Are new technologies undermining the laws of war?

Braden R. Allenby

Abstract
Throughout history, new military technologies have had profound ramifications: The rise of gunpowder and cannon created economies of scale that encouraged the emergence of nation-states, and Prussia used railroads to surprise the Austrians at Königgrätz, beginning the end of the Austrian Empire. Today, emerging military technologies—including unmanned aerial vehicles, directed-energy weapons, lethal autonomous robots, and cyber weapons—raise the prospect of upheavals in military practice so fundamental that they challenge assumptions underlying long-established international laws of war, particularly those relating to the primacy of the state and the geographic bounds of warfare. But the laws of war have been developed over a long period, with commentary and input from many cultures. What would seem appropriate in this age of extraordinary technological change, the author concludes, is a reconsideration of the laws of war in a deliberate and focused international dialogue that includes a range of cultural and institutional perspectives.

Keywords
emerging technologies, international humanitarian law, laws of armed conflict, laws of war, military technologies

Although the armed forces are inherently conservative, almost every senior officer in any modern military can reel off cases when technological advance changed military history. New security technologies have often had profound cultural and social implications: Chariots, which required supporting personnel and money to operate, privileged aristocratic warriors; stirrups elevated the mounted horseman and made the steppe warrior with his composite bow feared for centuries; the rise of gunpowder and cannon profoundly changed the logistics necessary to field an army, and thereby created economies of scale in military activities that encouraged the rise of nation-states. Indeed, historians have coined the term “gunpowder empire” to refer to those states—the Turkish Ottoman Empire, the Safavid Empire of Persia, the Mughal Empire in India, the Russian state, Spain and the Spanish New World, among others—that arose in part as the potency of gunpowder technology played out over time.

Some battles are famous for the role that technology played in them: In 1866, for example, the Prussians, up until then
a second-class European power, used railroads to surprise the Austrians at Königgrätz, in a battle that marked the rise of Prussia to great-power status and, conversely, contributed to the beginning of the end of the Austrian Empire. More recently, the integrated air-land-battle technologies used during the Desert Storm invasion of Iraq in 1991 resulted in an estimated 20,000 to 30,000 Iraqi military casualties, with fewer than 200 coalition military casualties from enemy action. That one-sided, 100-hour US victory led China (among other countries) to re-evaluate its entire defense strategy.

Today’s emerging military technologies—including unmanned aerial vehicles, directed-energy weapons, lethal autonomous robots, and cyber weapons such as the extraordinary Stuxnet—raise the prospect of upheavals in military practices so fundamental that they challenge long-established laws of war. The possibility of weapons that make their own decisions about targeting and killing humans, for example, has ethical implications obvious and frightening enough to have entered popular culture.

But even a cursory investigation indicates that the relationship between technological change and the laws of war is more complex than it first appears. Accelerating evolution across the technological frontier and dramatic increases in the numbers and kinds of social institutions at play around the world are blurring previously clear boundaries between military and civil entities and state and non-state actors. Moreover, all leading nations today share an understanding: Scientific and technological capability and innovation are critical competencies for great-power status. And because the United States has an acknowledged primacy in terms of conventional forces, the nations and groups that compete with it increasingly think in terms of asymmetric warfare that often raises issues lying beyond established norms of military conduct.

But both technology and broader social and political changes—such as the rise of global, networked terrorist institutions—could be undermining the laws of war. More broadly, if long-standing legal, cultural, and civil institutions are being destabilized by modern rates of technological change, there may be ways to make them more adaptable. The rate and nature of such change could mean that, at some point, old institutions must be jettisoned in favor of new ones. When talking about technology and the laws of war, one is also talking about just one example of a more general concern: How well will the world adapt to rapidly changing conditions that make previous assumptions and belief systems increasingly arbitrary, partial, and obsolete?

**Laws of war?**

The idea that there should be laws governing war is only one of three general perspectives. The realist perspective holds that, because states are not bound by anything save their own self-interest, whatever needs to be done to protect that national interest is permissible. It follows from this viewpoint that the idea of laws of war is a category mistake. On the other end of the spectrum, the pacifist perspective holds that war is entirely evil, and that no war can be ethical or moral. In such a view, any attempt to make war more palatable, such as developing norms and laws of war that reduce collateral damage, is simply
lipstick on a pig; worse yet, by pretending to make the pig less ugly, it undercuts the real issue, which is that a pig will always be a pig. Very few actors hold to these perspectives in their pure form, which means that most countries and militaries today adhere to a middle way that includes some form of the laws of war.

The laws of war can be broken down into three categories. The first, *jus ad bellum*, deals with questions of when countries can legally and ethically initiate conflict. In the modern world, this will generally be when a country is attacked, or when it is defending another country that has been attacked. Preemptive aggression is controversial in international law, especially when evidence that a country is actually about to be attacked seems not to be overwhelming (as was the issue with the US invasion of Iraq in 2003). The rights to self-defense and “other-defense” are enshrined in Article 51 of the United Nations Charter; many legal commenters would argue that when situations are unclear, as in a civil war or internal genocide, or when preemptive strikes are at issue, UN Security Council authorization is necessary. Such arguments also make the important point that the UN and particularly the Security Council play a critical role in much of this area of international law. Actually, though, this area is not well codified: In the 2003 Iraq War, the Bush administration made non-trivial legal arguments that the US invasion was justified, based on previous UN votes concerning Iraq and weapons of mass destruction and on grounds of self-defense against terrorism, even though the Security Council did not explicitly approve the preemptive attack. Regardless of how one views that conflict, it is instructive that the Bush administration felt compelled to engage international law on the *jus ad bellum* issues—and equally instructive that, while advocates make strong arguments on both sides, it is not blindingly clear that the administration’s arguments were legally wrong.

The second category of the laws of war, *jus in bello*, concerns ethical and legal behavior once conflict is under way. This body of law is familiar to anyone who has been a member of the military and trained in the requirements of the Geneva and Hague conventions, as well as the many other applicable formal treaties and statutes. This second category is generally referred to as international humanitarian law, or the law of armed conflict. Although a complex and detailed area of law, a few of its fundamental principles are worth emphasizing because emerging technologies could interact with them in ways that undermine their authority or universality, challenging the legal structures built upon them. Perhaps the most important is the principle of distinction (sometimes called discrimination): Combatants must distinguish between civilian non-combatants and combatants, and between civilian assets and military assets; they can only intentionally attack military targets. A related principle is proportionality; a combatant’s activities must be proportionate to their military objectives and responses must be proportionate to the circumstances. A soldier cannot, therefore, respond with lethal force to a shouted insult, nor can a nation launch a nuclear strike in response to a border incident. The requirements of distinction and proportionality do not rule out collateral damage—civilian death and the destruction of non-military objects—so long as
the military action is otherwise lawful and the military objective is worth the unintended collateral damage. (Intended collateral damage is simply an attack on civilians, which is clearly unlawful.) There are a number of other provisions; for example, combatants may not use weapons that are *mala in se*, or evil in themselves, such as nerve gas.

The third category of the laws of war, far less developed in history and theory than the first two, has been called *jus post bellum*, and involves issues arising from creating a just peace. Though few norms and principles in this area are widely accepted, the potential benefits of considering this stage of conflict are obvious: Would an agreement less punitive than the Treaty of Versailles have lessened the possibility of World War II? If regime change is the goal of a conflict, what are the rules that govern the post-war process that produces a new regime? What are the legal and ethical quagmires associated with reconciliation with regimes that have committed atrocities, if reconciliation enables a negotiated end to a conflict?

Because *jus post bellum* is relatively new, it is less tied to historical precedent and less locked in to institutions and legal documents, so questions about existing laws and norms of war arise primarily in regard to *jus ad bellum* and *jus in bello*.

**Technology and war**

Technological evolution and military activity have been coupled throughout history. War often poses major threats to the existence of societies; new technology can provide critical advantages—and create difficult challenges when the rate of technological change is high. But the relationship between technological advance, military practice, and social change is complex. The following three observations only begin to illustrate that complexity.

First, especially in complex situations such as war, technology is coupled to many other functions, such as administration, logistics, bureaucracy, and politics. A significant change in technology can therefore result in a co-evolutionary spiral, as associated changes ripple across a network of social, cultural, institutional, built, and natural systems. This rippling tends not to comport with either utopian fantasies of happy technological solutions to complex human situations (arguably part of the naive neoconservative conceptualization of the 2003 Iraq War) or dystopian fantasies of technology run amok on its own. After all, nuclear weapons are, potentially, the amok-running technology par excellence, and human systems and behaviors (with perhaps some luck) are what have so far forestalled nuclear disaster. This observation matters; many participants in debates about military and security technologies, regardless of where they fall on a utopian-to-dystopian scale, often focus on technologies as if they, and not the people who design, deploy, manage, or oppose them, are what counts.

Second comes a related observation: The rules by which people try to govern conflict play an important role in managing the destructive impacts of technology. It is therefore critical to know when technological advances and associated social, institutional, and psychological changes challenge such rules, so they may be adjusted or redrawn. Since fundamental change is now emerging unpredictably across the technological frontier, and the geopolitical
structure of conflict is shifting from the relatively defined outlines of the Cold War to a much more complex environment, the rule changes required are not easy to explicate or address. Moreover, there is significant inertia in the system, since many people and institutions are invested in the success of the existing frameworks for regulating war.

A third point is hinted at by the famous line attributed to theorist Leon Trotsky: “You may not be interested in war, but war is interested in you!” (Actually, this may be a generous translation of a more doctrinaire observation about the dialectic, but it is effective nonetheless.) The technologies of war interact and co-evolve with civil institutions and cultures in ways that are often unexpected and significant. The value of a cyborg insect, or a small robot that is part of a battlefield-wide computational grid, may be quite obvious in the military context, especially in counterinsurgency environments. But the same devices, as they filter back to highly partisan media organizations and armies of divorce lawyers who want information on spouses of their clients, may have quite different implications. As military radio frequency identification, biometric, and sensor technologies—all of which are proving to be quite useful in the complex combat environment of Afghanistan and other counterinsurgency conflicts—are shifted from theater operations to civil society, the implications for privacy and civil rights could be negative and substantial. Technologies that enable more direct design of human bodies and cognition could be very effective for warriors, but if not reversible, they could raise difficult issues for social stability when designed humans return to civil society. History clearly warns of the inequitable way that many societies have dealt with race, gender, and physical and sexual-preference differences. It’s a harsh question, but one that should be asked: Will cyborgs be welcomed home from the front?

As historical example strongly suggests, new technologies are likely to destabilize internal military cultures and practices as well. Today, for example, the US armed forces are trying to manage the transition from manned combat aircraft to unmanned, remotely controlled unmanned aerial vehicles, and on to largely autonomous air vehicles. The new technology requires not just different skills, but fundamental shifts in military culture and organization as well: Leaders who emerged from traditional air combat environments will not necessarily have the same values or behave in the same way as leaders who excel in the Air Force because of their ability to play advanced video games whose graphics and operation closely mimic the real world of pilotless aircraft. And subtle questions of culture and organization matter when, for example, autonomous combat aircraft raise questions of compliance with the laws of war.

**Changing contexts**

The laws of war and international humanitarian law are challenged today not just by technology, but by a perfect storm of cultural and geopolitical change. Many of the working assumptions that have been stable over much of the past centuries, and which have formed an unquestioned but critical underpinning for existing laws and norms, are stable no more. A look at four emerging military technologies helps illustrate this disruption.
Why, for example, are military unmanned aerial vehicles so contentious? They are, in one analysis, just another platform for keeping an eye on, and striking, the enemy from the air. But with the increasing deployment of unmanned aerial vehicles, the United States has asserted the right to make strikes around the world, a position driven not by the technology itself, but by the global nature of terrorism and the jihadist movement. This new conceptualization of the battle zone, however, sits uncomfortably with the assumption underlying the laws of war: When those laws were conceptualized, combat zones were geographically constrained and obvious, making it relatively easy to differentiate between combatants and non-combatants.

Unmanned aerial vehicles raise other issues, as well: An unmanned US aircraft may be operated by the US Air Force, in which case international humanitarian law will be applied in full. Or it may be operated by the CIA, in which case the only law that may apply is the law of the country where the event takes place. Or the unmanned aerial vehicle might be operated by a private military contractor, in which case it is not clear what law might apply. To make things worse, the ever-expanding battlefield might be occupied simultaneously by the same model of remotely piloted aircraft, controlled by different actors operating under all three of these legal regimes in ways that are not at all transparent or institutionalized. Attributing this complexity to unmanned aerial vehicle technology is a mistake of attribution; it’s like blaming your computer for the Facebook posting that your sweetheart used to break up with you.

And what about directed energy weapons, such as the US Army’s Active Denial System, a non-lethal weapon that causes those who are targeted to feel a painful heating sensation? It is ideal for crowd control. But if you are in a combat zone, and you need to control a crowd, the military method has been and remains simple: a machine gun. Non-lethal crowd control is a policing function, not a combat function—so the technology becomes useful only as pure military objectives fragment into policing, nation-building, and other functions. The norms embedded in the laws of war are those applicable to combat, not to policing; the more that one tries to apply them to policing, the more one compounds yet another category mistake. That such technologies are needed for military operations in the Afghan and Pakistan border areas simply reflects a fact of the new technological, cultural, and geopolitical order: Combat is today only one of the functions that a military finds itself struggling to manage. The old mental models and vocabulary of the laws of war break down under the challenges of this new complexity.

Lethal autonomous robots are machines programmed and deployed with the ability to identify, track, and eliminate targets without human intervention—even, in theory, if those targets are other human beings. The implications of such creations have so far been a source of much heat and far less light regarding the applicability of the laws and norms of warfare. Indeed, such machines are already deployed in the Korean DMZ; some US weapon systems, such as the Aegis fire control computer system on some US naval vessels, usually operate under the control of humans but have an autonomous mode that allows the weapon to operate on its own in extreme conditions. Why? In part,
the move toward autonomous weapons is a response to the increasing speed and complexity of modern warfare; the ability of humans to keep up can only be augmented to a certain degree. A ship under coordinated attack with modern weapons is toast if it relies on human perceptual and cognitive cycle times for its defense. Efficiency and demographics also play a role in military autonomy: Most countries with world-power aspirations are aging, and the number of young people available to become boots on the ground will inevitably go down at some point. In this context, autonomous weapons become, simply, the substitution of capital for labor.

While highly contentious, autonomous weapons do not necessarily pose the foundational challenge to the laws of war that other military technologies can. Much of the ethical discussion revolves around whether lethal autonomous robots—whatever they may end up looking like, or doing—will be able to, for instance, discriminate between military and civilian targets the way that humans do. This is a factual question that depends on future research and development for resolution; efforts to answer it definitively right now tend to represent the triumph of ideology over technological reality. But humans clearly do not always themselves comply with the discrimination requirement of international humanitarian law, leading to a sub-discussion: Must a robot be perfect in its compliance with international law, or simply much better than humans?

If there is a game-changer among these four examples, it’s probably the revolution in cyber weaponry, which raises a multitude of intertwined legal and social questions. For example, cyber networks are routinely and heavily dual use—that is, civilian and military traffic travels through them. These uses overlap to a far greater degree than, say, an occasional military convoy on a highway system. Moreover, such networks are by their nature not bound by geography; a signal from two allied nations may pass through many other nations that facilitate the information transfer.

This global mixing of civilian and military activity poses interesting challenges to a body of law and practice that, after all, grew up in the physical world. For example, if a military command implementing an attack passes from the United Kingdom to the United States via South Korean servers, those servers, and the South Korean technicians who operate them, could or could not be potential targets for response from the opposing military power, depending on how one interprets current international laws. The same could hold for US information technology and communications firms like Microsoft and Google, which provide much functionality to these dual-use networks and hence to the US military and which could be considered war-supporting entities equivalent to munitions factories, and therefore legitimate targets, or not, depending on legal reasoning. Determining who is and is not a combatant also becomes difficult in the cyber realm. When Russia invaded Georgia in the 2008 South Ossetia War, groups such as the criminal hacker organization Russian Business Network simultaneously attacked Georgian Internet resources, which could make RBN members combatants subject to military attack, or, simply, civilians, depending on one’s point of view. Many nations appear to use informal, patriotic privateer parties to augment their conflicts with others. Are such entities responsible
for compliance with international humanitarian law, or are they only subject to local civil and criminal law? If the latter, just how effective will that be?

More seriously, the essence of cyber warfare is non-attribution: It is very difficult, especially in real time, to pierce the anonymity of the Internet and identify attackers. Even in the case of Stuxnet—a computer worm sophisticated enough to attack the supervisory control and data acquisition software of Iran’s nuclear centrifuge operations—it is difficult to assert the source with certainty, although winks and nudges indicate that it most probably originated with the United States and Israel. Because most such attacks rely on tricking opponents into using malware, they may well violate international humanitarian law strictures against “perfidy,” traditional forms of which might include falsely marking tanks as hospital vehicles. Attribution is a critical issue for other reasons: Under jus ad bellum, a nation can legally respond when attacked. Suppose someone puts a host of logic bombs in your country’s networks—your transportation infrastructure networks, your energy and grid networks, and so forth—but doesn’t activate them. Whether your country can legally retaliate, and if it can, against whom are open questions. A tank comes from an identifiable party; a computer worm, not necessarily.

**Unsatisfying answers**

Experts are beginning to focus on the legal questions raised by emerging, disruptive military technologies and associated cultural and geopolitical changes, but so far their answers are not entirely satisfactory. The US Department of Justice white paper (2011) that explains the legal basis by which it justifies lethal unmanned aerial vehicle attacks anywhere in the world has the air of a document that is trying hard to stretch existing laws over gaping holes that they were never meant to cover—and in fact don’t. Global terrorism by non-state actors who are not part of any military, do not act at the behest of any state, are highly mobile at a global scale, may be acting militarily only a small percent of their time, and view the world as their battlefield and civilians as prime targets is not a form of conflict the laws of war were designed to cover. But then, national criminal laws are also too limited to be effective against global jihadism, except in special cases.

NATO’s Cooperative Cyber Defence Centre of Excellence has written the Tallinn Manual (2013) in an effort to address some of the relevant legal issues raised by cyber warfare, but many of them, such as lack of attribution, remain difficult to deal with in legal codes. It is difficult to say when a country actually has been attacked, or what level of proof regarding an attacker’s identity is required before a response would be deemed to comply with the laws of war. And although this essay has focused on four technologies, the entire technology frontier is in rapid and unpredictable motion. International law could be challenged, for example, by the advent of true cyborg systems, with humans directly linked via computer–brain interfaces to geographically remote weapons. The challenge to existing humanitarian law could be at least as serious if a nation or nations begin to genetically engineer warriors.

War becomes something new when, as in Afghanistan, it combines a witches’ brew of local and regional state and
non-state actors and involves global networks of intelligence and terrorism. It is one thing for military organizations to span the world. But now individual weapon systems are global in scale in real time, with unmanned aerial vehicles operating throughout the Middle East—controlled from bases in Nevada. Is the NATO soldier along the Afghanistan–Pakistan border there to engage in combat, to conduct espionage, to police, or to nation-build? Each of these very different missions requires different organizational culture, training, and technology, and they are governed by very different legal and ethical regimes.

New military technologies have short-term and obvious institutional implications, but also longer-term and more fundamental impacts on military organization and structure. The scope and rate of technological change now under way suggest that a revolution in military operations and culture is also under way. The rise of gunpowder armies in Europe created economies of scale in military operations that were an important factor in the ascendancy of kingdoms over earlier feudal forms of social organization. Now, one cannot look at the speed and scale of technological change without wondering how it will affect not just military organization but the structure of society itself.

**Careful changes in the laws of war**

It is highly unlikely that the dramatic impacts of emerging military technologies and changing institutional and geopolitical contexts render the laws of war—as a body of law, institutions, and practices—obsolete. Fundamental, pervasive technological changes across virtually all relevant domains will, however, destabilize at least some of the deep assumptions underlying the laws of war. One of those involves the primacy of the state, a long-standing fixture of all international law. Another assumption—that warfare is inherently kinetic, and that the battlefield upon which it occurs is obvious and bounded—also shows at least some fraying at the edges. Another question: Should the international community be so doctrinaire about assuming that the condition called war is still separable from other, increasingly intertwined conditions of conflict such as policing and terroristic violence? The integrated use of very different types of organizations—military, police, espionage, nongovernmental, and private for-profit—in a wide range of conflict situations brings different norms and legal structures into play, calling out for clarity as to which might apply, and which need to be updated to fit current circumstances.

Even so, truly discontinuous change in human systems is very rare. The laws of war constitute a body of formal and informal law, norms, and practices that have been developed over a long period, with commentary and input from many cultures. It is neither desirable nor likely that such a robust and developed framework should suddenly become totally obsolete. As a practical matter, there will certainly continue to be conventional military conflicts between states that should continue to be governed by the existing laws of war. Even in non-traditional environments, the laws of war would apply to conventional operations. That unmanned aerial vehicles may attack terrorist leaders in Yemen does not mean that NATO forces in Afghanistan can ignore international
humanitarian law. Of course, this situation also illustrates some of the difficult issues that arise as different legal and ethical regimes intersect in the same operational domain.

What would seem to be appropriate, therefore, is neither the wholesale rejection of the laws of war nor the comfortable assumption that only minor tweaks to them are necessary. Rather, these laws should be reconsidered in a deliberate and focused national and international dialogue that includes, to the extent practicable, different cultural and institutional perspectives. In establishing such a dialogue, it would be helpful to realize that the superiority of the conventional forces of the United States creates strong pressures for asymmetric warfare; that the idea of geographically bounded conflict is questionable in a world of global non-state terrorism, global cyber networks that are clearly dual use, and unrestricted warfare strategies; and that the state-oriented perspective of existing international humanitarian law is inadequate. Individual militaries should conduct war games and scenario exercises that are specifically designed to challenge the assumptions and norms embedded in the laws of war, to identify gaps and weaknesses that require responses. These activities should aim to generate options that will enable ethical responses to unpredictable change and encourage agile and adaptive institutions and legal frameworks, rather than sub rosa efforts to undermine existing and still appropriate law. Those with serious interest in international humanitarian law and associated institutions should not regard such initiatives as threats, but as recognition of the importance of the laws of war and a desire to maintain them in the face of accelerating change.

The challenges to the laws of war posed by technological evolution and associated social and geopolitical changes are not unique to this domain. Neuroscience may soon challenge humanity’s assumptions about free will and perhaps destabilize ideas about legal, especially criminal, liability; the planet may be geo-engineered in response to climate change; and the human being may increasingly become a design space. Maintaining institutional and social continuity while responding responsibly, rationally, and ethically to such profound and unpredictable change is a skill that heretofore the human species and its societies have not managed well. The impact of emerging technologies on the laws of war might be viewed as a case study and an important learning opportunity for humankind as it struggles to adapt to the complexity that it has already wrought, but has yet to learn to manage.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes
1. Unmanned aerial vehicles are often called drones, a term avoided here to limit confusion with military drones, i.e., airborne targets.
2. One can argue about interpretation; one cannot argue that the US military fails to consider international law under such circumstances.

References

Author biography
Braden R. Allenby is Lincoln Professor of Engineering and Ethics; President’s Professor of Civil, Environmental and Sustainable Engineering; founding chair of the Consortium for Emerging Technologies, Military Operations, and National Security; and founding director of the Center for Earth Systems Engineering and Management at Arizona State University. He received his bachelor of arts from Yale University, his law degree and master of economics from the University of Virginia, and his master of science and doctorate in environmental sciences from Rutgers University. He is past president of the International Society for Industrial Ecology; a member and ex-chair of the American Association for the Advancement of Science Committee on Science, Engineering, and Public Policy; a Batten Fellow in Residence at the University of Virginia’s Darden Graduate School of Business Administration; and a fellow of the Royal Society of Arts.