The Principle of Distinction and Weapon Systems on the Contemporary Battlefield

Michael N. Schmitt *

Abstract

This article examines, primarily from the perspective of U.S. forces, the challenges faced by technologically advantaged forces on the asymmetrical battlefield vis-à-vis the legal principle of distinction. Distinction, the linchpin of international humanitarian law, requires that parties to a conflict conduct their operations in a manner that distinguishes between combatants and civilians, as well as between civilian objects and military objectives. Paradoxically, the technological edge that advanced militaries enjoy over their enemies may present problems in terms of ensuring compliance with the distinction principle, particularly at the tactical level of warfare. The conflict in Iraq has demonstrated that on an asymmetrical battlefield, the weaker party may adopt tactics that violate the norm in order to offset its technological disadvantage. When this occurs, compliance by the advantaged party is also complicated. Safeguarding the principle of distinction, therefore, requires altering the cost-benefit calculations of the side facing defeat at the hands of its stronger opponent.

Keywords: asymmetry, distinction, military objective, proportionality, international humanitarian law, law of war, *jus in bello*

For United States forces on the modern battlefield, application of the principle of distinction poses novel challenges. Quite paradoxically, many of these challenges result from the extraordinary technological advantage the U.S. military enjoys over its enemies. This article examines such challenges, primarily at the tactical level of warfare.[1]

In its *Nuclear Weapons* advisory opinion, the International Court of Justice labeled distinction one of two "cardinal" principles of international humanitarian law.[2] This "intransgressible" norm rises to the level of customary law in both international and non-international armed conflict, a status acknowledged by the United States in the 2007

* Michael N. Schmitt is the Charles H. Stockton Professor of International Law at the United States Naval War College in Newport, RI. The views expressed herein are those of the author in his personal capacity, and do not represent the views of the United States Navy or the government of the United States.

1 In U.S. military doctrine, the tactical level of warfare is the level "at which battles and engagements are planned and executed…." It is distinguished from the operational and strategic levels of warfare. Joint Chiefs of Staff, Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* (Washington, D.C.: U.S. Department of Defense, 12 April 2001), as amended through 17 October 2007, at 532.

2 *Threat of Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. Rep., para. 78.

Commander's Handbook on the Law of Naval Operations, its most current manual of international humanitarian law (IHL).[3]

Article 48 of the 1977 Protocol Additional I, which provides that "[p]arties 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," codifies the core principle,[4] while specific rules prohibiting attacks on civilians, civilian objects, and specially protected individuals and objects, such as those who are *hors de combat* and medical facilities, further operationalize it.[5] The United States, which is not a Party to the Protocol, recognizes most such rules as customary law.[6]

Within the general framework of distinction, the proportionality principle and the requirement to take precautions in attack are of particular relevance for U.S. forces. The former prohibits attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[7] The latter requires an attacker to take precautions that minimize effects on the civilian population. These include, among others, doing "everything feasible" to verify that the proposed target is a lawful military objective; choosing weapons and tactics so as to minimize collateral damage to civilian objects and incidental injury to civilians; and selecting that target from among potential targets offering "similar military advantage," the attack on which causes the least collateral damage and incidental injury.[8] Although the *Commander's Handbook* sets out the precautions requirements in lesser detail than the Protocol, U.S. practice demonstrates general acceptance of its core notions.[9]

---

3 See *Threat of Use of Nuclear Weapons*, para. 79, for characterization as intransgressible. On the customary nature of the principle, see International Committee of the Red Cross, Customary International Humanitarian Law, Rules 1 & 7 (2005) [hereinafter CIHL]; Michael N. Schmitt, Charles H.B Garraway and Yoram Dinstein, *The San Remo Manual on the Law of Non-International Armed Conflict: With Commentary* (San Remo: International Institute of Humanitarian Law, 2006), para. 1.2.2, reprinted in *Israel Yearbook on Human Rights* 36 (2006) (Special Supplement); and Naval Warfare Pamphlet 1-14M, *The Commander's Handbook on the Law of Naval Operations*, para. 8.2 (July 2007) [hereinafter NWP 1-14M].

4 Protocol Additional (I) to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 12 December 1977, 1125 UNTS 3, 16 International Legal Materials 1391 (1977) [hereinafter API].

5 See esp. API, art. 51.2 ("The civilian population as such, as well as individual civilians, shall not be the object of attack.") and API, art. 52.1 ("Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives."). The CIHL suggests that the following are specially protected under customary IHL: medical and religious personnel and objects, humanitarian relief personnel and objects, journalists, protected zones, cultural property, works and installations containing dangerous forces, the natural environment, and those who are *hors de combat* (wounded, sick, shipwrecked, those who have surrendered, prisoners of war). CIHL, Parts II and V.

6 See generally the prohibitions contained in NWP 1-14M, especially Chapter 8.

7 CIHL, Rule 14; API, arts. 51.5(b), 57.2(a)(iii), 57.2(b); NWP 1-14M, para. 8.3.1.

8 CIHL, Rules 15-21; API, art. 57.

9 NWP 1-14M, para. 8.3.1.

The conflicts in Afghanistan (Operation Enduring Freedom) and Iraq (Operation Iraqi Freedom) aptly illustrate the phenomenon of asymmetrical technological advantages driving a disadvantaged enemy to adopt asymmetrical means (weapons) and methods (tactics) of its own that endanger application of these prescriptive norms.[10] Combating an asymmetrical opponent involves avoiding enemy strengths, leveraging one's advantages, and exploiting enemy weaknesses and vulnerabilities. Generally conceived of in "methods and means" terms, it may also encompass direct and indirect communication (with one's own public, the enemy public, other states, and the international community), often through diplomacy, the media, and non-governmental organizations; economic wherewithal, both in terms of ability to fund the war effort and the use of sanctions and other economic tools; logistics; law, particularly limitations on the use of force; and morality.[11]

With regard to asymmetry, technological superiority best characterizes the position of U.S. forces in Afghanistan and Iraq. U.S. weapons have greater firepower, range, and precision. High-tech surveillance and reconnaissance platforms, together with other intelligence assets, render the battlefield incredibly transparent. Communications systems are redundant, pervasive, and secure, thereby allowing U.S. commanders an unprecedented degree of command and control over their forces. From conducting attacks with unmanned combat aerial vehicles piloted from the United States, such as the MQ-9 Reaper, to logging into military "chat rooms" with Blue Force Tracker laptops in the remote mountains of Afghanistan, the technological wizardry is nothing short of dazzling.

These assets allow U.S. forces to "get inside the enemy's OODA (observe, orient, decide, act) loop." In other words, they can observe enemy forces, analyze their actions, disseminate information, determine an effective course of action, act, and evaluate the effects of their operations much more quickly than their opponents. In theory, repeatedly doing so stuns the enemy into a purely reactive mode, for it can only act once U.S. operations are either well under way or complete. In extreme cases, the enemy simply shuts down out of a sense of helplessness.

Although pundits might dispute the purported benefits of asymmetry, there is no denying that, on any battlefield the United States has found itself on, or is likely to for the foreseeable future, technological asymmetry is a dominant reality. This reality generates a number of consequences.

---

[10] Such practices were outlined in a series of discussions held with U.S. commanders, military intelligence officers, and judge advocates conducted at the United States Naval War College. Some of the practices are further described in Michael N. Schmitt, "Conduct of Hostilities During Operation Iraqi Freedom: An International Humanitarian Law Assessment," *Yearbook of International Humanitarian Law* 6 (2003), as well as Michael N. Schmitt, "Asymmetrical Warfare and International Humanitarian Law," in *International Humanitarian Law Facing New Challenges*, eds. Wolff Heintschel von Heinegg and Volker Epping (Berlin: Springer Verlag, 2007), and the sources cited therein.

[11] Asymmetry occurs at every level of war. For instance, at the strategic level it can relate to the ability to form and maintain alliances. At the operational level, an ability to command and control forces over large areas and across time may yield asymmetrical advantage, and at the tactical level advanced weaponry yields immediate superiority over a lesser-equipped opponent.

First, the reach and precision of U.S. weapon systems is such that range, geography, weather, and enemy defenses pose only slight obstacles to the conduct of operations across the enemy's land, sea, air, and cyber-territory. Lines of battle have become battlespaces in which legal norms (such as the prohibition on conducting operations in neutral territory), not technological limitations, define operational boundaries. Recall that the first attack of Operation Iraqi Freedom consisted of a cruise missile strike near Baghdad against Saddam Hussein.

Second, an enemy identifiable on an open battlefield will usually be killed by his or her technologically superior opponent, often with a minimal risk to the attacker. As a result, hostilities inevitably migrate to urban or other dense, congested areas. Yet even in such areas, identification as a participant in the hostilities places one at extreme risk. The same dynamic applies to weapon systems and other equipment. Once located and identified as such, the technologically advantaged opponent can typically destroy them, almost effortlessly.

In such an environment, the disadvantaged party must seek its own asymmetrical advantages. Predictably, U.S. opponents have done exactly that. Consider the means of warfare (weapons) to which they have turned. Lacking access to the global high-tech weapons acquisition network (or the financial wherewithal to acquire such systems and know-how to employ them), the enemy in both Afghanistan and Iraq is countering U.S. superiority by leveraging low-tech weaponry. This has been accomplished in a number of ways.

Small arms from the vast licit and illicit global market have found their way into both countries. Furthermore, in Afghanistan small arms were already widely possessed by the warring factions, whereas in Iraq they soon became available when Coalition forces failed to secure and safeguard weapons storage areas of the Iraqi military. Although small arms might not be horribly useful when facing a high-tech enemy on the open battlefield, they are effective in urban and guerrilla operations, which typically involve ambushes and other hit-and-run tactics.

U.S. opponents have also turned to "unconventional" weapons. For instance, improvised explosive devices (IEDs) and vehicle-borne improvised explosive devices (VBIEDs) can be built using such "off-the-shelf" material (commercially available and intended for civilian use) as mobile phones, cars, copper wire, fertilizer, and gasoline. Explosive material can also derive from U.S. and Coalition unexploded ordnance (UXO) or indigenous abandoned ordnance (AXO), like that recovered from Iraqi Army ammunition depots.

In another example, computers linked to the Internet are increasingly employed for such tasks as communications and gathering information from open sources, especially as the Iraqi network comes back on-line. In the future, computer network attacks directly against U.S. military (and perhaps civilian) systems are inevitable, for the heavy U.S. military reliance on computers surely represents an irresistible vulnerability for the enemy. Similarly, low-tech forces have turned to mobile phones as excellent tools for command and control and intelligence gathering and dissemination.

Sadly, the disadvantaged sides in today's asymmetrical conflicts have also adopted unlawful means of warfare.[12] For instance, dead bodies and the wounded have been booby-trapped in violation of the customary norms of international law codified in Protocol II of the Convention on Certain Conventional Weapons.[13] U.S. opponents have also resorted to the use of suicide bombers. While it is not a violation of international humanitarian law to give one's life to kill enemy combatants and civilian direct participants in hostilities, it is a breach to perfidiously feign civilian status in order to get close enough to the enemy to conduct a suicide attack.[14] If an attack is designed to kill even a single civilian, the suicide bomber would be guilty of a war crime.[15]

Such asymmetrical means of warfare present U.S. commanders with a number of challenges in the area of distinction. The most obvious is developing effective counter-systems. Consider IEDs and VBIEDs. The United States and its allies have successfully used existing electronic warfare platforms like the EA6B Prowler to "jam" radio signals that detonate IEDs. Although jamming sometimes interferes with civilian activities or damages civilian equipment, by and large the harm is minimal, at least relative to the military advantage accruing from protecting one's own forces.

Operationally speaking, it would be preferable to detonate the IEDs in advance, because destruction precludes their use in future attacks. Therefore, U.S. forces are turning to new radio-controlled counter-IED systems that transmit signals that cause the IEDs to explode before they can be effectively used. The challenge for any commander employing such systems should be apparent—a lack of knowledge as to the location of the bomb at the time of detonation complicates the proportionality calculation enormously. Might it detonate while a civilian vehicle is passing? What if the IED is being carried though a crowded civilian area on its way to placement alongside a road? What if an undeployed IED is in a house or other building containing civilians? What if there are a number of such devices in the same location, such that the resulting explosion will be huge? And so on.

As these examples illustrate, counter-systems intended for use against threats (whether individuals or weapons) that are difficult to reliably locate or identify can heighten the risk to civilians and civilian property. Unfortunately, in an asymmetrical conflict, a difficult-to-

---

[12] Complicating matters, no Additional Protocol I, Article 36, review is conducted prior to the fielding of such weapons, nor are they generally subject to arms control agreements or transfer monitoring. In other words, their use lies beyond legal and practical control. Article 36 provides that "[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

[13] CIHL, Rule 80; Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, art. 6, 10 October 1980, 1342 U.N.T.S. 168, as amended, 3 May 1996, art. 7, 35 International Legal Materials 1206 (1996), to the 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, 10 October 1980, 1342 U.N.T.S. 137.

[14] At least according to API, art. 37.1(c).

[15] API, art. 85.3(a); Rome Statute of the International Criminal Court, art. 8.2(b)(i), 17 July 1998, UN Doc. A/CONF. 183/9*, 37 International Legal Materials 1002 (1998).

locate or identify weapon or combatant is exactly what one needs to offset an adversary's technological advantage.[16]

Commanders face countless other challenges when seeking to apply the distinction principle in such an environment. Many items used by the weaker side are dual-use – that is, they have both military and civilian purposes. This fact makes it difficult for U.S. forces to distinguish weapons, weapon components, and other military items from their civilian equivalents. As an example, when soldiers spot an individual on a mobile phone, what conclusion should they draw? That the caller is gathering intelligence? Preparing to detonate a bomb? Calling home? Is a truck carrying fertilizer that has been stopped at a roadblock transporting bomb making material or agricultural chemicals? Does an empty car by the side of the road contain a VBIED or has it been parked by its owner while running errands? Is an individual spotted at night carrying a rifle doing so to attack U.S. forces or to defend himself from violent criminals or sectarian militia?

Dramatic asymmetry in weaponry has a particularly pernicious effect, namely the creation of a sense that somehow the fight is unfair, that the advantaged party is a "bully."[17] Sensitive to this reality, commanders are concerned that their actions might be characterized as disproportionate – not necessarily in the sense of the legal principle, but rather in terms of inequality of force. For example, a video clip that has circulated on the Internet depicts an Iraqi insurgent with an AK-47 automatic rifle being killed by a U.S. tank shot. The video evoked a visceral reaction on the part of some viewers that the tank crew had acted wrongfully. Yet, there is no legal distinction between killing a combatant with a tank shell or a rifle bullet (except that of the expected relative collateral damage and incidental injury, if any). When technological asymmetry generates a "bully" perception, commanders justifiably worry that even their lawful actions will be styled unfair or unlawful.

Finally, U.S. forces today wield an impressive array of information operations (IO) capabilities, including the ability to conduct computer network attacks (CNA). IO assets offer an astonishing technological advantage. However, the legality of "striking" certain "target sets" against which such capabilities would be useful—like broadcasting facilities, websites, email systems, and financial assets—remains unsettled. Two schools of thought dominate. The first, based on a strict reading of the definition of "attack" found in Article 49 of Additional Protocol I,[18] argues that the prohibition on attacking civilians or civilian objects applies only to "violent" operations, i.e., those likely to cause death or injury to the former or destruction of or damage to the latter.[19] The other embraces an expansive reading of the notion of attack, focusing on Article 48's language limiting operations to those

---

[16] Of course, certain steps can be taken to limit the risk to civilians and civilian property. These include use outside areas populated by civilians, use when civilians are unlikely to be present, limiting the range or direction of the system, and barring civilians from the area while the system is in use.

[17] See discussion of the "bully syndrome" in Michael N. Schmitt, "21st Century Conflict: Can the Law Survive?" *Melbourne Journal of International Law* 8:2 (2007).

[18] "'Attacks' means acts of violence against the adversary, whether in offence or in defense." API, art. 49.1.

[19] See Michael N. Schmitt, "Wired Warfare: Computer Network Attack and International Law," *International Review of the Red Cross* 84:846 (June 2002): 365–99.

directed against military objectives (and combatants). This interpretation would prohibit most forms of CNA against civilian "cyber-targets," even if the consequences did not involve death, injury, destruction, or damage.[20] U.S. forces controlling CNA and other IO assets must therefore be sensitive to the possibility that their operations, even if compliant with the law as interpreted by the first school of thought, may generate criticism from those adopting the more restrictive approach.

As problematic for U.S. commanders as the weapons used by technologically disadvantaged opponents are the methods they adopt. There is, as noted above, a general tendency for weaker forces to move into densely-built areas populated by civilians. This tactic makes them difficult to locate, identify, and target, particularly since they are unlikely to be wearing uniforms. Additionally, because disadvantaged forces are likely to lose any direct confrontation with the superior U.S. forces, they tend to engage in "shoot and scoot" tactics. In other words, they fire at U.S. forces and immediately flee. There is also a growing tendency to use vulnerable groups for military purposes. In particular, U.S. opponents have used women to gather intelligence, transport supplies, and conduct attacks, sometimes in the form of suicide bombings.

Especially troublesome from a distinction perspective is the adoption of unlawful tactics that leverage the protection the principle extends to civilians and civilian objects. U.S. opponents have, among others, employed both voluntary and involuntary human shields, feigned civilian status in order to conduct surprise attacks, and exploited locations enjoying special protection under IHL. During the 2004 battle for Fallujah, to cite one example, Iraqi insurgents used sixty of the one hundred mosques in the city for military purposes. In some cases, they used them for weapons storage and mustering points; the minarets were particularly valuable as sniping locations and observation points.

These tactics amount to patent breaches of customary international humanitarian law, as well as violations of Additional Protocol I for the Parties thereto.[21] However, it is important to understand that they equally constitute logical tactical responses to technological asymmetry. They variously improve the enemy's ability to avoid detection, hinder U.S. attacks, locate U.S. forces, and get close enough to conduct attacks against them.

More than the immediate battlefield implications of such methods and means of warfare must be considered. U.S. opponents have now adopted "lawfare" as a method of warfare to counter U.S. advantage. In lawfare, one side in a conflict attempts to paint the other as unlawful so as to undercut the adversary's domestic and international support and to bolster the resistance of its own military and public. There is certainly no problem with conducting lawfare against an opponent that is in fact violating the law; to do so enhances the likelihood of IHL's enforcement. But lawfare is often employed in the absence of violation. One classic technique is to ensure that the media has access to gruesome scenes of civilian death, suffering, and destruction. How can anyone fairly evaluate such images and

[20] See Knut Dormann, "Applicability of the Additional Protocols to Computer Network Attack," in *International Experts Conference on Computer Network Attack and the Applicability of International Humanitarian Law: Proceedings*, ed. Karin Bystrom (Stockholm: Swedish National Defense College, 2005).

[21] API, arts. 37, 51, 53.

reports in the absence of knowledge as to the military advantage the attackers expected to gain through the operation?

In Iraq, the enemy has even "baited" U.S. forces in an attempt to create exploitable collateral damage and incidental injury. The use of civilian shields best exemplifies this practice. Likewise, Iraqi insurgents have launched mortar shells from civilian areas in the hope that U.S. forces will respond with counter-battery fire. That lawfare has become an accepted counter to technological advantage was perhaps best illustrated by Hezbollah's adoption of similar tactics, such as firing rockets from civilian apartment complexes, during the 2006 Israeli incursion into Lebanon.[22]

There have even been cases of U.S. opponents dispensing altogether with the principle of distinction, especially during the occupation of Iraq. Unable to prevail by targeting occupation forces, they attacked individuals and groups who qualified as civilians under IHL, including police, politicians, representatives of non-governmental organizations (including, tragically, the ICRC and UN), and the public itself. By shifting the conceptual centre of gravity from the military to the civilian population, the insurgents sought to deter cooperation with the occupation regime and to create a level of instability that would be ripe for exploitation. The civilian violence also weakened international support for the continuation of Coalition operations, including in nations that had contributed troops.

Such tactics have presented U.S. commanders with an array of distinction challenges. Significantly, the phenomenon of combat migrating to populated areas has made application of the principle arduous; after all, in urban warfare many legitimate targets lie in close proximity to civilians and civilian objects. Thus, proportionality issues loom large, as do requirements for precautions in attack regarding weapons, tactics, and target selection. At times, proportionality even bars U.S. forces from striking valuable targets at all because the likely collateral damage and incidental injury would be excessive relative to the anticipated military advantage. Additionally, potential civilian casualties sometimes result in a moral pause that exceeds legal requirements. U.S. troops have often refrained from executing operations that would otherwise be lawful out of concern for the affected civilian population.

It is self-evident that methods of warfare that directly exploit civilian protections for military ends only exacerbate matters. If enemy combatants elect, for instance, to dispense with uniforms, the U.S. soldier on the ground has little way to distinguish combatants and civilians directly participating in hostilities from innocent civilians. As a result, U.S. forces sometimes adopt "self-defense"-style rules of engagement (ROE), under which an individual must perform a "hostile act" or demonstrate "hostile intent" before being engaged. Doing so is driven by policy, not legal, concerns about the practical problem of distinction in contemporary conflict; IHL's much more liberal scheme would allow engaging an en-

[22] See Israel Ministry of Foreign Affairs, "Preserving Humanitarian Principles While Combating Terrorism: Israel's Struggle with Hizbullah in the Lebanon War," Diplomatic Note 1 (April 2007), 7; UN Human Rights Council, Special Rapporteur, Mission to Lebanon and Israel, "Report of Investigation sent to UN General Assembly" (2 October 2006), 14.

emy combatant or civilian directly participating in hostilities at almost any time and anywhere, regardless of whether he posed an immediate threat.[23]

Even when ROE-imposed restrictions exceed those of IHL, civilians can remain at risk. As mentioned, the disadvantaged side in an asymmetrical conflict often adopts a "shoot and scoot" approach to attacks. One common tactic adopted by Iraqi insurgents is to fire a rocket propelled grenade (RPG) down an alley at a U.S. vehicle passing on a cross street. In the vehicle under attack, confusion momentarily reigns as young soldiers look through smoke to see civilians running in every direction. Since insurgents wear civilian clothing, the soldiers struggle to determine who launched the attack. If the soldiers spot a young male fleeing through the streets, they will logically assume he had attacked them and engage him. But, in fact, the real attacker probably fled the scene as soon as he fired, since it would be suicidal to stay and fight the U.S. forces. What the U.S. soldiers actually saw was an innocent civilian running for shelter in the knowledge that a gunfight was about to break out. The risk posed to civilians by the adoption of tactics designed to compensate for technological weakness should be clear.

Along the same lines, U.S. commanders are being forced to deal with the enemy practice of baiting them into causing collateral damage and incidental injury. They are cognizant of the lawfare dynamic, and therefore are highly sensitized to the consequences attendant to civilian casualties, even when they are not excessive as a matter of law. For example, U.S. forces seldom respond with return fire against mortars fired from urban areas, and there are no reported cases of striking targets that were voluntarily or involuntarily shielded by civilians. Inequitably, then, tactics that include knowing violations of humanitarian law can prove highly effective in offsetting an adversary's technological advantage.

A further challenge for U.S. commanders is how to use their weaponry effectively in this type of battle. Once the enemy immerses itself within the civilian population and fails to distinguish itself, high-tech systems become dramatically less effective. In the first place, many involve indirect fire—i.e., the weapons used do not rely on visual (or other reliable sensors) monitoring of the target area in real-time. But absent a real-time picture, collateral damage and incidental injury estimates for urban attacks become increasingly unreliable over time. Of course, known patterns of civilian behavior (e.g., fewer civilians will be on a bridge at 2 AM than during the day) can alleviate the likely incidence of civilian harm, but as every combat commander understands, unpredictable fluidity always

[23] The issue of when a civilian directly participating in conflict may be attacked remains controversial, and is the subject of a major study being conducted by a group of experts under the auspices of the ICRC. Reports of this study are at www.icrc.org/Web/eng/siteeng0.nsf/ html/participation-hostilities-ihl-311205; the group's final "interpretive guidance" will be released in 2008. For judicial treatment of the matter by the Israeli Supreme Court, see HCJ 796/02, *The Public Committee against Torture in Israel v. Israel (et al.)* (Dec. 2006) [Targeting Killing case]. For academic treatment of the issue in articles relied on by the Court, see Michael N. Schmitt, "Direct Participation in Hostilities and 21st Century Armed Conflict," in *Crisis Management and Humanitarian Protection*, eds. Horst Fischer, Ulrike Froissart, Wolff Heintschel von Heinegg, Christian Raap (Berlin: Berliner Wissenschafts-Verlag, 2004) and Michael N. Schmitt, "Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees," *Chicago Journal of International Law* 5 (2005): 511–46.

characterizes the urban battlespace. Inability to view the target in real-time also facilitates baiting tactics, particularly those executed through "shoot and scoot" methods. The example of counter-battery fire against mortar attacks cited above exemplifies this reality.

It must also be recognized that the intended usage of some weapons fielded by U.S. forces assumes a relatively identifiable target. The sniper rifle is highly effective, for instance, but only if the sniper can reliably pick out his victim. The same applies to night vision goggles. Imagine an individual walking with a shovel along a road at night. Absent a uniform or other distinguishing clothing, is he an insurgent burying an IED or a farmer going home? Or consider pre-planned aerial attacks, i.e., those against fixed targets, planned in advance. In classic hostilities, they are conducted against military objectives readily identifiable as such: bases, airfields, naval docking facilities, rail lines and other lines of communications serving military purposes, armament factories, and the like. Such entities, consistent with the mandate of Article 58 of Additional Protocol I, are usually located away from concentrations of civilians.[24] In Iraq, by contrast, "military" objectives against which pre-planned operations might be useful were often originally civilian in character and are present in urban areas, factors which render attack with weaponry designed for easily identifiable targets problematic.

Finally, commanders are struggling with cultural sensitivities bearing on the principle of distinction, both those of the enemy population and its own soldiers. For instance, and as noted, insurgents regularly use mosques for weapons storage and other purposes. The fact that U.S. forces are hesitant about entering mosques (or conducting operations which might damage them) has not been lost on their opponents. Similarly, U.S. forces, because of their own sensitivities (and those of the population), hesitate to search women; typically, only female soldiers do so. Again, this lesson has not been missed by the enemy. The October 2007 capture in Afghanistan of a tall Siberian red-headed blue-eyed male foreign fighter wearing a burqa is bizarrely illustrative.[25]

Violations of the principle of distinction and other IHL norms by U.S. opponents have clearly affected the attitude of soldiers in the field. A 2006 survey by U.S. military mental health specialists in Iraq produced shocking results. Only 47 percent of the soldiers and 38 percent of the marines surveyed believed they should treat all non-combatants with dignity and respect. 17 percent of both groups suggested that all non-combatants should be treated as insurgents, while 39 percent of the marines and 36 percent of the soldiers would accept torture to gather critical intelligence about insurgents. 12 percent of the marines and 9 percent of the soldiers had unnecessarily damaged or destroyed Iraqi property, and only 40 percent of the marines and 55 percent of the soldiers would report another for "injuring or killing an innocent non-combatant," despite having received training that doing so is re-

[24] API, art. 58 provides that parties "shall, to the maximum extent feasible … endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives; avoid locating military objectives within or near densely populated areas; [and] take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations."

[25] David Rohde, "Foreign Fighters of Harsher Bent Bolster Taliban," *New York Times* (30 October 2007), 1.

quired.[26] The point is that when one side violates the law, it becomes very difficult for the other side's commanders and non-commissioned officers to maintain respect for that law among the troops.

As is usually the case, the news is not all bad. The advanced technologies that contribute to a technologically disadvantaged party's unlawful methods and means of warfare can clearly serve humanitarian ends. The precision of modern weaponry allows an attack to avoid much of the collateral damage and incidental injury it might otherwise cause. The attacker also has a greater capability to estimate likely collateral damage in advance of an attack using modern intelligence, surveillance, and reconnaissance assets. Likewise, its ability to assess the results of a strike is enhanced, thereby lowering the requirement for follow-up attacks (which might harm civilians and civilian property) in order to ensure the target has been neutralized. Additionally, advanced visual, voice, and computer communications equipment allow for better command and control of forces in contact with the enemy, helping them to avoid civilian consequences. Of course, the variety and diverse capabilities of systems available to modern militaries measurably increase the options available to them in terms of verifying potential targets and selecting those weapons, tactics, and targets to achieve their objectives while minimizing civilian casualties. In that regard, the distinction requirement to take precautions in attack is fostered.

Conclusion

Somewhat paradoxically, the vast superiority in weapons systems and other military technology enjoyed by U.S. forces has impelled their enemies toward methods and means of warfare that often violate distinction norms, thereby complicating compliance with their own distinction obligations. One might conclude that the problem lies in asymmetry and that, therefore, the remedy lies in somehow equalizing the battle. It does not, nor would militarily powerful states accept such a premise. Rather, the key lies in the fact that technologically disadvantaged parties to a conflict often rationally conclude that it is more advantageous to violate the norms of IHL than it is costly. It is this cost-benefit calculation that must be altered. How to do so in a way that is practical, while preserving the existing protections for the civilian population inherent in the principle of distinction, is a subject that merits further study.

[26] Office of the Surgeon, Multinational Force-Iraq and Office of the Surgeon General, U.S. Army Medical Command, Mental Health Advisory Team ("MHAT") IV Operation Iraqi Freedom 05–07: Final Report (17 November 2006), 35–38.