geneva Conventions of 1949 memorialized the basic ground rules for warfare.[57] The 1977 Protocol I to the Geneva Conventions established the "Basic Rule" on discrimination which remains valid, if somewhat more difficult to apply to the facts of IW. "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[58] Article

---

57. "In view of the large number of states parties to the 1949 Geneva Conventions and the status which the Conventions have acquired in the international community, it is reasonable to assume that the Conventions are (at least in large part) declaratory of customary international law." Roberts & Guelff, *supra* note 6, at 170.

The 1949 Geneva Conventions are comprised of: (1) Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; (2) Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; (3) Geneva Convention Relative to the Treatment of Prisoners of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; (4) Geneva Convention Relative to the Protection of Civilian Persons in Time of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV].

See also Respect for Human Rights in Armed Conflicts, G.A. Res. 2444, U.N. G.A.O.R., 23rd Sess., Supp. No. 18, at 50, U.N. Doc. A/7218 (1968) (affirming these general principles: (a) that the right of the parties to a conflict to adopt means of injuring the enemy is not unlimited; (b) that it is prohibited to launch attacks against the civilian populations as such; and (c) that distinction must be made at all times between persons taking part in the hostilities and members of the civilian population to the effect that the latter be spared as much as possible). General Assembly resolutions are recommendations that can become law when accepted by the international community. *See* THE LAWS OF WAR: A COMPREHENSIVE COLLECTION OF PRIMARY DOCUMENTS ON INTERNATIONAL LAWS GOVERNING ARMED CONFLICT, at xxii (Michael Reisman & Chris T. Antoniou eds., 1994).

58. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), *opened for signature* Dec. 12, 1977, art. 48., 1125 U.N.T.S. 3 (1979) [hereinafter Protocol I]. "Although the U.S. military takes the position that an attacker should accept some responsibility to minimize collateral civilian casualties," the United States has not ratified Protocol I because it shifts the burden to segregate civilians from military objectives to the attacker from its traditional situation where the defender carried this obligation. Danielle L. Infeld, Note, *Precision-guided Munitions Demonstrated Their Pinpoint Accuracy in Desert Storm; but Is a Country Obligated to Use Precision Technology to Minimize Collateral Civilian Injury and Damage?*, 26 GEO. WASH. J. INT'L L. & ECON. 109, 123 (1992).

51 protects civilian populations, and 51(4) defines unlawfully indiscriminate attacks as:

> (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians without distinction.[59]

Even read within the context of Protocol I's Part IV on Civilian Population, this may appear to be self-reflective or even meaningless protection, but it has been given flesh. As the International Court of Justice[60] recently held, this regime does not by itself preclude operations that have a secondary or collateral impact on civilians as long as the intended target is an armed force or other military objective.[61]

The Protocol's Article 43 expands on the basic rule.

> The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party.[62]

These are the parties for whom the prohibitions apply, prohibiting them from using force to harm non-military objectives and acknowledging them as legitimate targets for lawful attacks. Article 52(2) then defines military objectives as those objects "which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the

---

59. Protocol I, *supra* note 58, art. 51.

60. "The International Court of Justice (ICJ) at The Hague has long had certain limited roles in respect of implementation of the laws of war . . . [but its] statute, with its built-in limitations on what types of cases may be brought to it and by whom, is likely to mean that it only will have to look at a minority of issues concerning the laws of war." Adam Roberts, *The Laws of War: Problems of Implementation in Contemporary Conflicts*, 6 DUKE J. COMP. & INT'L L. 11, 43 (1995).

61. *See* Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 35 I.L.M. 809 (I.C.J. 1996).

62. Protocol I, *supra* note 58, art. 43.

circumstances ruling at the time, offers a definite military advantage."[63] These legal definitions, however, only lead to consideration of the questions, not the answers. Distinguishing legitimate targets still requires a context with which to test the facts.

The traditional tools for distinguishing civilian from military personnel or operators are not as readily available as they were before the advent of long-range bombardment and telecommunications.[64] During the three centuries between 1648 and 1945, combatants generally wore uniforms that visibly distinguished them from noncombatants before the engagement.[65] Likewise, most warfare involved physical proximity. Whether using edge weapons or projectiles, most combatants could see each other and distinguish combatants from noncombatants. The major exception here is aerial bombardment by airplane or missile. Even then, those soldiers doing the targeting still bore the burden of making realistic distinctions—an obligation unfortunately honored only in the breach.[66]

Whether they are wearing military uniforms or not is inconsequential when the parties cannot see each other. The person launching a computer virus to attack an American military communications system, for example, might be sitting in the basement

---

63. *Id.* art. 52(2). The definition is emphasized by the U.S. Navy. *See* UNITED STATES, DEPARTMENT OF THE NAVY, OFFICE OF THE CHIEF OF NAVAL OPERATIONS, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, NWP 9, ¶ 8.1.1 (Supp. July 1987) [hereinafter COMMANDER'S HANDBOOK], *cited in* Roberts & Guelff, *supra* note 6, at 5 n.11.

64. Distinguishing civilians from military personnel has traditionally been a matter of recognizing the military professionalism which has organized the officer corps of the western powers since the early nineteenth century. *See* SAMUEL HUNTINGTON, SOLDIER AND THE STATE (1957). Still, uniformed soldiers fighting others organized into particular standing units that had trained and been armed together goes back to at least the end of the Thirty Years War, when rulers and people alike recoiled from the horror of unbridled warfare where distinctions between combatants and noncombatants had disintegrated. *See* Michael Howard, *Constraints on Warfare*, *in* LAWS OF WAR, *supra* note 4, at 4 ("The nightmare days of the Thirty Years War when troops, themselves desperate and starving, tortured, slaughtered, and burned their way across Europe were not prolonged into the following century."). See also Howard's classic, MICHAEL HOWARD, WAR IN EUROPEAN HISTORY ch. 2 (1976).

65. Technically this has been true only for professional or conscription armies. The combatants of the colonized world (*i.e.*, the indigenous peoples of the Americas, Africa, Asia and the Pacific) did not usually wear recognizable uniforms. This cultural difference between the imperial powers and the colonized world only fed the cultural, religious, geo-political, and economic forces that undermined the constraints on warfare when it was between cultures. That is to say, the restraints on the western way of war usually did not apply in conflicts between Western Europeans and the rest of the world. *See* Howard, *supra* note 64, at 5, 8.

66. *See* Tami Davis Biddle, *Air Power*, *in* LAWS OF WAR, *supra* note 4, at 152-54; David Alan Rosenberg, *Nuclear War Planning*, *in* LAWS OF WAR, *supra* note 4, at 165-66. *See generally* W. Hays Parks, *Air War and the Law of War*, 32 A.F. L. REV. 1, 89-168 (1990). During the inter-war period, the 1923 Hague Rules of Aerial Warfare "were regarded as an authoritative attempt to clarify and formulate rules of air warfare...." Roberts & Guelff, *supra* note 6, at 121.

of a publicly traded telephone company wearing a nun's habit. Instead of a military uniform, she would be wearing the symbol of clergy—a protected group, and she would be sitting in a privately owned building also doubly protected by being private and vital to the well-being of society. Even assuming she is indeed a nun and not an impostor, she would nonetheless also be a combatant subject to a proportional response, such as the destruction of her own computer or the local area network. In IW, there is no physical proximity to permit distinguishing combatants from non-combatants visually. Moreover, in IW, she *would be* a combatant and subject to proportional response. In fact, if the target of her attack did not have the means to respond with his own IW measures, he could reasonably bomb the building in which she is believed to be sitting—again a proportional response but one that returns kinetic destruction for that created by electronic communications.

Despite these differences, three traditional principles remain valuable for discriminating between legitimate and illegitimate targets: military necessity, humanity, and chivalry. Under customary international law, military planners must balance all three.[67] Under U.S. law, military officers must be taught to grapple with these issues.[68] These three principles are also used for determining proportionality and are, thus, critical for the legitimate undertaking of IW.

First, the principle of military necessity demands that "[o]nly that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources may be applied."[69] Moreover, military necessity is an especially complicated

---

67. "Customary law is found in the practice of states, how many is not precisely stated, . . . which is binding upon all persons of international law irrespective of treaty commitments." HILAIRE MCCOUBREY, INTERNATIONAL HUMANITARIAN LAW: THE REGULATION OF ARMED CONFLICTS 192 (1990). The United States is bound by customary international law. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 (1987); Louis Henkin, *International Law as Law in the United States*, 82 MICH. L. REV. 1555 (1984).

68. U.S. Dep't of Defense, DOD Law of War Program, DOD Directive 5100.77 (1979). *See also* Almond, *The Teaching and Dissemination of the Geneva Conventions and International Humanitarian Law in the United States*, 31 AM. U. L. REV. 981 (1982). Nonetheless, when I served on the faculty of the United States Air War College in 1995-1996, fulfillment of this requirement seemed to have lapsed from the core curriculum. When I pointed this out, a leading JAG lawyer was brought in for a mandatory lecture. Apparently, since my departure, the War College has allowed this program to lapse again.

69. COMMANDER'S HANDBOOK, *supra* note 63. *See also* OFFICE OF THE JUDGE ADVOCATE GENERAL, DEP'T OF THE NAVY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 5.2 (1989), *cited in* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE: INFORMATION OPERATIONS, THE LAWS OF WAR AND THE UNITED STATES STANDING RULES OF ENGAGEMENT, at L-13 (1987).

argument in an era of one superpower. The United States has at its disposal a vastly greater variety of military and political tools than any other state, past or present. For the United States, therefore, military necessity often cannot mean that an act is strictly necessary. For the foreseeable future at least, there will almost always exist alternatives that could not reasonably be measured against each other (*i.e.*, conventional or information operations, economic or diplomatic sanctions, etc.). Moreover, only one state could plausibly threaten the existence of the United States. Notwithstanding the fact that the U.S. has a variety of options in most scenarios, questions of military necessity in IW do not seem different from those involved in deciding whether to undertake traditional operations. Instead, they focus more on targets and objectives than means. To this extent, IW does not substantially alter the decision-making process.

Second, the IW planner or operator must weigh the humanity of his actions. Unnecessary suffering and destruction of humanity must be avoided—a principle widely shared and embodied in the Martens Clause of the 1907 Hague Convention (IV). "[T]he inhabitants and the belligerents remain under the protection and the rule of the *principles of the law of nations*, as they result from the usages established among civilized peoples, from *the laws of humanity*, and *the dictates of the public conscience*."[70] No mere precatory overture, the Martens Clause is embodied in an article common to each of the four 1949 Geneva Conventions. They note that the fact of denouncing the Convention

> shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfil by virtue of the *principles of the law of nations*, as they result from the usages established among civilized peoples, from *the laws of humanity and the dictates of the public conscience*.[71]

---

70. Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, pmbl. (emphasis added) [hereinafter Hague IV].

71. Geneva Convention I, *supra* note 57, art. 63; Geneva Convention II, *supra* note 57, art. 62; Geneva Convention III, *supra* note 57, art. 142; Geneva Convention IV, *supra* note 57, art. 158 (emphasis added). This principle was likewise confirmed by the 1977 Geneva Protocol I, *see supra* note 58, art. 1; the 1977 Geneva Protocol II, *see* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), *opened for signature* Apr. 10, 1981, pmbl., 1125 U.N.T.S. 609 (1979) [hereinafter Protocol II]; and the 1981 UN Weapons Convention, *see* Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, *opened for signature* Apr. 10, 1981, pmbl, 19 I.L.M. 1523 (1980). *See also* Roberts & Guelff, *supra* note 6, at 4 & n.8.

The law of humanity also restrains armed conflict in U.S. LOAC.[72]

As with military necessity, humanity in armed conflict is a relative value. It might favor an IW operation, for example, when the only military alternative is dropping a large explosive on or near the same target. On the other hand, it might halt an information attack that would disable the computers controlling not only air defense but also civilian aviation or an automated subway system. Clearly, humanitarian principles prohibit acts justified solely by the Sherman-esque logic that "war is cruelty . . . the crueller it is, the sooner it will be over."[73] The principle of humanity appears to argue in favor of applying information operations if the alternatives threaten greater physical destruction and loss of life.

Third, IW planners and operators remain bound by the enduring, if amorphous, principles of chivalry. In many societies this might mean distinguishing between male and female targets, despite the various treaties and national laws banning distinctions based on sex alone.[74] Leaving aside distinctions based on sex, chivalry still protects the young, old, and helpless even beyond the consideration given all noncombatants. Chivalry also bans treachery or perfidy. The 1977 Geneva Protocol I bans "[a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence . . . ."[75] Perfidy includes: 1) feigning of intent to negotiate or surrender, 2) feigning incapacitation, 3) feigning civilian, noncombatant status, and 4) feigning protected status by use of signs or uniforms of the UN or neutral states. On the other hand, ruse of war is not prohibited, which requires drawing yet

---

72. *See* COMMANDER'S HANDBOOK, *supra* note 63, ¶5.2; AIR FORCE JUDGE ADVOCATE GENERAL SCHOOL, THE MILITARY COMMANDER AND THE LAW 580 (1994).

73. HERMAN HATHAWAY & ARCHER JONES, HOW THE NORTH WON 548 (1983). While U.S. Civil War general William T. Sherman is renowned for having made a military strategy of this notion, he is far from alone in history. *See, e.g.*, Harold Selesky, *Colonial America*, *in* LAWS OF WAR, *supra* note 4, at 61 (the British conquerors of Ireland justified their atrocities as expedient); Biddle, *supra* note 66, at 147 & n.23-24, 29, 34, 36 (strategic air power theorists believed that bombing civilians would destabilize the enemy society and economy, eventually toppling the state). Even the vaunted Lieber Code includes a strand of this now-outlawed logic. *See* Lieber Code, *supra* note 12, art. XXXIX ("The more vigorously wars are pursued, the better it is for humanity. Sharp wars are brief.").

74. *See, e.g.*, International Covenant on Civil and Political Rights, Dec. 16, 1966, art. 2.1, 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, art. 2.2., 993 U.N.T.S. 3; Convention on the Elimination of All Forms of Discrimination Against Women, Dec. 18, 1979, G.A. Res. 180 (XXXIV), (1979), 19 I.L.M. 33 (1980).

75. Protocol I, *supra* note 58, art. 37. For the obligations of chivalry, *see also* COMMANDER'S HANDBOOK, *supra* note 63, ¶ 5.1.

another fine distinction under sometimes urgent circumstances.[76] Legitimate ruses include camouflage, decoys, mock operations, and misinformation.

In a contemporary conflict, application of these chivalric principles may seem daunting. However, the differences now are more about cultural change than about the employment of particular weapons systems. Military strategist Edward Luttwak believes chivalry is no longer relevant because it is an atavistic throw-back to a more romantic era of warfare.[77] Yet, while chivalry may seem archaic today, it retains some normative value. While neither courts nor legislatures have spoken on this issue, analogy strongly weighs against sending a logic bomb disguised as e-mail from the International Committee of the Red Cross (ICRC) or even from "Microsoft Software Support"—where such a message might be permissible without perfidious labels.[78] Using ICRC and Microsoft tags would constitute an illegitimate act of perfidy, much as would disguising any dangerous military intruder in the form of an innocuous invitee. Chivalry does not, however, appear to ban many other types of clandestine entry into an opponent's system, for instance, through trap doors, or by camouflaged instructions from an ally.

In many instances, chivalry may not weigh heavily in the decision over whether to undertake IW, if only because the penalty for underestimating chivalry is not likely to be applied unless the perpetrator loses the war and the evidence and forum exist to convict her of a war crime. It is difficult to imagine a realistic penalty for the espionage-like offense of gaining access to a computer by pretending to be one of the penetrated party's own military personnel. Traditionally a spy may be executed if local law permits,[79] but if she returns home, then she is safe from prosecution for espionage.[80] In IW, spying may

---

76. *See* Protocol I, *supra* note 58, art. 37 §§ 1-2; Hague IV, *supra* note 70, art. 24. *See also* AIR FORCE JUDGE ADVOCATE GENERAL SCHOOL, *supra* note 72, at 581.

77. *See* Edward N. Luttwak, *Toward Post-Heroic Warfare*, FOREIGN AFF. (May/June 1995).

78. *See* Protocol I, *supra* note 58, art. 38; *see also* PRIMER, *supra* note 26, at 17-18; Richard Aldrich, *The International Legal Implications of Information Warfare*, AIRPOWER J. 108 (Fall 1996). A logic bomb functions like a virus that could selectively degrade or even destroy the computer hosting it.

79. Hague IV, *supra* note 70, art. 29 states: "A person can only be considered a spy when, acting clandestinely or on false pretenses, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party." Article 30 requires merely that a "spy taken in the acts shall not be punished without previous trial." The Geneva Convention IV, governing suspected spies in occupied territory, merely requires a fair trial. *See* Geneva Convention IV, *supra* note 57, pt. I, art. 5.

80. For similar treatment in time of war, see Hague IV, *supra* note 70, art. 31.

occur from the safety of a windowless office in Fort Meade or Shaw AFB, headquarters of the National Security Agency and the Air Force's IW center, respectively. The spy is already home and already safe. Chivalry, therefore, will play only a minor role in IW.

While it is important to weigh military necessity, humanity, and chivalry, some categories of outright impermissible activities present themselves in the area of IW. "The right of belligerents to adopt means of injuring the enemy is not unlimited."[81] Nonetheless, the planner may still balance these three principles to decide whether the targets are protected by international law. At one extreme are legitimate targets—military objectives such as army bases, ships of war, weapons depots, and intelligence headquarters. That is not to say that these may all be destroyed for any or no reason. The principles of *jus ad bellum*, proportionality, military necessity, chivalry, and humanity continue to constrain the treatment of enemy combatants and other military objectives. At the other extreme of the spectrum are those objectives that are strongly protected by international law, such as religious, cultural, and medical facilities. Between these *per se* categories, there remains a large intermediate area where reasonableness demands weighing military necessity, humanity, and chivalry as well as proportionality. As with conventional war planning, info-warriors must consider the *per se* categories and also the more questionable targets.

For nearly a century, certain categories of objects have been beyond the reach of lawful attack. The Hague Convention on Land Warfare (1907) requires that:

> In sieges and bombardments all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes.[82]

However, to prevent the rule from being abused to protect otherwise legitimate targets, the convention further demands segregation. "It is the duty of the besieged to indicate the presence of such buildings or places by distinctive and visible signs, which shall be notified to the

81. *Id.* art. 22.

82. Hague IV, *supra* note 70, art. 27.

enemy beforehand."[83] These specially protected objects include civilian hospitals, cultural, historical, or religious sites, reservoirs of dangerous forces (including dams and nuclear power plants), food and other supplies necessary for human life.[84]

During the most recent large-scale international armed conflict, the Persian Gulf War of 1990-91, Iraq abused these constraints. Among other transgressions, the Iraqi leadership hid military intelligence operations beneath children's milk processing plants and placed military aircraft amidst cultural artifacts.[85] President Saddam Hussein had constructed dozens of statues of himself that were placed among otherwise legitimate targets. This left planners with the dilemma of deciding if the statues were "cultural property" deserving the protection of the Convention. With each of these acts, Hussein flouted his obligation as a defender to segregate military from civilian objectives. In other words, Hussein abused the laws of war, casting the legitimate activities of the Allies in a light of illegitimacy before the CNN court of world opinion. In the future, these cynical games may undermine a state's willingness to risk its own forces in order to adhere to the principle of discrimination as between legitimate and illegitimate targets.

Nonetheless, responsible states should continue to try to restore discrimination and the defender's obligation to segregate. IW may facilitate this restoration, or at least make it easier. For instance, if undertaken cautiously, IW may allow a state to disable certain targets that would be protected from more destructive forms of attack. Thus, a state actor could possibly attack information systems within protected sites with an impact that may not rise to the level of destruction that the conventions prohibit. An IW attack could disable an Iraqi intelligence center, instead of using 2,000-pound bombs to destroy it and the children's shelter beneath it. Likewise, destroying a dam is generally

---

83. *Id.* Because these provisions failed to protect cultural property in World War II, a stronger convention was sought by the international community. The result was the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240-88 [hereinafter 1954 Hague Conv.]. The principles it embodies were most recently affirmed in Protocol I, *supra* note 58, art. 53 and Geneva Protocol II, *supra* note 71, art. 16. This "special protection may be viewed as a part of customary international law." Roberts & Guelff, *supra* note 6, at 340.

84. *See* Hague IV, *supra* note 70, art. 27; 1954 Hague Conv., *supra* note 83, at 240. To receive this protection, however, cultural property must be "situated at an adequate distance from any large industrial centre or from any important military objective constituting a vulnerable point . . . [and] are not used for military purposes." *Id.* art. 8(1)(a)-(b), at 246.

85. Iraq purposefully located legitimate military targets near its civilian population, civilian objects, and cultural property. *See* U.S. DEP'T OF DEFENSE, CONDUCT OF THE PERSIAN GULF WAR: FINAL REPORT TO CONGRESS 125-26, app. O, at O-14 (1992); Infeld, *supra* note 58, at 137.

prohibited by Protocol I.[86] But temporarily disabling the dam's electronic control system would not be prohibited if doing so does not unleash a torrent or deprive civilians of water for the purpose of denying them sustenance. The Protocol seeks to avoid the horror of unleashing dangerous forces in a way that would harm civilians. It does not seek to ban outright the denial of a dam's energy or even of its water to an enemy. Here IW would be a more flexible and useful tool than explosives which would likely release the deadly forces—or permanently deprive the civilians of drinking water.

Likewise, IW might enable an operator to disengage a regional electric grid temporarily where he would be prohibited from destroying it. The Hague regime prohibits the "attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended . . . ."[87] This does not mean that an information warrior can attack a village's power grid or telecommunications network intentionally, justified merely by the fact that the grid or network has some electronic defenses.[88] However, because the village's infrastructure is tied into a regional or national network that is defended by the military, it may be damaged as the collateral effect to an information strike on a military target. This impact, however, is likely to be far less serious under an IW attack which puts it out of commission temporarily, compared to an explosion that would kill people and cause damage requiring more money, time, and resources to

---

86. "Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population." Protocol I, *supra* note 58, art 56(1). The Protocol does make limited exceptions for those works being used "for other than [their] normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support. . . ." *Id.* art. 56(2)(a).

Additionally, the Protocol makes it prohibited to "attack, destroy, remove, or render useless objects indispensable to the survival of the civilian population . . . for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive . . . ." *Id.* art. 54(2).

87. Hague IV, *supra* note 70, art. 25. *See also* Hague Draft Rules on Aerial Warfare, arts. 22-26, *reprinted in* 32 AM. J. INT'L L. 12 (Supp. 1938), Roberts & Guelff, *supra* note 6, at 121, 126-28.

88. "Customary practice has been that military equipment such as units and bases, and economic targets such as power sources, industry, transportation, and command and control centers, are always legitimate targets. This includes transportation and communications systems. However, 'the inherent nature of an object is not controlling; its value to the enemy or the perceived value of its destruction is the determinant.' Even traditional civilian objects, such as private homes, if used for military purposes, may be attacked. The important factor is to determine if the target makes an effective contribution to the enemy's military operations; if it does, it is subject to attack, wherever located, even if within heavily populated areas." Infeld, *supra* note 58, at 122 (citations omitted); *see also* UNITED STATES DEPARTMENT OF THE AIR FORCE, AN INTRODUCTION TO AIR FORCE TARGETING, AFP 200-17, at 9 (1989)).

repair. Thus, IW might permit operations against targets that are generally protected by international conventions. In doing so, it would not undermine those agreements but rather would strengthen them by aligning military means to their desired outcomes.

As noted above, in order to protect civilians and civilian objects, the defender must not thwart the intent of the principle of discrimination; he has an obligation to segregate them from military objectives. Protocol I requires that: "to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack."[89] This obligation is relatively straightforward in naval combat where armed forces move by military vessels alone. At home, however, states rely on their civilian infrastructure almost entirely to move large numbers of troops; highways, railroads, and frequently airports are not duplicated by solely military systems. Moreover, where armed forces once communicated among themselves—via military media such as couriers, runners, pigeons, walkie-talkie, or unsecured telegraph or telephone lines—they now share the info-sphere with civilians everywhere. In IW, segregation presents many new challenges.

In the information age, military operations are increasingly reliant upon advanced communications; information and critical infrastructure are shared, frequently gutting the defender's reasonable ability to segregate the military from the civilian.[90] Modern military forces rely on mixed-use telecommunications media, including telephones, faxes, and e-mail, that travel over the civilian-owned or operated networks. Even with the unmatched material wealth of the United States, DOD telecommunications relies heavily on public networks.[91] If the wealthiest nation does not have the resources to segregate its command and control systems from the civilian communications network, then one would not expect the remainder of the world to do so.

Deciding whether to destroy civilian communications systems, therefore, requires careful balancing. However, the scale has never

---

89. Protocol I, *supra* note 58, art. 44(3). Recall also Protocol I, article 48's Basic Rule: "In order to ensure respect for and protection of the civilian population and civilian objects, *the Parties* to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." (emphasis added to show that the burden falls both on attacker and defender).

90. "Warfare is no longer primarily a function of who puts the most capital labor, and technology on the battlefield, but of who has the best information about the battlefield." Arquilla & Ronfeldt, *supra* note 19, at144.

91. This despite the military origins of the ARPANET/Internet.

clearly materialized. If the measure is lives saved, then IW offers great possibilities for expanding the realm of legitimate targets, because it enables operators to target systems for quiet disablement rather than explosive destruction. To this extent, patterns of legitimate usage should develop as they have for other precision weapons such as laser- or GPS-guided munitions. The USAF apparently believes the correct legal formula for planning should be that the attack must be likely to produce a military advantage that outweighs the civilian casualties and damage.[92] This demands weighing the importance of navigation systems, communications systems, and electrical grid systems to the opponent's military effort.[93] The balancing process appears to beg the question of how to value these systems. Does one measure in lives saved or lost; dollars spared, saved, risked; or only in permanent physical destruction? IW offers a theoretical opportunity that conventional weapons do not; degrading a system could be more readily reversible in ways that physical destruction could not. This means that lives could be saved while the systems become inoperative, either permanently or briefly. Does this therefore mean that reversible attacks will be launched against civilians or civilian infrastructure more freely? Maybe. Does IW strengthen adherence to the norms of discrimination? If the goal is to protect civilian lifestyles as much as possible during the operation, then the answer is "no." If the aim is to contain war's destructiveness and to facilitate restoration of civil society after the conflict, then the answer is "quite probably yes."

IV. A MODEL PROTOCOL

To announce the fact that the laws of war continue to apply, an international legal convention guiding the conduct of information operations would be extremely valuable. Rather than creating new rules, the convention would work best if it codified customary international law and applied some of the facts to the existing constraints on warfare.[94] Such a protocol might read in relevant part:

---

92. Writing in an unofficial capacity, Colonel Owen E. Jensen states: "Cut or deny *all* the enemy's information-transfer media—telephone, radio frequencies (RF), cable, and other means of transmission. Sever the nervous system. Deny, disrupt, degrade, or destroy *every* transmission." Col. Owen E. Jensen, *Information Warfare: Principles of Third-Wave War*, 8 AIRPOWER J. 35, 37 (Winter 1994). Colonel Jensen is not a lawyer. *See also* Aldrich, *supra* note 78, at 105-09.

93. *See* PRIMER, *supra* note 26, at 18.

94. Among others, Robert and Guelff note that "[t]echnological developments in the methods of conducting war have increased the extent to which the written law is inadequate or absent." Roberts & Guelff, *supra* note 6, at 15.

1. In deciding whether and how to undertake military information operations, each Party agrees to balance the principles of: (a) military necessity; (b) proportionality; and (c) discrimination . . . .

   . . . .

   (c) In discriminating between military objectives and impermissible targets, each Party agrees to balance humanity, chivalry, and the likelihood that the objectives could be achieved without physical destruction.
2. Ratification of this convention confers jurisdiction under the International Criminal Court (ICC) war crimes clause and, failing that, to *ad hoc* international or regional courts vested with appropriate jurisdiction.

The proposal is crafted to circumvent some unstated problems. First, the proposed protocol would apply only to state parties, in an era when many transnational aggressors are not states. This makes sense with the framework of most humanitarian law, which currently applies only to states. States remain the fundamental units of the international system. As non-governmental organizations and groups gain political and legal recognition in the global (*i.e.*, not merely "international") system, then they, too, could sign and become parties. In that eventuality, this protocol, like Protocol I, would protect non-state actors as well as state parties.

Second, the proposed protocol does not contain a definition of an information operation. Instead of defining "military information operations," the ICC (or the *ad hoc* judicial system) could build a body of case law that would allow for more flexible, fact- and context-sensitive interpretations much as has been done with crimes against humanity or the "just following orders" defense.[95] Because states voluntarily submit to a court's jurisdiction, they could opt out if the case law develops unfairly or in a way that they find disagreeable. That would not, however, halt the creation of new customary international law and eventually *jus cogens*. Should the day come when people can agree upon a definition, it could be added by judicial interpretation, in a dispute or in an advisory opinion.

Third, the model protocol avoids the potential evidentiary problems in a way that may compel those who undertake information operations to document their efforts to fight fairly. Such a requirement will

95. *See* Beth Van Schaack, *The Definition of Crimes Against Humanity: Resolving the Incoherence*, 37 COLUM. J. TRANSNAT'L L. 787 (1999).

reinforce caution. In addition, computer systems for tracing and tracking a user's keystrokes are increasingly capable—a trend likely to continue as long as commercial users can profit from research about their customers.

Fourth, the principles of humanity and chivalry are very difficult to judge as between societies of different cultures. This problem is central to the laws of war in general. However, inter-societal conflict frequently involves problems of cultural insensitivity; this is not an argument for abandoning efforts to generate and encourage global norms constraining conflict.

Finally, like Protocol I, the model protocol does not mention a duty on the defender to segregate military from non-military objectives. Acknowledging the insurmountable economic obstacles to creating redundant military infrastructure, this convention would shift most of the burden of discrimination to the attacker. This might well result in hindering the development of IW capabilities—a reasonable outcome. On the other hand, the court would have the discretion to decide when the defender unjustly placed its civilians or civilian infrastructure in harm's way.

V. CONCLUSION

Discrimination remains critical to the legitimate use of force in the information age. LOAC is facing some of its greatest challenges in keeping up with astounding technological changes. The capacity to compute, communicate, and store information doubles every year or two. LOAC faces not only many challenges in the short run but also a change in the nature of warfare that is more dramatic than any in the past two millennia. Still, the principles of military necessity, humanity, and chivalry provide valuable limitations. Diligent, creative, and intelligent application of these principles should see LOAC well into the twenty-first century. An IW protocol and resort to the proposed ICC should help.

Mark R. Shulman[*]

---

* A.B. Yale College 1985 (History); M.St. Oxford University 1986 (History); C.Phil. University of California, Berkeley 1989 (History); Ph.D. University of California, Berkeley 1990 (History); J.D. candidate, Columbia University School of Law, 1999. I would like to thank Jonathan Bush, W. Darrell Phillips, and Matthew Waxman for their thoughtful comments on previous drafts of this Note.

APPENDIX I: ACRONYMS AND ABBREVIATIONS

AFB	USAF Air Force Base
APC	Armored Personnel Carrier
ARPANET	DOD's Advanced Research Projects Agency-funded progenitor to the Internet.
CENTCOM	Central Command
COMPUSEC	Computer Security
C^3	Command, Control, and Communications
CIA	Central Intelligence Agency
DISA	DOD Defense Information Systems Agency
DOD	Department of Defense
EMP	Electro-magnetic pulse (used in this Note to refer to non-nuclear explosion created EMP)
FBI	Federal Bureau of Investigation
GA	United Nations General Assembly
ICC	International Criminal Court (proposed)
ICRC	International Committee of the Red Cross
I.L.M.	International Legal Materials, American Society of International Law
IW	Information Warfare
JAG	Judge Advocate General
KGB	*Komitet Gosudarstvennoy Bezopastnosti* (Committee for State Security, USSR)
LOAC	Law of Armed Conflict
NRC	National Research Council
NSA	National Security Agency
PCCIP	President's Commission on Critical Infrastructure Protection
RF	Radio frequencies
SAIC	Science Applications International Corporation
SIGINT	Signals Intelligence—information derived from intercepting electromagnetic (radio) waves
U.N.T.S.	United Nations Treaty Series
USA	United States Army
USAF	United States Air Force
USN	United States Navy

APPENDIX II: TYPES OF WARFARE

	OFFENSIVE DEFENSE	DEFENSIVE DEFENSE	SECURITY (STRICTLY DEFENSIVE)
LAND WAR	Desert Storm	Desert Shield	Perimeter lookouts; sentries
NAVAL WAR	Landing at Normandy	Coastal defense monitors	Sentries looking for saboteurs or mines
IW	Destroying C^3 systems	Destroying an attacking computer	Fire-walls