

II

Mission Impossible? International Law and the Changing Character of War

John F. Murphy*

As a participant in the conference “International Law and the Changing Character of War,” in this article I hope to present and support the thesis reflected in the title to this essay, i.e., that the use and abuse of international law and the changing character of war have combined to place major obstacles in the way of the successful prosecution of armed conflict by US forces and their allies. In support of this thesis, I shall be drawing extensively on examples arising out of “the changing character of weapon systems” panel, but I shall also be exploring other dimensions of “the changing character of war” to buttress this support.

I. Challenges Posed by the Changing Character of Weapon Systems

In the panel “The Changing Character of Weapon Systems: Unmanned Systems/Unmanned Vehicles,” an overarching theme was the issue whether the use of these new weapon systems was compatible with international law. As noted in particular in Professor Pedrozo’s article,¹ the criticisms of the use of unmanned systems to attack adversaries outside of traditional combat zones like Afghanistan and Iraq have

* Professor of Law, Villanova University School of Law. I want to acknowledge the excellent research assistance of John (Sean) E. Jennings III and Carolyn (Carly) Studer, third-year students at Villanova University School of Law, on this article.

Mission Impossible? International Law and the Changing Character of War

been especially sharp. The primary focus of the critics has been on the Central Intelligence Agency's (CIA) use of armed drones, a prime example of an unmanned aerial system or unmanned aerial vehicle, to kill leaders of the Taliban or Al-Qaeda in the Federally Administered Tribal Areas (FATA) of Pakistan.

I make no attempt to address all of the numerous arguments advanced by the critics of the drone attacks, but rather limit my discussion to two closely related arguments: first, that the civilian nature of the CIA personnel utilizing the armed drones precludes them from engaging in armed conflict, and if they engage in armed conflict, this renders them "unlawful combatants"; and second, outside of Afghanistan and Iraq, the United States is not engaged in an armed conflict with the Taliban, Al-Qaeda or any other militant or terrorist group. If such attacks occur outside of an armed conflict, they must be treated as criminal acts and not armed attacks that give rise to the right to use military force in self-defense. Rather, they must be combated by law enforcement measures and governed by international human rights law, not the law of armed conflict, or, as some prefer to call it, international humanitarian law. Because armed drones are not law enforcement tools, the critics contend, they may not be used outside of combat zones.

The Effect of the CIA's Status as a Civilian Government Agency

One of the most persistent critics of the CIA's use of armed drones has been Mary Ellen O'Connell, holder of the Robert & Marion Short Chair in Law at Notre Dame University. According to Professor O'Connell, the CIA is not bound by the Uniform Code of Military Justice of the United States to respect the laws and customs of war and therefore it does not.² Moreover, according to O'Connell:

Under the law of armed conflict, only lawful combatants have the right to use force during an armed conflict. Lawful combatants are the members of a state's regular armed forces. The CIA are not members of the U.S. armed forces. They do not wear uniforms. They are not subject to the military chain of command. They are not trained in the laws of war, including the fundamental targeting principles of distinction, necessity, proportionality, and humanity.³

O'Connell's remarks presume that the law of armed conflict governs the CIA's use of armed drones in the FATA in Pakistan. This is a debatable point; we shall return to the issue below. But assuming *arguendo* that it does, the law of armed conflict does not prohibit civilians, including intelligence agents, from participating in hostilities. As Pedrozo points out,⁴ even Philip Alston, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, in his study on targeted killings, has conceded this point.⁵ Moreover, the use of armed drones by CIA personnel does not necessarily constitute a war crime if it results in a death in the FATA.⁶

Only if the killing itself is conducted in a manner prohibited by the law of armed conflict, e.g., it involves the deliberate targeting of civilians not directly participating in hostilities, does it constitute a war crime. Under such circumstances, it is irrelevant who conducts the targeted killing, intelligence personnel or State armed forces; the actor who committed the killing, plus those who authorized it, can be prosecuted for war crimes.⁷

The civilian status of the CIA personnel does have other significant consequences. First, if they are captured by the enemy, they are not entitled to prisoner of war status. It is a matter of some debate whether they are to be treated as civilians or as unlawful combatants while they are detained.⁸ Second, they may be attacked, either as members of an organized armed group or as civilian direct participants in hostilities. Third, they enjoy no belligerent immunity for their actions and thus may be prosecuted, either for war crimes (e.g., deliberately killing civilians) or domestic crimes (e.g., murder) in a national court.⁹ In other words, the absence of the right on the part of CIA personnel to participate directly in hostilities within the meaning of Article 43(2) of Additional Protocol I¹⁰ has consequences, but is not in itself a violation of the law of armed conflict.

At this writing, the media are full of commentary on the release of 75,000 US military documents on the war in Afghanistan by WikiLeaks. Although much of the commentary has focused on reports in the documents of Pakistan's Inter-Services Intelligence Directorate assisting the Taliban in Afghanistan in their use of improvised explosive devices (IEDs) against members of the Afghan government and coalition forces, there are also many reports in the documents of the fallibility of aerial drones. For example, one document reported that communications were lost with a Reaper drone, armed with Hellfire missiles and 500-pound bombs, and an F-15 fighter plane had to be ordered to shoot it down before it crossed into Tajikistan.¹¹ These documents also reportedly indicate that some reports of civilian casualties were never made public.¹²

At this writing there are also conflicting reports about an attack by coalition forces occurring on July 23, 2010 that Afghan sources claim killed fifty-two civilians, a claim that has been denied by NATO officials, who stated that an investigation NATO was conducting "has thus far revealed no evidence of civilians injured or killed."¹³ To be sure, reports of large numbers of civilians killed in Afghanistan are not something new. Indeed, tensions between the Karzai government and the US government over civilian casualties allegedly caused by airstrikes have been a long-standing problem. As I stated on another occasion:

Although the law of armed conflict clearly prohibits an intentional direct attack against the civilian population as such, and indeed categorizes it as a war crime, "there can be

Mission Impossible? International Law and the Changing Character of War

no assurance attacks against combatants and other military objectives will not result in civilian casualties in or near such military objectives.” In the latter case, the civilian casualties are known as “collateral damage” and do not give rise to accountability of the attacker. Nonetheless, as the sovereign government of Afghanistan, President Karzai can order the complete cessation of airstrikes (he has done so on occasion), and as a matter of international law, the United States and its allies are bound to comply—even though such airstrikes are a crucially important factor in the battle against the Taliban, and the Taliban regularly intermingle among the civilian population in order to use them as human shields (itself a violation of the law of armed conflict) and then use civilian casualties as part of their war propaganda effort. In short, the Taliban has been successfully engaging in so-called “lawfare,” using false accusations of violations of the *jus in bello* in order to win public opinion to their side.¹⁴

Although the documents released by WikiLeaks apparently do not report the intentional targeting of civilians by CIA personnel in either Afghanistan or Pakistan, they do “suggest that the CIA has sharply increased its use of paramilitary units in Afghanistan, and provide details of unintended killings of civilians by Task Force 373, a secret unit set up to kill or capture militant leaders.”¹⁵ Such unintended killings do not constitute war crimes but they greatly undermine the war effort and increase the pressure on the Afghan government to prevent their recurrence,¹⁶ as well as provide material for the Taliban war propaganda effort.

The civilian status of the CIA drones also has legal significance. Rule 17 (a) of the air and missile warfare manual,¹⁷ which, while it has no official status, is the product of a team of experts on the law of armed conflict and has been well received by governments, provides that only military aircraft are entitled to engage in armed attacks. There is no question that CIA drones are not military aircraft. It is arguable that rule 17 (a) of the manual reflects customary international law. If this argument is valid, the use of CIA drones in an international armed conflict would be a violation of the customary law of armed conflict.¹⁸

There is a serious issue, however, as to whether the CIA drones are being used in an “international armed conflict,” because of the ambiguity of the concept as applied to current circumstances. In his leading treatise on the law of international armed conflict, Yoram Dinstein defines an international armed conflict as limited to conflicts “raging between two or more sovereign States.”¹⁹ As Dinstein acknowledges, however, “drawing a line of demarcation between inter-State and intra-State armed conflicts is not as simple as it appears to be at a cursory glance.”²⁰ He points to Afghanistan in 2001 as an example. Prior to 2001 the Taliban regime fought a long-standing civil war with the Northern Alliance, which clearly constituted solely an internal armed conflict. In 2001, however, the Taliban regime, which because of its control over most of the territory of Afghanistan constituted the de facto government of Afghanistan, “got itself embroiled in an inter-State war

with an American-led Coalition as a result of providing shelter and support to the Al-Qaeda terrorists who had launched the notorious attack against the US on 11 September of that year”²¹

Under current circumstances, however, the Taliban are no longer the de facto government of Afghanistan. Rather, the Karzai government is both the de facto and de jure government of Afghanistan. For their part the Taliban are involved in an insurgency against the Karzai government and use the FATA as a safe haven from which their forces and Al-Qaeda forces launch cross-border attacks into Afghanistan. Moreover, because of the deteriorating situation between the Taliban in Pakistan and the Pakistan government, it is arguable that the Taliban in Pakistan have launched an insurgency against the Pakistan government.

If this scenario has some plausibility, then some further comments by Dinstein may be apposite:

A non-international armed conflict arising in State A may also have spillover horizontal effects within a neighboring country (State B). . . . In this scenario, insurgents against the Government of State A find temporary shelter within State B and ignite another “civil war,” this time against the Government of State B. As long as the two governments of States A and B (acting separately or in cooperation with each other) wage hostilities against the insurgents, the two simultaneous conflicts—despite their cross-border effect—remain non-international in character. But if the two Governments become embroiled in combat against each other, the armed conflict changes its character and becomes inter-State.²²

One may plausibly argue that Afghanistan and Pakistan are currently in the same position as States A and B in Dinstein’s hypothetical. If so, it needs to be noted further that, although there are tensions between the Pakistan and Karzai governments, there is at present no armed combat between them. It well may be, then, that the conflicts in both Afghanistan and Pakistan should be classified as non-international in character.

If it is correct to classify both of these conflicts as non-international, the civil status of CIA personnel or of CIA drones becomes irrelevant. This is because there is no counterpart in the law of non-international armed conflicts to Article 43(2) of Additional Protocol I. To the contrary, States often use their police and intelligence services in the fight against rebels. As to the status of aircraft, rule 17 (a) of the air and missile warfare manual’s requirement that only military aircraft are entitled to engage in armed attacks expressly does not apply to non-international armed conflicts.

Parenthetically, it may be noted that in *Hamdan v. Rumsfeld*,²³ the US Supreme Court rejected the assertion by the US government that since Al-Qaeda was not a

Mission Impossible? International Law and the Changing Character of War

State and had not accepted to be governed by the rules set forth in the Geneva Conventions, its affiliates could not invoke their protections. Rather, the Court held that the so-called “war on terror” was a non-international armed conflict, and therefore that at a minimum Article 3, which is common to all the Geneva Conventions, applies to the conflict with Al-Qaeda. The validity of this holding as a matter of international law is debatable, however, since, as Dinstein has argued, “from the vantage point of international law . . . a non-international armed conflict cannot possibly assume global dimensions.”²⁴ Michael Schmitt buttresses this conclusion by noting that Common Article 3 itself defines the conflict to which it applies as “not of an international character occurring in the territory of one of the High Contracting Parties.”²⁵

Even the language Schmitt quotes from Common Article 3, however, has been subject to different interpretations. On the one hand, it can be interpreted as referring only to “internal” armed conflicts, that is, civil wars or insurgencies. This appears to be the interpretation Schmitt favors. On the other hand, it can be interpreted as referring more broadly to any armed conflict that is not between States. This appears to be the interpretation that the US Supreme Court in *Hamdan* favors. Under the latter approach the phrase means occurring in the territory of “at least one of the High Contracting Parties.”²⁶

These arguments favoring conflicting interpretations of Common Article 3, while interesting, need not be resolved for purposes of resolving the issue of the effect of the CIA’s civilian status, because neither interpretation would support the proposition that the “war on terror” is an international armed conflict. In this case, then, the civilian status of the CIA is irrelevant for determining whether the CIA’s use of drones is compatible with international law.

As Schmitt has noted, however, the Supreme Court in *Hamdan* “neglected to explain how it arrived at the determination that the ‘war’ with Al Qaeda qualified as an ‘armed conflict,’ a term of art in the law of war”²⁷ and the “condition precedent for applicability of the law of war.”²⁸ We now turn to this issue.

Is the United States Engaged in an Armed Conflict with Al-Qaeda or Any Other Militant or Terrorist Group?

Neither the Geneva Conventions nor Additional Protocol I contains a definition of an “armed conflict.” In contrast, Additional Protocol II defines non-international armed conflicts in such a way as to sharply limit the scope of the Protocol.²⁹ Paragraph 1 of Article 1 of Additional Protocol II applies to all armed conflicts not covered by Additional Protocol I and

which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.

Paragraph 2 of Additional Protocol II then provides that “[t]his Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts.”

In the 1995 *Tadic* Interlocutory Appeal on Jurisdiction,³⁰ the International Criminal Tribunal for the former Yugoslavia addressed the preliminary issue of the existence of an armed conflict in response to a contention by the defendant that there had been no active hostilities in the area of the alleged crimes at the relevant time:

[W]e find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there.³¹

The question whether the US conflict with Al-Qaeda qualifies as an armed conflict is not easily answered. The only time this conflict could have qualified as an international armed conflict would have been when the United States invaded Afghanistan in 2001 and then only to the extent that Al-Qaeda forces were integrated into the Taliban forces, the de facto army of Afghanistan. At present, as noted previously, both the Taliban and Al-Qaeda are fighting as insurgents in Afghanistan, and it is arguable that the conflict there now is an internal armed conflict. The conflict in Afghanistan may even be within the scope of Additional Protocol II because arguably the Taliban and Al-Qaeda exercise such control over parts of southern Afghanistan as to enable them “to carry out sustained and concerted military operations.” These operations, the argument would continue, constitute “protracted” internal armed violence rather than just “isolated and sporadic” armed violence.

Assuming *arguendo* the validity of these arguments, they do not pertain outside of Afghanistan, and Al-Qaeda violence in other places would not seem to fall within the scope of Additional Protocol II. It must be noted, however, that the

Mission Impossible? International Law and the Changing Character of War

United States is not a party to Additional Protocol II, and it is debatable whether the Protocol's definition of an internal armed conflict is part of customary international law. Alternatively, some commentators have argued that the law of armed conflict, or international humanitarian law, is a "living" body of doctrine that aims to protect people to the maximum extent possible and thus should be interpreted in a way that fills gaps. They point to the Appeals Chamber decision in the *Tadic* case to support the proposition that for purposes of Common Article 3, "armed conflict" should be broadly interpreted to cover as many people as possible.³²

Even if the conflict between the United States and Al-Qaeda and other militant or terrorist groups is not an "armed conflict" within the meaning of the law of armed conflict, it does not necessarily follow that the drone attacks in Pakistan violate international law. As discussed at some length in Professor Pedrozo's article, the drone attacks in Pakistan are compatible with the United Nations Charter, specifically Article 2(4) and Article 51, as an exercise of the right of self-defense.³³ For my purposes, I will comment on only one aspect of the debate over self-defense: Article 51's requirement that the use of armed force be in response to an armed attack.³⁴

The proper interpretation and application of Article 51 have been the subject of much debate.³⁵ One of the most hotly debated issues has been whether Article 51 simply preserves the right of self-defense as it existed under customary international law prior to adoption of the Charter or places further limits on that right. Prior to the adoption of the Charter, the test most cited by the commentators for judging whether the use of force was justified as an act of self-defense was that of US Secretary of State Daniel Webster in the *Caroline* case, i.e., whether the "necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation."³⁶

The words "if an armed attack occurs" have raised the issue as to whether Article 51 has limited the scope of the self-defense doctrine. Some have argued that the words should be read narrowly so as to eliminate the possibility of anticipatory self-defense that other commentators have argued is available under the *Caroline* criteria.³⁷ There is no need to try to resolve this debate for present purposes, because there is no doubt that US and coalition forces have been subject to numerous and continuous armed attacks by Al-Qaeda and Taliban forces based in the FATA and that the use of armed force in the form of drones is necessary to try to prevent the continuation of such attacks. Moreover, as President Obama has recognized, the United States "cannot tolerate a safe-haven for terrorists whose location is known, and whose intentions are clear,"³⁸ because it is difficult, if not impossible, to win a conflict against insurgents if they are able to retreat to a safe haven in another country.

In sum, then, it appears that the claim that the CIA use of drones in Afghanistan and Pakistan is incompatible with international law is not well-founded. But merely having the better legal case in this argument may constitute a pyrrhic victory if the use of drones results in Al-Qaeda and the Taliban gaining more popular support in Afghanistan and Pakistan and increased recruits for their forces.

In his article Professor Pedrozo denies that the use of drones has resulted in more popular support for Al-Qaeda and the Taliban or has in any way assisted Al-Qaeda recruitment efforts. To support his contention, Pedrozo points out that the arguments of opponents are based on exaggerated civilian casualty figures and usefully notes the results of various independent studies indicating, *inter alia*, that drone strikes have effectively impaired Al-Qaeda operations and have not aided Al-Qaeda recruitment efforts.³⁹

Although the results of these studies are encouraging, I am not entirely convinced that they demonstrate the ineffectiveness of Al-Qaeda and Taliban propaganda. For example, although they demonstrate that civilian casualty figures are exaggerated, it is not clear that this message is effectively bought home to either the Afghan or Pakistani government or, more important, the large coterie of young Muslim men who are the primary target of Al-Qaeda and Taliban propaganda.

General Stanley A. McChrystal, who was in charge of US forces in Afghanistan until he was removed by President Obama in June 2010 because of unacceptable remarks made about the President's national security team to a journalist writing for *Rolling Stone* magazine, responded to pressure from the Karzai government and human rights advocates who claimed that US drone and other armed attacks were resulting in unacceptable numbers of Afghan civilian deaths by issuing a directive that placed significant restrictions on US troops attacking people suspected of being militants or destroying buildings used to harbor insurgents. Troops widely complained that the restrictions exposed them to excess risk by limiting their right to use force in self-defense. When General David H. Petraeus, who was appointed to replace McChrystal, took over command of American and NATO forces on July 4, 2010, he was faced with a difficult choice. On the one hand, he was sensitive to the need of his troops to protect themselves. On the other, the restrictions were reportedly popular with Afghan officials and human rights advocates who claimed that the restrictions had led to a significant reduction in Afghan civilian deaths.⁴⁰ At this writing Petraeus is reportedly ready to issue a new tactical directive that will expand restrictions on artillery strikes and aerial bombardment but clarify that troops have the right to self-defense. His goal will reportedly be to "persuade the troops that the unpopular rules will pay off in trust won on the ground."⁴¹

On August 1, 2010, Petraeus distributed counterinsurgency guidelines to troops. Reportedly, a large part of these guidelines, written by General Petraeus, is

Mission Impossible? International Law and the Changing Character of War

aimed at the information side of the war. For example, he writes, “Be first with the truth. Beat the insurgents and malign actors to the headlines.” “Avoid premature declarations of success.” “Strive to underpromise and overdeliver.” When things go wrong, he says, tell the truth: “Avoid spinning, and don’t try to ‘dress up’ an ugly situation. Acknowledge setbacks and failures, including civilian casualties, and then state how we’ll respond and what we’ve learned.” “Live our values,” he writes. “This is what distinguishes us from our enemies.”⁴²

As was the case when he was in command of US and coalition forces in Iraq, General Petraeus has long understood that there is no purely military solution to the conflict in Afghanistan, and that success on the information side is crucial to a political resolution. One hopes that this does not prove to be a mission impossible in Afghanistan.⁴³

Before turning away from drones to other examples of unmanned systems and unmanned vehicles, it should be noted that on August 3, 2010, the American Civil Liberties Union and the Center for Constitutional Rights filed a suit in a US district court seeking declaratory and injunctive relief against alleged improper US governmental interference with the right of legal representation.⁴⁴ According to the complaint, the plaintiffs were retained by Nasser Al-Aulaqi to provide legal representation in connection with the government’s reported decision to add his son, US citizen Anwar Al-Aulaqi, to its list of suspected terrorists approved for targeted killings. Regulations of the Office of Foreign Assets Control (OFAC) make it illegal for attorneys to provide legal services to any individual whose assets have been blocked on the basis of his being a terrorist without a license from OFAC. In the absence of such a license it would be a criminal offense under OFAC regulations for the plaintiffs to file a lawsuit on Anwar Al-Aulaqi’s father’s behalf seeking to protect the constitutional rights of his US citizen son.

On July 23, 2010, the plaintiffs submitted to OFAC an application to provide “uncompensated legal representation to Nasser al-Aulaqi as representative of the interests of his son, Anwar al-Aulaqi, who remains in hiding” in Yemen.⁴⁵ OFAC refused to grant the requested license. The plaintiffs contend, among other things, that they have a First Amendment right to represent clients in litigation consistent with their organizational missions.

Elsewhere in their complaint the plaintiffs make it clear that they wish to “represent Nasser al-Aulaqi in connection with the government’s reported decision to add his son to its list of suspected terrorists approved for targeted killings”⁴⁶ and plan to file a lawsuit to block the government’s plan.

On August 30, 2010, the American Civil Liberties Union and the Center for Constitutional Rights filed a lawsuit in the United States District Court for the District of Columbia on behalf of Nasser Al-Aulaqi, on his own behalf, and as “Next

Friend” of his son Anwar Al-Aulaqi seeking declaratory and injunctive relief against the US government.⁴⁷ In particular, the plaintiff sought a declaration from the court that the US Constitution and international law prohibit the government from

carrying out targeted killings outside of armed conflict except as a last resort to protect against concrete, specific and imminent threats of death or serious physical injury; and an injunction prohibiting the targeted killing of US citizen Anwar Al-Aulaqi outside this narrow context. Plaintiff also sought an injunction requiring the government to disclose the standards under which it determines whether US citizens can be targeted for death.⁴⁸

The American Civil Liberties Union and the Center for Constitutional Rights were able to file this lawsuit on Mr. Al-Aulaqi’s behalf because the Treasury Department, reversing its earlier position, granted them a license to do so. The lawsuit challenging the Treasury’s regulations is, at this writing, still pending.⁴⁹

On December 7, 2010, the District Court for the District of Columbia dismissed Nasser Al-Aulaqi’s suit in an eighty-three-page opinion on the ground of lack of jurisdiction.⁵⁰ The court ruled that the plaintiff did not have standing to bring the suit and that the political question doctrine barred the court from considering the merits of the plaintiff’s suit.

Other Unmanned Systems/Unmanned Vehicles: The Rise of Robotics

Most, some would say too much, of the present focus on the changing character of weapon systems has been on drones. It is arguable that drones are the tip of the iceberg and that in the not too distant future they will be replaced by new technological marvels created by the rising science of robotics. Because of the exponential growth of robots and their use in armed conflict, the line between science and science fiction has become ever more blurred.

Although drones are unmanned aerial vehicles, or UAVs, it is noteworthy that they are controlled by human operators, many of them located in Nevada—or at least normally they are controlled. As noted previously, one of the documents released by WikiLeaks reported that communications were lost with a Reaper drone, armed with Hellfire missiles and 500-pound bombs, in Afghanistan and it was necessary to order an F-15 fighter aircraft to shoot it down to prevent it from crossing into Tajikistan.⁵¹ There are other examples of military technology running amok.

For example, in his groundbreaking book, *Wired for War*, P.W. Singer describes the following incident:

Mission Impossible? International Law and the Changing Character of War

Just before nine in the morning on October 12, 2007, the 10th Anti-Aircraft Regiment began its role in the South African military's annual Seboka training exercise. The operation involved some five-thousand troops from seventeen other units, so the pressure was on to get everything right. But the unit's automated MK5 antiaircraft system, sporting two 35 mm cannons linked up to a computer, appeared to jam. As a follow-up report recounts, this apparently "caused a 'runaway.'" The description of what happened next is chilling. "There was nowhere to hide. The rogue gun began firing wildly, spraying high-explosive shells at a rate of 550 a minute, swinging around through 360 degrees like a high-pressure hose."

The young female officer in charge rushed forward to try to shut down the robotic gun, but, continues the report, "she couldn't, because the computer gremlin had taken over." The automated gun shot her and she collapsed to the ground. The gun's auto-loading magazines held five hundred high-explosive rounds. By the time they were emptied, nine soldiers were dead (including the officer) and fourteen seriously injured, all because of what was later called a "software glitch."⁵²

As Singer's tour de force makes clear, robots are now operating in the air, on land, and in and under the sea. An early, and crucially important, use of robots on land was as part of an explosive ordnance disposal (EOD) team that was responsible for disarming and disposing of IEDs. The robots involved in this exercise are called PackBots. They have proven to be very efficient at their jobs, and as a team's commander quoted by Singer reportedly put it, "when a robot dies, you don't have to write a letter to his mother."⁵³

The use of robots has increased exponentially. For example, in Iraq in 2003, when the US and coalition forces invaded, there were no robotic units on the ground. By the end of 2005, they numbered 2,400, and by 2008, they were estimated to reach 12,000.⁵⁴ Initially, they were used for non-killing purposes, such as disabling or destroying IEDs or for surveillance, but increasingly, like the aerial drones, they have been used to kill enemies and destroy enemy property.

For example, the TALON is a robot used in Iraq as part of an EOD team. But its manufacturer, Foster-Miller Inc., remodeled the TALON into a "killer app," the Special Weapons Observation Reconnaissance Detection System, or SWORDS. The new design allows soldiers to mount various weapons on the robot, including "an M-16 rifle, a machine gun, and a grenade or rocket launcher." Another example is the MARCBOT (Multi-Function Agile Remote-Controlled Robot). According to Singer:

One of the smallest but most commonly used robots in Iraq, the MARCBOT looks like a toy truck with a video camera mounted on a tiny, antenna-like mast. Costing only \$5,000, this miniscule bot is used to scout for enemies and to search under cars for

hidden explosives. The MARCBOT isn't just notable for its small size; it was the first ground robot to draw blood in Iraq. One unit of U.S. soldiers jury-rigged their MARCBOTs to carry Claymore anti-personnel mines. If they thought an insurgent was hiding in an alley, they would send a MARCBOT down first and, if they found someone waiting in ambush, take him out with the Claymore.⁵⁵

As Singer makes exhaustively clear, there are numerous kinds of military robots in use, including those with the capacity to kill, on land, in the air, and on or under the sea.⁵⁶ It is clear, moreover, that their numbers will continue to increase. As Singer notes,

[a]t a congressional hearing on February 8, 2000, it finally all came together for military robotics on the "demand" side. Senator John Warner from Virginia, the powerful chairman of the Senate Armed Services Committee, laid down a gauntlet, mandating into the Pentagon's budget that by 2010, one-third of all the aircraft designed to attack behind enemy lines be unmanned, and that by 2015, one-third of all ground combat vehicles be driverless.⁵⁷

After the Al-Qaeda terrorist attack on September 11, 2001, according to Singer, one robotics executive was told by his Pentagon buyers that his company should "make 'em [robots] as fast as you can."⁵⁸

For purposes of legal analysis of the legal issues these robots currently or might in the future raise, Darren Stewart has usefully broken them down into two categories: automated and autonomous.⁵⁹ "Automated" has been defined thus: "[a] society is automated when its production is dominated by machines to the extent that machines are given priority over men in the performance of human tasks."⁶⁰ This clearly is the situation envisaged by Senator Warner's mandate to the Pentagon of 2000. "Autonomous" is defined as "self-governing, independent."⁶¹

The crucial difference between the two categories of robots would seem to be that the automated robots are, at least theoretically, fully under the control of a human being, or to use the military term, there is a "human in the loop." By contrast, autonomous robots are independent of human control and, some would argue, because of artificial intelligence have become more intelligent, more capable than humans and, as a result, are better positioned to make crucial life-and-death decisions in war.⁶²

The problem, as noted by Stewart, is that at present there are no autonomous weapon systems in use, with the exception of one South Korean system used in the demilitarized zone separating the two Koreas.⁶³ Hence, only the automated robots currently raise issues of the legality of their use. For their part, possible legal issues involving the use of autonomous robots are currently a matter of pure speculation.

Mission Impossible? International Law and the Changing Character of War

By definition, automated robots have a human in the loop who has the ultimate responsibility for what the automated robot does. The human in the loop would therefore have the responsibility to ensure that in selecting its targets a military killing robot adhered to the principles of the law of armed conflict, including military necessity, proportionality and distinction, and would suffer the consequences of a failure on the part of the robot to do so. It is important to note decisions to shoot cannot be delegated to a computer.

Perhaps the most tragic example of a failure to rely on human judgment, rather than that of a computer, was the July 3, 1988 incident involving a patrol mission of the *USS Vincennes* in the Persian Gulf. On that day the radar system of the *Vincennes*, called Aegis, spotted Iran Air Flight 655, an Airbus passenger jet, flying on a consistent course and speed and broadcasting a radar and radio signal that showed it to be a civilian aircraft. The automated radar system of the *Vincennes*, however, had been designed for use against attacking Soviet bombers in the open ocean of the North Atlantic, not for dealing with skies crowded with civilian aircraft like those over the Gulf. The computer system assigned the plane an icon that on the screen made it appear to be an Iranian F-14 fighter. Singer recounts the tragic denouement of this incident:

Though the hard data were telling the human crew that the plane wasn't a fighter jet, they trusted the computer more. Aegis was in semi-automatic mode, giving it the least amount of autonomy, but not one of the 18 sailors and officers in the command crew challenged the computer's wisdom. They authorized it to fire. (That they even had the authority to do so without seeking permission from more senior officers in the fleet, as their counterparts on any other ship would have had to do, was itself a product of the fact that the Navy had greater confidence in Aegis than in a human-crewed ship without it.) Only after the fact did the crew members realize that they had accidentally shot down an airliner, killing all 290 passengers and crew, including 66 children.⁶⁴

As Yoram Dinstein notes, civilian airliners carrying civilian passengers are "singled out for special protection."⁶⁵ He cites the *Vincennes* incident, however, as an example of the reality that "the speed of modern electronics often creates grave problems of erroneous identification."⁶⁶ Singer adds, quoting retired Army colonel Thomas Adams, that the coming weapons "will be too fast, too small, too numerous, and will create an environment too complex for humans to direct."⁶⁷

If the "coming weapons" will be too complex for humans to direct, someone, or, more precisely perhaps, something, will have to take over the job. Here we enter into the murky world of artificial intelligence, or AI. And here also we move from automated robotics to autonomous robotics.

It is, however, debatable, to say the least, whether artificial intelligence will ever progress to the point where robots will be in a position to apply, on their own, such vital principles of armed conflict as military necessity, proportionality and distinction. The argument against artificial intelligence ever progressing to this point is based, at least in part, on the reality that robots lack the moral sense that humans possess, the capacity to make an empathic response, and in general the ability to draw on their humanity.

In his book, Singer quotes a senior military analyst at Human Rights Watch, a leading human rights non-governmental organization, to illustrate the problems that would be caused by the complete absence of a human element in the targeted killing environment:

“You can’t just download international law into a computer. The situations are complicated; it goes beyond black-and-white decisions.” He explains how figuring out legitimate military targets is getting more difficult in war, especially as conflict actors increasingly fight in the midst of civilian areas like cities and even use civilians for cover. Citing examples he dealt with in his own career, he asks, if a tank is parked inside a schoolyard, is it legitimate to strike? How about if it is driving out of the village and a group of children catch a ride on top?⁶⁸

There is also the tricky issue of accountability for war crimes. As Dinstein notes in his treatise, “War crimes, like all other international crimes, have two constituent elements: (a) the criminal act (*actus reus*) and (b) a criminal intent or at least a criminal consciousness (*mens rea*).”⁶⁹ But a robot has no capacity for either a criminal intent or a criminal consciousness. Moreover, as a practical matter, it would make no sense to apply criminal penalties to robots. Accordingly, even if the day may come when it will be possible to have fully autonomous robots, it will still be necessary to have a human in the loop, at least in a position of command responsibility. In other words, the robots would not be totally autonomous but subject to the commands of a human commander. As Dinstein has instructed:

A commander bears criminal responsibility not only for orders that he issues to his subordinates to commit war crimes. He is answerable for his acts of omission as much as for his acts of commission. These acts of omission relate to failure of proper supervision and control by a commander, designed to ensure that his subordinates do not perpetrate war crimes on their own initiative. Of course, the same commander may be individually accountable twice: once for having given orders to his subordinates to commit certain war crimes, and additionally for knowingly allowing them to commit other war crimes which go beyond those orders.⁷⁰

Mission Impossible? International Law and the Changing Character of War

To be sure, a commander would not be responsible for a robot deciding on its own to commit a violation of the law of armed conflict, unless he or she was aware that such violations were taking place and was in a position to take steps to exercise the necessary effective command and control to prevent or at least bring to a halt such violations. If the robot's actions were caused by a design defect, the remedy might be a civil action in tort against the manufacturer of the robot or perhaps the software engineer involved in the manufacturing process rather than a criminal proceeding.⁷¹

II. Challenges Posed by the Use of Force in Cyberspace

One challenge posed by the use of force in cyberspace may be similar to a primary issue arising out of the so-called war on terror: what is the appropriate legal regime to apply, criminal law and procedure or the law of armed conflict?⁷² In an essay, "Computer Network Attacks by Terrorists: Some Legal Dimensions," published in 2002, I suggested that "the applicable legal regime becomes international criminal law rather than provisions of the UN Charter governing the use of force and the maintenance of international peace and security."⁷³ My conclusion at that time, however, was premised on the assumption that the use of force in cyberspace did not involve State sponsorship of the terrorist attack or any other kind of State involvement in the attack. Recent developments call into question the validity of this assumption.

To be sure, another conclusion I reached in my 2002 essay remains true today: the majority of computer network attacks "may cause disruption of vital systems leading to widespread inconvenience, possibly to some degree of public alarm, but . . . do not directly threaten life."⁷⁴ But recent computer network attacks have been very disruptive indeed. For example, Google, the world's largest Internet search engine, announced in January 2010 that it had been targeted by hackers in 2009, and that the attacks resulted in breaches of its security infrastructure and theft of Google's intellectual property and other data.⁷⁵ What made this attack especially disturbing for the US government was that Google traced the attacks to hackers operating out of China.⁷⁶ Many have insinuated that the Chinese government participated in the attacks, especially because the attacks included the hacking of e-mail accounts belonging to Tibetan human rights activists and journalists,⁷⁷ but there is no conclusive evidence of the Chinese government's involvement in the attacks.

China is not the only traditional economic and military adversary of the United States that has been linked to cyber attacks in recent years. Hackers located in Russia carried out an attack on several of Estonia's government websites in 2007, prompting many to conclude that the Russian government was either formally or

informally behind the attacks.⁷⁸ The attacks came in successive waves, first compromising the Estonian government sites, then infiltrating newspapers, television stations, schools and banks within the country.⁷⁹ The Russian government denied any involvement in the cyber disruptions, but the timing was very suspicious because the attacks occurred the same day that Estonia removed a Soviet-era war monument from the center of its capital city, Tallinn, a controversial move that was preceded by months of diplomatic tensions between the two countries and caused protestors in Moscow to stage several protests.⁸⁰ The Russian government was again implicated in computer attacks in 2008 when Georgia's Internet infrastructure was barraged with "denial of service" attacks that crippled many of its main governmental websites.⁸¹ As the timing of the cyber attacks coincided exactly with Russia's military incursion into Georgia, the Georgia government accused Russia of carrying out the cyber attacks in coordination with its physical military operations.⁸²

In addition to US businesses, vital US national defense agencies have been attacked in recent years.⁸³ For example, the Department of Defense was the target of computer network attacks in 1998, 2003 and 2007, when classified information was stolen.⁸⁴ The perpetrators of these attacks were deemed "unknown foreign intruders," but many commentators suggested the presence of Chinese or Russian footprints, especially since these types of attacks on US national defense systems are thought to be possible only through foreign State participation.⁸⁵

It is, however, difficult to respond to cyber attacks when it is uncertain who or what has engaged in the attack. Hence, the current emphasis appears to be on bolstering US cyber security and protecting US infrastructure from intrusions from criminal hackers, State actors and terrorists. For example, President Barack Obama is continuing to implement the Comprehensive National Cybersecurity Initiative that was created by the George W. Bush administration.⁸⁶ This program is intended to unify the efforts of various government agencies to protect commercial and governmental cyber security, and increase our preparedness for potential attacks. Goals for this initiative include building an international framework to address computer network attacks and the creation of an identity management strategy that would balance the privacy and security interests of individual Internet users.

Despite these efforts, current evidence indicates that the United States is not up to the task of preventing or mitigating the damage of a large-scale computer network attack. In early 2010 the Pentagon conducted a simulated computer attack aimed at paralyzing the country's power grids, communications systems and financial networks to see how the government might respond; the results were not encouraging.⁸⁷ According to military officers who participated in the simulation,

Mission Impossible? International Law and the Changing Character of War

the “enemy had all the advantages: stealth, anonymity and unpredictability.”⁸⁸ No one could pinpoint which country the attack originated from, thus eliminating the possibility of any retaliatory action, and the legal authorization to respond to the attack was unclear because no one could determine “if the attack was an act of vandalism, an attempt at commercial theft, or a State-sponsored effort to cripple the United States, perhaps as a prelude to a conventional war.”⁸⁹

If, and this is a big if, it proves possible to prove that the cyber attack was State-sponsored, the issue of whether it constituted an “armed attack” within the meaning of Article 51 of the UN Charter may arise and, even if it amounts to an armed attack, the kind of response that would meet the criteria of necessity and proportionality could be difficult to determine. Presumably, if the attack resulted in bringing down power stations, refineries, banks and air traffic control systems with resultant loss of life and property, this would constitute an armed attack, but absent such destructive effect, the case is less clear. In his article in this volume, Michael Schmitt has pointed out that in the cyber attack on Georgia there was no loss of life or property.⁹⁰

As the *Economist* has recently noted, “there are few, if any, rules in cyberspace of the kind that govern behavior, even warfare, in other domains.”⁹¹ To remedy this lacuna, the *Economist* suggests that States start talking about arms control on the Internet. Talks have already begun, but it is not clear how successful they will be. In another forum I have tried to identify some of the dimensions of the problem:

In the introduction to this study, it is suggested that the rapidity of change in modern life creates great instability and even chaos in some situations. The rapidity of change is particularly pronounced in the technological and scientific arenas whose considerable complexity makes it difficult for the slow-moving treaty process to adapt. A recent example of this problem is the dispute between the United States and Russia over how to counter cyberwar attacks that could wreak havoc on computer systems and the Internet. Russia favors an international treaty along the lines of those negotiated for chemical weapons and has pushed hard for that approach. The United States, however, argues that a treaty is unnecessary and instead advocates improved cooperation among international law enforcement groups. In the U.S. view, if these groups cooperate to make cyberspace more secure against criminal intrusions, this will also make cyberspace more secure against military campaigns. Trying to reach common ground over an approach is complicated, given that a significant proportion of the attacks against American targets are coming from China and Russia. Also, Russian calls for broader international oversight of the Internet have met strong U.S. resistance to agreements that would allow governments to censor the Internet because they would provide cover for totalitarian regimes. The United States argues further that a treaty would be ineffective because it can be impossible to determine if an Internet attack originated from a government, a hacker loyal to that government, or a rogue acting independently. The unique challenge of cyberspace is that governments can carry out

deceptive attacks to which they cannot be linked. After computer attacks in Estonia in April 2007 and in the nation of Georgia in August 2008, the Russian government denied involvement and independent observers said the attacks could have been carried out by nationalist sympathizers or by criminal gangs. Although the United States and Russia have failed to reach agreement on the proper approach to counter cyberwar attacks, arms control experts say that major governments are reaching a point of no return in heading off a cyberwar arms race.⁹²

The United States and Russia have been talking about the possibility of entering into a bilateral agreement. Even if they are able to overcome the obstacles to reaching agreement between them, it is highly unlikely it would prove possible to conclude a global agreement. This is because since the early 1990s it has proven almost impossible to get agreement among the now almost two hundred member States of the world community on global treaties to deal with the severest problems facing humanity, such as climate change, nuclear proliferation, terrorism, pandemics, trade protectionism and many more.⁹³ Perhaps reflecting an awareness of this difficulty, the *Economist* has suggested “more modest accords, or even just informal ‘rules of the road’ that would raise the political cost of cyber-attacks.” Examples might include

a deal to prevent the crude “denial-of-service” assaults that brought down Estonian and Georgian websites with a mass of bogus requests for information; NATO and the European Union could make it clear that attacks in cyberspace, as in the real world, will provoke a response; the UN or signatories of the Geneva Conventions could declare that cyber-attacks on civilian facilities are, like physical attacks with bomb and bullet, out of bounds in war⁹⁴

Whether these or other more “modest” steps would be effective or lead to formal, “legal” arrangements to establish an arms control regime for cyberspace is debatable.

Moreover, it is important to recognize that although terrorist groups such as Al-Qaeda are not thought to possess enough technological capability at present (without State support) to carry out a major cyber attack that would result in loss of life and property, it is envisioned that within the next decade they could pose such a threat.⁹⁵ Al-Qaeda and its ilk, of course, will not recognize the legitimacy of either modest, informal or formal legal arrangements to establish an arms control regime for cyberspace. They also will enjoy certain advantages because of the asymmetric nature of armed conflict in cyberspace. They will be able to launch a cyber attack from any place they may be located while disguising their location through various computer moves. Applying the principles of military necessity, proportionality and distinction against terrorist cyber attacks will be especially

Mission Impossible? International Law and the Changing Character of War

challenging since the terrorists may be even more heavily embedded in the civilian population than usual when launching attacks. William J. Lynn III, US Deputy Secretary of Defense, recently pointed out some of the advantages enemies of the United States enjoy in asymmetric cyber warfare:

The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target. Knowing this, many militaries are developing offensive capabilities in cyberspace, and more than 100 foreign intelligence organizations are trying to break into U.S. networks. Some governments already have the capacity to disrupt elements of the U.S. information infrastructure.

In cyberspace, the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks' weaknesses. Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyberwarfare is like maneuver warfare, in that speed and agility matter most. To stay ahead of its pursuers, the United States must constantly adjust and improve its defenses.⁹⁶

Later in his essay Lynn notes that it will be necessary to adopt a new approach to deterrence, expresses doubts about the feasibility of traditional arms control regimes, and suggests the need for a new approach to international behavior in cyberspace:

Given these circumstances, deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation. The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace. (Traditional arms regimes would likely fail to deter cyberattacks because of the challenges of attribution, which make verification of compliance almost impossible. If there are to be international norms of behavior in cyberspace, they may have to follow a different model, such as that of public health or law enforcement.)⁹⁷

In short the legal and technological challenges the United States faces in responding effectively to the asymmetric nature of cyber warfare are daunting, and success is not assured. Meeting these challenges is especially difficult when US

forces are forced to adopt a purely defensive posture. In traditional armed conflict, it is the offensive power of the US military that affords it such a marked advantage. As the various panels at the conference demonstrated, however, in asymmetric warfare the United States, more often than not, finds itself on the defensive. The next, and concluding, section of this article considers a few more dimensions of the asymmetry problem and the impact they have on the chances of US forces succeeding in their mission.

III. The Multifaceted Nature of Asymmetric Warfare

As Professor Wolff Heintschel von Heinegg points out,⁹⁸ one of a number of possible definitions of asymmetric warfare is that it is warfare where one of the parties to the armed conflict tries to compensate for its perceived disadvantages vis-à-vis the other party or parties by adopting methods and strategies that are clear violations of the law of armed conflict, e.g., perfidy, suicide bombings and the use of human shields, especially civilians. What is particularly disturbing about asymmetric warfare is that violators of the law of armed conflict gain considerable military advantage in many instances by the adoption of such tactics because they can be extremely effective in countering the normally vastly superior military capabilities of the other party.

Both in Iraq and in Afghanistan the enemy consists of insurgents who embed themselves into the civilian populations, a clear violation of the law of armed conflict. In Iraq a standard tactic of the insurgents was to use children as human shields in firefights with US and coalition forces. In Afghanistan, as noted earlier in this article, there have been sharp factual disputes between NATO and local residents over whether NATO air raids have resulted in civilian deaths, as alleged by the local residents, or, as contended by NATO, in the deaths of insurgents who had opened fire on NATO forces before they were killed.⁹⁹ Regardless of which side is correct in this debate, the result has been a substantial reduction in the number of airstrikes.

General Charles Dunlap, a retired US Air Force judge advocate, regards the decision in Afghanistan to sharply reduce the number of airstrikes as a serious mistake. He contends that “it is often overlooked that during the surge [in Iraq], thousands of insurgents were captured or killed by American special operation forces and airstrikes. I do believe, firmly, that the much-derided killing and capturing actually was the key to success.”¹⁰⁰ In support of his argument Dunlap adds that during the Iraq surge, airstrikes increased to five times previous levels.

US military officers in Afghanistan counter these arguments by claiming that special operations raids in 2010 resulted in the deaths of hundreds of militant leaders, while the restrictions on airpower saved Afghan lives and improved

Mission Impossible? International Law and the Changing Character of War

relations with the government. Others argue that the Iraqis themselves were responsible for the reduction of violence: Sunni insurgents who turned against Al-Qaeda, and Shiite militias who embraced a ceasefire with the Sunni.¹⁰¹ For his part, James Dubik, a retired lieutenant general who oversaw the training of the Iraqi military during the surge, reportedly stated: “The decisiveness of the surge came from an aggregate of factors—more like a thunderstorm than a single cause and effect.”¹⁰² He believes that General Petraeus will look for the same aggregate effect in Afghanistan.

In both Iraq and Afghanistan, however, as well as more generally in the worldwide conflict (no longer “war”) with Al-Qaeda and affiliated terrorist groups, the struggle for “hearts and minds” or, if one prefers, the “propaganda war” is of crucial importance. And as indicated earlier in this article, it appears that the enemy has been able to counter the advantages that the United States and its allies would normally enjoy. Perhaps the most recent example of this is the apparent impact of the current debate in the United States over whether a mosque should be permitted to be built in the vicinity of where the Twin Towers were destroyed on 9/11. Some exceedingly inflammatory negative remarks about Islam made by some opponents of building the mosque in that vicinity have reportedly resulted in significant increases in the number of recruits for Al-Qaeda. The First Amendment protects such remarks, but unwittingly they constitute grist for Al-Qaeda’s propaganda mill.

At this writing, the papers are full of still another dispute between NATO and Afghan officials over the results of a NATO airstrike.¹⁰³ According to Afghan officials, the airstrike hit the election convoy of an Afghan parliamentary candidate, wounding him and killing as many as ten campaign aides. But the NATO version is that the strike killed a senior militant leader. US Secretary of Defense Robert Gates, who was visiting Afghanistan at the time, reportedly stated that the airstrike targeted and killed a “very senior official” from the Islamic Movement of Uzbekistan, or IMU, a militant group the United States has designated as a terrorist organization.¹⁰⁴ NATO officials said that the airstrike killed and injured up to twelve insurgents after NATO forces identified several armed men in a sedan that was part of a six-car convoy. Only the sedan was hit, they said.

There seems to be no current mechanism in Afghanistan for resolving these disputes over the results of NATO airstrikes. But there also seems to be little doubt that, regardless of their veracity, frequent reports of attacks resulting in civilian casualties are undermining the counterinsurgency effort, which is aimed at protecting the population and shoring up support for the Afghan government.

Two other factors loom large when one is considering the problem of civilian deaths arising from the armed conflict in Afghanistan. The first, as noted before, is

the difficulty in distinguishing between combatants and civilians in asymmetric warfare. The second, it is important to note, is that the United Nations has reported that 70 percent of civilians who die in violence in Afghanistan are killed by insurgents.¹⁰⁵

Yet it is always the United States and NATO who are on the defensive when claims of civilian casualties are raised. In his concluding remarks at the conference, Yoram Dinstein deplored this constantly defensive posture. As he pointed out, the enemy has successfully engaged in lawfare, the use and abuse of legal argument, to leave the impression that the law of armed conflict demands there be *no* civilian casualties. It does not, of course, and this reality should be aggressively brought home to the people of Afghanistan and elsewhere. It should also be brought home to them that the enemy constantly engages in lawless behavior and, as pointed out by the United Nations, consistently kills its own civilians in armed conflict. Dinstein's call for the United States and its allies to abandon their defensive posture and take the offense to demonstrate, stressing their own efforts to comply with the law of armed conflict, the lawlessness and brutality of Al-Qaeda, the Taliban and their ilk is compelling.¹⁰⁶

The enemies in both Iraq and Afghanistan are insurgents, and the United States and its allies are involved in counterinsurgency in both countries. General Petraeus was in charge of the counterinsurgency in Iraq and has now assumed a similar role in Afghanistan. He was, moreover, the primary architect of the 2006 *U.S. Army/Marine Corps Counterinsurgency Field Manual*.¹⁰⁷ The Manual, regarded as the "bible" of counterinsurgency, raises the crucial issue of the time required for a well-run counterinsurgency strategy to work. Sara Sewall, a former Pentagon official who wrote the introduction to the University of Chicago edition of the manual, for one is skeptical that the US public will be willing to "supply greater concentrations of forces, accept higher casualties, fund serious nation-building and stay many long years to conduct counterinsurgency by the book."¹⁰⁸ In light of current developments, with the withdrawal of all US combat troops from Iraq—amid indications that the Iraqi army and police may not be able to provide adequate security on their own¹⁰⁹—and a plan to start withdrawing combat troops from Afghanistan in the summer of 2011, Sewall's skepticism would appear well justified.

Notes

1. See Raul A. "Pete" Pedrozo, *Use of Unmanned Systems to Combat Terrorism*, which is Chapter IX in this volume, at 217, 218–19.

2. See Mary Ellen O'Connell, *Unlawful Killing with Combat Drones: A Case Study of Pakistan, 2004–2009*, at 8 (Notre Dame Law School Legal Studies Research Paper No. 09-43, 2010), available at <http://ssrn.com/abstract=1501144>.

Mission Impossible? International Law and the Changing Character of War

3. *Id.*
4. See Pedrozo, *supra* note 1, at 240.
5. See Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Study on Targeted Killings*, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston), available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf> [hereinafter Study on Targeted Killings].
6. For discussion of the distinction between war criminals and unlawful combatants, see YORAM DINSTEIN, *THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT* 266–70 (2d ed. 2010).
7. See Study on Targeted Killing, *supra* note 5, ¶ 72.
8. I am indebted to Professor Michael N. Schmitt of Durham University Law School in the United Kingdom for this observation.
9. *Id.*
10. Article 43(2) of Additional Protocol I provides: “Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.” Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.
11. See Matthew Green, *Chilling view of conflict exposed*, FINANCIAL TIMES, July 27, 2010, at 2.
12. *Id.*
13. Richard A. Oppel Jr. & Taimoor Shah, *Afghans Say Attack Killed 52 Civilians; NATO Differs*, NEW YORK TIMES, July 27, 2010, at A4.
14. John F. Murphy, *Afghanistan, Hard Choices and the Future of International Law*, 39 ISRAEL YEARBOOK ON HUMAN RIGHTS 69, 91–92 (2009).
15. Green, *supra* note 11.
16. In response to reports that a NATO attack on July 23, 2010 allegedly killed fifty-two civilians, President Hamid Karzai reportedly condemned the attack as “both morally and humanly unacceptable,” and the Afghan government issued a statement saying “success over terrorism does not come with fighting in Afghan villages, but by targeting its sanctuaries and financial and ideological sources across the borders.” Oppel & Shah, *supra* note 13.
17. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, *MANUAL ON INTERNATIONAL LAWS APPLICABLE TO AIR AND MISSILE WARFARE* (2009), available at <http://ihlresearch.org/amw/HPCR%20Manual.pdf>.
18. I am indebted to Professor Schmitt for bringing this argument to my attention.
19. DINSTEIN, *supra* note 6, at xiii & 26.
20. *Id.* at 26.
21. *Id.* at 27.
22. *Id.*
23. *Hamdan v. Rumsfeld*, 548 U.S. 557, 630–31 (2006).
24. DINSTEIN, *supra* note 6, at 56.
25. Michael N. Schmitt, *The United States Supreme Court and Detainees in the War on Terror*, 37 ISRAEL YEARBOOK ON HUMAN RIGHTS 33, 68 (2007).
26. See DAVID LUBAN, JULIE R. O’SULLIVAN & DAVID P. STEWART, *INTERNATIONAL AND TRANSNATIONAL CRIMINAL LAW* 1060, 1063 n.2 (2010).
27. Schmitt, *supra* note 25, at 69.
28. *Id.* at 67 n.134.

29. See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609.

30. Prosecutor v. Tadic, Case No. IT-94-1-AR72, Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

31. *Id.*, ¶ 70.

32. *Id.*, ¶¶ 67, 70.

33. See Pedrozo, *supra* note 1, at 219–27.

34. Article 51 of the UN Charter provides in pertinent part: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”

35. For discussion of some of these issues, see John F. Murphy, *Force and Arms*, in 1 UNITED NATIONS LEGAL ORDER 247, 257–70 (Oscar Schachter & Christopher C. Joyner eds., 1995).

36. Quoted in J. MOORE, DIGEST OF INTERNATIONAL LAW 412 (1906).

37. It is noteworthy that Yoram Dinstein is of the view that “reliance on that [*Caroline*] incident is misplaced.” YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 184 (4th ed. 2005). Among the reasons given to support this view is that “[t]here was nothing anticipatory about the British action against the *Caroline* steamboat on US soil, inasmuch as use of the *Caroline* for transporting men and materials across the Niagara River—in support of an anti-British rebellion in Canada—had already been in progress.” *Id.* at 184–85.

38. Quoted in Pedrozo, *supra* note 1, at 242.

39. *Id.* 246–48.

40. See Richard A. O'Connell Jr. & Rod Nordland, *Petraeus to Expand Efforts to Protect Afghan Civilians*, NEW YORK TIMES, Aug. 4, 2010, at A10.

41. *Id.*

42. *Id.*

43. On August 4, 2010, the *New York Times* reported that Pakistan's President, Asif Ali Zardari, was quoted in *Le Monde*, a leading French newspaper, as saying that coalition forces were losing the war in Afghanistan because they had “lost the battle to win hearts and minds” of Afghans, and that the Taliban's success lay “in knowing how to wait” for NATO forces to withdraw. See John F. Burns, *Afghan War Is Being Lost, Pakistani President Says*, NEW YORK TIMES, Aug. 4, 2010, at A8.

44. American Civil Liberties Union, American Civil Liberties Union Foundation, and Center for Constitutional Rights v. Timothy F. Geithner, Secretary of the Treasury and Adam J. Szubin, Director of the Office of Foreign Asset Control, Complaint for Declaratory and Injunctive Relief, United States District Court for the District of Columbia, Aug. 3, 2010, available at <http://www.aclu.org/files/assets/2-OFACComplaintFinal.pdf>.

45. *Id.* at 3.

46. *Id.* at 9.

47. Nasser Al-Aulaqi v. Barack H. Obama, Leon C. Panetta, and Robert M. Gates, Complaint for Declaratory and Injunctive Relief, No. 10-cv-01469 (D.D.C. Aug. 30, 2010), available at <http://www.aclu.org/national-security/al-aulaqi-v-obama-complaint>.

48. *Id.*, ¶ 6.

49. See Scott Shane, *Rights Groups Sue U.S. on Effort to Kill Cleric*, NEW YORK TIMES, Aug. 31, 2010, at A6.

50. Nasser Al-Aulaqi v. Barack H. Obama, Robert M. Gates, and Leon E. Panetta, 727 F. Supp. 2d 1 (2010).

Mission Impossible? International Law and the Changing Character of War

51. See *supra* text accompanying note 11.
52. P.W. SINGER, WIRED FOR WAR 196 (2009).
53. P.W. Singer, *Robots at War: The New Battlefield*, WILSON QUARTERLY, Winter 2009, at 30, available at <http://www.wilsonquarterly.com/article.cfm?aid=1313>.
54. *Id.*
55. *Id.*
56. See SINGER, *supra* note 52. Between pages 308 and 309, Singer has inserted pictures of, and commentary on, a great variety of robots in many different situations. See also Singer, *supra* note 53, for extensive commentary on the different kinds of robots.
57. SINGER, *supra* note 52, at 59.
58. *Id.*
59. See Darren M. Stewart, *New Technology and the Law of Armed Conflict*, which is Chapter X in this volume, at 271, 273–84
60. See OXFORD ENGLISH DICTIONARY 320–21 (2d ed. 1989), quoting the November 1962 *Catholic Gazette*.
61. *Id.*
62. See generally Singer, *supra* note 53, who quotes various military officers and defense officials.
63. See Stewart, *supra* note 59, at 281.
64. Singer, *supra* note 53.
65. See DINSTEIN, *supra* note 6, at 117, citing H.B. Robertson, *The Status of Civil Aircraft in Armed Conflict*, 27 ISRAEL YEARBOOK ON HUMAN RIGHTS 113, 126 (1997).
66. *Id.*
67. Singer, *supra* note 53.
68. SINGER, *supra* note 52, at 389, quoting Marc Garlasco of Human Rights Watch.
69. DINSTEIN, *supra* note 6, at 279.
70. *Id.* at 271. As Dinstein notes, *id.* at 276, the most recent international instrument dealing with command responsibility is the Rome Statute of the International Criminal Court, which provides in Article 28:

In addition to other grounds of criminal responsibility under this Statute for crimes within the jurisdiction of the Court:

1. A military commander or person effectively acting as a military commander shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control, or effective authority and control as the case may be, as a result of his or her failure to exercise control properly over such forces, where:

- (a) That military commander or person either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes; and

- (b) That military commander or person failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution.

2. With respect to superior and subordinate relationships not described in paragraph 1, a superior shall be criminally responsible for crimes within the jurisdiction of the Court committed by subordinates under his or her effective authority and control, as a result of his or her failure to exercise control properly over such subordinates where:

- (a) The superior either knew, or consciously disregarded information which clearly indicated, that the subordinates were committing or about to commit such crimes;
- (b) The crimes concerned activities that were within the effective responsibility and control of the superior; and
- (c) The superior failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution.

Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.

71. See, on this point, SINGER, *supra* note 52, at 389.

72. For consideration of this issue as it applies to the “new terrorism,” see John F. Murphy, *Challenges of the “New Terrorism,”* in ROUTLEDGE HANDBOOK OF INTERNATIONAL LAW 281, 284 (David Armstrong ed., 2009).

73. John F. Murphy, *Computer Network Attacks by Terrorists: Some Legal Dimensions*, in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 323, 327 (Michael N. Schmitt & Brian T. O’Donnell eds., 2002) (Vol. 76, US Naval War College International Law Studies).

74. *Id.*

75. See John Markoff, *Google Asks Spy Agency for Help with Inquiry into Cyberattacks*, NEW YORK TIMES, Feb. 4, 2010, at A6.

76. See Miguel Helft & John Markoff, *In Rebuke of China, Focus Falls on Cyber Security*, NEW YORK TIMES, Jan. 13, 2010, at A1.

77. *Id.*

78. See Steven Lee Myers, *‘E-stonia’ Accuses Russia of Computer Attacks*, NYTIMES.COM (May 17, 2007), <http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html>.

79. *Id.*

80. *Id.*

81. See John Markoff, *Before the Gunfire, Cyberattacks*, NYTIMES.COM (Aug. 12, 2008), <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

82. *Id.*

83. See Interview by Terry Gross, National Public Radio, with James Lewis, *Assessing the Threat of Cyberterrorism* (Feb. 10, 2010), transcript available at <http://www.npr.org/templates/transcript/transcript.php?storyId=123531188> [hereinafter Lewis Interview].

84. *Id.*

85. *Id.*

86. See John Markoff, *U.S. to Reveal Rules on Internet Security*, NEW YORK TIMES, Mar. 1, 2010, at A14.

87. See David Sanger, *In Digital Combat, U.S. Finds No Easy Deterrent*, NEW YORK TIMES, Jan. 25, 2010, at A1.

88. *Id.*

89. *Id.*

90. See Michael Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, which is Chapter V in this volume, at 89, 97.

91. *Cyberwar*, ECONOMIST, July 3, 2010, at 11.

92. JOHN F. MURPHY, *THE EVOLVING DIMENSIONS OF INTERNATIONAL LAW: HARD CHOICES FOR THE WORLD COMMUNITY* 266–67 (2010).

93. See, in this connection, *id.* at 267–68.

94. *Cyberwar*, *supra* note 91, at 11–12.

95. See Lewis Interview, *supra* note 83.

Mission Impossible? International Law and the Changing Character of War

96. William J. Lynn III, *Defending a New Domain*, FOREIGN AFFAIRS, Sept.–Oct. 2010, at 97, 98–99.

97. *Id.* at 99–100.

98. See Wolff Heintschel von Heinegg, *Asymmetric Warfare: How to Respond?*, which is Chapter XVII in this volume, at 463, 470–73.

99. See Alissa J. Rubin, *In Afghanistan, More Attacks on Officials and a Protest Over a Deadly NATO Raid*, NEW YORK TIMES, Aug. 19, 2010, at A6, col. 1.

100. As quoted in Julian E. Barnes, *Battle Centers on Surge*, WALL STREET JOURNAL, Aug. 27, 2010, at A9.

101. *Id.*

102. As quoted in *id.*

103. See Adam B. Ellick & Sangar Rahimi, *Accounts Differ on Strike by NATO in Afghanistan*, NEW YORK TIMES, Sept. 3, 2010, at A6; Maria Abi-Habib, Julian E. Barnes & Habib Totakhil, *Deaths Disputed in Afghan Airstrike*, WALL STREET JOURNAL, Sept. 3, 2010, at A8.

104. See Abi-Habib, Barnes & Totakhil, *supra* note 103.

105. See Ellick & Rahimi, *supra* note 103.

106. See Yoram Dinstejn, *Concluding Remarks: LOAC and Attempts to Abuse or Subvert It*, which is Chapter XVIII in this volume, at 483.

107. HEADQUARTERS, DEPARTMENT OF THE ARMY & HEADQUARTERS, MARINE CORPS COMBAT DEVELOPMENT COMMAND, FM 3-24/MCWP 3-33.5, THE U.S. ARMY/MARINE CORPS COUNTERINSURGENCY FIELD MANUAL (University of Chicago Press 2007) (2006).

108. Sarah Sewall, *A Radical Field Manual*, *Introduction to id.* at xxi, xxxviii–xxxix.

109. See Steven Lee Myers & Duraid Adnan, *Attack Shows Lasting Threat to U.S. in Iraq*, NEW YORK TIMES, Sept. 6, 2010, at A1.