2009

LAW AND WAR IN THE VIRTUAL ERA

Jack M. Beard
University of Nebraska College of Law, jbeard2@unl.edu

103 AM. J. INT'L L. 409 (2009).

LAW AND WAR IN THE VIRTUAL ERA

By Jack M. Beard[*]

Since the first attempts by states to use law to regulate armed conflict, legal constraints have often failed to protect civilians from the adverse effects of war. Advances in military technology have usually not improved this situation and have instead made law even more distant and less relevant to the suffering of civilians in wartime.[1] The massive, indiscriminate incendiary bombing campaigns against major urban areas in World War II spoke volumes about the irrelevance of fundamental legal principles and rules designed to protect civilian populations in wartime. Law and lawyers were in fact far removed, physically and operationally, from the cockpits of the United States bombers flying over Tokyo, whose aircrews were focused on surviving their missions. They struggled with limited information about their assigned targets and conducted their operations with rudimentary preflight instructions that directed them, for example, to avoid destroying the palace of the Japanese emperor but left them free to submerge entire residential areas of the city in a sea of flames.

Fifty-six years after the war with Japan, the United States began a military campaign against a new enemy, the Taliban regime in Afghanistan. In contrast to World War II and the human aircrews over Japan, this war on its first night found a robot, the Predator MX-1 (an unmanned aerial vehicle, or UAV), surveilling the roads leading out of that country's capital city, Kabul. The Predator was equipped with missiles that could be fired by a crew thousands of miles away in the United States controlling the vehicle via a satellite link. It appeared to have an opportunity to kill the fleeing leader of the Taliban regime, Mullah Omar, together with his closest cohorts. The legal office at the U.S. Central Command (CENTCOM) reportedly raised various concerns about the air strike, including the likelihood that it would cause excessive civilian casualties, and the attack was aborted.[2]

The aborted 2001 Predator attack over Kabul involved a previously unimaginable level of safety for the faraway crew conducting the attack, an aircraft that could "loiter" over targets

[*] Professorial Lecturer, UCLA School of Law; former Associate Deputy General Counsel (International Affairs), Department of Defense. The author was also assigned as a Lieutenant Colonel in the U.S. Army Reserve to the International and Operational Law Division, Office of The Judge Advocate General, Department of the Army. He greatly appreciates comments by David Koplow and Stephen Yeazell on earlier drafts and also thanks Daniel Laidman for research assistance.

[1] For example, long-range artillery, aircraft, and missiles each dramatically expanded the battlefield and in so doing threatened ever-increasing numbers of civilians, greatly complicating compliance with practices or rules obliging military forces to distinguish combatants from noncombatants.

[2] *See* REBECCA GRANT, THE AFGHAN AIR WAR 17 (Air Force Association Special Report, 2002), *available at* http://www.afa.org/media/reports/afghanbook/Afghanbk.pdf; Evan Thomas & Daniel Klaidman, *The Battle Within,* NEWSWEEK, Sept. 15, 2003, at 40; Seymour Hersh, *King's Ransom: How Vulnerable Are the Saudi Royals*? NEW YORKER, Oct. 22, 2001, at 35. Ultimately, the decision whether the convoy could be fired upon by the CIA-operated Predator had to be made by the commander in chief of CENTCOM, as advised by CENTCOM Judge Advocate General officers.

unimpeded by the limits of human pilots, and an extraordinary level of legal review for an air strike in progress. The attack thus demonstrates several key aspects of a new era of warfare made possible by recent advances in remotely controlled or semiautomated "virtual" military technologies.[3] This article examines the way these virtual technologies are purposely expanding important military capabilities while unintentionally transforming modern military operations, military information resources, the structure of military organizations, and the role of lawyers within these organizations. Unanticipated applications of virtual military capabilities are creating unprecedented levels of transparency and are unexpectedly making international law more relevant than ever to armed conflicts. This new relevance especially bears on long-ignored or easily manipulated legal principles and rules that bar attacks on legitimate military targets if those attacks are likely to result in excessive or disproportionate civilian casualties. Such principles and rules are now gaining unheard-of traction and renewed meaning as the new—and very real—virtual era dawns.

Part I of this article briefly examines the rise of virtual military technologies and assesses their transformational extrahuman capabilities, which now enable military forces to conduct "persistent surveillance." Part II describes the transformational aspects of "virtual distance" associated with these new technologies and contrasts them with the characteristics of conventional notions of distance associated with manned military vehicles and platforms. This part next analyzes the way these virtual technologies are intentionally changing warfare while their informational capabilities and other attributes are unintentionally changing the missions and operations of military forces and the structure and culture of military institutions. The importance of these new technologies ultimately extends beyond new missions and capabilities to encompass fundamental changes in hierarchical military structures and even the definition of victory in war itself.

Part III examines how the extrahuman capabilities of virtual technologies and aspects of virtual distance in weaponry are unexpectedly revitalizing key *jus in bello* principles of the law of war[4] that protect civilians from the effects of hostilities, facilitating their emergence as more serious constraints on military operations. Part III also shows how this new "law of virtual war"

[3] While the term "virtual" was once used in common parlance only to describe something imaginary—and in the military context has often been associated with computer-simulated war games or simulated "virtual reality" training techniques—it is now increasingly used as well to encompass and describe a wide variety of technologically assisted remote operations of *real* activities. The new era of virtual offices and classrooms, in which humans work on projects by proxy or at a distance, and virtual equipment, such as fences that function through networks of tower-mounted sensors and surveillance gear, can now appropriately be said to include military operations that rely on a growing assortment of vehicles, platforms, and weapons controlled, managed, and directed by personnel at distant sites. For purposes of this article, "virtual military technologies" comprise nonexpendable and remotely controlled or semiautonomous weapons systems, robots, naval craft, and ground and aerial vehicles. They do not include ballistic or semiballistic missiles, cruise missiles, artillery projectiles, and precision-guided munitions (which are also excluded from the definition of "UAVs" by the U.S. military).

[4] *Jus in bello* refers to that part of the law of war governing the conduct of armed conflicts. In its modern form, the law of war can also be referred to as the "law of armed conflict" and "international humanitarian law." U.S. law, such as the Uniform Code of Military Justice, contains important references to the law of war, ensuring that this older term will continue to require the attention of scholars who will interpret it consistently with growing commentary linked to the more contemporary term "international humanitarian law." The Supreme Court, when forced to opine on the subject, has concluded that the term "law of war" includes at a minimum "the four Geneva Conventions signed in 1949," and must be read consistently with the "rules and precepts of the law of nations" as applied in *Ex parte Quirin*, 317 U.S. 1, 28 (1942). *See* Hamdan v. Rumsfeld*,* 548 U.S. 557, 613 (2006).

continues to be informed by the increasingly common fusion of human and machine in sophisticated weapons systems and how these advanced technologies are adding new responsibilities to the duty to take precautionary measures. Part IV concludes with some observations on the future of virtual military technologies and the law of war.

I. The Dawn of the Virtual Era

The Relentless Pursuit of New Military Technology and Its Unintended Consequences

Historically, the possibility that conflicts between states will be conducted by force has led to intense competition by states "in the arts and the instruments of force."[5] It is thus not surprising that the most industrialized countries have been preoccupied, especially since 1939, with achieving military-technological improvements and have devoted enormous amounts of funding to military-related research-and-development projects.[6] It is in this context that some scholars suggest that military science has mobilized society, as seen by the way that military projects and a military-related agenda dominate the work of engineers and scientists, particularly in the United States.[7]

The U.S. military-technological experience represents a consistent, but exaggerated, variation of historical trends in this area, as Americans have displayed an almost boundless confidence in the power of science and technology to promote "progress" and have tended to trust in the power of military technology to translate into success in war.[8] This fundamental belief in the power of military-technological achievements does not mean, however, that decision makers in the United States— or in any other industrialized country—feel compelled to give careful consideration to the overall ramifications of such achievements before pursuing them. Technological advances can actually occur with little deliberation about their long-term consequences, and the implications of all the potential applications of new weapons systems may therefore be largely unforeseen.[9] The relentless pursuit of new military technology, in conjunction with the militarization of science in modern society, also means that scientific and technological developments are now more likely than ever to be quickly applied to warfare.[10] This

[5] Kenneth N. Waltz, Theory of International Politics 127 (1979). This competition is heightened by the inherently relative nature of military power and the high-stakes security environment, which makes states believe that there is little room left for error. *See* Robert Jervis, *Security Regimes*, *in* International Regimes 173, 173–74 (Stephen D. Krasner ed., 1983).

[6] *See* Donald A. MacKenzie & Judy Wajcman, *Introduction* to pt. 4, *Technological Determinism and Weaponry, in* Social Shaping of Technology 343 (Donald A. MacKenzie & Judy Wajcman eds., 2d ed. 1999).

[7] Chris H. Gray, Postmodern War: The New Politics of Conflict 231 (1997) (noting that as many as half of all engineers and scientists in the United States are working for the military or on military problems, or otherwise working in accord with military priorities).

[8] *See, e.g.*, Evan Thomas & John Barry, *War's New Science,* Newsweek, Feb. 18, 1991, at 38 ("Americans have always looked to science for their answers, in war as in everything else."). Some have suggested that the U.S. attachment to new military technology even borders on "technophilia." *E.g.,* Manuel De Landa, War in the Age of Intelligent Machines 29, 225 (1991).

[9] Such unintended consequences may arise in a variety of contexts, including the proliferation of new weapons in the hands of enemy states or nonstate actors, resulting changes in the ways wars are waged, commercial spin-offs of technologies that were once monopolized by the military, and unforeseen applications of new technologies.

[10] This phenomenon stands in contrast to the less prominent role that science played in warfare in some earlier societies. *See, e.g.,* Gray, *supra* note 7, at 231 (noting that wheels were used on toys for hundreds of years before they were used on chariots and that gunpowder was used for fireworks in China long before it was used to revolutionize warfare).

rapid deployment of new military technologies increases the possibility that scientific and technological advances may ironically yield results that ultimately diminish, rather than enhance, the power of states seeking military advantage through the acquisition of these weapons systems.

The Road to Virtual Weapons Systems

Driven by various institutional, strategic, monetary, and practical objectives (and not mainly by humanitarian considerations), the U.S. military has long endeavored to achieve more accurate bombing capabilities.[11] These efforts led to the development and deployment of a variety of precision-guided munitions (PGMs) that became prominent in the Persian Gulf war of 1991. The introduction of PGMs and other "high-tech" weapons intensified the search for new technology to obtain more and better supporting intelligence, surveillance, and reconnaissance (ISR) data for targeting. In the security environment that followed the events of September 11, 2001, new U.S. strategic priorities further emphasized the need for expanded ISR capabilities, particularly to realize the key operational goal of "[d]eny[ing] enemies sanctuary by developing capabilities for persistent surveillance, tracking, and rapid engagement."[12] Unlike conventional ISR missions, "persistent surveillance" entailed the systematic, sustained, and real-time observation of many different areas, places, persons, and things.[13] These new information requirements called for new technological solutions.[14] UAVs, which had seen only limited use before 9/11,[15] emerged as the key technological enabler for meeting the critical persistent surveillance requirement.[16]

Although UAVs that now provide previously unimaginable amounts of data were deployed on a very limited or experimental basis less than ten years ago, they have become an integral part of U.S. military operations and are increasingly being produced, deployed, and in many

[11] A bomb that could improve the likelihood of achieving a one-shot, one-kill ratio not only would be a bargain, but also would increase the capability to destroy hard targets and reduce the number of sorties required for any one mission. It would further mean that weapons could be released from safer distances and altitudes. *See* STEPHEN BUDIANSKY, AIR POWER: THE MEN, MACHINES, AND IDEAS THAT REVOLUTIONIZED WAR, FROM *KITTY HAWK* TO GULF WAR II 408–09 (2004).

[12] DONALD H. RUMSFELD, 2002 ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS 3, *available at* http://www.dod.gov/execsec/adr2002/index.htm.

[13] Robert K. Ackerman, *Persistent Surveillance Comes into View,* SIGNAL MAG., May 2002, at 18 (quoting a senior official in the Department of Defense on how persistent surveillance highlights the difference between the information needs of the intelligence community (which may be inclined toward "every so often") and those of the military (which generally is looking for "whatever 'now' is defined as")).

[14] While satellites are adequate for certain intelligence purposes, they provide coverage of specific locations for intermittent periods only. U-2 spy planes and other manned high-altitude aircraft provide more extended surveillance coverage but are limited by the risks they pose to pilots and human limits that constrain the number and length of required missions.

[15] Israel demonstrated how UAVs could perform critical and dangerous ISR missions by using them in 1982 to identify Syrian antiaircraft batteries and monitor Syrian airfields. BUDIANSKY, *supra* note 11, at 404–05. Limited U.S. deployments of UAVs over Bosnia in 1995 and in the Kosovo conflict in 1999 further demonstrated these capabilities.

[16] Ackerman, *supra* note 13, at 18. A growing array of UAVs is making this requirement a reality. For example, the Predator has been supplemented by the RQ-4A Global Hawk, which can operate at higher altitudes, remain aloft for up to thirty-six hours, and survey an area of forty thousand square miles using high-resolution Synthetic Aperture Radar and electro-optical/infrared sensors. *See Global Hawk to Fly over Canada in January*, AEROSPACE DAILY & DEF. REP., Dec. 15, 1999.

cases exported by a growing number of other states.[17] The use of such virtual military technology continues to grow at an astounding pace; the scope of unmanned missions and capabilities keeps on expanding; and the worldwide demand for UAVs, led by the United States, is dramatically rising each year.[18] The ability of UAVs to linger over targets for extended periods of time in perilous conditions illustrates one of the reasons for the attractiveness of virtual technologies to military planners in the United States and elsewhere: they give the human operator a virtual working environment while they perform the dirty, dull, or dangerous missions.[19] Virtual technologies that can engage in such missions are not limited to UAVs, but also encompass new and varied land and sea applications designed to support key emerging missions, such as the detection and disarming of roadside explosive devices in Iraq and Afghanistan by unmanned ground vehicles and robots.[20] The U.S. Congress in particular has been eager to sustain and advance this conversion to virtual technologies, and in 2001 mandated that a full third of essential U.S. military aircraft and ground combat vehicles be unmanned by 2015.[21] These weapons systems, especially UAVs, are playing an increasingly significant role in the military operations of more and more countries.[22]

II. The Effect of Virtual Technologies on Military Operations and Institutions

Although virtual military technologies are ideally suited for so-called dirty, dull, or dangerous missions, two more fundamental dimensions or aspects of these technologies help explain their transformational effects on military institutions, military operations, and the law of war: the new "virtual distance" that they create between humans and the battlefield, and their new virtual "extrahuman" capabilities. The U.S. military planned to use these two aspects of virtual weapons systems to obtain both unprecedented quantities and types of ISR data for targeting,

[17] *See* J. R. Wilson, *UAV Worldwide Roundup 2009,* AEROSPACE AMERICA, Apr. 2009, at 30, 30 ("The proliferation of UAVs continues to accelerate, with a growing number of companies, countries, and innovative designs entering the market."). As early as 2005, at least forty-one countries were operating eighty models of UAVs. OFFICE OF THE SECRETARY OF DEFENSE, UNMANNED AIRCRAFT SYSTEMS ROADMAP, 2005–2030, at 38 (2005).

[18] While the United States leads the market in research and development, production, and spending, European and Asian investment in UAVs is rapidly growing. *See* Larry Dickerson, *New Respect for UAVs*, AVIATION WK. & SPACE TECH., Jan. 26, 2009, at 94. The United Kingdom, France, and Germany lead Europe in this field, with over ninety different aircraft or variants, from some thirty manufacturers. UAV programs are also under way in many countries in Asia, including China, India, Japan, South Korea, Malaysia, Singapore, and Taiwan. "Israel remains one of the world's major UAV suppliers . . . ." J. R. Wilson, *UAV Worldwide Roundup—2005*, AEROSPACE AMERICA, Sept. 2005, at 26, 29.

[19] OFFICE OF THE SECRETARY OF DEFENSE, *supra* note 17, at 1–2.

[20] Ramon Lopez, *Foiling Bombs and Bad Guys*, DEF. TECH. INT'L, Dec. 1, 2007, at 30 (noting that from 2004 to 2006, unmanned ground vehicles/robots increased from 160 to 4000 in Iraq and Afghanistan, performing nearly 30,000 explosive ordnance disposal missions and neutralizing more than 11,000 improvised explosive devices in 2006 alone).

[21] Section 220(a) of the National Defense Authorization Act, Fiscal Year 2001, Pub. L. No. 106-398, 114 Stat. 1654, 1654A-38 (2000), states that by 2010, one-third of the aircraft in the operational deep strike force should be unmanned, and that by 2015, one-third of the army's Future Combat Systems' operational ground combat vehicles should be unmanned.

[22] For example, Israel made significant use of UAVs against Hezbollah in the 2006 fighting in southern Lebanon; Georgia used UAVs in the 2008 Russo-Georgian conflict to monitor the activities of separatist forces and provide targeting data for Georgian artillery units; and Iran has a growing inventory of UAVs and has apparently been using some of them over Iraq. *See* Dickerson, *supra* note 18; Ned Parker, *U.S. Says It Downed Iran Drone over Iraq*, L.A. TIMES, Mar. 17, 2009, at A23.

as well as new attack capabilities. Unintended and profound consequences, however, have accompanied the accomplishment of these objectives.

Intentional Changes: New Attack Capabilities

Although the first UAVs were used only to collect ISR data, more recently they have been equipped with a growing array of missiles, as well as laser designators with new target acquisition capabilities; the result is new hunter-killer UAVs like the MQ-9 Reaper.[23] As intended, the extrahuman capabilities of virtual technologies have dramatically expanded attack capabilities. UAVs now not only perform persistent surveillance to identify and track targets—on missions that may exceed the limited endurance and skills of human pilots—but also constitute lethal weapons platforms with a continuous presence, enabling attacks on more targets in more situations than ever before. In addition to ensuring that remotely located human pilots will not be killed or captured, UAVs have the ability to designate targets, which means that laser-guided bombs do not require humans to be near the target on the ground or in the air to carry out this key function.

The problematic humanitarian and legal implications of the intended application of new virtual weapons systems correspond with their objective: they dramatically expand the potential list of targets that can be effectively attacked. The full meaning of this new attack capability is still unfolding, but it has clearly manifested itself to this point in at least two emerging patterns: first, UAVs have become an indispensable tool in the targeted killing of key individuals in terrorist organizations;[24] and, second, UAV capabilities now allow military forces to strike much more comprehensive lists of key "strategic" targets. Similar questions, albeit on a more limited scale, were raised by the emergence of PGMs in the 1990s, inspiring considerable commentary about the consequences and significance of more precise targeting capabilities. Although some viewed precision as potentially ushering in a new humanitarian era in armed conflict,[25] it has raised its own set of humanitarian issues. These issues, made even more salient by virtual technologies, force states to confront some difficult and fundamental questions, for example: What kind of persons can be specifically targeted with these weapons or, put another way, who now constitutes a "combatant"? And what kinds of targets can legitimately be attacked as strategic military objectives?[26]

[23] *See* U.S. Air Force, *MQ-1 Predator Unmanned Aircraft System* (Sept. 2008), *at* http://www.af.mil/information/factsheets/factsheet.asp?id=122; John A. Tirpak, *UAVs with Bite,* A.F. MAG., Jan. 2007, at 46.

[24] *See, e.g.*, Greg Miller, *U.S. Strikes Stagger Al Qaeda*, L.A. TIMES, Mar. 21, 2009, at A1 (noting that since Aug. 31, 2008, the Central Intelligence Agency has carried out an "expansive targeted killing program" that has involved "at least 38 Predator strikes in northwest Pakistan"); David Morgan, *U.S. Targeted-Killings of Al Qaeda Suspects Rising*, REUTERS, Jan. 18, 2006. One of the first notable UAV air strikes was launched in Yemen in 2002 (by a CIA-operated Predator). *See* James Risen & Judith Miller, *C.I.A. Is Reported to Kill a Leader of Qaeda in Yemen*, N.Y. TIMES, Nov. 5, 2002, at A1.

[25] *See, e.g.*, Tami Davis Biddle, *Air Power*, *in* THE LAWS OF WAR: CONSTRAINTS ON WARFARE IN THE WESTERN WORLD 140, 141 (Michael Howard, George J. Andreopoulos, & Mark R. Shulman eds., 1994) (suggesting that the emergence of more accurate bombing capabilities might lead to a convergence of "ethics and efficiency" that could "bolster the prospects for adherence to international norms").

[26] This question has continued to grow in importance since PGMs were used against new types of targets in the 1991 Gulf war. *See* Roger Normand & Chris af Jochnick, *The Legitimation of Violence: A Critical Analysis of the Gulf War*, 35 HARV. INT'L L.J. 387, 389 (1994) ("Until the Gulf War, the definition of 'military objective' had never really been tested, largely because belligerents lacked the capacity to bypass enemy forces to strike at nonmilitary targets.").

The continuing efforts by lawyers in the international community to answer these two questions are complex and lie beyond the scope of this article. Opposition to the targeted killing of individuals raises important questions, such as: Where does the "war on terror" end and where does domestic law enforcement begin? Do national borders remain as barriers to this type of military action or does war now exist everywhere, all the time?[27] As for the type of targets that can be counted as legitimate military objectives, a debate has raged since the 1991 Gulf war about "effects based" targeting and the propriety of attacking various economic and industrial infrastructure sites or other strategic targets closely linked to the center of gravity of an enemy regime and its war efforts.[28] Such issues highlight how precision targeting alone has not solved the problem of protecting civilians from the effects of hostilities and may instead be presenting new threats.[29]

While UAVs greatly improve the ability of military forces to identify, track, target, and then destroy specific objectives, this significant expansion in attack capabilities is in one sense only an incremental change in nature, since it builds upon recent major technological advances in guided precision targeting. On the other hand, the virtual "persistent surveillance" capabilities and new virtual operating environments for humans represent powerful, transformational forces that can limit the full application of these new, expanded targeting capabilities. Such unforeseen and ironic consequences begin with the effects that these new virtual technologies have on the military organizations responsible for their operation.

Unintentional Changes

Changes in military structures and operations. The extrahuman capabilities of UAVs have enabled the U.S. military for the first time in history to engage in persistent surveillance over large, distant areas of the globe. Smaller versions of UAVs (as well as some unmanned ground vehicles), which can be carried by individual soldiers and launched or set in motion by hand, supplement these assets by acquiring real-time tactical information in areas that might otherwise be inaccessible to their human operators.[30] Thanks to these new virtual sur-

[27] *See generally* Rosa E. Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675 (2004); W. Jason Fisher, *Targeted Killing, Norms, and International Law*, 45 COLUM. J. TRANSNAT'L L. 711 (2007).

[28] "Effects based targeting" seeks to identify "specific links, nodes, or objects" that, if attacked, will fulfill certain desired objectives. Tony Montgomery, *Legal Perspective from the EUCOM Targeting Cell, in* LEGAL AND ETHICAL LESSONS OF NATO'S KOSOVO CAMPAIGN 189, 190 (Naval War C. Int'l L. Stud. No. 78, Andru E. Wall ed., 2003) [hereinafter LEGAL & ETHICAL LESSONS]. Such targeting may include attacks on a state's strategic infrastructure that are designed to coerce a regime into complying with specific demands.

[29] For example, Judge James E. Baker warned of "the impending collision among the law of armed conflict, the doctrine of effects-based targeting, and a shared desire to limit collateral casualties and consequences to the fullest extent possible." James E. Baker, *Judging Kosovo: The Legal Process, the Law of Armed Conflict, and the Commander in Chief, in* LEGAL & ETHICAL LESSONS, *supra* note 28, at 7, 8. Human rights groups are rightly concerned about the humanitarian consequences of any expansion of the definition of persons and facilities that can be legitimately targeted in armed conflicts. *See, e.g.*, MIDDLE EAST WATCH, NEEDLESS DEATHS IN THE GULF WAR 177–93 (1991) (noting how the precise bombing of Iraq's electrical grid in the Gulf war shut down most Iraqi water treatment plants, contributing to many civilian deaths from water-borne diseases).

[30] *See, e.g.,* David Eshel, *Tiny and Unafraid: Small UAVs Fly High in Tactical Operations*, DEF. TECH. INT'L, May 1, 2008, at 32, 36. Small military units can use these micro-UAVs to obtain information on what is "over the next hill" or "around the next block."

veillance capabilities, military commanders now abound in more recorded and real-time information than once was even imaginable. Yet for this vast amount of new data to be effectively used, fundamental changes in military operations and organization are necessary.

While military commanders and strategists are fond of referring to technology that provides a perceived advantage over the enemy as a "force multiplier," they may overlook the fact that for such technology to be genuinely effective, it must also be viewed as a "force modifier."[31] The success of new military technologies has thus depended on how well they function in a particular state's military structure and operations, often requiring major corresponding changes in organization, logistics, doctrine, strategy, and tactics. Even commentators who emphasize the importance of military technology in so-called revolutions in military affairs acknowledge that technical advances alone rarely make genuine revolutions.[32]

The vast quantities and new types of ISR data generated by virtual military technologies have little value to military forces if they do not reach the appropriate commanders or other decision makers in a timely manner. The use of such data remains an enormous challenge for even the most powerful, technologically sophisticated states: linear organizational schemes or vertical bureaucracies like those that have predominated in the U.S. military establishment are especially ill-suited to taking advantage of large amounts of new intelligence information.[33] Accordingly, as long as advanced information systems associated with virtual military technologies are tied to obsolete hierarchical structures, the advantages that these systems hold out to U.S. forces probably cannot be fully realized, if at all.[34] Unlike network-centric systems (on which terrorists and other militant groups rely in what some call "netwar"[35]), traditional linear structures and processes found in most military institutions are likely to result in making too little information available to the subordinate units that need it, while possibly producing an overload of data at other levels—with negative consequences for all operations, especially targeting.[36]

Harnessing the potential benefits of information supplied by new virtual military technologies in a way that allows individuals to draw on these resources to deal with new asymmetrical

[31] JOHN ARQUILLA & DAVID RONFELDT, THE ADVENT OF NETWAR 44 (Rand, 1996). For this reason, it has sometimes proven difficult for new weapons systems to be integrated into particular societies and their war-fighting machines. *See* DE LANDA, *supra* note 8, at 27.

[32] *See* MAX BOOT, WAR MADE NEW 10 (2006) ("No technical advance by itself made a revolution; it was how people responded to technology that produced seismic shifts in warfare.").

[33] Military organizational structures often impede the effective, timely dissemination of intelligence—making too little information available to those who need it—by forcing commanders to submit their intelligence requirements through a cumbersome system that validates, consolidates, and assigns priority to these requirements at various levels; to request authorization for the use of the necessary intelligence assets from a centralized system; and to wait for the information to be collected, analyzed, put in usable form, and sent back through the same cumbersome structure. *See* THOMAS X. HAMMES, THE SLING AND THE STONE: ON WAR IN THE 21ST CENTURY 192–93 (2006).

[34] *Id.* at 193 ("[T]he premier benefit of the Information Age—immediate access to current intelligence—is nullified by the way we route it through our vertical bureaucracy.").

[35] ARQUILLA & RONFELDT, *supra* note 31, at 5, 44 (defining "netwar" as "an emerging mode of conflict and crime at societal levels, involving measures short of war, in which the protagonists use—indeed, depend on using—network forms of organization, doctrine, strategy, and communication").

[36] HAMMES, *supra* note 33, at 193 (noting that linear military bureaucracies discourage subordinate units from accessing intelligence information directly, via the Internet, which can result in "limiting . . . the variety and timeliness of the information available to our decision makers").

threats thus requires the reorganization of military hierarchical structures related to the collection, processing, and dissemination of such data; major cultural adjustments; and fundamental changes in planning, doctrine, and operations.[37] Key network-oriented reforms must be implemented if military commanders are to take advantage of the "unblinking eye" capability of virtual technologies. Such reforms include creating adaptive networks so that commanders at all levels can directly access both important real-time information[38] and the results of prolonged surveillance of specific targets. In the context of U.S. counterinsurgency (COIN) operations in Iraq and Afghanistan, this kind of change is contributing to what has been called a "significant metamorphosis of intelligence operations." As part of this metamorphosis, the "decentralized control of intelligence assets" has become a key tenet of emerging COIN doctrine.[39] This radically expanded control of new intelligence assets also reflects the key COIN concept that "higher commanders owe it to their subordinates to push as many capabilities as possible down to their level."[40] While the effects of the surge in U.S. combat troops in Iraq have been widely noted, it can be argued that another, more transformational "surge" occurred in the increased and highly successful use by subordinate ground forces of new intelligence capabilities, especially the full motion video provided by UAVs.[41]

The new virtual technologies and the capacity for persistent surveillance have given unprecedented intelligence capabilities to U.S. and allied military forces in Iraq and Afghanistan, as well as to military commanders in a growing number of countries. Just as this information continues to lead inescapably to fundamental changes in the structure and operations of military organizations, so it is also reshaping the capability of military commanders and their advisers to comply with law-of-war obligations, while unexpectedly transforming the work of lawyers and other personnel who are responsible for planning and approving attacks that may cause incidental civilian casualties.

Personnel changes. Modern warfare, as practiced by powerful states like the United States, is managed by professionals in vast and complex bureaucracies. Major technological changes that spawn new methods of warfare and related organizational changes often pose significant personnel challenges to these bureaucracies. One component that is profoundly affected by the new types of information generated by these technologies—one that plays a key role in ensuring compliance with law-of-war obligations and preventing civilian casualties—is the lawyers.

[37] Ackerman, *supra* note 13, at 20; Joris Janssen Lok, *Empty Battlefield; Commanders Urge New Tactics to Prevail in Asymmetric Campaigns,* DEF. TECH. INT'L, May 1, 2007, at 12.

[38] American ground troops are increasingly equipped with laptops so they can access networks to download real-time video from UAVs operating overhead; according to the commander of one Predator squadron, they "want more and more of it." Charles J. Hanley, *Unmanned Reapers Bound for Iraq, Afghanistan*, A.F. TIMES, July 17, 2007, *at* http://www.airforcetimes.com.

[39] Raymond T. Odierno [now commanding general, Multinational Force–Iraq], Nichoel E. Brooks, & Francesco P. Mastracchio, *ISR Evolution in the Iraqi Theatre*, 50 JOINT FORCES Q. 51, 52 (2008).

[40] *Id.*; THE U.S. ARMY–MARINE CORPS COUNTERINSURGENCY FIELD MANUAL 47 (U.S. Army Field Manual No. 3–24, 2007) [hereinafter U.S. COIN FIELD MANUAL].

[41] *See* Greg Miller & Julian E. Barnes, *Special Drones Pursue Militias,* L.A. TIMES, Sept. 12, 2008, at A1 (discussing the use against extremists in Pakistan of UAVs "equipped with sophisticated new surveillance systems that were instrumental in crippling the insurgency in Iraq"); Odierno, Brooks, & Mastracchio, *supra* note 39*,* at 53 (discussing the successful use in Iraq of a "new ISR model" that involves the allocation and apportionment of full motion video assets that offer ground commanders greater flexibility and accessibility to information); Walter Pincus, *Gadgets That Collect Information Are Also Gathering Success*, WASH. POST, Sept. 15, 2008, at A18 (suburban ed.) ("'ISR' has become the new silver bullet in counterinsurgency.").

The information produced by virtual technologies enters a war-fighting bureaucracy increasingly dominated by the work of large, active, and varied groups of military and civilian lawyers. Laws, rules, and regulations pervade almost every aspect of the modern U.S. military institution and also form an integral part of the complex military social system, essential for its discipline and operations.[42] Consistently with the view of some scholars that war itself has evolved into a legal institution, lawyers have predictably become a common fixture in all of its dimensions.[43] Although lawyers have always participated in the nation's military operations, U.S. military lawyers (and their modern civilian legal counterparts in the Department of Defense) assumed a particularly prominent role in the 1991 Gulf war.[44] Since then, the armed services have embedded lawyers throughout the military establishment, from planning cells to command posts.[45] This practice, which reflects a greater degree of legal review of military activities than ever before, has become routinized and codified in a multitude of regulations, such as a Joint Chiefs of Staff instruction directing that "all operation plans . . . , concept plans, rules of engagement, execute orders, deployment orders, policies, and directives are [to be] reviewed by the command legal adviser to ensure compliance with domestic and international law."[46]

The Kosovo conflict of 1999, a military operation in which NATO relied exclusively on air power, marked an important new stage in the increasing prominence and influence of lawyers in armed conflict. This prominence was both confirmed and sharply criticized by some commentators who argued that "NATO lawyers constrained even the preparation of options for decisive combat" and that in their most extreme alleged actions, NATO's lawyers "became, in effect, [NATO's] tactical commanders."[47] Since the Kosovo conflict, the direct involvement of lawyers in military operations has further expanded, reflecting emerging trends in the legalization of war, the greater complexity of military-civic operations, the rising appreciation by commanders of the utility of legal support in their multidimensional missions, and, as discussed below, the growing use of law as a strategic asset. All these factors have contributed to the forward deployment of lawyers in ever-increasing numbers.[48] The virtual era, however, inaugurated an entirely new type of "forward deployment" for lawyers.

One key aspect of virtual distance from the battlefield is the corresponding proximity of virtual military operations to headquarters. While the pilots of conventional manned aircraft could communicate with their superiors who, in turn, could communicate with senior policy

[42] *See* DAVID KENNEDY, OF WAR AND LAW 33 (2006) (further observing that "[w]arfare has become rule and regulation").

[43] *Id.* at 13–45.

[44] *See* U.S. DEP'T OF DEFENSE, CONDUCT OF THE PERSIAN GULF WAR: FINAL REPORT TO CONGRESS 607 n.31 (1992) (noting that lawyers provided advice on legal issues at every level of command in all phases of Operations Desert Shield and Desert Storm); Charles J. Dunlap Jr., Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts 16 (Nov. 19, 2001) (paper presented at Harvard University, Humanitarian Challenges in Military Intervention Workshop), *available at* http://www.hks.harvard.edu/cchrp/Web%20Working%20Papers/Use%20of%20Force/Dunlap2001.pdf.

[45] Dunlap, *supra* note 44, at 16.

[46] Chairman, Joint Chiefs of Staff Instruction (CJCSI) 5810.01A, Implementation of the DoD Law of War Program, para. 6(c)(5) (Aug. 27, 1999).

[47] Richard K. Betts, *Compromised Command; Inside NATO's First War*, FOREIGN AFF., July/Aug. 2001, at 126, 130.

[48] During the 1991 Gulf war, the U.S. Army alone deployed more than two hundred lawyers in the theater of operation, a significantly higher per capita deployment than in either the Vietnam War or World War II. *See* Steven Keeva, *Lawyers in the War Room*, A.B.A. J., Dec. 1991, at 52, 54.

officials and lawyers, the crew operating a UAV is much more easily connected with, and thus effectively closer to, headquarters. In this sense, virtual technology is radically advancing an important trend in modern military technology: facilitating "the ability for all levels of authority to scrutinize and to involve themselves in the battle itself."[49]

The improved access to higher-level policy scrutiny afforded by virtual technologies may be complemented by additional time for the consideration of targets (because of the comparatively longer time that UAVs may loiter over targets) and the greater possibility of meaningful legal reviews at all levels of authority. Where now is the lawyer's client? The distant, relatively inaccessible cockpit of conventional, manned attack aircraft has given way to a trailer or compartment in a less restrictive, virtual environment at a secure U.S. military or intelligence facility linked to lawyers throughout the command structure. This situation probably puts a lawyer advising on targeting decisions in a considerably better position to provide meaningful and timely counsel. Incidents such as the aborted 2001 UAV attack on Mullah Omar vividly illustrate the expanding and sometimes controversial contours of legal oversight made possible by virtual technologies. Some senior officials in the Bush administration are said later to have strongly criticized the handling of the UAV attack on Mullah Omar and the role that lawyers played in the effort.[50] Notwithstanding the frustrations that individual military and civilian officials may express at the increasingly direct role that lawyers play in U.S. military operations, virtual technology is likely to continue to ensure the closer involvement of lawyers in the planning and execution of many attacks.

The emerging, unintended consequences of the ubiquitous information generated by the new virtual surveillance capabilities are momentous for both military commanders and their lawyers. Lawyers in military and government bureaucracies can be expected to perceive that persons may be held accountable for the knowledge imparted by new types and quantities of information and to be concerned about the standards governing its use. From these truths the lawyer may see, before others do, that the ubiquitous information flowing from persistent surveillance brings with it new expectations, together with unprecedented levels of transparency. As lawyers contemplate how to discharge their duties properly and fulfill their own due diligence requirements (particularly when advising on targeting decisions), the availability of new types of information can change the meaning of what constitutes an appropriate legal review. In place of the limited, sporadic information issued by satellites and manned aircraft, virtual technologies can supply lawyers and planners with data that encompass all visible activities around a target on a continuous basis. The same "unblinking eye" that enables persistent surveillance of a target long before an attack can thus capture, albeit not as its intended purpose, the presence at that site of civilians that would be endangered by any planned attack.

[49] Scott A. Cooper, *The Politics of Airstrikes: Why Generals Distrust Politicians, and Vice Versa*, POL'Y REV., June/July 2001, at 55, 58.

[50] Hersh, *supra* note 2, at 40 (reporting that "[d]ays afterward, top Administration officials were still seething about the incident" and that the failure left Defense Secretary Donald H. Rumsfeld "kicking a lot of glass and breaking doors"). Although Secretary Rumsfeld would later deny that lawyers were responsible for the aborted attack, he soon coincidentally tried without success to impose a significant reduction in the number of lawyers in uniform. *See* MICHAEL BYERS, WAR LAW 121 (2005); David Rennie, *Bush Orders Shoot to Kill on Terrorists; CIA Is Given Secret List of 24 Enemy Targets*, DAILY TELEGRAPH (London), Dec. 16, 2002, at 1. This action was consistent, however, with one of Secretary Rumsfeld's previously expounded rules of life and good government: "Reduce the number of lawyers. They are like beavers—they get in the middle of the stream and dam it up." Donald Rumsfeld, *Manager's Journal: Rumsfeld's Rules,* WALL ST. J., Jan. 29, 2001, at A26.

While the content of new virtually provided information has important ramifications, the possible *presence* of such data also has profound and unintended consequences. These consequences extend to activities before, during, and after an attack. The availability of more relevant information entails new responsibilities for obtaining and properly using it in planning an attack. Furthermore, although lawyers and others involved in reviewing or planning attacks might once have accepted many limits on their ability to access potentially relevant data, the network-centric intelligence systems spawned by new virtual operational requirements will presumably raise not only the accessibility of such data, but also the expectation of receiving it throughout the military structure. Prior to authorizing an attack, lawyers, planners, and commanders nowadays must consider the unprecedented new video record that may be created, especially if an attack risks harm to civilians and is likely to be scrutinized later. During the operation, the possibility that an attack may need to be suspended because of changes in the attack scenario (including the sudden detection of civilians at or near the target) will be dramatically increased by the same virtual surveillance that makes the attack itself possible. Pilots and aircrews are not immune from concerns in this area, since their actions may be recorded by the same intelligence assets used to facilitate their targeting.[51]

After an attack, virtual technologies are making many military operations more transparent by radically expanding a process that began in earnest during the 1991 Gulf war when U.S. officials first showed video footage of attacks from the bomb cameras on PGMs. Since only a small fraction of the bombs used in the Gulf war were actually PGMs, the selected bomb-camera video footage was shown at Defense Department briefings for demonstration and publicity purposes. This situation started to change in 1999 during the NATO confrontation with Serbia over Kosovo, as American officials struggled to explain the basis for specific controversial attacks and to account for collateral bomb damage. Facing intense criticism by human rights groups and the Serbian government, U.S. and NATO officials attempted to rebut allegations of misconduct by any means available, which led them to apply existing technological capabilities in unintended ways by systematically using bomb-camera videos to support their counterarguments.[52]

At international briefings since the Kosovo conflict, U.S. officials have increasingly displayed videos and other imagery to document their version of attacks, alleged enemy actions, and various other incidents. For example, U.S. officials recently used videos to help make their case with respect to an alleged Iranian provocation of a U.S. warship in the Straits of Hormuz, the alleged presence of North Korean workers at a reportedly nuclear facility in Syria, and the accidental shooting of twelve Pakistani soldiers allegedly mistaken for Taliban militants in the

[51] For pilots and aircrews, virtually provided surveillance may add immeasurably to the underappreciated burdens of accountability that were introduced by PGM bomb-camera videos. *See* Cooper, *supra* note 49, at 58–59 (quoting the commander of U.S. Air Forces in Europe during the Kosovo conflict: "Here we put this young man in this situation where he knows that this bomb is enroute to the target, and the videotape that is recording in the cockpit is running, that an hour after he leaves that tape is going to be graded by the Commander of the United States Air Forces in Europe, the Supreme Allied Commander Europe, and probably the President of the United States.").

[52] During the Kosovo conflict U.S. officials ultimately became so focused on the need for effective public relations and accountability measures that, for the first time in any armed conflict, an active archive of MPEG image files was established and made available on the Internet; it contained bomb-camera videos of NATO air strikes, organized chronologically by specific target designations. The video record remains online. *See* NATO's Role in Kosovo: Video, *at* http://www.nato.int/kosovo/video.htm.

mountainous region near the Afghan border (as recorded by a UAV flying overhead).[53] The introduction of virtual surveillance capabilities dramatically increases the pressure on states to deploy information to rebut accusations of misconduct on the part of their military forces. By failing to come forward with information to support its account of events, a government with such capabilities is more likely than ever to face criticism and inspire doubts about its claims, whether or not such information actually exists. This new level of expected transparency for military operations was embodied in requests by news organizations to the U.S. Air Force for UAV-generated video coverage of various attacks involving U.S. forces in Iraq; these requests were granted and resulted in the posting on Internet news sites of portions of the requested footage.[54]

The effects of these rising public expectations and greater levels of transparency are unfolding as the new virtual surveillance systems are being widely deployed for the first time in history. While this process continues, lawyers, attack planners, and military commanders are grappling with their new responsibilities. One measure of these developments that also reflects how the war-fighting bureaucracy of a powerful state like the United States comes to terms with the grim prospect of civilian deaths, political pressures, legal constraints, and the ever-increasing scrutiny of a legalized and humanized international society is a set of documents referred to as "Rules of Engagement."[55] It is here that key policy, legal, and operational interests are balanced and many important targeting restrictions are established.[56] Lawyers already play a prominent part in the development of these rules,[57] but the increasing transparency of military operations made possible by virtual technologies and the likelihood that more military operations will ultimately have to be explained and defended will further elevate their role and the level of scrutiny they may apply. Even now, lawyers, in advising attack planners, often take a broad view of potential humanitarian considerations and propose restraints on operations that go far beyond more permissive rules of engagement.[58] These restrictions have sometimes constrained U.S. forces in ways that enemy action could not have done, particularly when public opinion has been a crucial factor.[59]

[53] Sheryl Gay Stolberg & Thom Shanker, *Bush Castigates Iran, Calling Naval Confrontation 'Provocative Act,'* N.Y. TIMES, Jan. 9, 2008, at A10; David Sanger, *Video Links North Koreans to Syria Reactor*, *U.S. Says*, N.Y. TIMES, Apr. 24, 2008, at A14; Jane Perlez, *Pakistani Fury over Airstrikes Imperils Training*, N.Y. TIMES, June 18, 2008, at A5.

[54] The U.S. Air Force released ten UAV video clips in response to requests from various television networks and CNN displayed portions of the clips. *See New Videos Show Predators at Work in Iraq,* CNN.COM (Feb. 9, 2005), *at* http://www.cnn.com/2005/WORLD/meast/02/08/predator.video/index.html.

[55] *See* U.S. DEP'T OF DEFENSE, DICTIONARY OF MILITARY AND ASSOCIATED TERMS (Joint Staff Pub. 1-02, as amended through Mar. 17, 2009) (defining rules of engagement as "[d]irectives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered").

[56] MATTHEW C. WAXMAN, INTERNATIONAL LAW AND THE POLITICS OF URBAN AIR OPERATIONS 31–32 (Rand, 2000).

[57] Dunlap, *supra* note 44, at 16.

[58] *See* KENNEDY, *supra* note 42, at 105 ("In some instances, the modern military's own internal rules of engagement are stricter than what traditional law in war requires. In the last years, moreover, we have seen military professionals among those most disturbed by the Bush administration's efforts to shrink or skirt humanitarian standards in their war on terror.").

[59] *See, e.g.*, WESLEY K. CLARK, WAGING MODERN WAR 444 (2001) (noting that restrictive rules of engagement in the 1999 Kosovo conflict meant that "[t]he weight of public opinion was doing to us what the Serb air defense system had failed to do: limit our strikes"); MICHAEL R. GORDON & BERNARD E. TRAINOR, THE GENERALS' WAR 326 (1994) (noting that in the aftermath of the controversial bombing of the Al Firdos bunker in the 1991

Aside from parts of rules of engagement that may be classified, their publicly available contents over the last several years serve as a barometer of progressively rising constraints on U.S. military operations imposed by social, political, diplomatic, and legal pressures.[60] Virtual technologies are both enlarging the role of lawyers and accelerating a process in which restrictive interpretations of the law of war may be becoming the *minimum* acceptable standard in the rules for attacks that risk civilian damage and injury. The capability provided by virtual technology to strike more targets and perform more missions thus comes at an unexpected and, for some military leaders, highly problematic cost: some of the most restrictive air-strike protocols and rules of engagement of all time.[61] These developments are also fundamentally linked to the contribution that the informational capabilities of virtual technologies are making to the contemporary concept of what constitutes victory in modern counterinsurgency operations.

Mission changes: redefining victory. The informational capabilities and new levels of transparency generated by virtual technologies operate in an international community that views international law as increasingly relevant to armed conflicts and civilian casualties as increasingly unacceptable. In this environment, virtual weapons systems can be seen as one reason for redefining victory in war. This new definition can be summed up in the simple formula now found in the latest version of the *U.S. Army-Marine Corps Counterinsurgency Field Manual*: "Lose Moral Legitimacy, Lose the War."[62]

Recent conflicts have continued to demonstrate to U.S. military and political leaders how allies and coalitions can be highly sensitive to perceived law-of-war and human rights violations and how such violations can undermine legitimacy, adversely affecting the "soft power" on which the leadership of many international cooperative activities depends.[63] Shocking images of the mistreatment of detainees at Abu Ghraib by U.S. military personnel preceded major changes in official COIN policies years, sadly, after the U.S. invasion of Iraq and only after much damage had been done.[64] These new policies state, for example, that the "[a]buse of detained persons is immoral, illegal, and unprofessional" and, citing the French experience in Algeria, conclude that the official condoning of torture leads to a loss of moral legitimacy.[65]

Gulf war, the air force concluded that "the political fallout from the Al Firdos raid had accomplished what the Iraqi air defenses could not: downtown Baghdad was to be attacked sparingly, if at all").

[60] WAXMAN, *supra* note 56, at 31.

[61] Mark Benjamin, *When Is an Accidental Civilian Death Not an Accident?* SALON.COM, July 30, 2007 (quoting a NATO spokesman on the adoption of a highly restrictive "zero tolerance" policy on civilian casualties in preplanned strikes in Afghanistan). Unfortunately, because of the subsequent resurgence of the Taliban in 2008, NATO greatly increased the use of air strikes in Afghanistan, reversing a trend in which civilian casualties had been declining and predictably endangering support for the NATO presence there. *See* Carlotta Gall, *Afghan President Assails U.S.-Led Airstrike That He Says Killed 95,* N.Y. TIMES, Aug. 24, 2008, at A6. These developments have contributed to a dramatic increase in the NATO forces' demand for UAVs and critical UAV surveillance capabilities. *See* David Ignatius, *What a Surge Can't Solve in Afghanistan*, WASH. POST, Sept. 28, 2008, at B7 (noting that Secretary of Defense Robert Gates has pushed for a major increase in ISR assets in Afghanistan); Anna Mulrine, *Drones Fill the Troops Gap in Afghanistan,* U.S. NEWS & WORLD REP., Sept. 25, 2008, at 30.

[62] U.S. COIN FIELD MANUAL, *supra* note 40, at 252.

[63] Richard B. Bilder & Detlev F. Vagts, *Speaking Law to Power: Lawyers and Torture*, 98 AJIL 689, 695 (2004) ("Unless U.S. foreign policy and actions in the 'war on terror' are seen by its own citizens and other nations as legitimate and in compliance with broadly accepted legal and moral standards, they may fail to gain domestic and international support.").

[64] *Id.*

[65] U.S. COIN FIELD MANUAL, *supra* note 40, at 251–52. U.S. counterinsurgency doctrine now emphasizes that international legal standards, including those found in common Article 3 of the Geneva Conventions, are applicable to the treatment of all detainees. *Id.* at 352. The manual further observes that by condoning torture in the Algerian

Because of similar concerns about the effects of images of dead and wounded civilians, U.S. forces fighting in Iraq also waged their own aggressive "information war" regarding alleged law-of-war violations; in some cases these concerns even dictated the targets of U.S. military operations.[66]

Incidental civilian casualties caused by U.S. attacks threaten the legitimacy of these military operations on a fundamental level, especially when humanitarian motives are invoked as a basis for U.S. intervention. By making such casualties more avoidable and thus even less politically acceptable, virtual technologies are helping to redefine success in warfare by underpinning U.S. policies that increasingly restrict the use of air strikes in COIN operations whenever civilian lives are threatened. Such policies underlie a new official "mind-set" about proportionality that "goes beyond the adherence to the rules of engagement."[67] While air strikes may be useful and permitted by the rules of engagement, the U.S. military establishment has been forced to recognize that an attack causing incidental harm to civilians potentially "turns people against the host-nation (HN) government and provides insurgents with a major propaganda victory."[68] Fortunately, the ISR capabilities that have dramatically improved the surveillance of targets for the purpose of air strikes have also made it possible to conduct new types of ground operations—resembling the maneuvers of special operations forces—that result in fewer overall casualties and more effective action against important insurgent or terrorist leaders.[69] In addition, the effectiveness of such operations, in contrast to air strikes that may cause much more extensive civilian casualties, helps explain recent changes in official U.S. COIN doctrine cautioning against the use of aerial bombing in many situations.[70]

While the law of war has always been accorded respect by U.S. military commanders and has long been incorporated into U.S. military training and doctrine,[71] it has assumed even greater importance in modern conflicts involving terrorists, insurgents, and other militant groups, even if those groups choose to ignore laws and humanitarian principles and instead focus on provoking their enemies and hiding among civilians. U.S. COIN doctrine now

conflict, France "degraded the ethical climate throughout the French Army," made the French "extremely vulnerable to enemy propaganda," and contributed to the ultimate French defeat. *Id.* at 252.

[66] Richard A. Oppel Jr. & Robert F. Worth, *G.I.'s Open Attack to Take Falluja from Iraq Rebels,* N.Y. TIMES, Nov. 8, 2004, at A1 ("This time around, the American military intends to fight its own information war, countering or squelching what has been one of the insurgents' most potent weapons."). In their attempt to reclaim the city of Fallujah, U.S. forces put priority on securing the main hospital because it had become "the source of rumors about heavy casualties." *Id.*

[67] U.S. COIN FIELD MANUAL, *supra* note 40, at 249 ("Fires that cause unnecessary harm or death to noncombatants may create more resistance and increase the insurgency's appeal— especially if the populace perceives a lack of discrimination in their use."); *see also* Adam B. Ellick, *Tensions Rise As Afghans Say U.S. Raid Kills Civilians*, N.Y. TIMES, Dec. 19, 2008, at A26.

[68] U.S. COIN FIELD MANUAL, *supra* note 40, at 364.

[69] *See, e.g.*, Odierno, Brooks, & Mastracchio, *supra* note 39, at 51 (discussing these new capabilities of conventional units in Iraq made possible by the sudden increase in ISR assets and the delegation down to brigade combat teams of the analysis and exploitation of those assets).

[70] U.S. COIN FIELD MANUAL, *supra* note 40, at 364–65 (listing numerous conditions and noting that "[e]ven when justified under the law of war, bombings that result in civilian casualties can bring media coverage that works to the insurgents' benefit").

[71] *See* W. Hays Parks, *Teaching the Law of War,* ARMY LAW, June 1987, at 4, 5 (noting the positive role that the law of war can play in maintaining discipline and efficiently employing U.S. forces, and how violations may increase enemy resistance and have other negative effects on the accomplishment of missions). Defense Department policy thus provides that "[m]embers of the DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations." U.S. Dep't of Defense, DoD Law of War Program, DoD Directive 2311.01E, §4.1 (May 9, 2006).

emphasizes that legitimacy and the law of war play an essential role in these conflicts and that "[b]oth insurgents and counterinsurgents are fighting for the support of the populace."[72] Acknowledging that U.S. operations will be measured against applicable international legal standards, U.S. COIN doctrine provides new opportunities for international law to serve as a basis for U.S. forces to engage with the civilian population.[73] The new relevance of international law has not been lost on terrorist groups and rogue states, even if they do not observe it: such groups and governments use new informational technologies to exploit images of dead civilians and other evidence of alleged law-of-war violations as part of a growing practice that some describe as "lawfare."[74]

Although most military theorists once viewed law as largely irrelevant to war, the political and moral legitimacy of military operations is increasingly linked to the observance of legal obligations, particularly those related to protection of the civilian population.[75] The United States has, sometimes inadvertently, had a hand in these developments. During the 1991 Gulf war, U.S. military forces used international law as a "strategic asset," conspicuously describing actions and objectives in legal terms and seeking to endow operations with the legitimacy of international law.[76] Multinational coalitions, viewed as conferring their own legitimacy on U.S. actions, were built on this basis as well.[77] American officials have learned that the single most important indicator of compliance with the law of war is the perceived respect for rules protecting the civilian population.[78] In post-9/11 conflicts, minimizing civilian casualties remains of great concern to any U.S. officials who want to maintain international coalitions against terrorists and other enemies.

Virtual military technologies have been instrumental in making international law relevant to armed conflicts, in part by bringing new levels of transparency to questions about the legitimacy of military operations and related notions of what constitutes victory in war. In addition,

[72] U.S. COIN FIELD MANUAL, *supra* note 40, at 52.

[73] While COIN doctrine encourages U.S. forces to make clear that they "do not intend to undermine or change the local religion or traditions," they nonetheless must find a legitimate basis for reducing "the effects of dysfunctional social practices that affect the ability to conduct effective security operations." *Id.* at 219.

[74] Dunlap, *supra* note 44, at 4. Dunlap argues that as U.S. military operations have come to depend on the legitimacy that may be provided by law, adversaries increasingly see this development "as a vulnerability to be exploited." *Id.* at 9–10; *see also* CLARK, *supra* note 59, at 443, 8 (noting that Serbian agents in the Kosovo conflict skillfully publicized apparent NATO law-of-war violations and that "new technologies impacted powerfully at the political levels. The instantaneous flow of news and especially imagery could overwhelm the ability of governments to explain, investigate, coordinate, and confirm.").

[75] *See, e.g.,* CARL VON CLAUSEWITZ, ON WAR 13 (Michael Howard & Peter Paret eds. & trans., Oxford 1976) (1832) ("Attached to force are certain self-imposed, imperceptible limitations hardly worth mentioning, known as international law and custom, but they scarcely weaken it."). International law has since become so interwoven into the fabric of international politics that it would probably impress many of its detractors of earlier eras: it is now, at a minimum, the type of *political* constraint that even Clausewitz would have respected. *Id.* at 252 (noting that "war is only a branch of political activity" and that "it is in no sense autonomous").

[76] *See* Normand & Jochnick, *supra* note 26, at 393–99; *see also* KENNEDY, *supra* note 42, at 8 (describing how the "humanist vocabulary of international law" has been "mobilized by the military as a strategic asset").

[77] One of the important lessons of the 1991 Gulf war was that the perceived compliance of U.S. military operations with the law of war was a key factor in persuading states to join and remain in the U.S.-led coalition. *See* BYERS, *supra* note 50, at 119–20; MICHAEL IGNATIEFF, VIRTUAL WAR 205 (Picador 2001) (2000) (observing that "[t]he legitimacy of [U.S.] military operations overseas depends on persuading other states to join as coalition partners" and that "coalition warfare is increasingly seen as the future of war").

[78] *See, e.g.*, CLARK, *supra* note 59, at 434 (describing the need of NATO forces in the 1999 Kosovo conflict to minimize, if not eliminate, civilian casualties as "the most pressing drumbeat of the campaign" and observing that "each incident of accidental harm to civilians sent shock waves up and down through NATO").

some weapons have themselves come to be viewed as conveying a certain type of legitimacy. Since virtual weapons systems are among the most prominent of the high-tech weapons now deployed by U.S. military forces, they are linked to a battle for "high-tech legitimacy" that was launched in an intensive U.S. public relations campaign in the 1991 Gulf war. Public statements by coalition officials during that war were often accompanied by the repetitive airing of selected bomb-camera videos, which gave the impression of the dawning of a new era of technologically enabled compliance with the law of war and avoidance of civilian casualties.[79] The authorities consistently stressed that high-tech weapons and precision air strikes enabled coalition forces to spare Iraqi civilians from the effects of war as much as possible.[80]

Years of viewing wars through selected images of PGMs hitting their intended targets have resulted in demands by both the American and the international publics for increasingly lower levels of civilian injuries.[81] The improved targeting capabilities afforded by virtual technologies promise to add to these expectations. Furthermore, the enhanced accuracy associated with even more advanced high-tech weapons will make it that much harder in the new virtual courtroom of public opinion to portray errant bombs and resulting civilian casualties as accidents.[82] Boasting about technological achievements has exposed the U.S. military to calls for compliance with ever-higher standards.[83] After the 1991 Gulf war, some Air Force officials admitted that by "overselling" its high-tech capabilities, the service had "unwittingly made itself vulnerable" to enemy strategies portraying U.S. forces as "insensitive to [the law of armed conflict] and human rights."[84] It is too late, however, for the United States to turn back. By portraying its high-tech weapons in the 1991 Gulf war and afterward as broadly serving humanitarian and international legal purposes and by intentionally using these weapons in the battle for legitimacy, the United States has imposed a burden on its virtual weapons systems. In addition to these high-tech expectations, virtual weapons systems bring with them a new level of transparency and control that makes it much easier to determine if a state is sincere in its efforts to achieve such legitimacy and comply with legal norms. With these innovations, they are also bringing new meaning to the legal norms themselves.

III. THE LAW OF VIRTUAL WAR

The Existing Legal Framework

Drawing heavily on conventions and customary international law dating to the nineteenth century, the modern law of war governing the conduct of military forces in armed conflicts (the

[79] Normand & Jochnick, *supra* note 26, at 393 ("Most politicians and commentators welcomed what they saw as a new paradigm in war and in law, conjuring visions of a global army using the latest military technology in the service of international law and justice.") (footnote omitted).

[80] *Id.* at 394; *see also* U.S. DEP'T OF DEFENSE, CONDUCT OF THE PERSIAN GULF CONFLICT: AN INTERIM REPORT TO CONGRESS 12-2, 12-3 (1991) (stating that coalition forces had "scrupulously adhered to . . . fundamental law of war proscriptions" in conducting "the most discriminate military campaign in history").

[81] WAXMAN, *supra* note 56, at 57–59.

[82] *Id.* at 59; Editorial, *How Precise Is Our Bombing?* N.Y. TIMES, Mar. 31, 2003, at A12 (noting that "the incessant boasting about the surgical accuracy of the attacks . . . raises expectations that every bomb will hit its target—and outrage around the world when one doesn't").

[83] KENNEDY, *supra* note 42, at 8 ("[H]ow should the U.S. military itself react to the escalating public demand that it wage war without collateral damage—or to the tendency to hold the military to an ever higher standard as its technological capabilities increase?").

[84] Dunlap, *supra* note 44, at 12–13.

jus in bello) is built on a set of general principles that give rise to specific prohibitions and requirements. These general principles hold that (1) states are limited in the means they may choose to conduct warfare;[85] (2) humanity at all times prohibits the infliction of unnecessary suffering;[86] (3) acts of violence and destruction superfluous to military necessity are prohibited;[87] and (4) the parties to an armed conflict must distinguish between the civilian population and combatants and between civilian and military objectives.[88] From these key general principles—limited permissible means of warfare, humanity, necessity, and distinction—flow additional principles and various specific rules and obligations.

Because key principles of the law of war proved to be highly elastic in their application and interpretation by states involved in armed conflicts during most of the twentieth century, an additional protocol to the four Geneva Conventions of 1949 was concluded in 1977 (Protocol I) that was designed to supplement, update, and formalize legal restraints on the means and methods of warfare to ensure more effective protection of the civilian population in international armed conflicts.[89] Although the United States is not a party to Protocol I, it accepts many of its most important provisions as binding obligations under customary international law.[90]

While the multilateral effort to draft Protocol I did not proceed without controversy, it did produce important clarifications and refinements of key law-of-war principles and specific rules relating to protection of the civilian population. First, before one can comply with the fundamental requirement of distinction and thus protect civilians and civilian objects from

[85] Hague Convention (IV) Respecting the Laws and Customs of War on Land, Art. 22, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague IV].

[86] Humanity was recognized as a fundamental principle of the law of war at the earliest stages of its development. *See* St. Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29/Dec. 11, 1868, 1 AJIL Supp. 95, 95 (1907) (declaring that the employment of arms that uselessly aggravate the sufferings of disabled men would be "contrary to the laws of humanity") [hereinafter St. Petersburg Declaration]. The application of the principle of humanity was extended and reaffirmed in the Hague Conventions of 1899 and 1907, to which the United States is a party (the 1907 Hague Regulations, annexed to Hague IV, *supra* note 85, remain among the most authoritative sources of law for the United States in its conduct of military operations).

[87] Regulations governing the U.S. Armed Forces recognize that the conduct of hostilities must be carried on within the limits of international law, including restraints imposed by the principles of humanity and military necessity, as well as distinction and proportionality. *See, e.g.*, U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, ch. 5 (NWP 1-14M, MCWP 5-12.1, COMDTPUB 5800.7A, 2007) [hereinafter NAVY COMMANDER'S HANDBOOK], *available at* http://www.usnwc.edu/cnws/ild/documents/1-14M_(July_2007)_(NWP).pdf; U.S. DEP'T OF THE AIR FORCE, TARGETING, app. A, at 88–90 (A.F. Doctrine Doc. 2-1.9, June 8, 2006); U.S. DEP'T OF THE ARMY, THE LAW OF LAND WARFARE, paras. 3(a), 41 (Field Manual 27-10, 1956).

[88] The principle of distinction is fundamental to the law of war and is accepted by the United States as a binding obligation under customary international law. *See* William H. Taft IV, *The Law of Armed Conflict After 9/11: Some Salient Features,* 28 YALE J. INT'L L. 319, 323 (2003) (describing distinction as a "bedrock" principle of the law of armed conflict).

[89] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, *opened for signature* Dec. 12, 1977, 1125 UNTS, *reprinted in* 16 ILM 1391 (1977) [hereinafter Protocol I].

[90] Michael J. Matheson [then deputy legal adviser of the U.S. Department of State], Remarks, *in Sixth Annual American Red Cross–Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 423, 426 (1987). Various key provisions of Protocol I are repeated verbatim or in substantially similar terms in regulations and manuals that govern the operations of each of the five services comprised by the U.S. Armed Forces.

hostilities, one must know who and what may be attacked. Thus, the initial rule regarding attacks is that the intended target must be a military objective and that civilians may never be intentionally targeted (sometimes referred to as the principle of discrimination).[91] Second, once a military objective is identified as the target, the attack may nevertheless be illegal if excessive collateral damage affecting civilians or civilian objects can be expected (the principle of proportionality).[92] Third, even when attacking a lawful target, one must take various additional "precautionary measures" to ensure adherence to proportionality requirements.[93]

Early multilateral attempts to insert proportionality into international armed conflicts offered little more than conceptual proclamations that war should be centered on an enemy state's military forces.[94] The radical reversal, however, in the relative number of civilian to military casualties in World War II served as an impetus for codifying proportionality and related precautionary measures as legal requisites of the *jus in bello*.[95] The resulting and most widely accepted definition of proportionality, set forth in Protocol I, prohibits a disproportionate attack by categorizing it as a special case of indiscrimination. Under this provision, states are prohibited from undertaking "[any] attack 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."[96]

At its core, however, the principle of proportionality still envisions that civilians may be harmed in the course of attacks against legitimate military objectives. Thus, in spite of modern human rights norms and its own humanitarian origins, the law of war does not categorically prohibit states from harming civilians. Furthermore, the indeterminacy of the principle of proportionality and underlying terms such as "excessive" has given military forces considerable discretion in conducting attacks. In practice, the proportionality principle has not protected civilian populations during many armed conflicts spanning the modern era of the law of war. Since that law was created with the participation of the most powerful states and has historically been interpreted by those states as a relatively permissive framework, it is not surprising that the application of the proportionality principle and related rules protecting civilians from hostilities has often been ineffective.[97]

Yet the proportionality principle is by no means a fiction; nor do states enjoy unfettered discretion in its implementation, particularly since it was codified in Protocol I in 1977. While in many contexts (such as the field of arms control) the indeterminacy of a legal provision doubtless undermines its legitimacy and invites unlawful behavior, proportionality has a rich history as a recognized principle of international law applied in many different areas; through this frequent application, it can be argued that proportionality has in fact "shed much of its

[91] Protocol I, *supra* note 89, Art. 48. This principle goes beyond prohibiting attacks against purely civilian targets; it also prohibits attacks that "are of a nature to strike military objectives and civilians or civilian objects without distinction." *Id.*, Art. 51(4).

[92] Articles 51(5)(b) and 57 of Protocol I, *supra* note 89, summarize the principle of proportionality, although the term itself does not appear; instead, the word "excessive" is used in relation to civilian casualties.

[93] *Id.*, ch. IV.

[94] *See, e.g.*, St. Petersburg Declaration, *supra* note 86 (providing that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy").

[95] Thomas M. Franck, *On Proportionality of Countermeasures in International Law,* 102 AJIL 715, 724 (2008).

[96] Protocol I, *supra* note 89, Art. 51(5)(b).

[97] *See* BYERS, *supra* note 50, at 153 (arguing that "[p]owerful countries have always shaped the international system to their advantage," including key international legal rules and concepts relating to the use of force).

indeterminacy" and for this reason has often played an important role in modulating various types of conflict between states.[98] Many variables may explain the widespread usage and continuing "compliance pull" of the proportionality principle, but key factors include the extent to which it has become an integral part of the thinking and conduct of states, the corresponding powerful influence it exerts on both judicial and political bodies, and its hold on the "imagination of the epistemic community in which it is used as the prism for viewing, arguing, and ultimately resolving disputes."[99] Virtual technologies and the new transparency they bring to military operations are dramatically strengthening this hold in the area of armed conflict by creating unprecedented opportunities for debating and applying the proportionality principle to the real world of attacks. As these technologies transform modern military operations and institutions, they are bringing new life and unheard-of traction to proportionality, reshaping the related duty to take precautionary measures, removing key factors that have been used by states to excuse noncompliance, and altering fundamental conditions that have previously limited the observance of key *jus in bello* obligations.

Virtual Distance: Giving Proportionality Traction

The obligation to refrain from disproportionate attacks often forces military commanders to make difficult decisions, to weigh the value of innocent human lives in relation to the capture or destruction of a particular military objective. While the proportionality test is unquestionably applicable to modern military operations—and failure by a commander to comply with obligations derived from proportionality can constitute a war crime[100]—the test is much easier to formulate in principle than to apply to a complex or uncertain set of circumstances. As a result, military commanders and states have enjoyed a great deal of discretion in making these evaluations. However, various aspects of the distance of virtual technologies from the battlefield dramatically change factors that previously were critical to such evaluations. This new "virtual" distance is giving proportionality requirements new significance by eliminating some of the key excuses that states have long used to escape responsibility for attacks that appear to cause excessive civilian casualties.

Risk. In examining and reviewing charges that NATO attacks on targets during the 1999 Kosovo conflict were unlawful, a committee established for that purpose within the Office of the Prosecutor for the International Criminal Tribunal for the Former Yugoslavia (ICTY Committee)[101] concluded that once it is decided that the proportionality principle applies, certain key questions must be resolved. These questions include the relative values to be assigned to the military advantage to be gained and the possible injury to noncombatants

[98] Franck, *supra* note 95, at 718.

[99] *Id.* at 717.

[100] *See, e.g.*, Rome Statute of the International Criminal Court, Art. 8(2)(b)(iv), July 17, 1998, 2187 UNTS 3. The necessary *mens rea* element for such an offense is "knowledge," which "means awareness that a circumstance exists or a consequence will occur in the ordinary course of events." *Id.*, Art. 30(3). The required *mens rea* need not be an intent to harm civilians but, instead, can be satisfied by a "reckless disregard" of such consequences. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 117 (2004).

[101] ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (June 8, 2000), *reprinted in* 39 ILM 1257 (2000) [hereinafter ICTY Report].

and/or the damage to civilian objects; the information to be included or excluded in totaling sums; and the "standard of measurement in time or space."[102] As difficult as these first three questions are, the committee added an important fourth one: "To what extent is a military commander obligated to expose his own forces to danger in order to limit civilian casualties or damage to civilian objects?"[103] In the context of conventional manned aircraft, exposure is often linked to the altitude at which aircraft must fly to launch attacks safely and avoid hostile ground fire.

To what extent a military commander should expose his forces to danger to minimize collateral damage is likely to be seen much differently by a military officer responsible for the well-being of his troops than by a human rights expert working at a nongovernmental organization. For example, human rights groups criticized the U.S. high-altitude bombing of Iraqi targets in the 1991Gulf war as having diminished bombing accuracy and unnecessarily endangering civilians.[104] The U.S. Defense Department, however, maintained that coalition forces had taken many steps to "provide the greatest possible accuracy and the least risk to civilian objects and the civilian population"—but explained that it had taken only those measures that could be implemented "[t]o the degree possible and consistent with *allowable risk* to aircraft and aircrews."[105]

The issue of the greater risks that high-altitude bombing may pose to civilians arose again during the Kosovo conflict when human rights groups complained that NATO gave priority to protecting its pilots rather than civilians.[106] In addressing these charges, the ICTY Committee noted that "NATO air commanders have a duty to take practicable measures to distinguish military objectives from civilians or civilian objectives," but nonetheless found that there was "nothing inherently unlawful about flying above the height which can be reached by enemy air defences."[107] While noting that the fifteen-thousand-foot minimum altitude adopted by NATO for a significant part of its air campaign meant that a target "could not be verified with the naked eye," the committee believed that modern technology allowed NATO to meet its obligation to distinguish "in the vast majority of cases during the bombing campaign."[108] Even though the safety of aircrews remains a compelling objective, such reasoning has enabled states with high-altitude bombing capabilities to avoid a fuller application of proportionality requirements to many of their aerial bombing operations.

One incident investigated by the ICTY Committee and described as "problematic" demonstrates both the continuing problem of distance in conventional air strikes and the potentially transformational effects of virtual distance. On April 14, 1999, NATO aircraft launched an attack on a convoy of vehicles traveling along the Djakovica-Prizren road in Kosovo. While

[102] *Id.*, para. 49.

[103] *Id.*

[104] Middle East Watch further noted that since over 90 percent of the bombs dropped in the Gulf war were "dumb" or unguided bombs, high-altitude bombing clearly increased the risks of civilian casualties, citing as proof the statement to that effect by former undersecretary of defense for research and engineering William J. Perry. MIDDLE EAST WATCH, *supra* note 29, at 116.

[105] *See* U.S. Dep't of Defense, *Report to Congress on the Conduct of the Persian Gulf War—Appendix on the Role of the Law of War* (Apr. 10, 1992), *reprinted in* 31 ILM 612, 622 (1992) (emphasis added).

[106] *See, e.g.,* Amnesty Int'l, *Kosovo: Amnesty International Concerns Relating to NATO Bombings*, AI Index EUR 70/069/1999, May 18, 1999.

[107] ICTY Report, *supra* note 101, para. 56.

[108] *Id.*

some of the details of the Djakovica incident remain unclear and initial accounts were confusing, NATO planes apparently mistook tractors and other civilian vehicles in the convoy for military equipment and struck what turned out to be a group of Kosovar Albanian refugees, killing at least seventy civilians.[109] NATO officials admitted having attacked civilian vehicles but argued that "when viewed with the *naked eye from the attack altitude* they appeared to be military vehicles."[110]

The ICTY Committee repeated that there was "nothing unlawful about operating at a height above Yugoslav air defences" but acknowledged that "it is difficult for any aircrew operating an aircraft flying at several hundred miles an hour and at a substantial height to distinguish between military and civilian vehicles in a convoy."[111] Unable to conclude that the NATO commanders and pilots involved in the Djakovica incident had displayed a degree of recklessness that would sustain war crimes charges, the committee reinforced the centrality of conventional notions of distance and risk to proportionality by conceding that "this incident is one where it appears the aircrews could have benefitted from lower altitude scrutiny of the target at an early stage."[112]

UAVs and other virtual technologies, which were used only on a limited or experimental basis during the Kosovo conflict, now increasingly enable military commanders to eliminate the exposure of aircrews to the risks of low-altitude missions, as well as the exposure of some ground forces to the danger of combat. The elimination of this fundamental tactical problem not only removes a key excuse that has often been used by states to limit the application of the principle of proportionality, but also dramatically affects what is "feasible" under the obligation in Protocol I to "take all feasible precautions in the choice of means and methods of attack."[113]

Environment. A military commander will naturally be concerned about exposing his forces to hostile fire in efforts to avoid civilian casualties during an attack. The immediate, personal concerns of the combat troops themselves may be expressed in such maxims as: "If the enemy is in range, so are you!" Fear of death or injury on the battlefield—as well as stress, anger, and revenge—can clearly cloud a person's judgment in ways detrimental to compliance with law-of-war obligations toward noncombatants.[114] This most fundamental distance problem—proximity to the terrible personal costs and stress of combat—is clearly a critical, limiting environmental factor that virtual technology radically alters: new virtual operating environments

[109] Michael R. Gordon, *Crisis in the Balkans: A NATO Account; NATO Admits Pilot Bombed 2d Convoy on Kosovo Road*, N.Y. TIMES, Apr. 20, 1999, at A12 (responding to Serbian claims that seventy-four civilians were killed in this incident, NATO officials said their pilots, flying at high altitude, had been convinced they were striking only military vehicles).

[110] ICTY Report, *supra* note 101, para. 67 (emphasis added).

[111] *Id.*, para. 69.

[112] *Id.*, para. 70.

[113] Protocol I, *supra* note 89, Art. 57(2)(a)(ii). Human rights groups argued that "inadequate precautions were taken to avoid civilian casualties" by NATO in the Djakovica incident because "higher altitude seems to have impeded a pilot from adequately identifying a target." *See, e.g.,* CIVILIAN DEATHS IN THE NATO AIR CAMPAIGN, 12 HUM. RTS. WATCH, NO. 1(D), Feb. 2000, *available at* http://www.hrw.org/reports/2000/nato/index.htm.

[114] *See, e.g.,* U.S. Army, Office of the Surgeon General, Mental Health Advisory Team IV, Final Report 4 (Nov. 17, 2006), *available at* http://www.armymedicine.army.mil/reports/mhat/mhat_iv/MHAT_IV_Report_17NOV06.pdf (finding, inter alia, that soldiers in Iraq who were angry, stressed, or anxious were more likely to report that they had mistreated noncombatants).

can free both commanders *and* their troops from many of the negative effects that the battlefield may have on attempts to prevent unnecessary harm to civilians.[115]

In addition to emotional and psychological factors, the responsibilities and limitations associated with the combat environment take a toll on the performance of all aspects of missions, including the careful and focused efforts that may be required to prevent disproportionate civilian casualties. One significant environmental factor that virtual technologies have radically altered is the multiple tasks confronting pilots when attacking a target and at the same time attempting to minimize collateral damage. Flying, navigating, targeting, and communicating while evading enemy defenses can be a formidable set of responsibilities, particularly for a single pilot flying aircraft like the F-16 planes involved in the Djakovica incident. This multiplicity of tasks impressed the ICTY Committee as an important factor in mitigating pilot responsibility for the extensive civilian casualties resulting from the attack.[116]

In the relative calm of an air-conditioned room far removed from the threat of enemy attack, the persons responsible for operating a UAV (such as a Predator or a Reaper) are required to perform far fewer tasks than the crew in conventional aircraft, while also benefiting from enhanced sensors to improve their targeting capabilities.[117] Although this virtual technology creates formidable attack capabilities, it also enhances the ability of the pilot and sensor operator(s) to focus on avoiding unnecessary civilian casualties, creating a new and more suitable environment for compliance with proportionality requirements and other law-of-war obligations.

Fatigue is another environmental factor that unquestionably affects the performance of combatants and their ability to comply with law-of-war obligations during attacks. This problem was highlighted in April 2002, when a "friendly fire" attack in Afghanistan by two pilots in the Illinois Air National Guard resulted in the deaths of four Canadian soldiers. Both pilots claimed that their judgment had been impaired by "go pills" containing the stimulant dexamphetamine, which had been prescribed to them by the U.S. Air Force as part of a fatigue management program.[118] While the duties of personnel operating a UAV in a virtual environment undoubtedly require great skill and are said to involve many of the same challenges as conventional operational missions, they do not require aircrews to push the limits of their physical

[115] In addition to eliminating the fear or hysteria that may lead to the taking of excessive measures in self-defense, virtual technologies offer humans in remote locations the opportunity to overcome other factors that might contribute to war crimes and the deaths of noncombatants: command-and-control structures are able to remain more intact; orders may be conveyed more clearly; and human senses augmented by technology may better define the enemy and battle conditions, helping to counter the phenomenon of "scenario fulfillment," i.e., a "distortion or neglect of contradictory information in stressful situations." RONALD C. ARKIN, GOVERNING LETHAL BEHAVIOR: EMBEDDING ETHICS IN A HYBRID DELIBERATIVE/REACTIVE ROBOT ARCHITECTURE 6 (Tech. Rep. GIT-GVU-07-11), *at* http://www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf.

[116] ICTY Report, *supra* note 101, para. 69.

[117] *See* Peter Almond, *Joystick Squadron: It's the RAF's Newest Combat Group: Pilotless Planes Flown from 8,000 Miles Away*, MAIL ON SUNDAY (London), July 6, 2008, at 55 (also noting the observations of British UAV pilots that the "cockpit" of a UAV has "far fewer obvious controls than a manned combat jet and almost none of the expensive electronic defences that protect a manned pilot from missile attack").

[118] Frank Main, *Guard Pilots Blame Drug in Fatal Bombing*, CHI. SUN-TIMES, Jan. 3, 2003, at 7 (further noting that "[t]he Air Force says the use of 'go pill' is voluntary," but quoting one of the pilots' lawyers as saying that "refusal to take uppers or downers is a career-ending decision"); *see also* Bruce Rolfsen, *Sliding Home; A B-1B Arrives with Landing Gear Up*, A.F. TIMES, Oct. 2, 2006.

endurance or to take stimulants to fight off fatigue. For example, British journalists, reporting on a new U.S.-based Royal Air Force squadron that operates unmanned British MQ-9 Reapers over Afghanistan, found the much less fatiguing schedule associated with this virtual environment especially impressive. Noting the reduced stress and healthier routine afforded UAV pilots assigned to this unit, they observed that "[f]lying has come a long way since the experiences of our Battle of Britain heroes."[119]

An incident that dramatically illustrates both the significance of virtual distance and the limiting environmental effects of conventional manned aircraft on efforts to prevent excessive civilian casualties occurred during the Kosovo conflict on April 12, 1999, when a NATO F-15E Strike Eagle launched two missiles at a railway bridge over the Grdilca Gorge in Serbia. Moments before the impact of the first electro-optically guided missile, a passenger train moved onto the bridge. According to the NATO commander, General Wesley Clark, the missile hit the train even though, at the last moment, the person guiding the bomb "caught a flash of movement that came into the screen and it was the train coming in. Unfortunately he couldn't dump the bomb at that point, it was locked . . . ."[120] The aircrew observed that the bridge was not destroyed but, apparently unaware that the disabled train was sitting on it, fired a second missile aimed at the other end of the bridge. Sadly, this missile also hit the train, killing many of the occupants and sparking international outrage. General Clark described the second missile hit as an "uncanny accident" in which the damaged train, obscured by smoke and clouds, had slid forward across the bridge and was again sighted too late to allow the missile to be diverted.[121] In the face of mounting international criticism, NATO released a bomb-camera video to support its version of events.[122]

In its review of another of the incidents it described as "problematic," the ICTY Committee concluded that the Grdilca bridge was a legitimate military objective, that the F-15 aircrew had not deliberately targeted the passenger train, and that the person controlling the bombs was required to target the bridge "over a very short period of time" and had "failed to recognize the arrival of the train while the first bomb was in flight."[123] While the committee members split over the legality of the second bombing, they could not conclude that the second attack displayed the necessary element of recklessness for initiating a war crimes investigation.[124] It can be inferred from their conclusions that the civilian casualties caused by this attack were not excessive and that the firing of the second missile must have involved a serious "human error in the heat of the moment" that was at least partially explained by the circumstances and con-

[119] Almond, *supra* note 117, at 55 (further reporting that "the pilots are free to leave the room mid-flight, get a coffee, do exercise, read a book or maybe phone their wives at their base near Las Vegas. One American pilot is even said to have left his base during a break from his shift to pick up his child from school."). Other observers note, however, that the prolonged "sensory isolation" associated with flying UAVs can sometimes be a source of great fatigue for pilots. *E.g.,* Aaron Retica, *Drone-Pilot Burnout*, N.Y. TIMES, Dec. 14, 2008, at MM55.

[120] NATO's Role in Kosovo, NATO Press Conference (Apr. 13, 1999), *available at* http://www.nato.int/kosovo/press/p990413a.htm (including the display and explanation by General Clark of two bomb-camera videos of the air strike).

[121] *Id.*

[122] This video, in MPEG format, remains posted on the NATO Web site, NATO's Role in Kosovo, Videos, Railway Bridge I & II (Apr. 13, 1999), *at* http://www.nato.int/kosovo/video.htm.

[123] ICTY Report, *supra* note 101, para. 62.

[124] *Id.*, para. 70.

ditions faced by the aircrew.[125] Among the conditions the committee appears to have considered significant were the limitations, discussed above, linked to conventional notions of distance and risk, including the need for the aircrew to perform multiple tasks while flying in a high-speed aircraft and "endeavouring to keep the aircraft in the air and safe from surrounding threats in a combat environment."[126]

NATO further based its justification for the many civilian casualties of the Grdilca bridge attack on another critical, limiting environmental factor, the inherent spatial limits of a cockpit. Operating at a high altitude, the aircrew could effectively view the target only through the camera in the electro-optical guidance system of each bomb. In the bomb-camera video of the attack, which was shown by General Clark in a NATO press briefing, the train is clearly seen approaching the bridge before the missile hits. However, as General Clark emphasized to the media, the person launching the missile on the aircraft was dependent on a small five-inch screen to guide the missile to its target and did not enjoy the benefit of the "much better view" on the video footage.[127] General Clark's comment implied that a bigger screen and a more complete picture, like the picture on the monitor available to the crew of a UAV, might have made a difference in a key aspect of this tragic attack and the ultimate judgment that it fell within the limits of proportionality.

Unable to see the target with their own eyes because of *distance*, and unable to get an adequate view of the target by means of the electro-optical guidance system on the bomb because of the technical limitations of these systems and the spatial limitations of the cockpit, the aircrew in the Grdilca incident demonstrated why the accuracy of PGMs can unquestionably be affected by distance when conventional aircraft are involved, notwithstanding remarks to the contrary by senior Pentagon officials.[128] While such limitations figured among those used to justify the many civilian casualties at the Grdilca bridge, they are radically altered by new virtual technologies. Had the "unblinking eye" of a UAV been in the vicinity, it could have provided an invaluable second, extrahuman view of the Grdilca bridge, adding immeasurably to the obscured and limited view of the aircrew while providing real-time data to UAV operators at a virtual location. Such benefits of virtual surveillance capabilities for the observance of law-of-war obligations merit more careful evaluation.

Extrahuman Virtual Capabilities

As noted, the principles of distinction and proportionality are easy to state but often difficult to apply. Article 57 of Protocol I, however, now summarizes the practical application of these principles in the form of more concrete rules. These rules, which appear to be part of customary international law[129] and are also substantially repeated in several U.S. military

[125] A. P. V. Rogers, *What Is a Legitimate Military Target? in* INTERNATIONAL CONFLICT AND SECURITY LAW: ESSAYS IN MEMORY OF HILAIRE MCCOUBREY 160, 167 (Richard Burchill, Nigel D. White, & Justin Morris eds., 2005).

[126] ICTY Report, *supra* note 101, para. 61.

[127] *Id.*, para. 59 (quoting General Clark).

[128] *See, e.g.*, MIDDLE EAST WATCH, *supra* note 29, at 116 (noting that in the aftermath of the Gulf war, Dr. Perry, the former undersecretary of defense for research and engineering, argued that the accuracy of precision-guided munitions "is independent of the altitude of delivery").

[129] *See* Prosecutor v. Kupreškić, No. IT-95-16-T, para. 524 (Jan. 14, 2000).

manuals,[130] require states to take certain "precautionary measures" in attacks. These measures include doing everything feasible to verify that the objectives to be attacked are military objectives; choosing means and methods of attack with a view to avoiding or minimizing incidental injury to civilians and civilian objects; refraining from launching an attack expected to be in breach of the principle of proportionality; and canceling or suspending an attack if it becomes apparent that the objective is not a military one or if the attack may be expected to be in breach of the principle of proportionality.[131]

The rules found in Article 57 not only limit the discretion of states but also constrain individuals. The personal significance of these obligations for military personnel—in the form of individual criminal responsibility—is heightened by their broad and explicit application to "those who plan or decide upon an attack."[132] Article 85 of Protocol I reinforces this burden on military personnel by providing that launching an indiscriminate attack in violation of the Article 57 prohibition on contravening the principle of proportionality can constitute a grave breach.[133]

The argument has been advanced that proportionality and the duty to take "all feasible precautions in the choice of means and methods of attack" include an obligation to use precision weaponry. Yet "feasible" is a contextual term;[134] the text of Protocol I contains no absolute requirement to use PGMs and no such obligation can be said to be mandated under customary international law.[135] If one considers PGMs in a *technological* context, such arguments have largely been overtaken by events: states that possess these weapons often prefer them to less advantageous and less accurate conventional munitions, for compelling fiscal, policy, and operational reasons.[136]

In the new era of virtual surveillance capabilities, a more cogent question about the meaning of the duty to "take all feasible precautions in the choice of means and methods of attack" concerns what is required with respect to the use of information assets in an attack. Virtual technologies have vastly expanded the information resources available to military commanders.

[130] *See, e.g.*, NAVY COMMANDER'S HANDBOOK, *supra* note 87, para. 8.3.1 ("Naval commanders must take all reasonable precautions, taking into account military and humanitarian considerations, to keep civilian casualties and damage to the minimum consistent with mission accomplishment and the security of the force."); DEP'T OF THE AIR FORCE, USAF INTELLIGENCE TARGETING GUIDE, paras. A4.3, A4.3.1 (A.F. Pamphlet 14-210, Feb. 1, 1998); U.S. DEP'T OF THE ARMY, *supra* note 87, para. 41; *see also* U.S. DEP'T OF THE AIR FORCE, INTERNATIONAL LAW—THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, at 5-9 to 5-10 (AFP 110-31, 1976, designated obsolete Dec. 20, 1995) (restating the provisions of Protocol I, Article 57 almost verbatim).

[131] Protocol I, *supra* note 89, Art. 57(2)(a)(i), (2)(a)(ii), (2)(a)(iii), & (2)(b).

[132] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, para. 2197 (Yves Sandoz, Christophe Swinarski, & Bruno Zimmermann eds., 1987) [hereinafter ICRC COMMENTARY] (noting that some states were even concerned that these words "could lay a heavy burden of responsibility on subordinate officers who are not always capable of taking such decisions").

[133] *Id.*, para. 2187 (referring to Art. 57(2)(a)(iii)).

[134] For example, NATO understands a "feasible" precaution to mean "that which is practicable or practically possible, taking into account all circumstances at the time, including those relevant to the success of military operations." ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 405, para. 8.1.2.1 n.18 (Naval War C. Int'l L. Stud. No. 73, A. R. Thomas & James C. Duncan eds., 1999).

[135] Michael N. Schmitt, *Precision Attack and International Humanitarian Law*, 87 INT'L REV. RED CROSS 445, 461 (2005). For a summary of such arguments, see *id.*

[136] *See* Sydney J. Freedberg Jr., *The Bills Come Due*, NAT'L J., Mar. 15, 2008, at 18 ("Today almost all bombs carried by U.S. aircraft are precision-guided.").

Although legal precedents in this area are scarce, at least one international tribunal has emphasized the appropriate use of *available* information as a key factor in determining individual criminal responsibility for disproportionate attacks.[137] The practical availability of so much new information also bears heavily on a commander's responsibility to minimize incidental civilian casualties under current U.S. military regulations.[138]

As indicated above, new strategies that require "persistent surveillance" also entail ever-expanding operational access at all levels of command to the new information resources. Because of these new technologies, strategies, and policies, what was previously not legally *feasible* is being radically altered by what is now operationally *required*. Thus, the legal, contextual constraints of feasibility that until recently allowed a U.S. military commander to argue that his or her obligation to deploy and use advanced ISR technologies was limited are being fundamentally changed by virtual technologies.[139]

In an effort to comply with the obligation under Article 57(2) of Protocol I to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects" and otherwise seek to prevent disproportionate civilian casualties, the U.S. military engages in an elaborate "collateral damage assessment" process in planning attacks. Such assessments often rely, at least in part, on computer programs that can more precisely model the potential civilian damage to be anticipated from a planned attack.[140] These programs calculate effects based on several factors, such as the size and type of the bomb to be used, the type of aircraft launching or dropping it, and the altitude at which the plane will fly. Since targeting decisions cannot, however, be totally abdicated to computers, commanders can and do authorize attacks that are not based solely on the results of computer-generated models.

Collateral damage assessment usually involves the active participation of lawyers.[141] While careful calculations and the meaningful involvement of competent legal counsel are necessary components of this process, the key to meaningful assessments is accurate intelligence—and its lack is the most common reason for their insufficiency.[142] Since targeting itself is essentially

[137] *See, e.g.*, Prosecutor v. Galić, No. IT-98-29-T, para. 58 (Dec. 5, 2003) (noting that in making such a determination, "it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of *the information available to him or her*, could have expected excessive civilian casualties to result from the attack") (emphasis added) (footnote omitted).

[138] *See, e.g.*, NAVY COMMANDER'S HANDBOOK, *supra* note 87, para. 8.1.2 (noting that "the commander must determine whether the anticipated incidental injuries and collateral damage would be excessive, on the basis of an honest and reasonable estimate of the facts *available* to him," and whether alternative possible methods of attack should be chosen to reduce civilian casualties and damage "in light of all the facts known or reasonably *available* to him") (emphasis added).

[139] Schmitt, *supra* note 135, at 461 (noting such "decisional factors" as time constraints on the ability to gather and process additional information, calculation of the extent to which such information would resolve uncertainties, competing demands on ISR resources, and risks to the systems and operators). These decisional factors are being reshaped by new virtual "persistent surveillance" capabilities, network-centric access to related ISR data throughout the command structure, the improving quality and types of information collected by virtual platforms (especially real-time data), and the complete lack of risk involved in the collection of information through these virtual systems.

[140] Bradley Graham, *Military Turns to Software to Cut Civilian Casualties*, WASH. POST, Feb. 21, 2003, at A18. (The military admits that this computer program originally bore the unfortunate name "Bugsplat" but was later renamed "FAST-CD" or "Fast Assessment Strike Tool—Collateral Damage.")

[141] *See generally* Dunlap, *supra* note 44.

[142] Benjamin, *supra* note 61 (quoting the deputy director of the U.S. Combined Air Operations Center in Qatar—the command hub responsible for air operations in both Iraq and Afghanistan—as saying that when immediate air support is requested and only limited information is available on the location of vulnerable civilians, "that is where you see most of the civilians being killed").

an intelligence function, commanders who are obligated to take precautionary measures to ensure distinction and proportionality in an attack also by implication are responsible for ensuring that, to the fullest of their abilities and to the extent "feasible," accurate intelligence is properly used in assessments of potential civilian damage. As the ICTY Committee observed, "The obligation to do everything feasible is high but not absolute. A military commander must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets. The commander must also direct his forces to use available technical means to properly identify targets during operations."[143] It follows from this reasoning that new virtual information resources that vastly increase the "available technical means to properly identify targets during operations" directly affect the individual responsibility of military commanders to take all feasible measures to verify military objectives and avoid excessive civilian casualties. Moreover, the committee's observations on a commander's duty under the law of war to set up and use appropriate intelligence-gathering mechanisms to verify military targets usefully illustrate the increasing willingness of international tribunals to apply the proportionality principle and related rules to difficult combat decisions.[144] The committee's work in this case further shows how video records of incidents, an information resource that has been radically improved and expanded by virtual surveillance capabilities, help open the door to "second opinions" about the lawfulness of specific military actions in a process that continues to increase the currency of the proportionality principle in resolving disputes.[145]

Because many new attack capabilities are inseparably linked to virtual information resources, virtual technologies are reshaping legal obligations related to overall attack planning. The potential impact of this new universe of information, especially on the duty to verify targets as military objectives, can be seen in the controversy over the U.S. air strike on the Al Firdos bunker in Baghdad on February 13, 1991.[146] This attack, which caused the greatest loss of civilian life of any single incident during the Gulf war, was described as a "pivotal moment" in the way the U.S. military approached targeting issues and an example of the "intersection of high technology and bad publicity."[147] Although the Iraqis had originally built the bunker to serve as an air raid shelter, the United States received intelligence that it had been converted into a headquarters for the Baath Party's secret police. Tragically, in addition to Iraqi intelligence operatives, many families had also relocated to the bunker, accounting for the subsequent deaths of approximately three hundred civilians, including over one hundred children.

[143] ICTY Report, *supra* note 101, para. 29. While the committee noted that "[b]oth the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used," the report predates large-scale deployment of UAVs and availability of related information resources. *Id.*

[144] Franck, *supra* note 95, at 736 (noting how the ICTY Report "sustains the conclusion that . . . it is perfectly possible to apply the principle of proportionality to combat decisions and render a plausible second opinion").

[145] *Id.* at 717 (arguing that some powerful, yet indeterminate, legal principles, such as proportionality, achieve success in helping to resolve disputes by "deliberately creating a space for 'second opinions' to which claims of disputants can be referred").

[146] *See* Michael W. Lewis, *The Law of Aerial Bombardment in the 1991 Gulf War*, 97 AJIL 481, 504 (2003).

[147] Benjamin, *supra* note 61 (noting that events like the Al Firdos bunker incident "gave birth to a modern military bureaucracy that could analyze and approve airstrikes based, in part, on anticipated civilian casualties"). Some military officers did not view the birth of this new bureaucracy favorably. *See* Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1, 34 (2005) ("[T]he al-Firdos bunker incident was a turning point, creating a preoccupation to minimize civilian casualties and any other collateral damage.").

The attack on the Al Firdos bunker was widely criticized. Some human rights groups suggested that the United States knew—or in any event should have known—that civilians had taken shelter in the bunker, and that the U.S. military was thus obligated to inform Iraq of its change in status from an air raid shelter to a military target.[148] U.S. officials emphasized, however, that their limited ISR capabilities were not able to establish that civilians were entering the bunker each night.[149] Information to that effect could have profoundly affected the decision to attack the bunker and today could be obtained through persistent surveillance by UAVs.[150]

If the United States could have reviewed images or other information indicating the presence of many civilians before the Al Firdos attack, U.S. commanders presumably would not have launched the operation—provided that the information helped them conclude that the expected significant loss of civilian life was indeed excessive in relation to the limited concrete and direct military advantage to be gained from destroying the bunker.[151] One can easily understand how access to more information could have changed collateral damage assessments like the one involving the Al Firdos bunker, but that conclusion assumes that critical information would have reached the appropriate decision makers in a timely fashion. As noted, however, the hierarchical, linear bureaucracies of large military organizations are not optimally organized to make use of large amounts of recent or real-time information. Such failings may in fact have played a part in the Al Firdos attack, since at least one U.S. official has suggested that even with its limited surveillance capabilities, the military was overloaded with relevant intelligence data.[152] This potential excuse or justification, however, for not using critical, available information to do "everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects" is losing force, as discussed above, because of the organizational changes required to support the operational applications of the ubiquitous information generated by persistent surveillance.

As virtual surveillance capabilities inescapably change both what is required for military operations and what is feasible as precautionary measures, lawyers will be key to improving access to the new information resources pertaining to the legal sufficiency of collateral damage assessments. Lawyers will be compelled to demand all available data relevant to their review of attacks that risk incidental civilian casualties, including prolonged imagery of targets that might show the presence of civilians. If such data are lacking despite the use of persistent surveillance, these lawyers (and afterward the critical media, interested nongovernmental

[148] MIDDLE EAST WATCH, *supra* note 29, at 128–47.

[149] R. Jeffrey Smith, *Building Was Targeted Months Ago as Shelter for Leaders*, WASH. POST, Feb. 14, 1991, at A25.

[150] *See* Lewis, *supra* note 146, at 504 (arguing that the contention that the United States had, or should have had, prior knowledge that civilians were in the Al Firdos bunker seems "flawed" because of inadequate intelligence resources: he notes that less than 3 percent of the total sorties flown during Operation Desert Storm were reconnaissance sorties and that "much-celebrated reconnaissance platforms such as the Predator and Global Hawk drones lay ten years in the future").

[151] A CENTCOM staff officer responsible for planning the attack was quoted as saying that "had we known that there were civilians in the bunker, it never would have been attacked." *Id.* at 503. Such sentiments, however, were viewed with skepticism by those who saw the U.S. campaign as being built upon a willingness to accept high civilian casualties. *See* Normand & Jochnick, *supra* note 26, at 402.

[152] Smith, *supra* note 149 (quoting a U.S. official as saying that "[w]e get a lot more intelligence data than we have time to look at," and observing that "there are literally thousands of targets worth looking at. It's hardly surprising that we didn't look at this the day before the raid.").

organizations, opportunistic adversaries, and a host of others with potential "second opinions") are likely to ask why such information was not collected or made available.

In addition to its role in preplanned strikes, information gained by virtual technologies is likely to have a profound impact on the duty of a commander under Article 57(2)(b) of Protocol I to terminate an ongoing attack when its continuance would appear to breach the principle of proportionality. Two examples from the Kosovo conflict help illustrate the point, though the necessary surveillance capability was not available at the time. First, in the case of the Grdilca bridge in Serbia, the crew members of the attacking aircraft did not abort the second attack because their already-limited visibility, which was further obscured by smoke, prevented them from seeing that the passenger train was still on the bridge. A virtual platform providing additional views and a longer loiter time would probably have proven invaluable in better surveilling the bridge with the stranded train still on it. Second, in the case of the convoy of civilian vehicles near Djakovica, the tragedy was compounded by the execution of a series of air strikes by several different planes that lasted over two hours. While the initial mistaken identification of military vehicles in the convoy raised one set of questions, the failure to suspend the attack in the face of mounting civilian casualties raised another. After allied officers at a NATO command center in Italy became concerned that the convoy did not appear to be traveling in a manner typical of Serbian military units, special observation planes were dispatched and pilots with binoculars identified civilian vehicles on the road.[153] Only then was the attack halted.

Even as virtual technologies enhance the surveillance capabilities of military personnel, they also make the military's own activities more perceptible before, during, and after attacks. Those who plan or decide upon an attack will increasingly do so with the knowledge that a much more complete record is being created of both their actions and the basis for their decisions. The new real-time data may give this record far more relevance than ever before in establishing a failure to suspend an ongoing attack that is causing disproportionate harm. With respect to the duty to take precautionary measures in the planning of attacks, this unprecedented level of transparency creates a record that can later be used to evaluate key elements of the collateral damage assessments, thus improving accountability by making the proportionality requirement more difficult to ignore and noncompliance more difficult to conceal.

Persistent surveillance through virtual technologies is also leading to unexpected and somewhat ironic changes in the inherently subjective risk assessment process itself. Although modern guided weapons are far more accurate than the iron bombs of World War II, a precision bombing attack in the virtual era may nevertheless entail a tragic certainty of death for a specific number of civilians located near the targeted military objective. Persistent surveillance may now enable attack planners to make much more precise estimates of how many civilians are likely to die in a particular strike. The perverse consequence of this new capability, not unnoticed by some human rights groups, is that civilian deaths in such attacks may be incidental but no longer are accidental.[154] The calculations associated with this new technological capability have reportedly become ever more exacting for military and government leaders as they grapple

[153] Gordon, *supra* note 109.

[154] Benjamin, *supra* note 61 (quoting Sarah Holewinski, executive director of the Campaign for Innocent Victims in Conflict, who observes of the decision to bomb targets with a certain number of likely civilian casualties: "They call them accidental deaths, but they are not . . . . They know what they are doing.").

with the maximum allowable number of anticipated civilian casualties from a given planned attack.[155]

The grim math of collateral damage assessments in the virtual era may at first seem repugnant, but it also means that those planning attacks cannot easily escape the reality of their likely human cost. This painful reality, however, is exactly the right starting point for required evaluations under the proportionality principle. The difficult balancing of humanity and military necessity that lies at the heart of the proportionality principle is thus being made more authentic by the unintended, virtually created new level of transparency.

The Fusion of Human and Machine

In addition to the possibility of human error that characterizes many apparent failures to take precautionary measures, states have drawn on the failings of machines, using expressions such as "technical malfunctions" to describe seemingly unavoidable causes of many unintended civilian casualties. This excuse, though often advanced by states in the permissive law-of-war framework, is undergoing intense pressure from a more technologically sophisticated, humanitarian-oriented, and highly watchful international community. This pressure is increased with each ill-advised statement by a government official exaggerating the accuracy of so-called smart bombs.[156]

The spectrum of excuses for errant bombings—including technical malfunctions, unavoidable accidents, and more avoidable human errors—highlights a fundamental problem stemming from advanced military weapons systems, especially virtual technologies: the increasing fusion of humans and machines in war. The combined functioning of man and machine that many advanced weapons systems require unfortunately does not eliminate the possibility of "accidental" civilian casualties. It does, however, increasingly blur the distinction between technical malfunction and human error. On one level, technology aids human operators of sophisticated weapons systems to such an extent that their own senses become partially mechanical. For example, the eyes of pilots who fly helicopters or fixed-wing aircraft at night by means of night-vision equipment function exclusively through a mechanical spectrum, one

[155] Bradley Graham, *U.S. Moved Early for Air Supremacy; Airstrikes on Iraqi Defenses Began Long Before Invasion, General Says*, WASH. POST, July 20, 2003, at A26 (noting that the former commander, U.S. Central Command Air Forces, confirmed that in the early stages of Operation Iraqi Freedom, approval to bomb targets if the deaths of thirty or more civilians might result had to be reserved for Secretary Rumsfeld, and that "[a]bout 40 or 50 targets fell in this category"). While the current limit on potential civilian casualties remains classified, a journalist who has interviewed intelligence analysts familiar with the policy notes that "[t]he days of the 'magic number' of 30 are over." Benjamin, *supra* note 61.

[156] PGMs are, of course, *guided* rather than *smart,* and a significant percentage of them fails to hit their targets. *See* Hunter Keeter, *Pentagon Estimates 70 Percent PGM Use in Possible War with Iraq,* DEFENSE DAILY, Mar. 6, 2003 (quoting a U.S. Central Command official that a failure rate "between 8 percent and 10 percent" can be expected for PGMs). This failure rate is based on how many PGMs fall "outside the usually-expected 21-foot circular error probable (CEP) associated with precision strikes." *Id.* The Department of Defense defines "CEP" as "the radius of a circle within which half of a missile's projectiles are expected to fall." DICTIONARY OF MILITARY AND ASSOCIATED TERMS, *supra* note 55. A long list of things can go wrong in modern aerial bombing missions, including mechanical or electronic malfunctions in navigation, flight control, guidance, or bomb release systems; changes in wind direction; severe atmospheric conditions that degrade visibility and the effectiveness of lasers; fluctuations in global positioning signals; failure of electronic packages on smart bombs, turning them into dumb bombs; and the falling of bombs from their racks in planes. *See* Michael Evans, *Smart Bombs Can Be Stupid,* TIMES (London), Oct. 25, 2001; Editorial, *How Precise Is Our Bombing?* N.Y. TIMES, Mar. 31, 2003, at A12.

that produces an enhanced-intensity range, as well as an enhanced spectral range that allows them to take advantage of nonvisible sources of electromagnetic radiation.

On another level, a key aspect of the merging of humans and military machines is seen in the growing number of high-tech weapons systems that depend on the prior programming of human operators, epitomized by missiles with "fire and forget" technology that seek and identify enemy targets on the basis of preprogrammed data such as global positioning coordinates, heat signatures, and electronic emissions. When one of these technologies fails, the faulty component of the system may be hard to identify; yet such failures raise questions about the human techniques and procedures involved in the targeting process, especially those related to the maintenance of accurate, accessible databases. This question becomes even more crucial when civilians are harmed by bombs that hit what military officials later describe as the "wrong target."

In the highly publicized case of the accidental U.S. bombing of the Chinese Embassy in Belgrade during the Kosovo conflict (for which the United States gave a detailed explanation, as well as millions of dollars in *ex gratia* payments to China and Chinese nationals), technical systems admittedly functioned superbly as a B-2 stealth bomber dropped five two-thousand-pound satellite-guided JDAM (Joint Direct Attack Munition) bombs on a target that corresponded with preprogrammed global positioning coordinates.[157] Unfortunately, the CIA had supplied coordinates for a purported Yugoslav arms agency that turned out to be those of the Chinese Embassy. Declaring that the human aircrews "had no idea they were . . . bombing the Chinese Embassy," the United States identified a series of "errors and omissions" that led to this disaster.[158] In response to intense criticism, U.S. officials made some important statements pertaining to responsibility for future failures of sophisticated weapons systems that are especially relevant to law-of-war obligations in the new virtual era. Reaffirming that the bombing was a mistake, Deputy Secretary of Defense John Hamre observed:

> Human beings will always make mistakes. . . . Where human failings are unintentional and purely accidental, . . . we need to look at the systems and processes we impose to guide and constrain individuals. Where did our systems and procedures fail? Do our systems and procedures allow too many human failings which can result in tragic outcomes?[159]

Secretary Hamre's admonition that, when high-tech attacks lead to tragic outcomes, the U.S. government must take responsibility for the overall systems and procedures on which modern weapons rely relates directly to the U.S. obligation to take precautionary measures under the law of war in the new virtual era. In view of the growing scrutiny of international society, the apparent failure of modern, complex weapons systems to be used in accordance with the principles of discrimination and proportionality can no longer be easily dismissed on

[157] *See* Sean D. Murphy, Contemporary Practice of the United States, 94 AJIL 127–31 (2000).

[158] Thomas Pickering [under secretary of state], Oral Presentation to the Chinese Government Regarding the Accidental Bombing of the P.R.C. Embassy in Belgrade (June 17, 1999), *at* http://www.state.gov/documents/organization/6524.doc (noting that these "errors and omissions" included a "severely flawed" technique that was used to locate the target, databases that did not contain the correct location of the Chinese Embassy, and a target review process that failed to catch either of these two fundamental errors).

[159] *Inadvertent Bombing of the Chinese Embassy in Belgrade, Yugoslavia, May 7, 1999: Hearing Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (July 22, 1999) (statement of John J. Hamre, deputy secretary of defense), *available at* http://www.dod.mil/dodgc/olc/docs/test99-7-22hamre.rtf [hereinafter Hamre Statement].

the basis of technical malfunctions or the unchecked operation of human failings. The combination of distant human operators and powerful remotely controlled and semiautomated weapons raises fundamental questions about the procedures and systems needed to support the programming and operation of these weapons for both operational and legal purposes.

Intelligence systems and resources are critical to the basic functions of virtual technologies and the improved targeting capabilities that they are intended to make possible. After the debacle of the bombing of the Chinese Embassy in Belgrade, U.S. officials conceded that the information and systems supporting new precision-targeting capabilities must at least be free of obsolete databases and "severely flawed" techniques.[160] Consequently, in the context of sophisticated virtual weaponry, feasible precautionary measures include more than just efforts to ensure access to accurate ISR data as part of the targeting process: systems and procedures must be established that better ensure the proper combined functioning of man and machine, that better "guide and constrain individuals" responsible for their operation. This goal amounts to more than evolving, good policy guidance: it increasingly appears to be part of an obligation, as reflected in Secretary Hamre's recognition of fundamental U.S. responsibilities related to new, sophisticated weapons technologies.[161]

In the new virtual era, the responsibilities of military forces vis-à-vis the civilian population *before* a "fire and forget" weapon is launched call for a reexamination of the obligation to verify military targets and the duty to take all feasible precautions in the choice of means and methods of attack. The scrutiny related to the former can now be said to extend beyond the narrow conventional weapons-based focus on which armaments or tactics are suited to a given attack. It must include an assessment of the key methods, procedures, and systems necessary to support the effective use of the virtual technologies to be deployed, including a careful evaluation of whether appropriate efforts are being made to ensure that databases are sufficiently accurate to catch mistakes by the human operators.[162] This is the new "virtual" basis required for precautionary measures.

Even before the duty to take precautionary measures in attacks was codified in Protocol I, commentators understood that the evaluation of information for long-distance attacks obtained from aerial reconnaissance "must include a serious check of its accuracy."[163] In one sense, as noted above, a modern, serious check for accuracy of targeting information appears to involve ensuring that virtual surveillance assets are used to confirm military objectives as part

[160] Pickering, *supra* note 158.

[161] Hamre Statement, *supra* note 159 (acknowledging that "I and my colleagues at DoD are absolutely responsible for the systems and procedures" and promising that "[i]f those systems and procedures permit failure or exacerbate honest error, we are absolutely responsible for fixing them"). While the ICTY Committee concluded that this incident resulted from "inadequacy of the supporting data bases" and flawed review procedures, it also took note of the U.S. apology, U.S. payments to China, reprimands of several U.S. officials, and the statements of Secretary Hamre and others, stressing that "[t]he US Government also claims to have taken corrective actions in order to assign individual responsibility *and to prevent mistakes such as this from occurring in the future.*" ICTY Report, *supra* note 101, paras. 83, 84 (emphasis added).

[162] As noted by Secretary Hamre:

> Fifty years ago we knew we couldn't discriminate between embassies and legitimate targets in a bombing campaign so we warned everyone accordingly and pressed ahead. We can't do that today and don't need to do that today. *But that means we have to have data bases that are sufficiently accurate to catch mistakes that will be made.*

Hamre Statement, *supra* note 159 (emphasis added).

[163] ICRC COMMENTARY, *supra* note 132, para. 2195.

of "available technical means." In another sense, however, the ability of military forces to count on any new types of information in evaluating the likelihood of excessive casualties will often hinge on the inclusion of that information in accessible databases—and it is now these databases themselves that must be checked for accuracy. For this reason, the public acknowledgment by U.S. leaders of their responsibility for maintaining updated, accurate databases to support high-tech weapons (that often depend on data generated by vast new virtual ISR capabilities) points to the emergence of a new type of obligatory precautionary measure. Such an obligation seems all the more essential and appropriate since the recent network-centric reforms in military organizations inspired by the operational utility of the information acquired through virtual technologies may make useful databases more accessible for proportionality assessments than ever before.

Accurate databases, increasingly full of vital information, are not an exotic, unusual, or burdensome safeguard that must be attached to military missions: they are an operational requirement related to successful targeting and the accomplishment of other mission objectives. Thus, maintaining accurate databases must be regarded as a minimal "feasible" precaution for the purposes of verifying objectives to be attacked and otherwise ensuring the proportionality of attacks in the virtual era. Failure to take this precaution in planning an attack that hits "the wrong target" will be difficult to defend in the context of increasing technological capabilities, a commitment to avoiding such mistakes, and an admitted higher duty of care. Noting with regret that the U.S. "no strike" system had not been adequate to prevent the mistaken attack on the Chinese Embassy because it had been "dependent on data bases which [were] not adequately updated," Secretary Hamre alluded to these ever-higher standards of care when he concluded that "the challenge lies in ensuring that the underlying data bases on which the system depends contain, to the *maximum extent* feasible, the most up-to-date information available."[164]

IV. Conclusion

Virtual military technologies are taking law, war, and military institutions on an uncharted path into the future at breakneck speed. Some of the transformational effects of these new weapons systems are clear; others are still emerging. One undeniable fact is that remotely controlled and semiautomated weapons systems are continuing to assume new, important roles in military operations in more and more countries throughout the world. Furthermore, the absence of humans as the actual combatants in armed conflicts seems to be steadily achieving acceptance and entering society's collective consciousness with relatively little reflection. Remotely controlled machines— or "virtual combatants"—are systematically replacing human combatants, paving the way for armed conflicts in which humans will increasingly be absent from the battlefield and many dangerous war-fighting missions.[165] At some point, the replacement of humans by virtual combatants and the corresponding lack of concern about the death or capture of military personnel could even challenge two conditions seen by some

[164] Hamre Statement, *supra* note 159 (emphasis added).

[165] Lopez, *supra* note 20, at 30 (noting that in addition to using robots to find and disable roadside bombs, the U.S. military has experimented with remote-control "weaponized robots" to perform dangerous duties in Iraq, including securing checkpoints and conducting "armed reconnaissance").

as limiting the willingness of states to comply fully with and enforce their law-of-war obligations in conflicts with terrorists: reciprocity and symmetry.[166] While states will always have humanitarian, political, strategic, and military reasons to comply with law-of-war obligations even if terrorists can be expected to ignore them, eliminating the need for reciprocity and symmetry could nonetheless contribute to relieving pressure on states to pursue harsher measures against terrorists and other militant groups outside the law-of-war framework.

The movement toward virtual combatants does not come without risks or dangers. The long-term and understudied consequences of replacing human combatants with virtual ones raises fundamental questions in many fields. One problematic area, which lies beyond the scope of this article, concerns the overall consequences of this phenomenon for the *jus ad bellum*, or international law governing *recourse* to war. Inasmuch as technological developments reduce the political costs of going to war by eliminating the risk that human operators will be killed or captured, some commentators fear that those developments will make it easier and more attractive for states to become involved in armed conflicts.[167]

The power of virtual technologies to improve the observance of the *jus in bello* gives rise to the contrasting concern that these technologies remain dependent on the competence of human operators. Who is to be entrusted with operating virtual weapons systems and how will those persons be affected by these technologies? Although it remains to be seen whether virtual technologies will create an elite class of techno-warriors, states will certainly have to focus on at least one key factor for future operators of these systems: aptitude. An increasingly high-tech U.S. Army already needs soldiers with a high degree of aptitude. A 2005 study by the Rand Corporation commissioned by the Pentagon evaluated a variety of factors affecting military performance; it found aptitude to be critical and concluded that it becomes even more important as tasks become more technical.[168]

The implications of the emerging robotic military model for human staffing, recruiting, and training requirements are complex and far-reaching. In shifting from a model in which the primary purpose of technology was to support human combatants to a model in which the role of humans is to support the technology, the robotic military will necessarily demand greater levels of technical competence from the human "robotists." As these demands for greater competence proliferate and virtual technologies merge humans and machines even more

[166] The reciprocity condition speaks to the mutual ability of belligerents to enforce law-of-war obligations by responding on a tit-for-tat basis to violations. The symmetry condition speaks to whether the two sides are so differently positioned that the burden of compliance falls unevenly on one of them. Some scholars argue that these conditions, rather than humanitarian considerations, serve as the primary basis for compliance with law-of-war obligations, making them particularly ill suited for fighting terrorists. *See, e.g.,* Eric A. Posner, *War, International Law, and Sovereignty: Reevaluating the Rules of the Game in a New Century: Terrorism and the Laws of War*, 5 CHI. J. INT'L L. 423 (2005).

[167] *See* BYERS, *supra* note 50, at 120 ("High-tech weaponry has reduced the dangers to US personnel, making it easier to sell war to domestic constituencies. . . . This change in thinking has led to a more cavalier approach to the *jus ad bellum*, as exemplified by the Bush Doctrine of pre-emptive self defence . . . ."); IGNATIEFF, *supra* note 77, at 179–80 ("If war becomes virtual—and without risk—democratic electorates may be more willing to fight especially if the cause is justified in the language of human rights and even democracy itself."). Some have also suggested that new intelligence systems and other sophisticated military technologies may give the leaders of powerful states erroneous feelings of control and understanding, leading to misjudgments that may increase their willingness to become involved in international armed conflicts. *See* HAMMES, *supra* note 33, at 194.

[168] JENNIFER KAVANAGH, DETERMINANTS OF PRODUCTIVITY FOR MILITARY PERSONNEL: A REVIEW OF FINDINGS ON THE CONTRIBUTION OF EXPERIENCE, TRAINING, AND APTITUDE TO MILITARY PERFORMANCE (Rand, 2005).

closely, each component of these new virtual weapons systems, along with the sum of their parts, will continue to be scrutinized. It is in this context and on this basis that law-of-war obligations in the virtual era will be assessed.

The virtual era is rapidly expanding to encompass the entire international community. The demand for UAVs, for example, is soaring as more and more countries, including many in the developing world, are obtaining and becoming familiar with virtual technologies and their ISR capabilities, in part because UAV systems cost much less than their manned counterparts.[169] The acquisition by many countries of UAVs manufactured in the United States, France, and Germany; by Georgia and India of UAVs manufactured in Israel; and by Pakistan and Egypt of UAVs manufactured in China demonstrates that the implications of the virtual era already extend far beyond U.S. military operations alone.[170] This growing worldwide familiarity with UAVs, even if some countries use them only for basic reconnaissance or artillery-spotting missions, will inescapably direct more attention in the future to the improving ability of military forces, especially those belonging to states that can afford to deploy many advanced systems, to verify objectives and take other precautionary measures to ensure observance of the proportionality principle in attacks.

Virtual technologies are thus on the verge of significantly shaping the views and conduct of all states, even those that do not possess them or cannot afford to deploy them in great numbers. New, extensive virtual surveillance capabilities come with new burdens for the states that benefit from them—burdens that are more and more likely to be invoked by poor or other less technologically advanced states in any discussion about the corresponding legal duties. The developed states that seek to avoid these burdens may again find themselves haunted by the new legal content of words such as "available." Once relied upon as permissive terms, these words may now unexpectedly impose constraints. For example, at the diplomatic conference that ultimately adopted Protocol I, one state observed that the obligation to identify military objectives as targets under Article 57(2) "depended to a large extent on the technical means of detection available to the belligerents."[171] In its *Commentary*, the International Committee of the Red Cross agreed, observing that "[s]ome belligerents might have information owing to a modern reconnaissance device, while other belligerents might not have this type of equipment."[172] Drawing on such considerations, less developed states can argue that richer countries with extensive, widely deployed and sophisticated virtual surveillance capabilities and unprecedented access to once-unimaginable levels of ISR information are subject to a higher standard of care in verifying targets as military objectives and taking other precautionary measures.

The more exacting legal standards likely to flow from virtual surveillance capabilities will not be diminished by the global newsroom, which increasingly enhances its reporting with video

[169] Ilya Kramnik, *Unmanned Aerial Vehicles Become More Sophisticated,* SPACE DAILY, Apr. 30, 2008, *at* http://www.spacedaily.com/reports/Unmanned_Aerial_Vehicles_Become_More_Sophisticated_999.html (noting that because UAVs require "only a rudimentary infrastructure" and are "smaller, cheaper and easier to maintain," the demand for them is becoming more widespread and states in the Third World increasingly consider them to be "the only alternative to conventional aircraft requiring expensive pilot-training programs and infrastructure").

[170] Israel and China, for example, each have over forty UAV models and variants, from at least ten different manufacturers in each country, and are exploiting lucrative export markets throughout Asia and Africa. Wilson, *supra* note 17, at 30. In the developing world, China exports UAVs to Bangladesh, Egypt, Pakistan, Sri Lanka, Tanzania, and Zambia. *See* Wilson, *supra* note 18, at 27.

[171] ICRC COMMENTARY, *supra* note 132, para. 2199 (commentary on Art. 57(2)(a)(i)).

[172] *Id.*

footage furnished by virtual platforms overhead. Even the five-day standoff and military action against Somali pirates holding an American hostage on a small lifeboat in a remote corner of the Indian Ocean in April 2009 were not exempt from news reports showing video footage from a UAV used by U.S. forces in the operation.[173] When a military operation is not successful or what actually happened is disputed, no small similarity may be remarked to the instant replay so familiar to American football fans; although it may lack the assigned referees, the process involves a close examination of digitally recorded facts, subjects disputed calls to wide public debate, prompts a more exacting application of rules, and sometimes leads to the refinement of those rules. Similarly, whether the home team likes the call or not, a new era of openness and debate has arrived, and with it new life for some of the rules on the playing field.

Virtual weapons systems are poised to transform the conditions of future battlefields for humans and change law, war, and military institutions in profound, far-reaching ways. While military-technological advances have routinely worsened the plight of civilians in war and made law an even more distant concern on the battlefield, virtual technologies are unexpectedly bringing laws that protect civilians closer to war than ever before. These technologies are in fact giving unprecedented traction, transparency, and relevance to venerable *jus in bello* rules that states have often ignored, manipulated, or consigned only to theoretical applications. At the same time, virtual technologies are refashioning the way military operations are conducted, the way military institutions function, and the way objectives are defined in war itself. The implications of the dawning virtual era deserve to be more carefully studied across a wide spectrum of human behavior. For the military institutions that must address the unfolding consequences of virtual technologies originally designed to help project military power, such a project is in some respects a study in irony.

[173] Edmund Sanders & Julian E. Barnes, *Pirates, Captive Sit in Navy's Shadow*, L.A. TIMES, Apr. 10, 2009, at A1. The UAV here, called the "ScanEagle," was launched from the U.S.S. *Bainbridge* and video footage that it provided was later shown on various news programs. It can be seen, for example, as *Scan Eagle Launches to Look for Pirates,* DAILYMOTION, Jan. 19, 2009, *at* http://www.dailymotion.com/video/x8xrw8_scan-eagle-launches-to-look-for-pir_auto.