10-1-2013

Non-State Armed Groups and Technology: The Humanitarian Tragedy at Our Doorstep?

Colonel Dave Wallace

Major Shane Reeves

ARTICLE

Non-State Armed Groups and Technology: The Humanitarian Tragedy at Our Doorstep?

Colonel Dave Wallace & Major Shane Reeves [*]

Abstract

Technological advances are altering the contemporary asymmetric conflicts between non-state armed groups and state actors. This article discusses the humanitarian consequences of these changing conflicts by first illustrating the dangers posed by non-state armed groups gaining access to advanced technologies. A subsequent examination of the increasing ability of non-state armed groups to use new technologies, such as cyber operations, to mitigate state actor advantages and the resultant risks to civilian populations follows. The article concludes that the humanitarian challenges presented by this growing intimacy between non-state armed groups and technology, whether through a potentially devastating attack or by the dramatic erosion to the principle of distinction, are immense and cannot be ignored.

> *In most wars, the same laws and principles hold true for each contending side. What varies is the way each opponent uses them, according to his ability, his particular situation, and his relative strength. Conventional war belongs to this general case. Revolutionary war, on the other hand, represents an exceptional case not only because, as we suspect, it has its special rules, different from those of the conventional war, but also because most of the rules applicable to one side do not work for the other. In a fight between a fly and a lion, the fly cannot deliver a knockout blow and the lion cannot fly. It is the same war for both camps in terms of space and time, yet there are two distinct 'warfare's—the revolutionary's and, shall we say, the counterrevolutionary's.*[1]

· Colonel Dave Wallace is a Professor and the Deputy Head, Department of Law at the United States Military Academy, West Point, New York. Major Shane Reeves is an Assistant Professor at the United States Military Academy, West Point. The views expressed here are their personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from their academic research of publicly available sources, not from protected operational information.

[1] DAVID GALULA, COUNTERINSURGENCY WARFARE: THEORY AND PRACTICE xii-xiii (Praeger Sec. Int'l 2006) (1964).

Table of Contents

I. INTRODUCTION

The paradoxes and dilemmas of armed conflict are constant[1] with these contradictions and puzzles readily apparent in asymmetrical warfare**.** Asymmetric warfare is defined as "leveraging inferior tactical or operational strength against the vulnerabilities of a superior opponent to achieve a disproportionate effect with the aim of undermining the opponent's will in order to achieve the asymmetric actor's strategic objectives."[2] The phenomenon, and challenge, of asymmetrical warfare is certainly not new: the earliest recorded example is contained in the Old Testament of the Bible as the fight between David and Goliath.[3]

Non-state armed groups practice asymmetric warfare, to a great extent, as a result of the technological superiority historically enjoyed by state actors.[4] However, state actors increasingly do not have a monopoly on advanced technologies as "globalization has transformed the process of technological innovation while lowering entry barriers for a wider range of actors to acquire

[1] MICHAEL L. GROSS, MORAL DILEMMAS OF MODERN WARFARE – TORTURE, ASSASSINATION, AND BLACKMAIL IN THE AGE OF ASYMMETRIC CONFLICT 21 (Cambridge Press, 2010).

[2] Kenneth F. McKenzie Jr., *The Rise of Asymmetric Threats: Priorities for Defense Planning, in* NAT'L DEF. UNIV., QDR 2001 STRATEGY-DRIVEN CHOICES FOR AMERICA'S SECURITY 75, 76 (Michele A. Flournoy ed., 2001).

[3] K.C. Dixit, *The Challenges of Asymmetric Warfare*, Institute for Defense Studies and Analysis, IDSA Comment, (Mar. 9, 2010), http://www.idsa.in/idsacomments/TheChallengesofAsymmetricWarfare_kcdixit_090310.

[4] *See, e.g.,* U.S. DEP'T OF ARMY, FIELD MANUAL 3–24/U.S. MARINE CORPS WARFIGHTING PUBLICATION 3–33.5, COUNTERINSURGENCY ix (2006) [hereinafter FM 3–24] ("The United States possesses overwhelming conventional military superiority. This capability has pushed its enemies to fight U.S. forces unconventionally, mixing modern technology with ancient techniques of insurgency and terrorism. Most enemies either do not try to defeat the United States with conventional operations or do not limit themselves to purely military means.").

advanced technologies."[5] As a result "non-state actors continue to gain influence and capabilities that, during the past century, remained largely the purview of states."[6] This unprecedented access to advanced technologies most likely is not enough to alter non-state armed groups' adherence to asymmetric warfare, but it does provide new ways for these groups to leverage their limited strengths "against the vulnerabilities of [their] superior opponent" in order to eventually achieve their strategic objectives.[7]

Regardless of potential access to new technologies, non-state armed groups are cognizant that state actors currently retain a technological advantage. This advantage is not insignificant as state actors are able to use technology to tip the scales heavily in their favor in contemporary military operations.[8] Non-state armed groups are therefore constantly searching for effective counter measures to minimize the technological superiority of the state actor. Perhaps nothing is more effective as a mitigation measure than a non-state armed group's willingness to ignore the Law of War's[9] sacrosanct protections for the civilian population and civilian objects[10] in order to reduce their operational

---

[5] U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT EXECUTIVE SUMMARY iv, (2010) *available at* http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf [hereinafter QDR].

[6] *Id.*

[7] McKenzie Jr., *supra* note 3, at 76. In asymmetric warfare the 'weaker' actor will maximize the use of their limited resources in order to negatively impact the psychological strength of the 'stronger' actor. *Id*. As non-state armed groups acquire advanced technology, they will most likely attempt to "compensate for material or other deficiencies" by using previously unattainable weaponry to affect the morale and will of the state actor. *Id*. at 77.

[8] *See, e.g.,* Gregory Viscusi & David Lerman, *French Air Power Begins, Ends NATO Campaign Over Libya With Sarkosky's Help*, BLOOMBERG (Oct. 20, 2011), http://www.bloomberg.com/news/2011-10-20/french-air-power-begins-ends-nato-air-campaign-over-libya.html (describing the critical importance of NATO air superiority in the toppling of the Qaddafi regime); Mark Mazzetti, Eric Schmitt, & Robert F. Worth, *Two Year Manhunt Led to Killing of Awlaki in Yemen*, N.Y. TIMES, Sept. 30, 2011, http://www.nytimes.com/2011/10/01/world/middle east/anwar-al-awlaki-is-killed-in-yemen.html?pagewanted =all (discussing the lethal capabilities of the U.S. drone program).

[9] *See* U.S. DEP'T OF DEF., DIRECTIVE 2311.01E: DOD LAW OF WAR PROGRAM, ¶ 3.1 (2006), *available at* http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf (defining the law of war as the part of international law that regulates the "conduct of armed hostilities" and is often called "the law of armed conflict"). The law of war, the law of armed conflict, and international humanitarian law are interchangeable. For the remainder of this article, we will use the term "law of war" as this traditional term clearly notates the *lex specialis* that governs during a time of armed conflict.

[10] *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] ("In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives . . . .").

risks.[11]

Exacerbating this humanitarian problem is the growing ability of non-state armed groups to discreetly and effectively conduct on-going operations while living amongst unsuspecting civilian populations. Advanced technology, and, in particular the rapid evolution of cyberspace, allows these groups to disperse widely across the globe without degrading their capabilities or agenda.[12] The threat to longstanding international norms and civilian populations by these tactics is obvious. Similarly, as non-state armed groups gain access to significantly advanced and lethal technology, they will not hesitate to target civilian populations if they believe this will exploit the weakness of their superior state actor foes.[13] The humanitarian consequences of non-state armed groups trying to "level the playing field" with state actors by either pursuing, or mitigating, advanced technology are therefore potentially devastating.

To support these propositions this article will first illustrate the humanitarian concerns posed by non-state armed groups gaining access to advanced technologies. A discussion of the erosion of civilian protections by non-state armed groups in an asymmetric war and the subsequent humanitarian risks will follow. Finally, the article will briefly summarize the uncertain humanitarian challenges facing the international community by the arrival of ever increasing advanced technology.

II. HOW ARMED GROUPS USE NEW TECHNOLOGY AND WHY

Asymmetric warfare encompasses a wide scope of theory, experience, conjecture, and definition. The underlying premise is that asymmetric warfare deals with unknowns, with surprise in terms of ends, ways, and means. As Professor Michael Schmitt insightfully notes, the asymmetry of warfare has

---

[11] *See, e.g.*, Human Rights Council, *Human Rights in Palestine and Other Occupied Arab Territories: Report of the United Nations Fact Finding Mission on the Gaza Conflict*, ¶¶ 439–98. U.N. Doc. A/HRC/12/48 (Sept. 15, 2009) [hereinafter Goldstone Report], *available at* http://www2.ohchr.org/english/bodies/hrcouncil/specialsession/9/docs/UNFFMGC_Report.pdf (detailing the various ways in which Palestinian Armed Groups violated the law of war in order to mitigate the conventional superiority of the Israeli Armed Forces).

[12] *See* Kelly Gables, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 57 (2010) ("The Internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks, and recruit others but also is increasingly being used to commit cyberterrorist acts. It is clear that the international community may only ignore cyberterrorism at its peril.").

[13] *See, e.g.,* Al-Qaeda's Fatwa (Feb. 23, 1998), *available at* http://www.pbs.org/newshour/updates/military/jan-june98/fatwa_1998.html ("The ruling to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it . . .").

many dimensions. That is, it operates across the spectrum of conflict from the tactical through the strategic levels of war. Asymmetry is also manifested in various forms: technological, doctrinal, normative, participatory and legal/moral.

Armed groups attempt to "balance the playing field" against states and their armed forces by using (or attempting to use) various means of warfare, including: unmanned aerial vehicles, weapons of mass destruction, surface-to-air missiles, information technology, and improvised explosive devices.

A. Drone Warfare

Drones are unmanned aerial vehicles that are remotely controlled by "pilots" who may be thousands of miles away from where the drone is flying.[14] In the air domain, drones are used to engage in reconnaissance and surveillance missions, to facilitate communications and locate and acquire targets.[15] By any measure, drones have proven to be extraordinarily successful in finding and killing targeted enemies[16] becoming a prevalent aspect of airpower.[17] Since 2001, drones have increasingly been the counter-terrorism weapons of choice. In that year, the U.S. Predator drone fleet numbered about ten; their mission set was generally limited to reconnaissance missions.[18] Since 2005, there has been a 1,200 percent increase in drone combat air patrols by the United States[19] with American intelligence officials call drones their most effective weapon against al-Qaeda and the Taliban.[20] Hardly a month passes without a report that another enemy leader has been killed by a drone-launched Hellfire missile.[21] With names like Predator, Global Hawk, Shadow, Raven and Wasp, these drones are an indispensable part of the U.S. efforts in Afghanistan and Iraq.[22]

---

[14] Mary Ellen O'Connell, *The Resort to Drones Under International Law*, 39 DENV. J. INT'L L. & POL'Y 585, 585(2011).

[15] WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 229 (2009).

[16] Ryan J. Vogel, *Drone Warfare and the Law of Armed Conflict*, 39 DENV. J. INT'L L. & POL'Y 101, 102 (2011).

[17] ROD THORNTON, ASYMMETRIC WARFARE, 94 (2010).

[18] *Id.* at 104.

[19] *Flight of the Drones*, ECONOMIST, October 8, 2011, *available at* http://www.economist.com/node/21531433.

[20] *Predator Drones and Unmanned Aerial Vehicles (UAVs)*, N.Y. TIMES, http://topics.nytimes.com. /top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html (last updated July 30, 2012).

[21] *See Flight of the Drones, supra* note 22.

[22] *See generally* P.W. Singer, *Military Robots and the Law of War*, NEW ATLANTIS, Winter 2009, *available at* http://www.thenewatlantis.com/ publications/military-robots-and-the-laws-of-war.

Drone technology is spreading rapidly with estimates of up to 50 countries developing or purchasing these systems.[23] Countries including Israel and the UK have used drones for combat operations while others only use them for surveillance purposes. China, for example, debuted a small drone equipped with a high-definition camera at a robotics trade show.[24] Of great concern are the growing commonality of drones and the increasing ability of non-state armed groups to acquire this technology.

Hezbollah reportedly deployed an Iranian-designed drone[25] and allegedly flew at least three Mirsad (Arabic for 'ambush') drones into Israel with each carrying a payload of approximately twenty-two pounds of explosives, packed with ball bearings.[26] A Hezbollah leader, bragging at a rally about targeting Israel, stated "[y]ou can load the Mirsad plane with a quantity of explosive ranging from 40 to 50 kilos and send it to its target, . . . do you want a power plant, water plant, military base? Anything!"[27] P.W. Singer notes that the use of drones is not limited to large-scale non-state armed groups, such as Hezbollah, and that more obscure groups are increasingly able to use or develop such technology.[28]

Contractors, such as the group previously known as Blackwater, added a section to their business seeking to rent out drones.[29] Additionally, drones have a number of commercial purposes increasing their proliferation around the world. Accordingly, non-state groups have greater access to such technology and their ability to use them is only limited by their imagination. For example, such groups could, in a cost effective manner, use drone technology to precisely attack otherwise hard to reach targets. Such attacks could even be aimed at critical infrastructure or the civilian population using weapons of mass destruction. Put differently, such armed groups could leverage drone technology to do far more damage, real and psychological, than

---

[23] *See* David Cortright, *The Scary Prospect of Global Drone Warfare*, CNN OPINION, http://www.cnn.com/2011/10/19/opinion/cortright-drones/index.html (last updated Oct. 14, 2011).

[24] Brianna Lee, *Things You Need to Know About Drones*, PBS, *available at* http://www.pbs.org/wnet/need-to-know/five-things/drones/12659.

[25] David Cortright, *The Scary Prospect of Global Drone Warfare*, CNN OPINION, http://www.cnn.com/2011 /10/19/opinion /cortright-drones/index.html (last updated Oct. 14, 2011).

[26] P.W. SINGER, WIRED FOR WAR, 264 (2009).

[27] *NBC Nightly News: Hezbollah drone threatens Israel* (NBC television broadcast Apr. 12, 2005), *available at* http://www.msnbc.msn.com/id/7477528/ns/nightly_news/t/hezbollah-drone-threatens-israel/.

[28] *See* SINGER, *supra* note 29, at 265.

[29] *Id.*

they could ever do with a suicide attack or a car filled with explosives.[30]

B. Weapons of Mass Destruction

Nuclear, chemical, and biological weapons are inherently terrorizing[31] and are the weapons state actors fear the most in the hands of non-state actors.[32] No other weapons can "level the playing field" between non-state armed groups and state actors as these weapons of mass destruction have the potential to kill millions of people quickly with relative ease.[33] In one of the many paradoxes of asymmetrical warfare, non-state actors can, and will, likely use such weapons if obtained, while their state adversaries, who already possess these weapons, cannot, and will not, used them.[34]

There have been reports that non-state armed groups continue to attempt to acquire such weapons. For example, "al-Qaeda's top leadership has demonstrated a sustained commitment to buy, steal or construct weapons of mass destruction."[35] In late 2001, Ayman Zawahiri stated, "[i]f you have $30 million, go to the black market in the central Asia, contact any disgruntled Soviet scientist and a lot of dozens of smart briefcase bombs are available."[36] Al-Qaeda announced its goal to "kill four million Americans" a few months later.[37] Osama bin Laden reportedly paid $1.5 million to a Sudanese military officer and acquired a uranium canister in 1993, which he hoped could be used as a mass destruction weapon.[38] In 1998, bin Laden declared that acquiring and using weapons of mass destruction was his Islamic duty and dispatched his senior operatives to attempt to purchase or develop nuclear and biochemical weapons of mass destruction.[39]

---

[30] Eugene Miasnikov, *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*, in CENTER FOR ARMS CONTROL, ENERGY AND ENVIRONMENTAL STUDIES MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY 4 (2005), http://www.armscontrol.ru/uav/uav-report.pdf.

[31] Jessica Stern, *Getting and Using the Weapons*, *in* TERRORISM AND COUNTERTERRORISM 182 (Russel B. Howard & Reid Sawyer eds. 2004).

[32] *See* THORNTON, *supra* note 20, at 33 (stating that non-state actors are capable of inflicting massive casualties and generating significant panic with weapons of mass destruction).

[33] DAN CALDWELL & ROBERT E. WILLIAMS, JR., SEEKING SECURITY IN AN INSECURE WORLD 49 (2006).

[34] THORNTON, *supra* note 20, at 33.

[35] Graham Allison, *Foreword* to Rolf Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality*, Belfer Ctr. for Sci. and Int'l Affairs, John F. Kennedy Sch. of Gov't (Jan. 2010), http://belfercenter.ksg. harvard.edu/files/al-aqaeda-wmd-threat.pdf.

[36] *Id.*

[37] *Id.*

[38] *See* ROHAN GUNARATNA & PETER CHALK, JANE'S COUNTER TERRORISM 41 (2002) (noting that al-Qaeda went so far as to test the canister with a Geiger counter to ensure it was radioactive).

[39] Rolf Mowatt-Larssen, *Al Qaeda's Pursuit of Weapons of Mass Destruction*, FOREIGN POLICY (Jan. 25, 2010) *available at* http://www.foreignpolicy.com/articles/2010/01/25/al_qaedas_pursuit_of_weapons_of_mass_

Non-state armed groups besides al-Qaeda, also use, or covet, weapons of mass destruction. For example, LTTE rebels (the Tamil Tigers), employed chlorine gas against a detachment of the Sri Lankan armed forces in Kiran, Eastern Sri Lanka obtaining the gas from a nearby paper mill.[40] Recalling the attack, an officer said, "[e]verything was dark when it exploded [reflecting his belief that the chemical weapon was delivered by mortar-fired projectiles], but there was a huge smoke, it was like when you set a fire. The ground was blackened where the projectiles hit."[41] On November 23, 1995, Chechen separatists placed a bomb containing 70 pounds of a mixture of cesium-137 and dynamite in Moscow's Ismailovsky Park.[42] Ultimately, the Chechen rebels opted not to explode the dirty bomb but instead informed the media of its location.[43]

The perceived threat of WMD use by non-state groups has been increased dramatically since the end of the Cold War.[44] Author Andrew O'Neill offered three reasons for this phenomenon. First, with the collapse of the Soviet Union in 1991, there has been significant concern about the physical security of the weapons of mass destruction in the territories of the former Soviet Union.[45] The second reason is the emergence of a new breed of non-state armed groups who are more likely to use lethal and indiscriminate forms of violence. Finally, the transnational nature of these groups makes no location, as illustrated by the attacks of September 11th, beyond their reach.[46]

C. *Missile Technology*

In 1986, the United States armed the Afghan Mujahideen with Stinger antiaircraft missiles to help them combat the Soviet Union.[47] At the time, the Stinger was considered a highly effective hand-held anti-aircraft missile

---

destruction?hidecomments=yes.

[40] *See* GUNARATNA & CHALK, *supra* note 41, at 42.

[41] Bruce Hoffman, *The first non-state use of a chemical weapon in warfare: the Tamil Tigers' assault on East Kiran*, 20 SMALL WARS & INSURGENCIES 463, 470 (2009), *available at* http://www.tandfonline.com/doi/full/10.1080/ 09592310903026969#tabModule.

[42] Graham Allison, *Nuclear Terrorism: How Serious a Threat to Russia?* RUSSIA IN GLOBAL AFFAIRS, Sept./Oct., (2004), *available at* http://belfercenter.ksg.harvard.edu/publication/660/nuclear_terrorism.html.

[43] *Id.*

[44] Andrew O'Neil, *Terrorist Use of Weapons of Mass Destruction: How Serious Is the Threat?*, 57 AUSTL. J. OF INT'L AFF. 99, 100 (2003) (arguing that even though WMD terrorism remains a real prospect, the ease with which such attacks can be carried out has been exaggerated).

[45] *Id.*

[46] *Id.*

[47] Alan J. Kuperman, *The Stinger Missile and the U.S. Intervention into Afghanistan*, 114 POL. SCI. Q. 219, 219 (1999).

capable of locking onto the heat signature of a helicopter or airplane engine. In his book, Holy War, Inc., author Peter L. Bergen noted once the Stinger missiles were deployed into the hands of the Mujahideen, the Soviets lost the air superiority they had previously enjoyed. Ahmad Shah Massoud, an Afghan military leader who played a leading role in driving the Soviet army out of Afghanistan once quipped, "[t]here are only two things the Afghan must have: the Koran and Singers."[48]

Shoulder-fired surface-to-air missiles in the hands of non-state actors pose a significant threat to passenger air travel, the commercial aviation industry, and military aircraft around the world. Since the 1970s, there have been over 40 civilian aircraft hit by such missiles.[49] It is believed that two dozen armed groups have gained access to surface-to-air missiles with the most popular remaining the shoulder-fired heating missiles.[50] Of great concern today is the possibility of a state collapse allowing their conventional arsenal, including such missiles, to slip into the hands of non-state armed groups.[51]

D. Improvised Explosive Devices (IEDs)

Often used by non-state actors who wage non-traditional warfare, so-called improvised explosive devises or IEDs can be made from almost any material and are designed to kill or maim.[52] Improvised explosive devices are the most lethal weapons of non-state groups participating in the conflicts of Afghanistan and Iraq. In Iraq, IEDs are responsible for two-thirds of coalition deaths while in Afghanistan such attacks have roughly tripled in the past two years.[53] Improvised explosive devices are global threats. From January to November 2011, outside of Iraq and Afghanistan, there have been 6,832 improvised explosive events in 111 countries resulting in 12,286 casualties. Such attacks were carried out by 40 regional and transnational threat networks of non-state

---

[48] PETER L. BERGEN, HOLY WAR, INC.: INSIDE THE SECRET WORLD OF OSAMA BIN LADEN (2001).

[49] *See* Fact Sheet, U.S. Dep't of State, *MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems* (July 31, 2008), http://merln.ndu.edu/archivepdf/terrorism/state/ 107632.pdf.

[50] *See* GUNARATNA & CHALK, *supra* note 41, at 642.

[51] *See, e.g.,* Addison Wiggin, *Where Will Libya's Shoulder-Fired Missiles Land?*, FORBES (Sept. 29, 2011), http://www.forbes.com/sites/greatspeculations/2011/09/29/where-will-libyas-shoulder-fired-missiles-land/ (discussing the great concern that the 20,000 missiles possessed by Libya at the time of the government's collapse would find their way into the hands of terrorists).

[52] *See Improvised Explosive Devices*, N.Y. TIMES TOPICS, http://topics.nytimes.com/topics/reference/timestopics/subjects/i/improvised_explosive_devices/index.html?offset=0&s=newest (last visited Feb. 20, 2012).

[53] *See Bombs Away*, ECONOMIST, (Mar. 4, 2010), *available at* http://www.economist.com/node/15582147.

actors.[54]

Because of the on going and increasing threat by IEDs in Iraq and Afghanistan, the United States established the Joint IED Defeat Organization, known as JIEDDO in February 2006.[55] In JIEDDO's Strategic Plan (2012-2016), Lieutenant General Michael Barbero stated:

> The IED is the weapon of choice for the overlapping consortium of networks operating along the entire threat continuum — criminal, insurgent, and terrorist alike. Threat networks use IEDs because they are cheap, readily available, easy to construct, lethal, and effective. The IED is a weapon used strategically to cause casualties, create the perception of insecurity, and influence national will. This threat is complex and transnational in nature, representing layers of interdependent, inter-connected global threat networks, and support systems.[56]

A basic IED has four components: an explosives charge, an initiator, a power source and an activation switch.[57] Most IEDs used by non-state actors are decidedly low-tech, jury-rigged affairs consisting of a few command wires, some fertilizer chemicals and wooden pressure plates. Others consist of leftover mines or plastic explosives that are detonated remotely by a cellphone.[58] However, not all IEDs are simple; non-state groups are becoming increasingly sophisticated in their design and production, particularly in terms of explosively formed projectiles and advanced triggers, which have caused disproportionate levels of casualties relative to the numbers of such devices employed.[59] An example from the conflict in Iraq illustrates this point. With the help of the Iranians, insurgents in Iraq deployed deadly devices known as explosively formed projectile (EFPs).[60] This type of IED is typically made from a pipe containing explosives and capped by a copper disk. When detonated, the copper disk is transformed into a molten jet of metal capable of penetrating

---

[54] Spencer Ackerman, *Pentagon: Future of Homemade Bombs Is High-Tech*, WIRED MAGAZINE (Feb. 14, 2012, 2:30 PM), http://www.wired.com/dangerroom/2012/02/jieddo-high-tech-bombs/ (citing *Counter Improvised Explosive Devise Strategic Plan*, JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORG. 2012-2016, 1–2 (Jan. 1, 2012), [hereinafter JIEDDO]*, available at* http://www.globalsecurity.org/military/library/policy/dod/jieddo-cied-plan-120116.pdf (last visited Sept. 30, 2012).

[55] *See generally* U.S. DEP'T OF DEF., DIRECTIVE 2000.19E, JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION (JIEDDO), *available at* http://www.dtic.mil/whs/directives/corres/pdf/200019p.pdf.

[56] *See* JIEDDO, *supra* note 57, at iii.

[57] *See* GUNARATNA & CHALK, *supra* note 41, at 29.

[58] *See* JIEDDO, *supra* note 57, at iii.

[59] *Id*.

[60] Tom Vanden Brook, *U.S. Blames Iran for New Bombs in Iraq*, USA TODAY (Jan. 30, 2007, 9:45 PM), http://www.usatoday.com/news/world/iraq/2007-01-30-ied-iran_x.htm.

armor thus operating the same as a U.S. anti-tank missile.[61]

The leading authorities on improvised explosive devices, JIEDDO, paint an alarming picture of the advances in IED technology. More specifically, it reports:

> In the future, devices will adopt ever more sophisticated technology, limited only by the terrorists' imaginations. . . .Future bomb makers will seek to incorporate such enhancements as peroxide- and hydrogen-based explosives; nanotechnology and flexible electronics; new forms of power, e.g., microbial fuel cells, non-metallic and solar; advanced communications (Bluetooth, 4G, Wi-Fi, broadband); optical initiators (using laser or telemetry more than infrared); and highly energetic and molecular materials. Indicators have shown that terrorist networks which innovate with these new technologies are also developing enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks. Bomb makers will take advantage of available technology and innovate in response to countermeasures — weapons will be more lethal and harder to detect and defeat.[62]

E. Information Technology

Information technology has revolutionized warfare and is central to state actor military dominance.[63] Such technology as the Global Positioning System, communications capabilities, sensors, advanced radar/sonar, cyber warfare capabilities, guided munitions, and much more have seemingly widened the capabilities gap with non-state armed groups. The paradox of a conflict between a state actor and anon-state armed groups is that such modern technology is both the great separator and the great equalizer.[64] Non-state groups, like al-Qaeda, Hezbollah, Iraqi insurgents and others, thrive in the information age because they are able to exploit—or threaten to—exploit many of the same information technologies that make state militaries so powerful. Such non-state armed groups have been stunningly innovative in their exploitation of technology.[65] Additionally, the more powerful the economy or military organization, the more likely they will rely on information technology,

---

[61] *Id.*

[62] JIEDDO, *supra* note 57, at 4.

[63] *See* Max Boot, *The Paradox of Military Technology,* NEW ATLANTIS, Fall 2006, *available at* http://www.thenewatlantis.com/publications/the-paradox-of-military-technology (noting that the United States has the most advanced weapons systems and sophisticated information technology in world; however, such technology is not a perfect shield against other kinds of destructive power).

[64] *Id.* (According to Boot, technological supremacy separates the United States from the rest of the world, and yet modern technology leaves America vulnerable to vicious groups and gangs armed with AK47s, car bombs, or portable WMDs).

[65] *See* SINGER, *supra* note 29, at 264.

which results in a greater vulnerability.[66]

In 2006, in the midst of an armed conflict with Israel in southern Lebanon, Hezbollah fighters were able to hack into the Israeli Army's computer and radio systems.[67] According to some reports, with the intelligence gained through the intercepts, Hezbollah was able to thwart Israeli tank assaults.[68] It is believed that Hezbollah used Iranian-supplied technology to accomplish this feat.[69] Commenting on the incident, author P.W. Singer stated that, "[n]otably, the group's Internet attacks on Israel originally appeared to come from a small south Texas cable company, a suburban Virginia cable provider and web-hosting servers in Delhi, Montreal, Brooklyn, and New Jersey. But these all had actually been 'hijacked' by Hezbollah hackers."[70]

Non-state armed groups fighting against coalition forces in Iraq and Afghanistan have also used information technology with great skill. Such groups post videos of their exploits on the Internet while also communicating through mobile phones, e-mails, and websites.[71] The Taliban is even using Twitter to wage war against the United States.[72] In Iraq, tech savvy insurgents use the Internet to recruit suicide bombers, spread propaganda, and even publish monthly online magazines.[73]

Cyberspace is now a war zone where many of the decisive battles of the twenty-first century will be played out.[74] The United States Department of Defense's Quadrennial Defense Review Report defines cyberspace as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including

---

[66] *See* THORNTON, *supra* note 20, at 55 (discussing the challenges and threats of asymmetric warfare in the 21st century).

[67] *See* SINGER, *supra* note 29, at 264.

[68] *E.g.* Mohamad Bazzi, *Hezbollah Cracked the Code*, NEWSDAY (Sept. 17, 2006, 8:00 PM), http://www .newsday.com/news/hezbollah-cracked-the-code-1.681121.

[69] *See* John Leyden, *Hezbollah Cracks Israeli Radio Code*, THE REGISTER (Sept. 20, 2006, 13:06 GMT), http://www.theregister.co.uk/2006/09/20/hezbollah_cracks_israeli_radio/.

[70] SINGER, *supra* note 29, at 264.

[71] *See* Michelle Nichols, *Tech-savvy Taliban Fights War in Cyberspace*, REUTERS (July 20, 2011, 4:13 AM), http://www.reuters.com/article/2011/07/20/us-afghanistan-taliban-technology-idUSTRE76J1HL20110720.

[72] Ernesto Londoño, *U.S. Military, Taliban Use Twitter to Wage War*, WASHINGTON POST, (Dec. 18, 2011), http://www.washingtonpost.com/world/asia_pacific/us-military-taliban-use-twitter-to-wage-war/2011/12/16/ gIQAKnJ320_story.html (stating that the International Security Assistance Force engages in a "near-daily battle" with the Taliban on Twitter).

[73] *See* Jonathan Curiel, *Terror.Com / Iraq's Tech-savvy Insurgents Are Finding Supporters and Luring Suicide-bomber Recruits over the Internet*, SFGATE (July 10, 2005, 4:00 AM), http://www.sfgate.com/news/article/ TERROR-COM-Iraq-s-savy-insurgesnts-are-2623261.php.

[74] *See* RICHARD A. CLARKE, CYBER WAR, 69 (2010).

the Internet and telecommunication networks."[75] Cofer Black, former head of the Central Intelligence Agency's Counter Terrorism Center, recently noted that it is likely that we will see more cyber attacks from al-Qaeda as cyber operations can be done remotely and are comparatively safer than strapping on a bomb.[76] A British Home Office report recently noted that "[s]ince the death of Osama bin Laden, al-Qaeda has explicitly called not only for acts of lone or individual terrorism but for 'cyber jihad."'[77]

III. COUNTERING NEW TECHNOLOGY WITH TECHNOLOGY

The aggressive pursuit of new technology by non-state armed groups clearly poses long-term humanitarian risks. However, of greater immediate humanitarian concern are the evolving mitigation methods, or tactics, used by non-state armed groups to counter the technological superiority of state actors. Increasingly adept at communicating, organizing, and operating from any location, non-state armed groups are less and less tied to "hot battlefields,"[78] and are more likely to shield their operations by deeply embedding within unsuspecting local populations across the world.[79] Additionally, technology, and

---

[75] *See* QDR, *supra* note 6, at 37.

[76] *ABC Nightly News: Former CIA Counter-Terror Chief: Al Qaeda Will Go Cyber*, (ABC television broadcast Aug. 4, 2011), *available at* http://abcnews.go.com/Blotter/cia-counter-terror-chief-al-qaeda-cyber/story?id=14224256.

[77] Duncan Gardham, *Terrorists Are Harnessing Hi-tech Communications, Government Warns*, THE TELEGRAPH (July 12, 2011, 7:18 PM), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8633311/Terrorists-are-harnessing-hi-tech-communications-government-warns.html.

[78] "Hot battlefields" is a term used to reference geographically contained conflicts. For example, Afghanistan, or until recently, Iraq would be construed as a "hot battlefield." *See, e.g.,* Ashley S. Deeks, *Pakistan's Sovereignty and The Killing of Osama Bin Laden*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (MAY 5, 2011), http://www.asil.org/insights110505.cfm ("[T]he most controversial aspect . . . is the U.S. argument that this conflict can and does extend beyond the "hot battlefield" of Afghanistan to wherever members of al Qaeda are found."); Margaret Talev, *U.S. to Attack Al-Qaeda Terrorists Beyond the 'Hot Battlefields,' Brennan Says,* BLOOMBERG (Sept. 16, 2001), http://www.bloomberg.com/news /2011- 09-16/u-s-will-hit-al-qaeda-beyond-hot-battlefields-obama-aide-brennan-says.html (discussing the use of military force against Al-Qaeda away from "hot battlefields" like Afghanistan).

[79] The illegality of using civilians as a "shield" is without question in international armed conflicts. *See* AP I, *supra* note 11, at art. 51(7) ("the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operation."); *See also* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 28, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 ("The presence of a protected person may not be used to render certain points or areas immune from military operations"); Rome Statute of the International Criminal Court art 8(2)(b)(xxiii), July 17, 1998, 37 I.L.M. 1002, 2187 U.N.T.S. 90 (listing as a war crime "[u]tilizing the presence of a civilian or other protected person to render certain points, areas or military forces immune from military

in particular cyber technology, now allows for these groups to conduct asymmetric activities with fewer risks and minimal resources thus further cloaking their existence. Broadly dispersed and quietly blended into various civilian population centers, state actor advantages are mitigated as the non-state actor is virtually indistinguishable from a civilian.[80] This pervasive exploitation of civilians, and the intentional assault on the principle of distinction, threatens the delicate balance between military necessity and humanity undercuts the paramount purpose of the Law of War.[81]

In general terms, non-state armed groups cannot survive direct and conventional conflicts with more technologically superior state opponents.[82] To compete, these groups consciously "avoid mirroring Western military organizations and approaches to war"[83] and "by operating well outside the moral framework of the traditional Western approach" to hostilities.[84] Unconstrained by these assumed "universal norms of behaviour"[85] non-state armed groups can seek advantages by practicing unorthodox, or even legally prohibited, approaches to warfare. The Law of War mandate requiring parties to a conflict to distinguish between civilians and conflict participants[86] is

---

operations."). Though not as clearly articulated, the prohibition on misusing civilians also exists in non-international armed conflicts. *See* Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict (Protocol II) art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II] (discussing general protections for civilians in non-international armed conflicts); GARY SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 100-01(2010) ("[W]ar crimes and grave breaches can indeed be committed in non-international common Article 3 armed conflicts.").

[80] Nils Melzer, *Foreword to Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL. 831, 833 (2010) (discussing the difficulties in contemporary armed conflicts due to the "blurring of the traditional distinctions and categories upon which the normative edifice of IHL has been built. . . .").

[81] *See Nils Melzer, Foreword to Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* 4, ICRC (May 2009) [hereinafter ICRC Interpretive Guidance], *available at* http://www.icrc.org/eng/assets /files/other/icrc-002-0990.pdf (stating that "the protection of civilians is one of the main goals of international humanitarian law.").

[82] *See generally* McKenzie Jr., *supra* note 3.

[83] *See infra* Section II for discussion on the various approaches to warfare adopted by contemporary non-state armed groups.

[84] McKenzie Jr., *supra* note 3, at 88.

[85] *Id.*

[86] *See* AP I, *supra* note 11, art. 48. The distinction requirement also applies in non-international armed conflict. *See* AP II, *supra* note 82, art. 13 (stating "[c]ivilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities"); *See also* SOLIS, *supra* note 82, at 254 (discussing the applicability of the principle of distinction in all conflicts); *Cf* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641, 646 (2010)

therefore an opportunity for the non-state armed group versus an obligation for the state actor.[87] Whereas the state actor must protect civilians, the non-state armed group simply views civilians as an asymmetric warfare asset that may be leveraged in order to gain an advantage against their state actor adversaries.[88]

Considering civilians as an "asset to be expended"[89] non-state armed groups blatantly ignore the general protections afforded non-combatants during hostilities.[90] Yet this callous disregard for long-standing humanitarian norms[91] is sadly not unusual or surprising. Despite the international impetus to protect civilians from the atrocities of war,[92] the state actor's resultant legal obligations perversely incentivises non-state actors to misuse civilians. Contemporary conflicts "waged between government forces and organized non-state armed groups" are routinely characterized by an "intermingling of civilians and armed actors" and a stubborn unwillingness of non-state actors to "adequately distinguish themselves from the civilian population."[93] As these conflicts are now the predominant form of warfare[94] this intentional misuse of civilians by non-state armed groups is a harsh reality driving a number of responses from state actors.

Though often perceived as "fighting with one arm tied behind [their] back" and admittedly causing much frustration, state actors recognize the importance of complying with the Law of War as "preserving the rule of law. . . constitutes an important component of [their] security stance."[95] State actors thus

("[c]ompliance with the distinction principle is required of all participants in warfare regardless of whether they fight for state armed forces or a non-State 'organized armed group.'").

[87] *See* SOLIS, *supra* note 82, at 254 (discussing the frequent disregard for the principle of distinction by non-state actors).

[88] *See generally* McKenzie Jr., *supra* note3, at 76.

[89] *Id*. at 88.

[90] *See, e.g.*, Laura King, *Afghanistan Arrests Preteen Would-be Bombers Months After Pardon*, LOS ANGELES TIMES, (Feb. 13, 2012), http://www.latimes.com/news/nationworld/world/la-fg-afghanistan-child-bombers-20120214,0,7784954.story (last visited Feb. 17, 2012) (describing how insurgents in Afghanistan are using young children as suicide bombers).

[91] *See*, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUG. 1949, 598 (Yves Sandoz, et. al. eds., 1987) [hereinafter Commentaries] ("It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected . . . . The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule.").

[92] *See Id*. (discussing the historical reason for protecting civilians and the particular need for a codification of this customary understanding following the brutality of World War II).

[93] ICRC Interpretive Guidance, *supra* note 84, at 4–5.

[94] *See* Watkin, *supra* note 89, at 653.

[95] *Id*. at 647 (citing HCJ 769/02 Pub. Comm. Against Torture in Israel v. Gov't of Israel 64 [2005] (Isr.), *available at* http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf

"operate under constraints when conducting operations," and in particular strive to comply with the distinction principle in these complex and messy conflicts.[96] Using a combination of policy mandates and advanced technology, state actors continually try to disentangle non-state actors from local populations. For example, the United States military, desperate to reduce civilian casualties in the often confusing environments of Iraq and Afghanistan, has universally implemented the Escalation of Force (EOF) process.[97] The EOF process trains American soldiers to work through a number of sequential steps in order to distinguish between a harmless civilian and an actual threat in hopes of gaining clarity before using deadly force.[98] Similarly, The North Atlantic Treaty Organization's (NATO) 6 July 2009 Tactical Directive imposed restrictions on a number of weapon systems and tactics in hopes of reducing civilian casualties in Afghanistan.[99]

State actors also rely heavily on technology to help determine who can be targeted.[100] The United States uses a scientific, heavily computerized, deliberate targeting process known as the Collateral Damage Estimation,[101] to ensure strict compliance with both the distinction and proportionality principles.[102] Non-lethal Unmanned Aerial Vehicles (UAV) are a common tool of government forces to help pierce the "fog of war" and decipher the intentions of individual actors in a conflict zone.[103] Precision-guided munitions allow for

---

(discussing pragmatic security reasons that a state will self-restrain their combat activities).

[96] *Id.* at 64–67.

[97] *See generally* Randall Bagwell, *The Threat Assessment Process (TAP): The Evolution of Escalation of Force*, ARMY LAW., Apr. 2008, at 5.

[98] *Id*. at 8 ("The goal . . . is to force the insurgent to self-identify while keeping innocent civilians from being mistaken for threats. This approach works primarily because it uses non-force measures to put potential threats into situations where they must either comply with or disobey the Soldiers' commands.").

[99] *See* Headquarters, Int'l Sec. Assistance Force, Tactical Dir. (July 6, 2009) [hereinafter Tactical Directive], *available at* http://www.nato.int/isaf/docu/official_texts/Tactical_Directive_090706.pdf.

[100] Watkin, *supra* note 89, at 646 ("At the heart of the question of who can be targeted is the principle of distinction.").

[101] *See generally* Gregory S. McNeal, *The U.S. Practice of Collateral Damage Estimation and Mitigation* (Nov. 9, 2011) (Unpublished Working Paper) (discussing the technical methodology employed by the United States for pre-planned targeting and its overarching goal of minimizing civilian casualties) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819583.

[102] The Principle of Proportionality determines whether "an attack . . . may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof [that will] be excessive in relation to the concrete and direct military advantage anticipated." AP I, *supra* note 11, at art. 51(5)(b).

[103] *See* Martin E. Dempsey, *Forward* to U.S. Army UAS Ctr. Of Excellence, "Eyes of the Army" U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035, U.S. ARMY, i (2010), http://www-rucker.army.mil/usaace/uas/ US%20Army%20UAS%C20RoadMap%202010%202035.pdf

extraordinarily accurate and discriminate targeting[104] while electronic intelligence gathering pinpoints clandestine non-state actors. Yet, despite these policy restrictions and technological advances, complying with the principle of distinction remains extraordinarily difficult for state actors[105] as "the principle . . . is easy to state" but challenging to implement.[106]

Implementation challenges are largely a result of the realities of contemporary conflicts. As non-state armed groups intentionally mix with civilians, the task of discerning an individual's status and their accompanying level of humanitarian protection[107] often falls to junior leaders and their soldiers.[108] Further, non-state armed groups are not passively using the civilian population as a shield from attack, but, in furtherance of their asymmetric strategy, will often attempt to draw a disproportionate response from the state actor in order to further a propaganda message.[109] Practical implementation of the principle of distinction in day-to-day operations therefore becomes the responsibility of the "soldiers and other fighters."[110] The enormity of this responsibility coupled with the complexity of the modern battlefield understandably leads to "confusion and uncertainty as to the distinction between legitimate military targets and persons protected against direct

---

(stating that unmanned aerial vehicles help to "broaden situational awareness" as well as improve the ability to "see, target, and destroy the enemy" in uncertain and complex environments).

[104] *See, e.g., Al-Qaeda's Anwar al-Awlaki killed in Yemen*, CBS NEWS (Sept. 30, 2011, 5:02 AM), http://www.cbsnews.com/stories/2011/09/30/501364/main20113732.shtml.

[105] See Melzer, *supra* note 83, at 833 (noting that the increased civilian involvement in modern warfare has led distinction problems between legitimate military targets and persons protected against direct attack.").

[106] Watkin, *supra* note 89, at 646.

[107] *See* SOLIS, *supra* note 82, at 187 ("On the battlefield, no one is without some status and an accompanying level of humanitarian protection.").

[108] *See* Charles C. Krulak, *The Strategic Corporal: Leadership in the Three Block War*, MARINES MAG. Jan. 1999, at 26, 30 (1999), *available at* http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm (stating the strategic corporal concept is a recognition that modern conflicts will see "the lines separating the levels of war, and distinguishing combatant from 'non-combatant,'" blur and "and adversaries, confounded by . . . [the state's] 'conventional' superiority, will resort to asymmetrical means to redress the imbalance." As a result, the success of the modern battlefield will "rest, increasingly, with the rifleman and with his ability to make the *right* decision at the *right* time at the point of contact.").

[109] *See* U.S. DEP'T OF ARMY, FM 3-24, *supra* note 5, at ¶ 1–152 (stating that non-state armed groups will "carry out a terrorist act or guerrilla raid" with the primary purpose of enticing the opposing actor "to overreact" in a way that can be exploited "—for example, opening fire on a crowd . . . ."); McKenzie Jr., *supra* note 3, at 77 (discussing how "asymmetric approaches can achieve powerful effect through manipulation of the psychological element.").

[110] Watkin, *supra* note 89, at 646.

attack."[111]

This "confusion and uncertainty" is a hallmark of the state actor conflict with the non-state armed group and creates significant humanitarian risks for civilian populations.[112] It is therefore particularly alarming that non-state armed groups are further complicating these conflicts by using advanced technology, and specifically information technology, to expand their operations across the entirety of the international community. Widely dispersed, yet capable of operating and collaborating through cyberspace, non-state armed groups are extensively transnational.[113] Further, the cyber domain allows for more discrete forms of terror activities with the contemporary non-state actor more likely to be a financier, strategic planner, or propagandist than a "traditional terrorist" operator.[114] A non-exhaustive list of examples includes: Anwar al-Awlaki, from a remote location in Yemen, encouraging and coordinating various terror operations, particularly in the United States, by using "Youtube, broader Internet sites, Facebook, [and] Twitter;"[115] al-Qaeda computer operatives widely publishing versions of bomb-making manuals, often in English, on the Internet to encourage remote training;[116] groups such

---

[111] Melzer, *supra* note 83, at 833.

[112] *See, e.g.*, Goldstone Report, *supra* note 12 (alleging a number of Law of War violations that involved civilians committed by both Israeli forces and Hamas during the conflict in Gaza from 27 December 2008 to 18 January 2009); *but see* State of Israel, *Gaza Operations Investigations: An Update* 32 (Jan. 2010), http://www.mfa. gov.il/NR/rdonlyres/8E841A98-1755-413DA1D2-8B30F64022BE/0/GazaOperationInvestigationsUpdate.pdf (refuting the Goldstone Reports findings); *See also* Kevin Sieff, *Afghan Civilian Deaths Hit Record High in 2011*, *U.N. Report Says*," WASH. POST, Feb. 4, 2012 http://www.washingtonpost.com/world/afghan-civilian-deaths-hit-record-high-in-2011-un-report-says/2012 /02/04/gIQAfyl9oQ_story.html (noting that the vast majority of the civilian deaths came from Taliban roadside or suicide bombings).

[113] *See* RUSSELL D. HOWARD & REID L. SAWYER, TERRORISM AND COUNTERTERRORISM –UNDERSTANDING THE NEW SECURITY ENVIRONMENT 77 (2004) (noting that al-Qaeda is a global network consisting of permanent or independently operating semi-permanent cells of trained militants that have a presence in more than seventy-six countries).

[114] *See, e.g.*, Brian Ross, *How Anwar al-Awlaki Inspired Terror From Across the Globe*, ABC NEWS THE BLOTTER http://abcnews.go.com/Blotter/anwar-al-awlaki-inspired-terror/story?id=14643383 (describing al-Awlaki as the "modern day terrorist" capable of using the internet to conduct terrorist activity).

[115] *Id*. ("While al-Awlaki was not the trigger-man in any of the 19 terror operations to which he is linked, U.S. officials and terror experts said that his hand was visible in all of them—whether by simply pushing the attackers over the violent edge or by personally guiding them through operations.").

[116] *See* Duncan Gardham, *Al-Qaeda Bomb Manual Published on Internet*, THE TELEGRAPH, (Feb. 22, 2012, 7:00 AM), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8232389/Al-Qaeda-bomb-manual-published-on-internet.html ("Published by al-Qaeda's Global Islamic Media Front" in order allow followers "to launch their own attacks, without training.").

asal-Qaeda, Hamas, Lashkare-Taiba, and Hezbollah, "mak[ing] extensive use of the Internet to raise and transfer needed funds to support their activities" as the Internet "offers a broad reach, timely efficiency, as well as a certain degree of anonymity and security for both donors and recipients."[117] These types of activities make the non-state actor not only exceedingly difficult to identify, these actions also make the global population, even if ignorant about the hostilities, potentially a de facto human shield. This trend towards decentralized, discrete non-state actor terrorist activity thus further blurs the lines drawn within the principle of distinction between conflict participant and civilian while dramatically increasing the civilian population's exposure to hostilities.

State actors are simply not prepared for this trend. Previous responses, whether policy mandates or sophisticated technology, relied upon to clarify individual status on the modern battlefield are of minimal use in these transnational conflicts. Rules of engagement, tactical directives, and soldier training are almost exclusively oriented on non-international conflicts within a specific geographic area.[118] Sophisticated technology is limited by resources and intelligence and thus difficult to employ without some parameters. These shortcomings ensure that non-state armed groups will continue to counter the technological superiority of state actors by exploiting the distinction principle. This leaves state actors and the international community again left with the seemingly impossible task of determining "how . . . the principle of distinction should be implemented in the challenging and complex circumstances of contemporary warfare."[119] This has become a contentious, and difficult to answer question.[120] But without an answer, the walls separating combatant and civilian will continue to crumble, creating the very real, and dangerous, possibility that warfare will again degenerate "into brutality and savagery."[121]

---

[117] Michael Jacobson, *Terrorist Financing and the Internet*, 33 STUD. IN CONFLICT AND TERRORISM 353 (2010).

[118] *See, e.g.,* Tactical Directive, *supra* note 102 (restricting NATO operations in Afghanistan).

[119] MELZNER, *supra* note 84, at 7.

[120] *Compare* MELZNER, *supra* note 84 (providing recommendations on how to implement the principle of distinction) *with* Watkin, *supra* note 89, *and* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT. SEC. J. 1, 5 (May 2010) (criticizing the Interpretive Guidance recommendations).

[121] Rob McLauglin, *The Law of Armed Conflict and International Human Rights Law: Some Paradigmatic Differences and Operational Implications*, 2010 Y.B. OF INT'L HUM. L. 213, 222 (citing United Kingdom Ministry of Defence, *The Manual on the Law of Armed Conflict,* 2004, ¶ 1.8.).

IV. CONCLUSION

The relationship between non-state armed groups and advanced technology creates a number of uncertain and frightening humanitarian challenges for the international community. The "widespread availability of sophisticated weapons and equipment . . . 'level the playing field' and negate [state actor's] traditional technological superiority"[122] while exponentially increasing the lethality of the non-state armed group. Unrestrained by law or morality, non-state armed groups' growing familiarity with unmanned aerial vehicles, weapons of mass destruction, surface-to-air missiles, information technology, and improvised explosive devices is extraordinarily dangerous. Similarly, while mitigating state actor technological superiority by commingling with civilians is not a new tactic,[123] advanced technology is allowing non-state armed groups to expand this tactic across the globe at an unprecedented rate.[124] Capable of supporting operations with seemingly benign activity, these widely dispersed non-state actors are difficult to identify and place previously safe civilian populations at risk. Additionally, this increased ability to use advanced technology to aggressively exploit the state obligation to distinguish between civilians and conflict participants de-legitimizes and undercuts this fundamental principle of the Law of War.

The necessity for the international community to recognize and address these ominous threats is clear. The humanitarian consequences of inaction place untold civilians at risk while raising troubling questions concerning the effectiveness of the Law of War to regulate contemporary conflicts. Facing "a complex and uncertain security landscape in which the pace of change continues to accelerate,"[125] the international community must adapt to this new reality and redouble previous efforts to stop this potential humanitarian crisis.

[122] Krulak, *supra* note 111.

[123] Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum*, 42 N.Y.U. J. INT'L L. & POL. 637, 637 (2010) ("the most intractable conflicts now include non-state armed groups that wear no uniform and purposefully commingle their fighters with civilian populations.").

[124] *Id.* ("Technological developments have expanded the capacity of individuals to apply lethal force while remaining located thousands of miles away from their targets.").

[125] QDR, *supra* note 6, at p. iii.