FOREIGN POLICY RESEARCH INSTITUTE

FOOTNOTES

"A nation must think before it acts." - Robert Strausz-Hupé

APRIL 2015

THINKING ABOUT MILITARY HISTORY IN AN AGE OF DRONES, HACKERS, AND IEDS

By Paul J. Springer

Paul J. Springer, Senior Fellow in the Foreign Policy Research Institute's Program on National Security, is an associate professor of comparative military history at the Air Command and Staff College, located at Maxwell Air Force Base, Alabama. This essay is based on a lecture delivered at our 2014 History Institute for Teachers at the First Division Museum, Wheaton, IL on America and Modern War: The American Military Post-Vietnam, our 10th weekend conference on American military history. Also see our E-Book American Military History: A Resource for Teachers and Students, jointly published by FPRI and the First Division Museum.

The views presented in this essay belong solely to the author, and do not represent the official positions of the U.S. government, Department of Defense, or U.S. Air Force.

We live in a transitional period in the history of human conflicts. Military robotics and cyber capabilities constitute a Revolution in Military Affairs (RMA) that will permanently alter the nature of warfare. The United States, which leads in the creation and adoption of these forms of technology, has the unique opportunity to shape the RMA and prevent some of its negative consequences, but only if it acts quickly and decisively to lead an international movement that can address the worst potential consequences of these developments. Absent such a determined effort, military robots and cyber capabilities are likely to make human conflict even more painful and costly, not only for uniformed military organizations but also for the noncombatant civilian populations of the world.

A Brief Introduction to RMAs

RMAs permanently alter the nature of warfare. Nations and non-state actors that accept and adapt to the changes presented by RMAs tend to gain a decisive advantage over non-adopters, such that RMAs offer the possibility of upsetting the pre-existing power structures of the global state system. These RMAs do not occur instantaneously, nor do they occur in a vacuum. Rather, they are the sum of changes in technology, doctrine, and strategy that collectively change the nature of conflicts. Over time, though, RMAs render previous conceptions of warfare obsolete. When the conditions for an RMA are created, there is a period of asymmetry, followed by a widespread adoption of the change as late-adopters realize their errors and rush to retain as much of their power as possible by changing their approach to warfare. While being first in an RMA is not always a lasting advantage, as the costs of first-adopter status can be prohibitively high, being last to adapt is almost always a recipe for disaster.

One of the most well-known RMAs in history serves to illustrate many of the key points of the RMA phenomenon. Gunpowder, in at least a rudimentary form, had been discovered in China by at least the Song Dynasty of the eleventh century, and might have been in existence even earlier. The benefits of gunpowder weaponry were not immediately obvious, although the innovation gradually spread through trade and conquest, reaching Europe in the thirteenth century. At that time, warfare was characterized by limited objectives for massively fortified positions. The pinnacle of field combatants, the heavily-armored, mounted knight, dominated the battlefields of the era, bolstered by armies of less-protected archers and men-at-

arms. Fortifications of the era had high walls, protective moats, and the ability to withstand long sieges. To conquer such a position required months, and possibly years, gradually wearing down the defenses and exhausting the supplies of the threatened castle. Once gunpowder artillery, even of a rudimentary sort, became common, the era of castles quickly ended, as the high walls could not withstand even the inaccurate cannon fire of the era. Likewise, knights' armor could not stop the power of a firearm's projectile, and thus became an expensive and mostly useless relic of the earlier era. Gunpowder permanently transformed the notion of warfare in Europe, and in turn triggered a fortification revolution, with new strongpoints constructed specifically to counteract the power of gunpowder weapons. Field armies also abandoned the old means of combat, adopting hand-held firearms that could inflict devastating wounds upon the enemy. Of course, early firearms had disadvantages. They were heavy, they usually failed in poor weather, their rate of fire was ridiculously slow, and their accuracy was dismal. To counter these problems, military theorists invented the notion of linear tactics, combined arms formations, and volley fire. By the sixteenth century, European armies utilizing gunpowder weapons had swept through enormous portions of the globe, conquering the New World empires of the Aztecs and the Incas, colonizing the coasts of the Americas and Africa, and completely overturning the previous world order. States that failed to adapt to the new system, or who did not have the capability to produce gunpowder weapons, simply ceased to exist, the victims of an RMA that swept aside the entire old concept of conflict.[1]

Setting Limits Upon Conflicts

Of course, not every observer of the gunpowder RMA considered it a positive development. Without gunpowder, after all, the widespread adoption of chattel slavery, the eradication of native populations outside of Europe, and the horrors of increasingly widespread warfare would not have been possible. One needs only examine the Thirty Years War to appreciate the terrible potential of gunpowder-wielding armies, particularly when bolstered by religious leadership calling for the annihilation of competing worldviews. After Europe nearly destroyed itself through that terrible conflict, a new desire for order emerged, codified by the Treaty of Westphalia and the establishment of formal state boundaries. Scholars such as Hugo de Grotius presented arguments about the types of behavior that should be forbidden in warfare, attempting to mitigate the very worst aspects of human conflict. The awful potential of gunpowder made the establishment of limits upon wartime behavior a desirable goal, and such limits could only be created during an era of peace. If every belligerent agreed upon a certain standard of behavior in war, or at the very least, agreed not to engage in the worst forms of action, the horrors of warfare might at least be somewhat limited. Later philosophers, most notably Charles-Louis Montesquieu and Emmerich de Vattel, built upon Grotius' arguments and established further norms of behavior in wartime. In general, the key considerations of wartime behavior can be summed up in two concepts: proportionality and discrimination.[2]

The notion of proportionality simply argues that any given action in a war should be proportionate to the type of conflict being fought. Essentially, it serves as a means to avoid a massive escalation of a conflict that might be contained at a much lower level. Proportionality does not require that every belligerent precisely copy the behavior of the enemy (although to do so would almost guarantee that a war would remain extremely limited), but it does require that a state actor give significant thought to the consequences before engaging in a disproportionate response. Of course, proportionality is, at least to a certain extent, in the eye of the actor, and what one belligerent considers an escalation in hostilities the other might consider a perfectly natural response. In theory, though, the proportionality idea should prevent one state from responding to a border incursion with a nuclear strike, and prohibits extremely powerful states from responding to minor provocations with full-scale attacks against weaker neighbors.[3]

Discrimination is the idea that warfare should be confined to military forces whenever possible. While it is an impossible standard to suggest that civilians should never be affected by interstate conflict, it is necessary that a belligerent's actions be able to specifically target the legitimate combatants and whenever possible spare the citizenry. Thus, if a weapon cannot be aimed in such a manner as to deliberately target a specific individual, vehicle, or unit, it could be considered indiscriminate. For this reason, general artillery bombardments of civilian populations are considered illegal, indiscriminate attacks, although that has not prevented their use from time to time. Likewise, area bombing of cities during World War II could easily be classified as an indiscriminate attack; to get around the prohibition, aerial attackers constantly claimed to be attacking a certain point

---

[1] P. W. Singer, *Wired for War* (New York: Penguin, 2009), 181-183; Colin S. Gray, *Strategy for Chaos* (London: Frank Cass, 2002), 69-73.

[2] Hugo de Grotius, *De Jure Belle ac Pacis*, trans. Francis W. Kelsey (1625; reprint, 1925), available at http://www.longang.com/exlibris/grotius/; Emmerich de Vattel, *The Law of Nations or the Principles of Natural Law* (1758), available at http://www.longang.com/exlibris/vattel/. For a shorter summary of the tenets of Just War, see Michael Walzer, *Just and Unjust War*, 4th ed. (New York: Basic Books, 2006).

[3] Keith Paulischek, "Proportionality in Warfare," *The New Atlantic* (Spring 2010): 21-34.

target of military value, and then wrote off the resulting collateral damage as the unfortunate result of an imprecise weapon. By the end of the war in the Pacific, even this degree of legal cover had largely been dropped, and the incendiary raids on Japanese cities demonstrated the dangerous potential of indiscriminate (and some would argue disproportionate) attacks.[4]

Warfare in the Twenty-First Century

Modern warfare in the twenty-first century has not been characterized by the large formations and attritional warfare of the World Wars, nor has it particularly resembled the large-scale insurgencies of the American war in Vietnam or the Soviet invasion of Afghanistan. Although American military forces would undoubtedly prefer most modern conflicts to resemble the Persian Gulf War, when an American-led coalition of nearly one million troops managed to drive the Iraqi occupiers out of Kuwait at a minimum of losses to the coalition forces, the coalition victory in 1991 demonstrated the futility of conducting such a war against the United States, NATO, or any of the permanent members of the United Nations Security Council. Rather, any belligerent that hoped to face off against the United States would need to negate many of the American advantages in technology, training, and logistics, and would need to seek to exploit perceived American weaknesses, if any could be found. In the run-up to the 2003 invasion of Iraq, it was evident to most military observers that the Iraqi Army had no chance of holding off an American-led attack. Its fortunes had only declined since 1991, while the coalition position in the region had been considerably strengthened. Aerial overflights gave a massive intelligence advantage to the coalition forces, which had a reasonably certain idea of the size, composition, and location of Iraqi combat units. Further, the coalition would commence any war with uncontested aerial dominance, an almost insurmountable advantage in twenty-first century conventional warfare.

The invasion commenced as planned, with a very quick drive from the Kuwaiti border directly toward Baghdad. The spearhead of the ground column gave little thought to flank security, which was effectively provided by the air cover overhead, and instead focused on quickly pushing into the Iraqi capital. Many American political leaders assumed that the Iraqi population would welcome the overthrow of Saddam Hussein, and would embrace the necessary short-term occupation of their homeland. Cultural misunderstandings aside, this mindset demonstrated both a shocking level of hubris and a total lack of awareness of the risks associated with moving into an urban occupation zone. Apparently, the lessons of the Battle of Mogadishu (1993), in which thousands of poorly-armed, completely untrained Somalis engaged much smaller American special operations forces in a two-day firefight that ended in an American fighting withdrawal after a successful raid, had failed to permeate the U.S. military. At the end of the fighting in Mogadishu, even though the Americans had inflicted more than 20-1 casualties upon their irregular attackers, it was the United States that abandoned the humanitarian mission and the militias that retained control of the city.

Countering the Coalition

In Iraq, an enormous number of well-trained troops who owed their position in Iraqi society to the Hussein regime proved far less amenable to life under coalition occupation than the planners had expected, especially after Paul Bremer's Coalition Provisional Authority government ordered the Iraqi military disbanded. Hussein's followers, particularly the special Saddam Fedayeen units, waited for the occupiers to move into the urban areas before launching a very widespread and well-coordinated insurgency. The urban locations largely negated American airpower and firepower advantages, as the resulting collateral damage from any heavy weapons use could be turned into a propaganda victory even if it initially ended in a tactical defeat. Further, the lack of raw numbers of coalition troops meant that many of the enormous weapons caches discovered in the march toward Baghdad remained unsecured, and open to plunder by any miscreants determined to resist the occupation. The insurgents quickly discovered that engaging in any form of direct tactical engagement with the American-led coalition forces was a recipe for disaster. On the other hand, the use of mines and roadside bombs soon became a favorite tactic of the insurgents. Soon, the number one casualty-creating activity for the Iraqi fighters was the use of improvised explosive devices (IEDs).

IEDs have a long history in warfare, stretching back to the first uses of gunpowder as an explosive. There has been almost an infinite variety of IED designs, but their basic premise is relatively simple. A bomb of some type is planted in the vicinity of where enemy troops are expected to pass, and detonated at a time when it can be expected to create the greatest number of casualties. Unlike land mines, an IED does not necessarily require the enemy to make direct contact with the device. Most, rather, are command-detonated at the most advantageous moment. This detonation might be through a mechanical device, an electronic pulse, or some form of wireless signal. The explosives themselves range from repurposed artillery shells buried in

[4] Geoffrey Darnton, "Information Warfare and the Laws of War," in *Cyberwar, Netwar and the Revolution in Military Affairs,* edited by Edward Halpin, Philippa Trevorrow, David Webb, and Steve Wright (New York: Palgrave Macmillan, 2006), 148-149.

the road to extremely complex shaped charges designed to create a penetrating effect capable of piercing even heavily armored vehicles. Although American forces were well-prepared for conventional combat operations, they had little initial ability to detect and counteract IEDs, and soon began to fall victim in staggering numbers. As the casualties mounted, public support for the war in Iraq steadily dropped, making the enemy able to offset many American advantages with a relatively simple device. Warfare is often characterized as a learning contest, and in the battle over IEDs, the concept certainly proved true. Each side sought to out-innovate the other, with the Americans developing better-armored vehicles designed to deflect bomb blasts; deploying jammers to block detonation signals; and clearing the roadways of any debris that might be used to conceal an explosive device. The insurgents, in turn, developed new ways to design and deploy their bombs, eventually hiding them in corpses, in heavily civilian areas, and in cars driven by unknowing accomplices. Unfortunately, the IED is a very easily-constructed weapon, the Internet is rife with instructions for how to construct simple yet effective devices. As the IED casualties mounted, the United States began to cast about for a new means of waging war that would not place so many U.S. troops directly in harm's way. The obvious solution was to find ways to wage war from afar, substituting machines for human combatants.

Military Robots and the Quest for Bloodless War

The search for a bloodless war led to the most terrifying development of warfare in the current century, specifically the emergence of robotic warfare. Although systems with a limited degree of robotic characteristics have been utilized in war for nearly a century, the newly-emerging machines are starting to be created with a level of environmental awareness and decision-making capabilities that are unprecedented. The mass media is currently enamored with the term "drone," although it is a thorough misnomer in that it evokes visions of a mindless machine carrying out its task without regard for the consequences or the surroundings. A remotely-piloted vehicle (RPV) has a human controller at some position, determining the actions of the machine, even if the pilot is not actually within the machine in question. The most common such systems are remotely-piloted aircraft (RPAs) which have become ubiquitous in the current American conflicts against terror organizations around the globe. However, the truly frightening machines, which have been designed and tested but not yet fielded, are those given autonomous control over lethal decision-making. Barring an international agreement to ban such devices, it is almost certain that one or more nations will choose to deploy such "killer robots" against an enemy, a move that will undoubtedly demonstrate their tactical utility, but which also might plunge the world into yet another arms race, one which could have devastating consequences for the human population of belligerent nations.

The earliest robotic military systems were simply unmanned flying bombs. The Kettering Bug was designed during World War I, but not put into production soon enough to be used against the enemy. The device, also called the flying torpedo, was an unmanned aircraft with a payload of explosives and enough fuel for a one-way trip toward an enemy position. It was preprogrammed to fly for a set number of minutes on a straight heading, at the end of which the engine cut out and sent the Bug plunging toward the enemy position. It had a range of fifty miles, but rarely managed to strike within a mile of the target.[5] By the end of World War II, the Germans had greatly improved the idea, firing off V-1 flying bombs toward Britain for the last several months of the war. These devices were essentially a bomb attached to a jet engine, their straight and level flight made them easy pickings for interceptors, which found the best countermeasure to be matching speed, altitude, and direction and then literally tipping the bomb over, causing it to crash into the English Channel.[6]

By the Vietnam War, the United States was fielding modified target drones outfitted with cameras to conduct aerial reconnaissance over contested territory. These aircraft really were drones, and could be sent into areas where a manned aircraft might face too much danger (or might cause an international incident if shot down). Dozens were sent across the Chinese border, with a number shot down by Chinese air defenses. On each occasion, the Chinese trumpeted their success in shooting down an American aircraft, but could not show off a captured pilot to complete the propaganda victory.[7] Shortly after the war ended, the United States began working on a series of remotely-piloted aircraft that might be able to gather much better intelligence because they could react to changing conditions on the ground. The most well-known such airframe, the General Atomics RQ-1 Predator, entered service in 1995. After some initial hiccups in its first deployments in the Balkans, the aircraft emerged as a key surveillance platform. Its long loiter time, relative low observability, and its ability to beam a data stream back to its operators made it a key tactical asset in the invasion and occupation of Afghanistan. In 2001, the military tested the idea

[5] Richard M. Clark, *Uninhabited Combat Aerial Vehicles: Airpower by the People, for the People, but Not with the People,* CADRE Paper No. 8 (Maxwell Air Force Base, AL: Air University Press, 2000), 8; Kenneth P. Werrell, *The Evolution of the Cruise Missile* (Maxwell Air Force Base, AL: Air University Press, 1985), 20.
[6] Werrell, *Cruise Missile,* 61-62; Michael Armitage, *Unmanned Aircraft* (London: Brassey's Defence Publishers, 1988), 7-16.
[7] William Wagner and William P. Sloan, *Fireflies and Other UAVs* (Leicester, UK: Midland, 1992), 11; Clark, *Uninhabited,* 12-15.

of firing AGM 114 Hellfire missiles from the Predator, thus allowing an operator the possibility of making an immediate attack upon a key target identified by the aircraft's sensors. From 2001 until 2009, Predators, and starting in 2007, MQ-9 Reapers, began to play an increasingly important role in the global fight against Al Qaeda, launching attacks in several countries and killing a number of key leaders of the terror organization and its affiliates.[8]

In the meantime, ground robotics also continued to advance, albeit with considerably less fanfare. One of the first goals for a fully-automated military system was the creation of a more effective air-defense system. The U.S. Navy debuted its Phalanx Close-in Weapons System (CIWS) in 1980. This radar-guided Gatling gun fires 20 millimeter shells at a rate of up to 4,500 per minute. It is designed to shoot down anti-ship missiles or attacking aircraft, each of which moves at a speed far too great for a human operator to have a realistic chance of scoring a hit. Thus, the Phalanx must, by definition, be fully automated, even if it has a human operator standing by to hopefully intervene if something goes wrong.[9] By 2003, a ground-based version of the system, the Centurion, was deployed for the mission of protecting American positions from rocket, mortar, and artillery projectiles. Other ground robots capable of combat missions include the iRobot PackBot, which has been most noted for its use in disarming explosives, but which can also be outfitted with weaponry, and the Talon SWORDS, a tracked robot that can carry rocket launchers, machine guns, or sniper rifles. While the SWORDS can be operated remotely by a human, it can at least theoretically be enabled to undertake autonomous operations.[10]

Currently, military robotics are moving in several developmental directions, including the creation of smaller, smarter, and more lethal variants. For many theorists, the true point of no return will be the deployment of a robotic weapon that is authorized to take human life without the permission of a human operator, often called the "man-in-the-loop." While some of the air defense platforms could theoretically kill in the performance of their duties, it is not necessarily their primary function, in that they exist to counter an aerial threat, not to kill enemy pilots. Many of the latest models in development, on the other hand, are envisioned to be extremely efficient killers, capable of eliminating targets without putting any friendly operators in harm's way, and with minimal collateral damage. It would not be difficult to marry a sophisticated facial-recognition software program to a camera-carrying platform with an attack capability, resulting in a robot that would be essentially a flying assassin, capable of loitering over an area and searching for an individual target, and then killing that target at the first opportunity.[11]

In the ongoing war against Al Qaeda and its allies, the United States, in particular, has become extremely reliant upon high-technology, remotely-operated systems. These platforms have allowed American decision-makers to largely wage war with impunity, secure in the knowledge that they can attack an enemy that cannot strike back against U.S. military personnel. However, no enemy in history has simply remained content to absorb the blows of an attacker and offer no retaliatory response. The attacks against Al Qaeda militants might keep American military personnel out of harm's way, but they also infuriate the citizenry in the areas where the attacks are launched, and almost certainly inspire attacks against whatever targets are within reach. Regrettably, those targets are far more likely to be civilians, including journalists, tourists, embassy personnel, or anyone else unfortunate enough to come within range.

The Advent of Cyberwar

The Internet can be not only an information source for designing weapons, but also the mechanism by which weaponry might be deployed. When the interconnection of computers was first envisioned, little thought was given for the security of such a network. Although the network itself massively expanded, the lack of an initial security protocol has led to endemic weaknesses within the infrastructure of the Internet.[12] As well, the computers and software upon which the Internet's functionality is based are filled with vulnerabilities that might be exploited by a knowledgeable computer user. By the 1990s, it was clear that an attacker could obtain control over a target computer, or at the very least, could significantly hinder its

---

[8] "Reaper Scores Insurgent Kill in Afghanistan," *Air Force Times*, October 29, 2010; Bureau of Investigative Journalism, "Covert Drone War," available at http://www.thebureauinvestigates.com/category/projects/drones/.

[9] Paul J. Springer, *Military Robots and Drones: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO, 2013), 53-54.

[10] Lorie Jewell, "Armed Robots to March into Battle," *Transformation* (December 6, 2004). Available at http://www.defense.gov/transformation/articles/2004-12/ta120604c.html; Damien McElroy, "Armed Robots Go to War in Iraq," *Telegraph* (London), August 5, 2007.

[11] Federation of American Scientists, "Low Cost Autonomous Attack System (LOCAAS) Miniature Munition Capability," available at http://fas.org/man/dod-101/sys/smart/locaas.htm; Pete Pachal, "Surveillance System Can Recognize a Face from 36 Million Others in One Second," mashable.com, http://mashable.com/2012/03/23/hitachi-face-recognition/.

[12] John V. Blane, ed. *Cyberwarfare: Terror at a Click* (New York: Novinka Books, 2002), 49; Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger Security International, 2013), 22.

function and ability to transmit useful information. Decades of experimentation with this new type of attack, usually dubbed cyber warfare, have only expanded the abilities of computer attackers, commonly referred to as hackers. The resources of states have been applied to developing cyber attack capabilities, and those nations that are most reliant upon cyber functions for both military and civilian infrastructure are by definition the most vulnerable to cyber attack.[13]

Thus far, cyber warfare has not directly caused a death, although many experts argue that it is only a matter of time before such an attack leads to a fatality. Cyber attacks have definitely contributed to military operations, though, with one of the most obvious examples being Operation Orchard. This incident involved an Israeli airstrike upon a suspected Syrian nuclear reactor that might have been used to produce nuclear weapons. In 2007, Israeli warplanes utterly destroyed the facility, which was still under construction by Syrian engineers assisted by North Korean advisors. Prior to the attack, a cyber attack rendered the Syrian air defense network inoperative by "spoofing" the radar operators' screens, essentially making the Israeli aircraft invisible on the screens. The first indication that anything was amiss came with the explosion of Israeli ordinance upon the Deir ez-Zor site, which was subsequently filled in and bulldozed by Syrian authorities, who also denied the existence of any nuclear program.[14]

The other most well-known, and somewhat mysterious cyber attack came in 2010, when an extremely sophisticated worm program was introduced to the Iranian nuclear reactor computer system at Natanz. The self-replicating program quickly spread throughout the Iranian network and searched for a very specific form of programmable logic controller used to run uranium-separation centrifuges. Upon locating its target, the worm then slightly modified the logic controllers' instructions, causing the centrifuges to undergo violent changes in their spinning frequencies. Over time, this destroyed a substantial portion of the centrifuges and greatly set back the Iranian nuclear program.[15] Even after the damage became evident, it was still more than a year before a little-known Belorussian cybersecurity firm announced that it had discovered a malignant program that it dubbed "Stuxnet." The program could only have been created with the resources possessed by an extremely advanced cyber state, although no nation has formally claimed responsibility for the attack. The most likely candidates, based upon both technological capability and political desire for such an outcome are the United States and Israel, but neither nation has responded to allegations of planting the program.[16]

The Need for New Limits Upon War

While these advanced platforms might offer the illusion of warfare with minimal human casualties, it is far more likely that they will only delay the inevitable human deaths that are created by war. The most fervent proponents of the devices tend to have two lines of argument. The first is that the robots might be able to create a permanent advantage for the first adopters of these devices, essentially locking in the current world power dynamic. However, given the low cost of entry into this field of innovation, this is an extremely unlikely, and quite frankly dangerous, idea of why to adopt such weaponry. The second is that warfare might be relegated to a conflict of machines, with the losing side in the robot war laid open to attack, but naturally conceding the argument that led to the conflict before facing attack. Unfortunately, previous RMAs have led to a similar argument, most recently when airpower advocates argued that warfare would become almost sterile after the adoption of military airplanes. Early airpower theorists like Hugh Trenchard, Billy Mitchell, and Giulio Douhet all argued that the aerial armadas of modern states would meet and fight for supremacy of the air. Once one side's airpower had triumphed, the loser would inevitably surrender rather than face the devastation of an uncontested aerial bombardment. Nearly a century of aerial warfare has demonstrated the farcical nature of this argument, and yet it continues to be spouted in numerous airpower arenas. Not even the massive devastation of German cities, the firebombing of Japan, and the atomic destruction of Hiroshima and Nagasaki caused the advocates to drop their assumption that enemies would refuse to withstand aerial attacks. It is highly unlikely that a robotic war would simply stop once one side exhausted its supply of machines—instead, the war would devolve from a contest to a slaughter, making the nature of human conflict infinitely worse, but with little or any mediation of the horrors of modern war. Only a deliberate effort to enact and enforce an outright ban of autonomous lethal military robots stands a chance of preventing such a conflict.

---

[13] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2009), 37-43.
[14] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Great Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 1-9; Richard Stiennon, *Surviving Cyber War* (Lanham, MD: Government Institutes, 2010), 54-55.
[15] Rosenzweig, *Cyber Warfare*, 2-12; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011), 102-105; Roman Poroshyn, *Stuxnet: The True Story of Hunt and Evolution* (Denver: Outskirts Press, 2013), 48-50.
[16] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014), 114-118.

The United States, as the foremost developer and user of military robotics, is the only world power that can take the lead on an effort to set limits upon the utilization of military robotics. Instead, though, the United States is doubling down on its investments in high technology killing machines, and essentially refusing to consider setting limits on what it currently considers to be a major asymmetrical advantage in the ongoing conflicts with Al Qaeda, the Islamic State, al-Shabaab, and other terror organizations. Every generation that engages in conflict is forced to examine the limits of acceptable behavior, and to consider whether or not the current rules are still an accurate reflection of the realities of warfare in their era. In the twenty-first century, the laws of armed conflict, developed before the advent of cyber warfare and military robotics, are simply not up to the task of providing an effective governance system for modern conflicts, and thus must be revised to reflect the new paradigm. If the United States does not take the lead in such an effort, the effort cannot succeed, and the likely future of military engagements will truly become more terrible for all involved.