ASU Lincoln Center for Applied Ethics
ARIZONA STATE UNIVERSITY

2012 Chautauqua Council Final Report

Implications of Emerging Military/Security Technologies for the Laws of War

Prepared by
Carolyn S. Mattick, Council Secretary
Braden R. Allenby, Council Chair
George R. Lucas, Jr., Council Co-Chair

This document is a summary of a week-long workshop, the 2012 Chautauqua Council on the Implications of Emerging Military/Security Technologies for the Laws of War, sponsored by the Lincoln Center for Applied Ethics at Arizona State University and held at the Chautauqua Institution in New York from July 29 to August 5, 2012. The intent of this document is to encourage dialog on these important issues among a broader public. It does not necessarily represent the views of any of the participants or those who have prepared it, nor of the institutions and organizations to which they belong, and the views, positions, hypotheticals, and conclusions contained herein should not be attributed to any individual or institution participating in or associated with the Council.

ASU LINCOLN CENTER for APPLIED ETHICS
ARIZONA STATE UNIVERSITY

Executive Summary

"Every age had its own kind of war,
its own limiting conditions,
and its own peculiar preconceptions."

– Baron Karl von Clausewitz [*Vom Krieg*, Book VIII]

Technology and armed conflict are inseparable. Yet, just as technological advancement imparts a military advantage to its owner; it simultaneously renders old norms obsolete and can destabilize social institutions – include the laws of armed conflict themselves. The 2012 Chautauqua Council on Emerging Technologies and 21st Century Conflict represented the first of potentially many meetings sponsored by the Lincoln Center for Applied Ethics in collaboration with the Consortium for Emerging Technologies, Military Operations, and National Security meant to identify gaps in current knowledge regarding the evolving nature of the battlefield and to help define an agenda for future research. Its ultimate goal is to produce intelligence that can enhance long term military and national security in the 21st century.

This inaugural meeting brought together a group of nationally-recognized scholars, leaders, and experts in fields including ethics, philosophy, policy, international law, and relevant technical disciplines as they relate to military operations and national security. These experts were asked to debate the question, "Are the Laws of War (and related legal, ethical, and governance mechanisms) rendered obsolete in whole or in part by emerging military/security technologies?" In order to focus the discussion and develop useful scenarios, the analysis was deliberately limited to three of the most significant new technologies: cyber warfare, robotics, and non-lethal weapons. These were discussed against a background of contextual changes that included the trend toward privatization of war (and state sponsored violence) and the democratization of weapons of mass destruction.

Ultimately the Council concluded that a series of solid legal principles exist, and that a useful first step is to assess emerging technologies against those principles to determine whether those existing legal principles continue to adequately address technologies as actually utilized in practice. If not, new laws and practices, among other measures, may be necessary. Indeed, this inaugural Council meeting highlighted a number of issues that will require ongoing consideration. Among these is the need for constant and active review of the laws of armed conflict (LOAC), also referred to as international humanitarian law (IHL), using tools such as scenario analysis of emerging technologies. Human enhancement, in particular, is an area of active technology development that could expose voids, disparities, or anachronisms in the laws of war.

The meeting closed with a research agenda raising two fundamental questions: (1) Regardless of any legal or ethical framework, if observed objectively, what norms of conflict do diverse cultures practice, including, in today's world, private firms and non-state actors? (2) Even though the existing laws of war continue to be refined and expanded, are they keeping pace with the conduct of war in a complex global context of rapidly-coevolving technologies? Both questions are expected to form the core of investigations to be carried out by Council members going forward. They will work somewhat independently but will meet annually to discuss results and coordinate future work.

The Council's work advances two agendas. First, in coordination with the Consortium for Emerging Technologies, Military Operations, and National Security, the Council seeks to help understand the implications of emerging technologies for existing military and security institutions, itself a critical question. Second, the Council is supported by the Lincoln Center for Applied Ethics at Arizona State

University in order to provide greater understanding, and case studies, regarding the broader question of how emerging technologies affect individuals, institutions, cultures, and society as a whole, a particularly critical issue in a period of rapid, unpredictable technological evolution.

As a definitional matter, this report will use "laws of war" to include the customary and written laws and regulations, and associated practices, that generally govern the initiation of, and conduct during, and after, conflict situations, including but not limited to, LOAC/IHL (in general, LOAC/IHL applies when conflict has already started, but does not govern the legitimacy of conflict initiation; for more information, see the website of the International Committee of the Red Cross, http://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf). Additionally, the concept of "war" should be understood broadly as including active conflicts between states, within states, and between state and non-state actors. It is an indication of the current state of affairs that one cannot identify "war" solely with kinetic or physical attack because of the possibility of cyber conflict: when cyber conflict is "merely" cybercrime, and when it rises to the level of "war" under applicable international norms, standards, and law, remains somewhat ill-defined.

Introduction

"You may not be interested in war, but war is interested in you."

– Attributed to Trotsky

Context and background

Throughout history, technological evolution and military activity have been linked. The existential challenge to society represented by warfare, combined with the immediate advantage that new technology can deliver, tends to accelerate technological innovation and diffusion. The relationships between the resulting technology systems, and consequent social and ethical issues and changes, are quite complex, however, and understanding and managing them to enhance long term military advantage and security is a critical and underappreciated challenge. This is particularly true when, as now, the rapid pace of technological change is itself accelerating, posing the risk of cultural backlashes that could affect both short term mission capabilities and longer-term security interests.

The purpose of the Council was principally to map the higher level challenges to military effectiveness and national security posed by emerging technologies, to identify gaps in current knowledge, and to provide information, insights and analysis that might, in turn, further the development of policies and procedures supporting strong military and national security capabilities at all scales. The Council's purpose was not in any sense to replicate or replace research and analysis focused on specific technologies, scenarios, or potential surprises; rather, it was to perform a qualitative, somewhat comprehensive, analysis to help form and guide policy across the sectors of specific technologies and their respective military and societal implications.

Emerging technologies and laws of war

The initial workshop focused on the area of the formal and traditional laws of war, evaluating earlier treaties and codified military practices in the context of emerging technologies and evolving social, institutional, and political trends. Specifically, the workshop was designed as a broad inquiry into how emerging technologies and trends are currently, and might in the future, affect the traditional laws and norms of military conflict (including the duty of governments to protect their citizens).

Underlying the inquiry was the Tradition of the Just War – in particular the criteria of *jus ad bellum* (just engagement in war) and *jus in bello* (just conduct in war) – alongside the body of international law within which the theory has gradually been codified (for those who may not be familiar with Just War theory, a summary is provided in Appendix A, p. 38). In fact, international treaties (including the 1868 Declaration of St. Petersburg and Protocol 1 of the Geneva Conventions in 1977) call upon nations to assess the conformance of emerging technologies with international law, but fail to impose a structure through which this could be accomplished. Thus the possibility exists that emerging technologies may be weaponized and deployed without adequate regard to the existing norms of armed conflict, or, alternatively, introduced into situations where existing norms and laws do not adequately address issues associated with emerging technologies, perhaps with devastating results. Although this workshop was not intended to prevent such occurrences, its participants aimed to project possible futures resulting from current trends in order to inspire and inform national and international dialog on armed conflict policy. It has also strived to lay a foundation upon which future research in this area can be based.

The importance of collaboration when analyzing the techno-security challenge becomes more apparent when one considers the multitude of variables at play (as shown in Figure 1). In sum, this figure indicates that Conflict in the 21st Century (at the center of the image) is influenced simultaneously by changes in

four domains: Civilian Systems, Military Operations and Culture, the Nature of Conflict, and evolving Military Technologies. Whereas many of the underlying dynamics of these variables have been relatively stable over past centuries, the accelerating pace of change has rendered many formerly-valid assumptions increasingly obsolete. Among these, for example, is the assumption that government atrocities directed at groups within their borders are not subject to intervention by the international community. Another is the assumption that states are the sole agents engaging in international conflicts (Al-Qaeda is a familiar counter-example of an avowedly non-state actor). An additional level of complexity is introduced when one considers that the four domains of change do not operate in isolation, but rather, are interdependent. Thus, national security has become a novel, highly unpredictable system that constitutes a formidable management challenge.

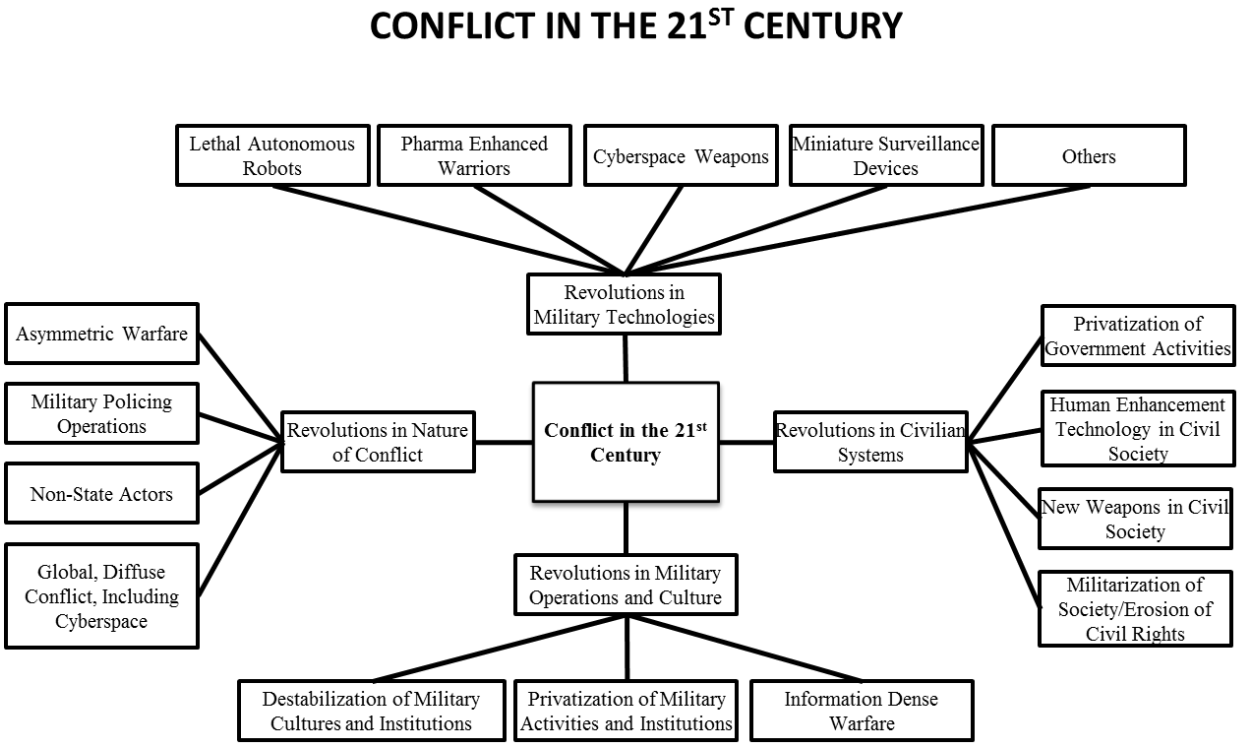

Figure 1. Framework for the observational science of conflict in the 21st century.[1]

The chart is meant to convey that a number of areas are changing simultaneously, but is not meant to depict all possible issues. It is important not to be technologically deterministic, but instead to realize that we live within a complex adaptive system.

With the above model in mind, the workshop was organized around the central question, "Are the Laws of War (and related legal, ethical, and governance mechanisms) rendered obsolete in whole or in part by emerging military/security technologies?" It further developed scenarios aimed at exploring the challenges of emerging military and security technologies, in a complex and unpredictable global context

[1] Based on Braden R. Allenby, *The Theory and Practice of Sustainable Engineering* (Upper Saddle River, NJ: Pearson Prentice-Hall, 2012), 294.

where the very nature of conflict itself is in flux. In order to focus the discussion and develop useful scenarios, the analysis was deliberately limited to three of the most significant new technologies: cyber warfare, robotics, and non-lethal weapons. These were discussed against a background of contextual changes that included the trend toward privatization of war (and state sponsored violence) and the democratization of weapons of mass destruction.

The 2012 Council

The 2012 Chautauqua Council on Emerging Technologies and 21st Century Conflict brought together a group of nationally-recognized scholars, with expertise in various subfields of ethics, policy, international law and the law of armed conflict, cyber conflict, non-lethal military technologies, and national security. They were joined by industrial, policy, philosophical, ethical, and military and security leaders and experts. Council members were chosen specifically for their wide variety of viewpoints and their ability to respond thoughtfully to opposing positions (a list with brief bios is provided in Appendix B). The overarching goal was to facilitate dynamic and productive dialog among multidisciplinary experts, who, over the course of 5 days, discussed whether the laws of war as they stand are adequate to address the challenges of conflict in the postmodern era of rapidly-evolving technology and global conflict.

Per the agenda (provided in Appendix C), the workshop began with an overview of the origins and current status of the laws of armed conflict, then moved on to discussions of specific emerging technologies and their interpretation within, and impact on, this legal-ethical framework. It next considered questions for future research on the topic of Emerging Technologies and 21st Century Conflict.

The workshop concluded with a public panel discussion on the morning of Saturday, August 4, 2012. The audience was presented with an overview of several of the topics addressed in the workshop. Among these were just war theory and international law of armed conflict, governance of technology, and the ethics of robots on the battlefield. The audience responded with interest, asking a number of critical provocative questions (see Appendix E). This process illustrated the dual goals of the Council: to engage in cutting edge substantive discussion of difficult questions of law, technology, and conflict; and to help educate the public to the importance of this domain, and expose them to some of the relevant issues and policy challenges.

Laws of War and 21st Century Conflict

"Man is first and foremost a legislative being. He seeks, through legislation, to impose order on chaos."

– Immanuel Kant

Background

Just war traditions are perhaps as old as warfare itself. Indeed, historical records suggest that combatants have long resorted to moral rules of conduct or codes of honor in order to limit the devastation of war – particularly with regard to the treatment of women, children, and prisoners. Similarly, just war theory encompasses a tradition that dates back to Aristotle, Cicero, and Augustine, and finds its origins in "a synthesis of classical Greco-Roman, as well as Christian, values."[2]

[2] Brian Orend, "War," Stanford Encyclopedia of Philosophy, 2005, plato.stanford.edu/entries/war/ (21 September 2012)

Just war theory

Just war theory can be broken down into three general categories: *jus ad bellum* which concerns the ethics of beginning a war, *jus in bello* which addresses actions taken within war, and *jus post bellum* which concerns the termination of armed conflict and peace agreements. There is a clear legal difference between *jus ad bellum* and *jus in bello*, although they are conceptually and historically intertwined. A war, for example, initially undertaken on behalf of a just cause (*jus ad bellum*) can become an unjust war if prosecuted through unjust means (*jus in bello*). By the same token, engaging in what turns out to be a morally or legally unjustified war does not absolve parties to the conflict from conducting hostilities in a moral and legal fashion (*jus in bello;* see Appendix A).

International Humanitarian Law

It was not until 1864 that the first of the Geneva Conventions, treaties that now form the core of International Humanitarian Law (IHL), was signed. The body of International Humanitarian Law, also referred to as the laws of armed conflict (LOAC), consists of two parts: humanitarian law, aiming primarily at protecting non-combatants, prisoners, and the wounded; and a number of specific treaties aimed at regulating the means and methods of armed conflict itself (including the 1899 and 2007 Hague Conventions). In addition to a number of formal treaties, conventions, and protocols, both IHL and laws regulating the conduct of hostilities also incorporate a substantial body of customary law which, despite a certain vagueness and informality, is often legally binding on all States and parties to a conflict.

International humanitarian law embodies five cardinal principles intended to limit the extent and destructiveness of armed conflict:

(i) Discrimination (or Distinction) – This principle requires the distinction of lawful combatants and military targets from civilians, wounded individuals, POWs, and civilian objects. Only valid military targets should be engaged.

(ii) Proportionality – This principle limits the degree of force utilized to that required to achieve a legitimate military objective. Excessive incidental losses and collateral damage, including inadvertent civilian injuries or loss of life, are prohibited.

(iii) Military necessity – This principle limits engagements and actions to those necessary to bring about a legitimate military objective. Combatants are required to target only those facilities, equipment, and military forces that make an effective contribution to military action, in order to weaken the enemy's ability to wage war as quickly as possible.

(iv) General prohibition on the employment of weapons of a nature to cause superfluous injury or unnecessary suffering – This principle prohibits the use of weapons and military tactics that would cause more suffering or injury than is necessary to defeat or debilitate enemy forces.[3]

(v) Command responsibility – This principle holds commanding officers responsible for the crimes committed by personnel under their control, and requires them to ensure that subordinates are trained in, and comply with, IHL.

These cardinal legal principles complement the older tradition of "Just War", in which a decision to go to war must satisfy three necessary conditions: there must be a compelling cause or justification; a public declaration to this effect must be issued by a legitimate authority; and the use of deadly force must be undertaken only as a last resort. Finally, the just war tradition also requires that tactics employed in the

[3] It is worth noting that superfluous injury and unnecessary suffering are terms within the law [API, article 35] but IHL does not define these terms.

conduct of hostilities must be both necessary and proportionate to their legitimate objective, and must in any case discriminate between combatants and non-combatants.

To conclude, IHL (both formal and customary) represents centuries of reflection by participants and practitioners of statecraft regarding better and worse methods of attaining national security, pursuing national interest, and managing international conflict. IHL is thus an important example of ongoing and perpetual public discourse about the moral norms appropriate to armed conflict. A question that was repeatedly discussed throughout the Council meeting, nonetheless, was whether existing legal statutes and understandings pertaining to armed conflict are perpetually "lagging behind" what is required to address innovations and transformations in 21st century wars, and whether the guiding principles and fundamental requirements are, in fact, as universally applicable as its advocates generally proclaim.

The United Nations Charter is the foundational treaty of the United Nations (UN) and is binding on its 193 member nations. While the UN Charter is independent of International Humanitarian Law, some of its articles address the rights of states to declare war. Hence, in some cases of international conflict, both IHL and the UN Charter apply.

Theoretical questions and existing IHL ambiguities

In beginning the discussion on the laws of war, a few compelling theoretical questions and issues arose. The first was the matter of ambiguity with respect to authority, priority, jurisdiction and hierarchy among various legal frameworks. For example, the legal framework applicable to a given armed conflict depends upon the nature of the adversaries. Hence, the law of armed conflict or IHL applies only in cases of international (state versus state) conflict. In this case, any armed exchange will trigger all 4 Geneva Conventions and their 1977 "Additional Protocol I." Armed conflict that is not between sovereign nation-states is typically governed by domestic law, although, even there, parties affected by the conflict must be treated humanely per IHL. In cases of significant intrastate violence, when the parties to the armed conflict are sufficiently organized (as in a civil war), Common Article 3 of the Geneva Conventions, Additional Protocol II of the Geneva Conventions, and customary international law are triggered. There is thus no unambiguous jurisdictional distinction or genuine priority or hierarchy among the various bodies of law governing armed conflict.

Moreover, there is a widely-held public perception in many quarters that the laws themselves are inchoate, mind-numbing, and ineffective. Indeed, despite their attempt to institutionalize high moral ideals, and certainly prior to the initiation of the International Criminal Court, international laws had no robust enforcement mechanism for violators. Nonetheless, the norms of just war and the requirements of IHL in particular, appear to garner wide respect within the international community at large, leading the Council to ponder where the contract lies? Between the states engaged in the conflict? Does one party show restraint if and only if the enemy does? Or is the contract more personal? Does it lie between soldiers and their fellow troops (as a kind of professional code of conduct), or is it between soldiers and their country? Is the contract, in the end, a kind of national or personal moral covenant?

These questions lead to larger issues of ethical and national relativism. On the one hand, some groups or parties to conflict, as a matter of descriptive fact, will not, and cannot be made to, respect the laws of war, and they may or may not be associated with a stable nation-state that can serve as a focus of sanctions. In light of this situation, critics of the very concept of international law wonder if there is a point to drafting and maintaining laws of armed conflict at all. On the other side, it could be argued that there will always be those that break the rules despite worldwide condemnation. It is nonetheless worthwhile to establish a set of laws that most people/cultures can agree on and abide by. For the purposes of the Council, both positions are considered important, especially if conflict continues to become more and more associated with non-state actors (e.g., Jihadist Islam). Given the increasing importance of private security firms and

semi- or non-governmental entities engaging in conflict, is a legal regime exclusively addressing (and conceptually grounded solely in) nation-states still adequate to the governance of armed conflict?

These questions arise against existing critiques of the LOAC framework. The "realist" school argues that there exist no ethical or moral controls on state action, because states have only interests, not ethical obligations, and certainly not ethical obligations derived from a specific, perhaps alien, culture. LOAC/IHL is, from this perspective, simply invalid. The "pacifist" school, on the other hand, argues that any war is itself unethical, so that any set of laws and norms that assumes the existence of war as its starting point is, itself, unethical – and especially so if, by making war more "acceptable," as LOAC/IHL arguably do, it makes war more likely. In practice, of course, such simplistic extremes are seldom encountered; more importantly, the Council, while recognizing these arguments, did not address them, as they are subject to longstanding and well documented study. Rather, the Council assumed that the middle ground, that of LOAC/IHL, was generally accepted among states, and that the more interesting and challenging question was: assuming the validity of the laws of war, are they being destabilized by the accelerating rate of change, and complexity, of emerging technologies?

Laws of war on the ground

In addition to the issues mentioned above, the laws can be confusing and perhaps frustrating to young soldiers faced with conflict for the first time. One such warfighter, with multiple tours of duty in Afghanistan, was quoted as saying to one of the participants of the Council, "your dumb ideas tie our hands and get us killed!" While his frustration was almost certainly complex in origin, it does in part indicate the difficulties of translating such high international ideals into the lessons of basic training, especially given the wide variety of individuals, and institutions, engaged in militaries around the world.

On the other hand, some participants thought that "education" was not the real problem. It was not that the wrong-doing or criminal actions at Abu Ghraib or Hamdania stemmed from ignorance of relevant law or rules of engagement, for example, but that the legal restrictions were not heeded or respected by the individuals involved in these incidents. Human rights may be discussed a lot, but that does not mean that they are actually a motivational factor in the behavior of troops in combat. The core issue in the field may not be whether or not a member of an opposing force has "rights." Instead, what may be at issues is a "psychological contract": that, for example, showing restraint may be good for the troops themselves. Such framings do not rely primarily on reciprocity or concern for the well-being of enemies or even civilians. The focus instead is upon leadership and good governance, including how specific military units are led, what officers are telling their troops, and the behavior they either tolerate or exemplify – such as whether a particular group of military leaders in the field decides to approve of, encourage, or discourage certain behaviors like desecrating enemy corpses.

Reflections on "Laws of War" in the 21st Century

To at least some extent, today's "postmodern" conflict is characterized by asymmetric warfare and an increased reliance on irregular forces such as private military contractors. Informal weapons (i.e., improvised explosive devices) are often used alongside more traditional ones. Moreover, the battlefield is seeing a trend toward increased use of technologies such as robotics, warrior enhancements, cyber weapons, and (likely in the near future) nanotechnology.

Meanwhile IHL continues to be refined and expanded through new treaties and customary practice, but is it keeping pace with the rapid evolution of the actual practice of warfare? Cyber warfare provides a good case example. When considered in light of the various cultural traditions of just war, or the five cardinal principles of IHL, it is theoretically possible to engage in an ethical and legal cyber conflict under certain conditions. A cyber war (or use of cyber weapons) would be justified, for example, whenever:

- It aims primarily or exclusively at military infrastructure and destroys little or no civilian infrastructure.
- It neither deliberately targets, nor ultimately inappropriately harms civilians.
- It degrades an adversary's ability to undertake highly destructive offensive operations.
- It is undertaken as a "last resort" (in the sense that all reasonable alternatives short of attack have been attempted to no avail, and further delay would only make the situation worse).

However, a closer inspection reveals a number of ambiguities. In particular, with regard to the principle of discrimination, is it even possible to ensure the safety and security of civilians and civilian infrastructure when military and non-military communication networks are highly coupled, and many cyber weapons are not very discriminatory (e.g., will spread from military to civilian cyber systems)? Moreover, what would constitute a "last resort"? Is it acceptable to undertake preemptive electronic measures to avoid a kinetic exchange (as some argue may be the case with Stuxnet)? Other issues arise with respect to proportionality, military necessity and attribution. What would constitute a proportional response to a massive cyber-attack? Another, similar, cyber-attack? At what point does a cyber-attack constitute grounds for a kinetic response? Finally, it is often difficult to discern the nation (or geographical location) of origin of a cyber-attack. If it is unclear who launched a weapon, or conducted a strike in cyberspace, how can the victimized State respond appropriately?

Themes highlighted by the Council

The foregoing scenarios of cyber warfare foreshadow a number of questions and themes that recurred throughout the Council's deliberations. First and foremost, as the cyber example highlights, there is the question of whether or not the laws of armed conflict are sufficient, at the present time, to address the new situations that novel military uses of emerging technology pose. Further, even though IHL continues to be refined and expanded through new treaties, is it keeping pace with the rapid evolution of the conduct of war?

A corollary to these questions is a situational one: Do new technologies really present novel issues for international humanitarian law, or can a historical precedent be found for each emerging technology? For example, later in the report, the question of robot autonomy will be discussed, posing apparently new and unprecedented problems. At what point, for example, can a weaponized system be considered autonomous? When does it become feasible and legal to omit direct human oversight and approval of the targeting decision? Of the firing decision? Yet such conundrums are not entirely without precedent. In World War II, for example, some bombsights were completely hands-off, while landmines are considered by some today to be autonomous systems operating within extremely narrow bounds of discretion. Have the dilemmas associated with autonomous systems, then, existed for some time, or does robotics present genuinely new ethical questions?

From this third theme comes a fourth: Some felt that the question of autonomy may actually be one of language and definitions. In fact, the lack of clear definitions for a number of terms ("human-in-the-loop", etc.) has opened the door to significant interpretation and debate. The Council repeatedly struggled with this issue. The final theme was the observed tension between creating laws and ethical rules of conduct, and occasionally encounter the need to break those rules when absolutely necessary.

Cyber Conflict

*"In my opinion, it's the **greatest** transfer of wealth in history."*

– GEN Keith Alexander, NSA director and CYBERCOM commander, on the $ billions of intellectual property lost to hackers suspected from China (Reuters, 9 July 2012)

Cyber-attacks occur in multiple domains and for a number of reasons, but always involve the use of information systems to execute (or to create the software ability to execute at some future time) a destructive action. The underlying motive may be military, political, economic, or criminal in nature and the aggressor may resort to cyber methods due their relatively low human, economic, and political costs. That is, cyber-attacks have the potential to return a great deal of information and/or create broad disruption – particularly in the realm of military C^3I (command, control, communication, and intelligence) – for a small initial investment, all while providing the perpetrator with a veil of anonymity. Cyber conflict is thus the ideal form of asymmetric warfare, used by the relatively poor and powerless against the wealthy and dominant.

Cyber-attacks may take advantage of a number of technical weaknesses including errors in software and network design (zero-day attacks) and system vulnerabilities (i.e., DDoS attacks and hacking). They may also take the form of deceptive practices as in the case of phishing scams, malicious links, or Trojan horse programs. However, with respect to security breaches, humans are often the weakest links, since they share USB drives which can harbor viruses, give up passwords, and unknowingly install malware. Moreover, law enforcement is not doing much to address cyber-attacks. While industry has assumed the responsibility to protect their systems, in many cases, the financial losses due to information security lapses often amounts to less than the cost of security to prevent such losses. Indeed, there may be a "public good" factor associated with cyber security in that the investment to protect electronic assets, though it would benefit everyone, is under-incentivized economically for individuals and firms. Cyberspace, as a result, remains the digital equivalent of the Wild West.

Turning now to cyber warfare specifically, a 2011 NATO publication indicated that the norms associated with cyber conflict are evolving (see Table 1). However, a number of open questions remain with regard to LOAC in cyberspace. A more in-depth treatment of these "fuzzy concepts" is presented in the next section.

Table 1. Evolving cyber-norms.[4]

Norm	Description
Territoriality	Information infrastructure located within a state's territory is subject to its control.
Responsibility	A cyber-attack launched from an information system located in a state's territory invokes the responsibility for the attack.
Cooperation	The fact that a cyber-attack has been conducted via the information system located in a state's territory creates a duty to cooperate with the victim state.
Self-Defense	The right to self-defense when facing a clear and imminent attack is guaranteed.
Data Exchange	Information infrastructure monitoring data is perceived personal unless provided for otherwise.
Duty of Care	The responsibility exists to implement a reasonable level of security in relevant information infrastructures.
Early Warning	The potential victims of an incoming cyber-attack should be notified.
Access to Information	The public has the right to be informed about threats to their lives, security, and well-being.
Criminality	Every nation has the responsibility to include the most common cyber offenses in its substantive criminal law.
Mandate	An organization's capacity to act (and regulate) derives from its mandate.

Fuzzy concepts

Another important theme throughout the workshop was the question of definitions in IHL and how they might apply to 21st Century Conflict. Below are some important concepts and ambiguities that result when viewed in the context of cyber war. As will be seen, there is difficulty in defining what constitutes a cyber-attack, cyber war, cyber artillery, etc.

Act of war

"Act of war" typically requires attribution and public declaration. War, as defined by Brian Orend (2000) is *"actual, intentional, and widespread armed conflict between political communities"*. Also recall from the introduction that a just war requires a compelling cause or justification (which implicitly requires attribution of an attack to an actor) and public declaration by a legitimate authority. These definitions are difficult to apply to cyber-attacks that are typically focused on local facilities, do not utilize kinetic weapons (and may not cause permanent physical damage at all), cannot be attributed to any one actor, and are often conducted without a public declaration of war. Nonetheless it is difficult to deny that some recent actions have the intuitive "feel" of an attack. One good example is the Stuxnet attack on Iran that

[4] Based on Eneken Tikk, "10 Rules of Behavior for Cyber Security." *NATO*, 2011, www.ccdcoe.org/articles/2011/Tikk_TenRulesForCyberSecurity.pdf (21 September 2012).

specifically targeted the control system of uranium enrichment centrifuges. The apparent goal was to shorten centrifuge lifespans and, ultimately, delay Iran's nuclear weapon program. While Iran accused Israel and the United States of developing Stuxnet, no proof was ever presented and war was never declared by any party. Hence, there is uncertainty as to what constitutes an "act of war" (*casus belli*) in cyberspace. Could malware ever constitute "arms"? At what point does a cyber-attack become an act of war?

Another example of cyber conflict occurred on September 6, 2007, when the Israeli Air Force bombed a nuclear site under construction at Dayr az-Zawr in Syria. Apparently having purchased access to software "backdoors" in a Syrian radar system, Israel allegedly disabled the system that would have alerted Syria to the incoming Israeli planes. The force then slipped past Israel air defenses, bombed the target, and exited without further incident. A number of questions illustrate the problem of clearly identifying the act of war. Did it occur:

- When the backdoor was coded?
- When the compromised computer component was installed?
- When the backdoor was sold to Israel?
- When the malware was introduced into the Syrian air defense system?
- When the malware was actually activated?
- When the physical system was damaged?
- Never?

Three important themes resulted from the above examples (political, legal, and practical). The first involves the political nature of attacks. It is worth emphasizing that in both the Stuxnet and Syrian radar cases, neither victim declared war on the aggressor, even though attribution was clear in the Syrian radar incident. While it is important not to underestimate the vote that the victim gets in the decision as to whether an act of war has been committed, it is easy to lose track of the possibility that a response is not always taken, or is even found to be necessary. Retaliation is a political decision. Just because something could trigger a war does not mean that it must. Furthermore, an awareness of the context for the action is important as it influences the response (armed vs. unarmed) which will in turn determine the level of escalation and ultimate endpoint of the conflict. So an awareness of the context and ultimate worst case scenarios is important for all parties involved.

From both a practical and legal standpoint, there is no difference between firing a missile and using software to disable an enemy's radar (although it may be a general case that recovery from a software attack will usually be easier than recovery from physical destruction of the asset in question). That is, it is the effect (or potential effect) that matters. However, there is simultaneously a legal gap between a cyber-attack and retaliation with force. Two regimes apply simultaneously: IHL and the UN charter. In the UN Charter parties are prohibited from using force unless they are either responding to an "armed attack" or their use of force is sanctioned by a Security Council resolution. IHL comes into play, in turn, by requiring that any response (whether conventional or cyber) be proportionate by employing only as much force as is required to attain the legitimate military objective for which purpose the attack is launched, and that it not deliberately target civilian noncombatants or civilian "objects." Cyber-attacks, especially when carried out in retaliation, are likely to violate, or threaten to violate, both of these cardinal principles of IHL.

Espionage

The Flame virus is believed to have succeeded in, effectively, turning personal computers into listening devices. That is, it could record key strokes, audio, screen shots, and network traffic on an infected

computer, and send that information to a command and control server. Yet this particular malware is not generally considered to constitute a cyber weapon. So where is the line between cyber snooping and cyber-attack? Note that this issue encompasses more than just the Internet; espionage in general does not count as an "act of war". Yet, when applied to cyberspace, the question becomes more salient since viruses can act on a much larger scale than human agents, and therefore inflict greater losses of privacy and security.

Prohibited actions

Treachery and perfidy refer to acts in which an enemy combatant is tricked into trusting an agent with the intent to betray that trust. Examples including waving a white flag of surrender while continuing to fight or pretended to be wounded in order to gain a military advantage. What counts as treachery or perfidy in cyber warfare? Could these definitions be extended to include actions such as selling a compromised radar system to Syria? Indeed, some critics have gone so far as to claim that all uses of cyber weapons constituted perfidy, inasmuch as their origin, exact target, and purpose are clothed in subterfuge. Whether this is too limited an interpretation of existing codes, or whether it indicates such codes are obsolete when applied to cyber conflicts, remains an open question.

Combatant

IHL protects a number of classes of actors from harm, including civilians and healthcare workers. But cyber warfare could challenge the definitions of these classes. For example, could a computer programmer developing a cyber weapon be considered an enemy combatant? What about an ISP (Internet Service Provider)? This issue actually extends beyond that of cyberspace, as the concept of combatant is generally evolving and expanding. Consider the "part-time" combatant who operates a UAV during the day and then goes home, perhaps attending his or her child's soccer game in the evening.

Some other, more conventional, examples also exist. Could Robert Oppenheimer, who led the Manhattan Project to develop the first atomic bomb, have been considered an enemy combatant? What about civilians working in weapons factories or supporting a war effort? A truck driver is not himself a legitimate target when he moves ammunition from depot A to depot B (though his truck is a legitimate target). However, once he is making a delivery to the front lines and is one causal step from the battlefield, he can be legitimately attacked even when he steps out of his truck.

More provocative examples exist, of course: based on analyses published by the People's Liberation Army, China might consider George Soros to be a terrorist. Falun Gong is another example. Could China legally send a missile to destroy Falun Gong members eating lunch in a civilian hotel? Hence the definition of "enemy combatant" may ultimately depend on the cultural construct of the State actor.

Self defense

In cyberspace, what events would justifiably trigger attacks in "self-defense" or to protect "national security"? Is a long sequence of individually trivial or modest incidents sufficient cause to invoke self-defense (so-called "death by a thousand cuts")? At what point does the danger posed by (for example) "back doors" and "Trojan horses" become "imminent"?

Ceasing hostilities

Do cyber-attacks promote or impede a lasting peace? Once a conflict has come to an end, can cyber-attacks be terminated easily? That is, should international law require the use of "ethical software," equipped with some sort of "off switch?" Moreover, rather than deleting data, should such cyber weapons

be required merely to encrypt it, so that the key can be turned over to the enemy upon resolution of the conflict (thereby keeping permanent collateral damage to a minimum)?

Death by 1000 cuts

"Death by 1000 cuts" or, alternatively, a "relentless attack", is a particularly difficult scenario requiring closer attention. Such a scenario would arise if small and incremental damage was inflicted to electronic, biological, or mechanical systems by hackers or enemies over a long period of time, eventually leading to significant impacts that might resemble damage done by a weapon of mass destruction. Note that the weapons used in a "1000 cuts" scenario could be electronic, chemical, or biological since the source can be difficult to identify in all cases.

Targets for such an attack might include financial systems, with the impacts being similar to those of economic sanctions. Interestingly, the UN Charter explicitly states that economic actions do not warrant an armed response, but this seems to reflect the model of economic actions such as sanctions taken by a state against another state, not a determined, long term cyber-attack by parties unknown against the economic stability of a state. However, given such an attack, who would be responsible for the harm? The originator? Or the victim of the attack who does not retaliate, or who persistently failed to take appropriate security precautions? This is analogous to the case of a frog in a pot of gradually warming water. The frog, oblivious to the pending danger of eventually boiling, is at least partially responsible in this instance for bringing about its own death.

Concluding remarks on cyber conflict

There was controversy among the group surrounding whether or not cyber warfare is currently being conducted according to existing laws of war. But there was more widespread agreement that cyber conflict at the scale the public is aware of is currently operating at a level below that at which international laws pertaining to the conduct of armed conflict would apply (discussions of cyber conflict reflect a context where much of the operational activities in the military and security domains are highly classified). There remained strong disagreement regarding the severity of the threat posed by cyber-attack. While cyber has the potential to be dramatic and escalatory, unless it does a lot of damage in the concrete forms of physical destruction, injury, or death, some council members opined that people might simply learn to live with the continued, low-level threat.

(Note: At the time of this discussion, a comprehensive document produced by NATO's Cooperative Cyber Defense Centre of Excellence, the National Cyber Security Framework Manual, also known as the Tallinn Manual, had not yet been released. The participants looked forward to the analyses contained in that volume.)

Robotics

"Should soldiers be robots? Isn't that largely what they are trained to be?

Should robots be soldiers? Could they be more humane than humans?"

Like any new technology, the use of robotic systems in combat must be done within applicable ethical and legal frameworks. Not to do so would be costly: breeches in military ethical conduct often have extremely serious consequences, both politically and pragmatically, as evidenced by the Abu Ghraib and Haditha incidents in Iraq, with their concomitant damage to the United States' public image worldwide. Accordingly, if militaries keep moving forward towards the deployment of intelligent autonomous

weaponized robots at its current rapid pace, these systems should be deployed ethically, in a manner consistent with both standing and mission-specific Rules of Engagement (ROEs) and other legal and ethical constraints.

To reiterate, the overarching theme for this workshop was not whether wars should exist, since virtually everyone, including the workshop participants, agree that wars are highly undesirable. Rather, given that history indicates that wars are likely to recur, the pressing consideration becomes: what is the appropriate role of robotics technology? How should robots be designed to be ethical?

There are four motivations for utilizing robots on the battlefield. The first is force multiplication: Deploying robots will reduce the total number of soldiers needed. This factor favors increasing the degree of autonomy for each system, since continuous and labor-intensive human oversight diminishes the force multiplication actually achievable. Second, robots have the effect of expanding the battlespace: they allow combat to be conducted over larger geographical areas. They further extend the warfighter's reach, allowing soldiers to strike enemies from ever more distant and safer locales. Additionally, robots reduce friendly casualties: they keep human fighters out of harm's way. And finally, simply put, robots save lives. In sum, the goal of military robotics is not to replace the human warfighter, but to extend the capability, scale, and effectiveness of the human fighting force, while reducing casualties (including civilians).

The further advantage of using of artificial intelligence (AI) and robotics for reducing the incidents of legal and ethical infractions in conflict situations is not yet within the scope or capacity of engineers and computer scientists at present. But this may change in the coming years, especially since anecdotal evidence suggests that defense agencies are very interested in the ethical dimensions of these new technologies.

Lethal robotics systems

In 2001, Congress set a goal for the Army, stating "...that, within 10 years, one-third of U.S. military operational deep strike aircraft would be unmanned, and, within 15 years, one-third of all U.S. military ground combat vehicles would be unmanned."[5] But note that the term "unmanned," like many other words discussed in this report, is somewhat ambiguous. It may refer to remotely-controlled systems, or completely autonomous systems. In either case, an "unmanned" system could be thought of as a "robot". As it turns out, however, the term "robot" is similarly fluid. By one definition, robots require the ability to sense the environment and affect change in that environment. Hence at the 1939 World's Fair, a compelling argument was made that a toaster is, in fact, a robot. By the same token, it could be argued that a land or sea mine is not only an autonomous robotic system, but a lethal autonomous robot. Mines are robots, just not mobile ones. The iRobot Roomba® represents a more conventional view of an autonomous robot. Note, however, that it has niche autonomy (i.e., within the framework of the floor of a home). Also note that autonomy does NOT imply sentience or free will. These concepts were not part of the Council's discussion of robots.

As implied above, robots used in warfare are quite diverse. One class of robots simply encompasses weapons. These robots are extensions of the warfighter; therefore the human remains in control at all times. In this case, standard battlefield ethics apply to the human-technology system. However, a growing class of robots may be programmed to act autonomously. In these cases, the unmanned system reserves the right to make its own local decisions regarding the direct application of force in the field, without requiring human consent. In some situations, the robot may be authorized (or programmed) to use lethal

[5] "U.S. Army Roadmap for Unmanned Systems: 2010-2035," www.fas.org/irp/program/collect/uas-army.pdf (21 September 2012), 5.

force. An example of such an autonomous system is iRobot's Packbot. Most models are capable of Tasering enemy combatants, though some come equipped with highly lethal high-speed guns.

The term "autonomous" could, in turn, refer to a spectrum of human involvement ranging from human-controlled to human-supervised, all the way up to fully autonomous decision-making and action. Again, it is important to remember that well-defined, standard terms remain elusive. Most currently-deployed military systems are able to maneuver and perhaps even target autonomously but require approval to fire. These include some torpedoes, Predator and Reaper drones, and Israel's Harpy missile system. Others have fully-autonomous modes and can fire without human authorization. Samsung SGR-A1 robots, used in the demilitarized zone (DMZ) at the border between North and South Korea, are such weapons, as are Navy Phalanx systems and Patriot missiles. In the future, grenade robots could, in principle, independently locate a target and decide whether or not to self-detonate after being thrown through a window.

Ethical questions surrounding military robots

By some accounts, no less than 47 nations are developing robots for the battlefield which makes autonomous lethality seem inevitable. Yet some protest as people realize that the ability for robots to make autonomous firing decisions raises some important ethical concerns that allegedly have yet to be addressed. The United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047[6] summarized the situation:

> *Authorizing a machine to make lethal combat decisions is contingent upon political and military leaders resolving legal and ethical questions. … Ethical discussions and policy decisions must take place in the near term … rather than allowing the development to take its own path apart from this critical guidance.*

In October, 2010, Reuters[7] wrote:

> *In a report to the U.N. General Assembly human rights committee, Christof Heyns said such systems [an apparent reference to U.S. drones that strike suspected Islamist militants] raised "serious concerns that have been almost entirely unexamined by human rights or humanitarian actors."*
>
> *"The international community urgently needs to address the legal, political, ethical and moral implications of the development of lethal robotic technologies," said Heyns, U.N. special rapporteur on extrajudicial executions.*

Whatever the final outcome, arguments are likely to be heated on both sides. Those leery of lethal autonomous robots may fear that they will simply refuse orders, eventually escalating into a "robots run amok" scenario reminiscent of science fiction stories. Others argue that robots simply cannot be programmed to discriminate appropriately between a combatant and a non-combatant. Even if this challenge can be overcome, there is the possibility that robot warriors will give political leaders the illusion of being able to conduct "risk-free" warfare. This may lead governments to engage more readily in armed conflict, and to hide the nature and costs of that conflict from the public. Other concerns include prospects for the proliferation of lethal autonomous systems to terrorist groups, or the vulnerabilities of such systems to cyber-attack or hijacking. For example, researchers at the University of Texas at Austin

[6] "United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047," 2009, 41.

[7] Patrick Worsnip, "U.N. urged to set up panel on ethics of robot weapons," *Reuters*, 2010, www.reuters.com/article/2010/10/22/us-un-rights-robots-idUSTRE69L5RL20101022 (21 September 2012).

have demonstrated the ability to take over a UAV with an unencrypted GPS system, alter its flight path, and even land it. Some feel that the only possible prohibition of lethal autonomy may come from international treaties.

By contrast, some suggest that future autonomous robots may be able to perform better than humans under battlefield conditions. The eventual development and use of a broad range of robotic sensors will give machines better equipment for battlefield observations than humans currently possess. Hence, prior to responding with lethal force, robotic systems will be able to integrate large quantities of information, from more sources, far faster than a human possibly could in real-time. Moreover, robots have the ability to act conservatively (i.e., they do not need to protect themselves in cases of low certainty of target identification). Further, they can be designed without the emotions that often cloud the judgment, or provoke anger and frustration in human combatants, tempting them to commit war crimes. Thus robots have the benefit of not being susceptible to stress or psychological trauma. Unlike human combatants, they will not lack appropriate knowledge or training, nor act out of anger or revenge, or be prone to ethical violations (abuse of prisoners, for example).

Regarding the very real challenge of combatant identification and distinction, there are a number of measures that can be used to limit or prevent collateral damage. First and foremost, robots could be employed, at least initially, in limited circumstances where the likelihood of civilian encounters can be minimized and where the situation is bounded enough that existing AI capabilities (e.g., expert systems) can be used. Examples of these "bounded" or highly scripted situations include room clearing, counter sniper operations, and DMZ or perimeter protection. Such robotic technology would be more appropriate for interstate warfare, rather than counterinsurgency operations. Further, robots can be programmed to perform a situational analysis whereby a number of criteria must be met before a shot can be fired. Individual systems are designed for specific situations. If the robot finds itself in an unexpected situation, it can be programmed to merely observe it (and not act).

Finally, most participants agreed that robots should be deployed alongside, and not as a replacement for, human combatants. A human presence on the battlefield should be maintained. When working on an integrated team combining human soldiers and autonomous systems, robots have the potential capability of independently and objectively monitoring ethical behavior in the battlefield by all parties and reporting infractions that might be observed. Tasers, for example, already come equipped with a "black box" that records the date, time, and duration of each use. Thus some technologists see significant advantages in developing "ethical" robots (aside from the obvious safety and asymmetric advantages). These include dramatically increased time for decision-making, more eyes on the target (so-called "persistent stare"), and the ability for the autonomous system to request advice from an IHL expert when needed ("lawyer in the loop").

Indeed, experts say that, if done correctly, the benefits of robotic systems could outweigh their problems such that it would effectively become a moral imperative to use them (Human Rights Watch takes a similar position on precision-guided missiles). Thus the future of military operations may involve highly coordinated and complex human-technological systems. That is, humans will work (both on the battlefield and remotely) with robot companions to accomplish missions. One challenge that remains for engineers is the tendency for humans to become very attached to their companion robots. When they are damaged, for example, soldiers do not want new ones, they want the old ones to be repaired. In short, humans might perversely come to embrace a doctrine of "no robot left behind." For soldiers, developing strong bonds with robots that are supposed to protect them (e.g., minesweepers), could ultimately get them killed. So designers are faced with the problem of making the robots likeable, but not *too* likeable.

The question of responsibility

In addition to the arguments listed above, a few specific and more subtle issues arise around lethal autonomous robots. One of these is the responsibility for the wrongful deaths of non-combatants. Perceived infractions of International Humanitarian Law by unmanned systems could result in war crime charges, political fallout, a negative effect on troop morale, hostility among the local population, and citizen reticence toward mission accomplishment. To some extent, however, this concern reflects a category mistake: war crimes are intentional acts that violate established law, and robots, certainly in the foreseeable future, will not be intentional. The appropriate analogy here is a soldier blaming the bullet he deliberately fired at a civilian for the war crime: no one is going to hold the bullet responsible. Instead, the agent that fired the bullet will clearly be held responsible. Similarly, a robot, just like any other military technology, may effectuate a war crime, but it is the individual who is responsible for the robot, not the robot, that is, and will be, liable for the act. The real question here is how to determine responsibility with a complicated and, at the beginning, somewhat novel piece of machinery, rather than trying to allocate responsibility in whole or in part to the machinery.

Humans in the loop

While it might seem that keeping humans involved in the decisions made by robots – particularly kill decisions – would alleviate these problems, the reality is not so simple. In fact, it raises many more questions. Specifically, how many "loops" can one "human" control? How complex a loop? Does that re-pose the question of genuine cognitive engagement required for direct oversight/accountability? What if the system fails to present the human with comprehensive or critical information for situational evaluation? Moreover, in many complex military systems, the human is the component with the "lowest bandwidth"—i.e., slowest rate of information processing. Hence, there is a tension between limited human cognitive ability and ensuring that optimal battlefield decisions are made. That is, it is possible that "sufficient" information for a human to make an informed decision is simply "too much" information for the human to process in a reasonable amount of time. This condition may be especially true in modern warfare, when intense and rapid attack involving numerous projectiles and forces may require the information processing power of robotic systems to keep up with the challenges; a human is simply incapable of the required speed and information processing capacity.

Thus even with humans in the loop, it is difficult to establish accountability. Responsibility may depend on the phase of operations in which the mistake occurred. There may even be a gap between the assumption of responsibility and the reality of responsibility: Just because we make someone accountable doesn't mean that they have actual responsibility.

Another very interesting corollary to keeping humans in the loop arises from remotely piloted UAVs. Some have likened these military operations to video games, charging that remote pilots have a "Playstation mentality" and that such "numbed" killing at a distance encourages escalated violence. While these assertions are thus far unsubstantiated (indeed, operators have been known to suffer from exhaustion and post-traumatic stress disorder), and modern war separates the actor from the actual killing in many ways (e.g., remotely delivered shells and other ordinance), other questions remain. In particular, are uniformed UAV operators in Nevada valid enemy targets? The laws of armed conflict seem to imply that they are.

In addition, despite that fact that the Air Force is now graduating more UAV pilots than manned pilots, operating unmanned systems is more labor-intensive (for now at least). While the Air Force currently uses only uniformed personnel to pilot unmanned systems, going forward it might be a reasonable solution for the armed forces to close any labor gaps by employing civilian or private military operators. However, having non-uniformed personnel in the kill chain could be problematic: non-military operators could

conceivably be found guilty of murder, at least under current law, and should be made aware of the risks. In a worst-case scenario, if there is no statute of limitations on murder and a former UAV operator is traveling in a nation that has an extradition treaty with a country in which military operations have been conducted, the wanted individual could be charged and tried. (The same issues also arise for private military contractors loading bombs into weapon systems closer to the battlefield.)

Concluding remarks on robotics

Many challenging research questions regarding lethality and autonomy of robotic systems have yet to be resolved, and to some extent the debate is characterized by selective choice of emotive hypotheticals. However, roboticists, political leaders, and citizens alike cannot ignore these difficult ethical issues. Instead, proactive management is necessary. What guarantees can engineers and roboticists offer in order to render the prospect of unfortunate or even unethical outcomes less possible? While unmanned systems may never perform flawlessly in battle, perhaps they can nonetheless perform more ethically and more reliably than is possible for human soldiers under similar conditions. Is it not everyone's responsibility to look for effective ways to reduce man's inhumanity to man? Research in ethical military robotics could and should be applied toward achieving this end.

Non-Lethal Military and Security Technologies

Non-lethal weapons are those that are meant to incapacitate, inflict pain, and cause disorientation in human targets, while minimizing fatalities, injuries, and damage to property. These weapons are often used to restrict access to an area or disperse a crowd – in other words, they are more likely to be useful in policing or crowd control, rather than combat, roles. Examples of some of the many available non-lethal technologies are given in Table 2. While many believe there are no true "non-lethal" weapons – only "less-lethal" – many are approved for use by law enforcement. However, a number of IHL provisions limit or prohibit a range of nonlethal weapons in armed conflict. In general, ICRC (International Committee of the Red Cross[8]) directives warn about weapons that intentionally cause "specific disease, specific abnormal physiological state, specific and permanent disability, or specific disfigurement" (cf., inhumane treatment). More specifically, the 1972 Biological Weapons Convention provides for multilateral disarmament and supplements the 1925 Geneva Protocol restrictions on biological weapons, which prevented use, but not possession or development. This is in contrast to the Chemical Weapons Convention (1993) that restricts chemical weapons for the purposes of armed conflict, though it allows them in four special circumstances: rescuing downed fighter pilots, prisoners of war, human shields, and riot control.

[8] Based in Geneva, Switzerland, the International Committee of the Red Cross (ICRC) is an impartial, neutral and independent humanitarian organization that provides protection and assistance to victims of armed conflict. As mandated by the Geneva Conventions, the ICRC acts as guardian of International Humanitarian Law and as an organizer and catalyst of its further development.

Table 2. Examples of non-lethal weapon types.[9]

Category	Type	Effects
Acoustical	Audible or Infra Sound	Incapacitation, Nausea, Vomiting
Optical	Lasers, Strobes	Temporary Blindness, Disorientation
Biological	Viruses and Toxins	Respiratory/Gastrointestinal Disease
Chemical	Calmatives Irritants (e.g., tear gas and pepper gas) Psychotropic Drugs	Unconsciousness Tearing, Choking Hallucination, Disorientation
Electromagnetic	Active Denial Systems (ADS)	Intensely Painful Burning Sensation
Neurological	Radio Frequency (RF) Functional Magnetic Resonance Imaging (fMRI) Transcranial Magnetic Stimulation (TMS)	Incapacitation Detect Mental States Alter Mental States

The nonlethal paradox

The ability to use nonlethal weapons for law enforcement purposes but not armed conflict caused Donald Rumsfeld, for example, to complain that "in many instances, our forces are allowed to shoot somebody and kill them, but they're not allowed to use a nonlethal riot control agent." Michael Gross refers to this as the "paradox of nonlethal weapons." He writes, "Nonlethal weapons are not weapons of mass destruction. They are specifically designed to temporarily incapacitate rather than kill. They produce no effects that extend beyond … war. Nor do they cause wounds that are especially difficult to treat. They seem, at first glance, to offer means that are both militarily useful and relatively friendly on the battlefield."[10]

This paradox finds its roots in the distinct bodies of law governing armed conflict and law enforcement. Law enforcement is governed by local statute and regulation, and human rights law, whereas IHL addresses armed conflict. Similarly, rules of force govern police actions whereas rules of engagement govern the actions of soldiers. Both LOAC and human rights law place limitations on the use of weapons on the battlefield.

Broadly speaking, certain kinds of weapons have historically been excluded from use in armed conflict for three reasons. These include the weapons' propensity to cause *superfluous injury* and *unnecessary suffering*, their *inhumane* nature, and State self-interest and reciprocity ("we won't use them because if we do, our opponents do"). One such prohibited weapon is the serrated bayonet: Not only does the bayonet disable an enemy, but the serrations effect a gaping wound when the bayonet is removed. And to what end? The enemy is already unlikely to return to the battlefield, so the serrations cause superfluous injury and unnecessary suffering. As President Grant said in a different context, "they produce increased suffering without any corresponding advantage to those using them." For the same reasons, a range of weaponry is banned under the laws of war. These include explosive and hollow point bullets, serrated

[9] Michael Gross, *Moral Dilemmas of Modern War: Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict* (Cambridge: Cambridge University Press, 2010), 78.

[10] Michael Gross, *Moral Dilemmas of Modern War: Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict* (Cambridge: Cambridge University Press, 2010), 77.

bayonets and barbed lances, explosive charges containing clear glass and other undetectable fragments (i.e., which surgeons cannot easily see during treatment).

Many non-lethal weapons do not meet the basic legal requirements applicable to weapons used in combat, particularly the requirement that non-combatants not be targeted, and the requirement of discrimination, whereas human rights law allows the use of indiscriminate weapons when necessary to protect civilians. Otherwise said, in battle, it is better to fire a gun than the Active Denial System (ADS) because the gun can discriminate between combatants and non-combatants. But in a police action targeting civilians, it is better to use the ADS because it carries less force. Moreover, if an ADS is used by a military force in a policing situation, and in doing so targets a non-combatant in order to save that person, such a use would be forbidden under IHL. Thus, the paradox: using a lethal weapon which kills, but does not target, non-combatants is legally preferable to using a non-lethal technology that targets, but in doing so avoids killing, a non-combatant.

The question of using non-lethal weapons on the battlefield remains an important one, however, for a number of reasons. First, in many modern situations militaries are not engaging only, or even primarily, in traditional combat; rather, they are conducting more and more police actions and, more broadly, nation building activities such as training local officials and providing security for community development in counterinsurgency environments. Moreover, as part of modern warfare the battlefield may well contain various classes of actors: traditional soldiers, private military contractors, insurgents and part time combatants, and civilians that may or may not be supporting the battle. Second, it is possible that individuals with NLWs, believing they are safe, may use them more liberally and less cautiously than they would with lethal weapons; while this might not be a problem in a full combat environment, it could be difficult in a mixed military/police situation.

Consider the 2002 Moscow Theater Siege when 40-50 Chechens took 850-900 hostages in a Moscow movie theater; the rebels demanded the removal of Russian forces from Chechnya. After a 2 ½ days, the Spetsnaz (Russian special forces) pumped a chemical agent—thought to be fentanyl or 3-methylfentanyl (a calmative agent meant to subdue the militants)—into the theater, initiating events that led to the death of 129 hostages, but allowing the others to be saved. This Siege was an example of an ambiguous military/police situation that did not fall clearly into either a category of armed conflict, or of law enforcement. Consequently, the appropriate rules and norms are not clear; it falls into a gray area of the Chemical Weapons Convention, for example, making the validity of the chemical weapon use questionable. Was the use of the chemical agent and its associated non-discrimination, inflicted suffering, and collateral damage acceptable to save hundreds more hostages?

A similarly challenging question is associated with weapons that cause blindness. Weapons designed to cause permanent blindness are banned by the 1995 United Nations Protocol on Blinding Laser Weapons (UNPBLW), implying that it is worse to be blind than dead. Moreover, weapons that cause temporary blindness (e.g., dazzlers) fall outside of UNPBLW restrictions, implying that temporary blindness does not constitute a superfluous injury or unnecessary suffering.

Concluding remarks on non-lethal weapons

While the workshop did not come to any specific conclusions with respect to non-lethal weapons, it did raise some important questions regarding whether nonlethal weapons can be more ethical than conventional weapons on the battlefield, even if illegal under current legal regimes. Moreover, the issue of technology governance was raised. For example, some types of chemical weapons have been banned before their potential value in reducing collateral damage associated with traditional combat operations, and before the advent of mixed military/policing operations, implying that technologies are sometimes banned before their implications were fully considered. This is not always the best management strategy,

especially since once practices are embedded in law and treaty, they are very difficult to change, even if conditions subsequently change or more recent data and technological evolution shift the appropriate cost/benefit analysis.

Proposed Research Agenda

The laws of war and the underlying norms and theories are often viewed in one of two ways. First, many assume that LOAC are institutionalized products of the Enlightenment based in Western philosophy and ethical systems. Others may see them simply as self-evidently reasonable and utilitarian. Both assessments render them unquestionable in terms of diverse human cultures. That is, human cultures may have very different norms with respect to armed conflict that have never been observed independent of the "preferred" or presumed-valid framework of LOAC. Moreover, these cultural norms may or may not be congruent. In fact, all human cultures may tend toward norms in conflict that are similar to each other, but may not resemble the laws of war as they currently stand. And, of course, some of the laws may be relatively more universal and less historically contingent than others: agreements that generally protect civilians may be more universal, for example, than laws which target one particular technology or practice.

Thus one proposal was the creation of an observational science centered on the laws of armed conflict in a globally-diverse context. In some ways, this would be analogous to trends in fields such as economics and philosophy, where "experimental" approaches, focusing on the way people and institutions are actually behaving, and why they think they are behaving that way, rather than simply developing speculative norms and models from abstract principles, is becoming more popular.

A central investigation will be to consider whether LOAC principles are universal, or merely unique to Western cultures, and whether some may be considered more universal than others. Otherwise stated, "What happens if you identify 3-4 different cultures (these might include Russia, China, Islam, and Latin America) and look at their behavior in conflict and identify the norms and ethics that they actually demonstrate?" How people actually behave in different forms of conflict (for example, internal informal conflicts as opposed to external state-to-state conflicts), and how they want conflict in their name to be carried out would be an important part of the investigation.

The science would objectively consider what conflict looks like from the outside and how it is organized, structured and conducted. The Council was careful to note that there is a difference between an observational science and the application of LOAC as it is implemented on the battlefield. The science is aimed at understanding what is actually going on but not imposing the observer's will on it, though forward-looking scenarios could absolutely be included in the scientific methodology. LOAC, by contrast, is both customary international law, and for most states formal treaty law, and is thus a legal reality.

An additional research goal is to establish a glossary of terms that are currently ill-defined with respect to modern conflict. This is not as trivial a research area as it might sound; indeed, definitions of key terms were a source of both confusion and debate within the Council itself. What are the relationships among "war," "conflict," "crime," "combat," and "police," for example? And even if robust definitions can be developed, will they remain stable in a period of rapid change? Is there even a "battlefield" anymore, especially in an age of pervasive cyber conflict? What is conflict now? Is a scenario of constant low level attacks - the Death by 1000 Cuts scenario – a conflict? These are non-trivial questions because often serious legal implications are engaged by such definitions: "combatant" versus "non-combatant," for example, or whether a state has been attacked in such a way as to justify a kinetic response under applicable laws of war.

Full set of workshop questions

The Council was asked to establish a set of research questions that they felt could and should be pursued as part of the research agenda. What follows is a consolidated list of these questions.

1. Is the law adequate to the task of governance of a conflict in the 21st century? Or of the design, manufacture, and use of emerging military technologies?
2. What limits should be imposed on the use of emerging technology?
3. Are modern technologies creating conditions in which the use of force is slipping out of the realm of legal and democratic accountability?
4. What is the difference between a combatant and noncombatant?
5. Should humanity ever allow autonomous robots to be armed regardless of whether those arms are lethal or "non-lethal"?
6. The human (in/on the loop) is moving further and further away from the firing decisions. What problems does this pose for future warfare?
7. Should intelligent machines be allowed to kill people?
8. Should cyber weapons be targeted toward civilians or civilian infrastructure?
9. Is cyber conflict a game-changer? There is a mechanism (hitting the enter key) that is similar to pulling the trigger of a gun. On the other hand, a gun has traceability, a software backdoor does not. How does it change the game?
10. Why do--or should--we limit nonlethal weapons that cause fewer deaths than approved lethal weapons? (For example, the laws of armed conflict preclude riot control agents that are not precluded for law enforcement officers.) This is what we called the "paradox of nonlethals."
11. Are modern technologies making it easier to resort to armed force? (at all levels from the policeman firing a Taser up to inter-state war)
12. Is it ethical or moral to weaponize drugs whose long term impacts on the individual self are not known?
13. What are the key assumptions that our current system relies on that, if changed, would destabilize the system as a whole. For example, is cyber an active attack? Does it destabilize international law? What if soldiers were designed without free will? What would that destabilize? This changes the assumption of responsibility in the military.

Scenario Planning

Scenarios are not meant to predict the future, but rather help individuals and groups think about new situations that could emerge. The Council took two separate approaches to scenario planning: a "development of scenarios by quadrant" method and a "war games" approach. The methods and outcomes for both are detailed with illustrative applications to some of the Council's issues in the next sections.

Development of scenarios by quadrant

Method

This approach begins with a group brainstorming about important future factors. Once this phase is complete, the factors are organized into groups and whittled down to 2 variables that become the axes of a two-dimensional graph. The origin of the axes should represent the situation at the present moment in time. Each of the four quadrants then represent one possible future where the variables have become exacerbated (right and up on the chart) or diminished (left and down). Sometimes a timeframe is established for the future scenario. Names are generally assigned to each quadrant to describe the scenario as accurately (but creatively) as possible. Finally the quadrants are populated with data and stories that explain how that scenario could come about.

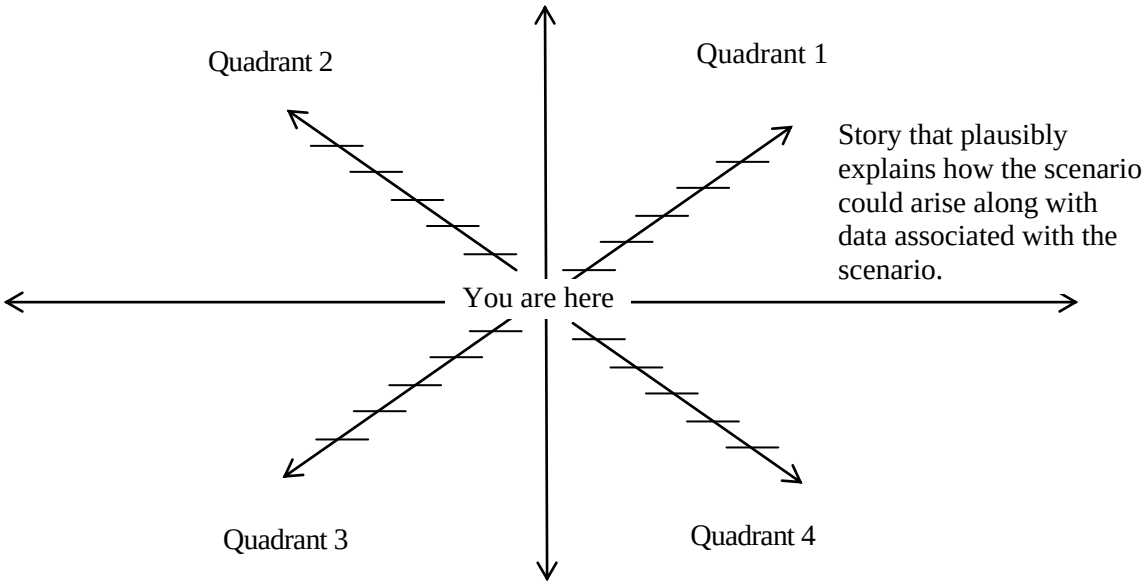

Figure 2. Example chart for development of scenarios by quadrant

Quadrant development

During the brainstorming phase, a number of factors were suggested as being appropriate axes, all of which were related to a few distinct themes. One such theme was governance of technology. For example, at some point there may be a treaty governing the autonomy of machines and robots. On the other hand, technological advancement may be exogenous (and simply a given). That is, treaties might not be the best way to manage technologies such as cyber weapons. The Internet is a good analogy: Who governs the Internet? Who enforces norms and constrains conduct by participants? Do cybercitizens accept their authority? The element of restrictive policy was identified as the X-axes for the first set of quadrants.

In relation to regulation and treaties, there was a question about how technological development might impact the future. That is, what would a future look like given accelerated technological advancement? By contrast, this method forces its users to consider the opposite end of the spectrum: Conditions of declining technological capability. Many participants felt that technological degradation was either

implausible or outside the interests of the group or both. Nonetheless, in the interest of utilizing the methodology correctly, participants acknowledged that a catastrophic occurrence that could set technology back a number of years was not out of the question.

These two factors then formed the axes of the first graph. As shown in Figure 3, policy restrictiveness is plotted on the X-axis and technological advancement formed the Y-axis. At this point, hypothetical scenarios seemed to spontaneously present themselves. For example, what would happen to the fundamental concepts of IHL if traditional jus ad bellum restraints degrade or devolve? Similarly, what if a major State (Japan, South Korea, India, Pakistan, Iran, Brazil, etc.) were to withdraw from existing international governance organizations or agreements (IHL, U.N., WTO, etc.)? This question highlights the tension between broad participation versus particular exceptionalism that brings about layered or tailored participation.

Two additional and interesting hypothetical questions also arose. First, at what point does a State's refusal to acknowledge armed conflict within borders constitute war crimes? And second, considering the Convention on Cybercrime, to what extent can and should the international community use armed force against a State that harbors cyber criminals within its borders?

Having formed the first set of scenario quadrants and discussed possible future scenarios, these factors were set aside and the brainstorming session resumed.

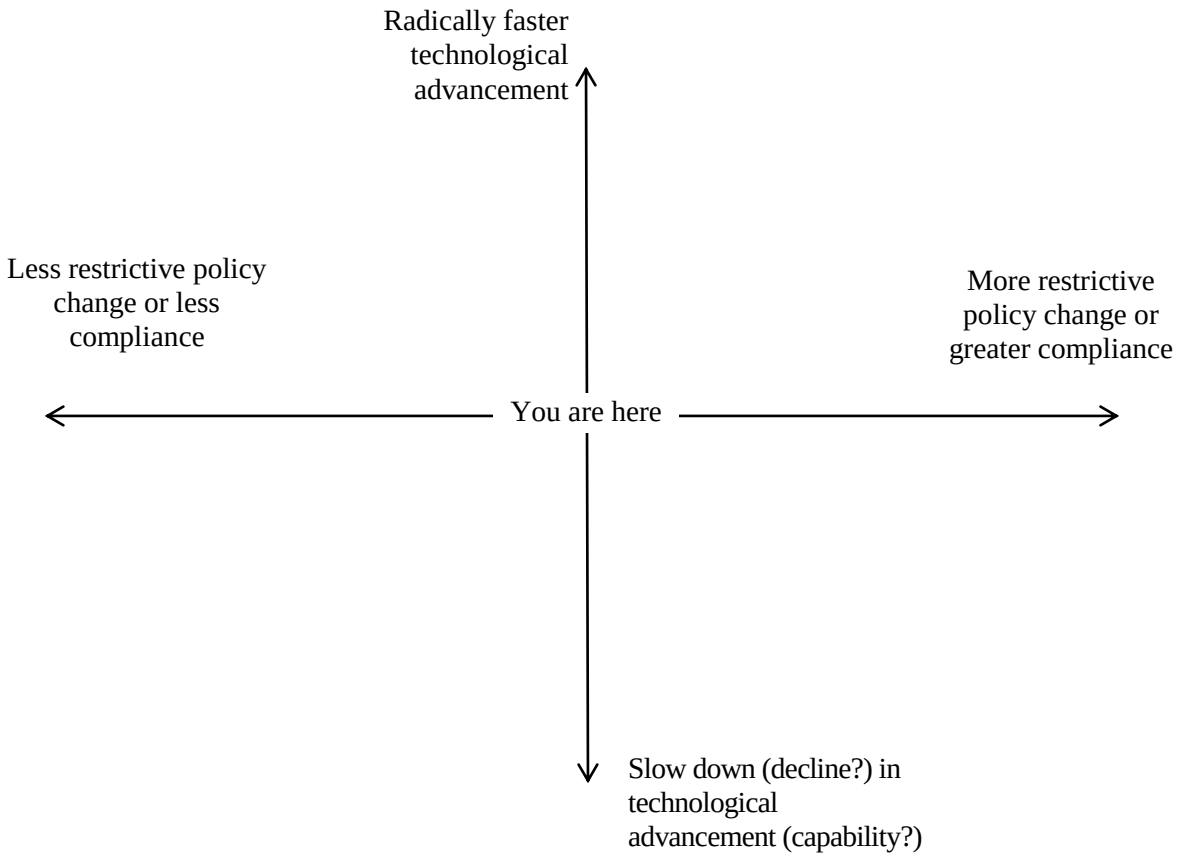

Figure 3. First set of axes for quadrant scenarios

The next theme to emerge from the process was that of the actors engaged in conflict. That is, nation-states have traditionally assumed a monopoly on violence, but that appears to be changing as attacks are starting to be organized by networks of militants and, in some cases, individual (sometimes suicide) bombers and shooters. Thus the participants wanted to explore both extremes of this spectrum and it appears as the X-axis in the second scenario diagram (shown in Figure 4).

The theme of conflict productivity was also explored as an axis title. Productive conflict was defined as dialog that occurs in a healthy democracy (managed conflict resulting in social/cultural/economic progress). This could be contrasted with unproductive conflict such as occurred in the Congo and Rwanda civil wars. The participants wondered what it would mean to segue from unproductive conflict to productive conflict and how productive conflict can be achieved. Thus, conflict type formed the Y-axis in the second quadrant diagram.

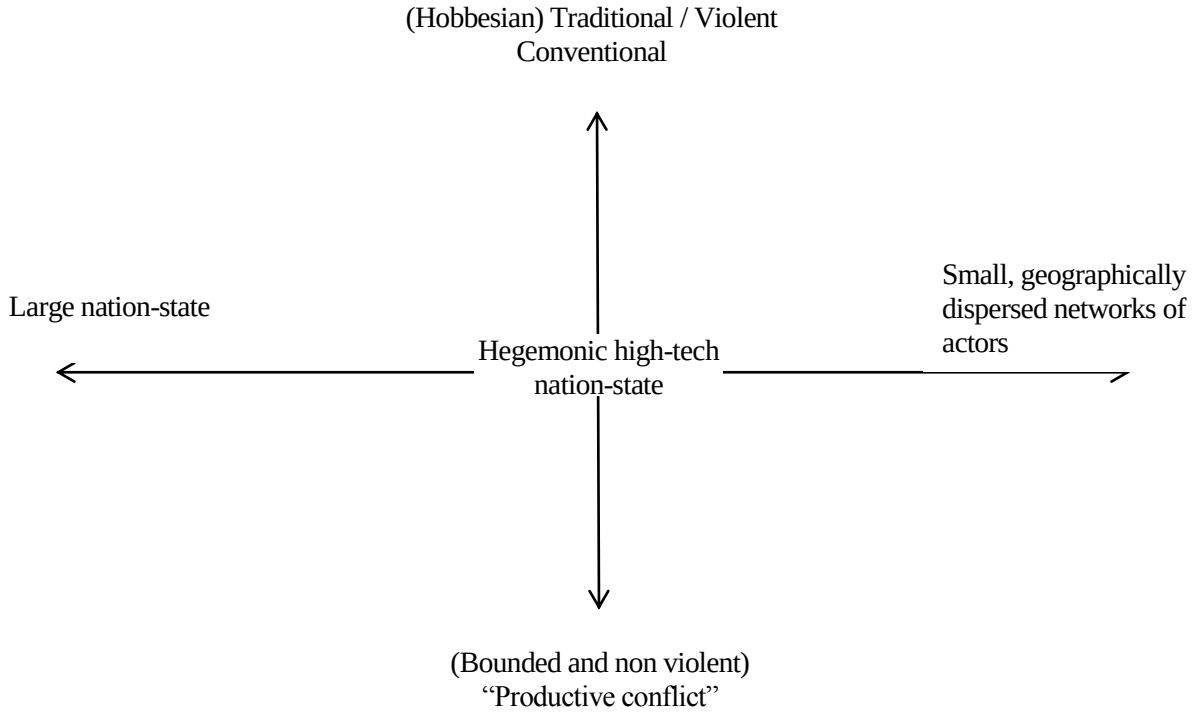

Figure 4. Second set of axes for quadrant scenarios

The participants next turned to specific military weapons technology. Within this theme, proposed relevant spectra included indiscriminate to discreet weapons, and lethal to non-lethal force. Participants also noted that context for the weapons is important, specifically the scale of conflict: small skirmishes to large wars. On this theoretical graph, it was expected that conflicts could be plotted in the quadrants, along with optimal application of the technologies. However, it immediately became clear that the users of the weapons were also important. Thus, it was proposed that law enforcement and military uses of technology form a third dimension, or Z-axis, on the graph, thus creating a total of eight "quadrants" (see Figure 5).

Once again, the axes made hypothetical questions become apparent. In this case, noting that the right lower rear quadrant was prohibited by IHL, participants asked: Is it ever permissible to inflict pain for purposes of behavioral control (e.g., use of ADS or Tasers for crowd control or military checkpoint management) where IHL specifically prohibits this as either "torture" or "inhumane treatment"? On a larger scale, this begins to point to a recurring theme in the proceedings at large: that of when, if at all, it is appropriate to act in direct violation of IHL.

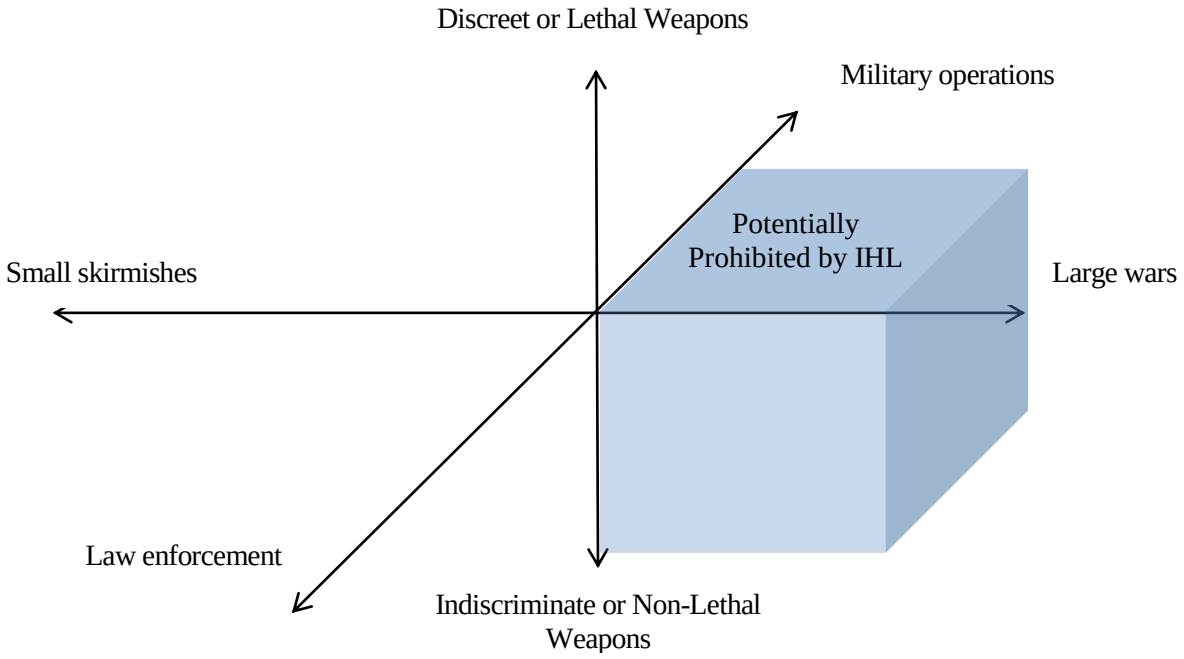

Figure 5. Third set of axes for quadrant scenarios

Although these were the only sets of axes to be created, a number of other themes were discussed and could form the basis of future scenarios. Among these were humanitarian factors. Questions along these lines included, what technological development scenarios could lead to less international tension, use of force, and concomitant humanitarian suffering? By the same token, the participants wondered, under what circumstances are humanitarian considerations so great that we might want to reconsider or even violate the principles of ethical war (discrimination, proportionality, etc.)? Once again, the question arose as to whether exceptions to IHL could, in some cases, actually lead to a more humane conflict.

The Council approached this methodology from the perspective of determining its overall usefulness, rather than determining whether specific instantiations of it were rigorously useful. This was in part because of time and resource constraints: a well-run scenario planning session would have required virtually all the time the Council had for its deliberations. Accordingly, the examples given above should be viewed from the perspective of proof of concept – it this method useful in attempting to explore difficult institutional, geopolitical, and normative contexts given disruptive and unpredictable technological change? – rather than as explicit scenario exercises. The Council concluded that these

methods had great promise, but required appropriate prior deliberation, construction of scenario spaces, and resource commitment.

War game: Ethics and governance of cyber conflict

> *"If you shut down our power grid, maybe we will put a missile down one of your smokestacks!"*
>
> – Anonymous U.S. military official, quoted May 31, 2011, on new U.S. Cyber Strategy

The Council next moved to a different approach to scenario creation and analysis: That of a war game. The scenario is presented here as a series of steps with important points of discussion associated with each step. The driving question for this scenario was this: *"Under what circumstances could a nation (the text refers to the fictitious nation of Ambia) launch a serious cyber-attack on US critical infrastructure, and what would appropriate responses be at each stage?"* The Council was then presented a narrative describing one path that would result in such a future.

Situation: There is tension between the US and Ambia (a large nuclear power). The US is considering a buildup of naval forces in international waters near Ambia when a blackout occurs in Fresno, California. Circumstances suggest the two events may be linked.

Step 1: The US tries to establish attribution. The best intelligence says, "We don't know who did it yet."

The assumption within the US Intelligence Community is that the Ambians want to delay US deployment two weeks and have therefore fired a "shot across the bow". In terms of defensive measures, the US does not have cyber defenses to deploy, but cyber weapons are typically used only once. Offensively, under international law, counter measures are allowed, but require attribution first. Otherwise the use of force is prohibited. Confirmation that the attack originated with the Ambian government would be regarded by the US as a military attack not because of the impact of the blackout on Fresno (assumed to be minimal), but because it would viewed as Ambia attempting to prevent the US from sailing where it wants in international waters. (The US has sailed near Ambia before.)

Step 2: The attack on Fresno is found to be similar to a previous penetration by Ambia on Cleveland's electrical grid.

Attribution has still not been confirmed. Some feel that this relatively innocent use of a known electronic back door, though suggestive, presents a new way to respond to and manage a threat. They suggest that, unless damage or loss of life occurs, the blackout is not an act of war, but merely posturing. Nonetheless, it is believed that the president gets to decide if it is war or not war. The question becomes, at what point does such a situation constitute "armed conflict"?

Step 3: The US scales up its forces near Ambia. A blackout occurs in McLean, Virginia, during a summer heat wave. Military officers are impacted. The Pentagon goes on emergency generators.

The US Intelligence Community is considering the underlying issue: Is it that the lights have gone out in Virginia? Or is it that the US has been shown to be vulnerable to cyber-attack? Or is it that the potential attack is directed against civilians for military purposes (restricting deployment of US Navy forces) – and, in spite of no loss of life and minimal damages under the scenario, is this a war crime in that civilians are targeted? The US contemplates further naval deployments, as well a non-armed attack in Ambia. However, the line between an armed and non-armed attack is not clear.

Step 4: The lights go out in the homes of Ambian Army generals. Ambian officials attribute the cyber-attacks on the US electrical grid to rogue hackers.

The US president considers whether he believes the attack came from a rogue hacker group (in real life, this would not be a surprise to the US government). The attack on Ambian targets is not attributed to any specific group, and the US denies direct responsibility. This highlights the difference between a cyber and kinetic attack: the source of a kinetic attack is never in question because it is almost always physically obvious. With cyber, on the other hand, there may be questions about whether an attack even occurred, or, if an event is defined as an attack by the receiving party, whether it was so intended by originators and if so, whom do they represent?

The US considers the economic consequences of military actions against Ambia. Everyone acknowledges that, though unlikely, escalation could ultimately lead to a nuclear exchange.

Step 5: Ambia knocks out the power at a number of military bases in the United States. This has now risen to the level of a real threat… with clear further capability.

Note that this is still not a clear assault on civilians (although it suggests that previous attacks may have been), but there is an overt threat coupled with a large blackout covering most, but not all, of the US. Advisors argue about the severity of the situation. Some note that the attack is reversible and that no generators were destroyed. Others suggest that the attack should now be considered the equivalent of a kinetic use of force and a kinetic response is now ethically justified. Consensus on an appropriate response remains elusive for three reasons. First, even if it is an attack, not all attacks require, or justify, responses. Second, that cyber hostilities are now in the open implies that earlier attacks, which did target civilians, derived from the same source, raising the political challenge of potential war crimes and what to do about them (will solving the crisis be more or less difficult if cyber forces may be subsequently charged with war crimes?). Third, and more fundamental, is the question of whether cyber is a "game-changer" in that it requires rethinking of existing regimes.

Meanwhile, power outages quickly become humanitarian crises as gasoline and water pumps stop working and food and water cannot be distributed.

War game debrief

The Council recognizes that there are analyses and data that indicate that other nations have actually penetrated the US electrical grid and other U.S. targets, commercial and governmental; though no malware has been found, at least one tunnel (backdoor, trapdoor) is known to exist. Hence this scenario, or a similar one, is a realistic threat. Moreover, the odds are high that additional tunnels exist but have not yet been discovered.

Among the many other issues this scenario raises is the conflict between an open society with free speech and privacy rights, and security concerns. In cyber, as with many other technologies, this conflict is very real, and is poorly resolved by secretive resolutions. An additional challenge is that many countries would be glad to impose significant constraints on Internet and cyber systems, but the US puts a high value on the preservation of privacy and free speech, giving it the difficult position in international discussions of defending cyber assets against undue intrusion and regulation, while still supporting important security goals.

Concluding remarks

At the conclusion of the scenario session, participants were asked to reflect on the experience. Overall, they felt that the exercise was valuable, but that neither approach was ideal. The quadrant scenarios method illuminated some important questions and had significant potential, but requires significant time and resources to conduct properly. Some suggested that an initial scoping process, which focused the scenarios on more concrete issues, might lead to the production of more useful specific results. By

contrast, the war game was specific but was not as useful in illuminating the larger ethical issues. It was, however, clear that questions arising from the laws of war as impacted by emerging technologies are highly complex and integrated across many domains, suggesting that methods such as these, which are useful for helping to frame and address such complexity, have a role to play in exercises such as the Council undertook.

Future Technologies and Research Topics

"Technology is becoming obsolete more and more rapidly: Technology lags behind technology."

Technologies the Council should consider in the future

Information and Communication Technologies

Information technologies are already important because they are enabling massive data search, analytics, and mining capabilities, and, through massive integration, are soon likely to enable crowd sourcing for military applications. Looking farther ahead, cryptography with quantum computing could provide unbreakable cyphers, with important implications for national security.

Robotics

Although robotics in general raise a number of questions already discussed, lethality and autonomy in particular, swarms of small, coordinated robots could soon be used to execute both fatal and disabling attacks on individual targets. Moreover, robots are expected to be deployed in greater numbers in the future, and fight alongside humans on the battlefield in coordinated operations. As individual mechanisms are coupled together over wide geographic spaces, it may become more difficult to determine exactly what the boundary of a "robot" actually is.

Nanotechnology

The implications of nanotechnology to the armed forces are important, but difficult to determine, in part because nanotechnology is primarily an enabling technology platform for other technologies: both biotechnology and ICT, for example, become more potent and evolve more quickly as developments in nanotechnology accelerate. This is a potentially large area for future focus.

Biotechnology

There is a broad spectrum of biotechnologies that should be studied. This ranges from cutting-edge synthetic biology (genetic sequences that can do interesting things), to the very low tech that includes attempts by insurgents to try to taint food in enemy mess halls. In part this is because the integration of the biological and the physical is proceeding very rapidly with unpredictable implications; and in part this is because biotechnology is a critical competence for designing humans.

Neuroscience

Advances in cognitive and neuroscience may unlock some very interesting military technologies in the near future. Among these are telepathic helmets that allow warfighters (and civilians) to communicate with each other remotely – and without the need to speak. Farther into the future, neuroscience could facilitate the "hacking" of the central nervous system. That is, as more knowledge of the brain is gained, the very thought patterns of individuals could be deliberately determined – including ethical codes and decision-making of not only soldiers, but commanders on up the chain. This of course raises issues of free will and responsibility, which is why the Council should add it to the research agenda.

Human enhancement

Technologies that will contribute to physically enhanced soldiers raised a number of difficult issues for the Council. They wondered about the legality (either in terms of IHL or domestic laws) of requiring service personnel to accept enhancements such as genetic modification. Further, under what conditions can individual soldiers opt out of military enhancements? Should recruiters be allowed to provide incentives for accepting physical alterations – diminished service requirements, perhaps? Should enhancements be required in order to receive promotions? What if an individual is drafted?

The Council also wondered about identity, theological, and social issues. Will enhanced personnel consider themselves superior to "natural" humans, and vice versa, thus creating cohesion within the groups but conflict between "classes"? Will supersoldiers show restraint when appropriate?

Beyond the individual, is a nation ethically obligated to enhance soldiers to the extent of its ability? Is a nation ethically bound to enhance warfighters to make them more accurate and discriminating? If enhancements may help a soldier to survive combat, must they ethically be provided? To what extent should the fighting force reflect society? Will permanent enhancements create a class of professional soldiers?

The question arose as to the nature and implications of an enhanced human corpus (chemically, biologically, etc.). Should an enhanced human be considered a weapon system? To what extent do the definitions change if the tools are inside versus outside the body? To what extent does accountability change? Could enhancements prevent a soldier from acting unethically?

Finally, typically any technology that can be used to enhance an individual could be used to de-enhance another. What are the implications of de-enhancing humans? On a large scale?

Chemical and material technologies

Turning now to chemical technologies, the Council expressed interest in agile manufacturing of niche substances. Specifically, microreactors are coming online that can synthesize pure, specialty chemicals on a relatively inexpensive, just-in-time, just-what-you-need basis. For example, hydrogen peroxide is a common chemical that can be purchased, diluted, from a drug store. However, when concentrated, it is a regulated toxic explosive. Microreactors can make small, non-reportable (low) quantities. For larger quantities, the microreactors can be run longer or in larger quantities.

3D printers are starting to enable agile – or "additive" – manufacturing. Most commercial models use benign materials for fabrication; however, some model can utilize metal and ceramic powders in addition to plastics, allowing them potentially to build almost anything, i.e. weapons on demand. The cycle time from field request to operational is thus very short (and, because the 3D printers are rapidly becoming less expensive, the democratization of weapons continues apace).

Geoengineering

Geoengineering is the ability to modify the Earth's climate with technological interventions. This may be of potential interest to states because changing global systems may well provide differential costs and benefits: global warming, for example, may open more areas of northern countries such as Canada and Russia to mining and agricultural exploitation. Some proposed geoengineering projects include placing solar reflectors into earth orbit in order to reduce the total incoming radiation, thus cooling the atmosphere. The Council was concerned that low-cost access to space (by private firms) could enable rogue global warming mitigation projects.

Similarly, others suggested that climate change might be seen by some as a weapon. That is, some nations that stand to benefit from global warming (in terms of growing food in higher latitudes, for example) might seek to increase overall greenhouse gas emissions in order to design the climate to benefit them and disadvantage enemy states at lower latitudes.

The problem with both of the above strategies is that the global climate system is not well understood, and earth systems are interconnected. Thus, the actual results of a deliberate attempt to change the climate are impossible to predict, making use of such a weapon highly problematic for a rational actor.

Even more targeted attempts to control the weather for military purposes were proposed and studies during the Cold War, and more sophisticated possibilities could be on the horizon. Such scenarios are addressed in Air Force 2020 where it is suggested that creating tornadoes in the US Midwest or disrupting the monsoon in India are possible future tactics.

Augmented cognition

Augmented cognition (aug cog) is the fusion of cognitive science and information technology for the purpose of compensating for low-bandwidth humans in increasingly complex environments. It is already being applied to automobiles in the non-military domain, for example. As technology becomes more pervasive in the human body, and particularly the brain, in ways that augment elements of human cognition, how do we ensure that humans are acting morally? As individual soldiers become elements of techno-human networks which display emergent behaviors, what are the implications for responsibility, agency, and control of behavior?

Hybrid/other

As with aug cog, technologies often merge for very specific and powerful ends. Another example of hybrid technology is that of behavior modeling and tracking. That is, by simply observing human behavior and movement (e.g., gait analysis), computer systems are increasingly able to diagnose conditions such as autism before they become apparent to physicians. Further, the same technology might find applications in security screening at airports and elsewhere. This leads to serious questions of privacy, particularly when such systems can be deployed anywhere. In the future, people may need to beware of lethal autonomous telephone poles.

In other settings, technology has evolved to the point where intelligent systems are capable of overriding human operators. On September 11, 2001, for example, the technology existed to prevent terrorists from flying planes into buildings (a computer override could have been installed/engaged). Yet, in that case as with many others, humans are often unnecessarily kept in control. The time has come to seriously consider when humans should be in charge and when machines should: Who/what knows best and when?

Thus far, this report has dealt with technologies that are relatively well understood because they are visible on the horizon: Neuroscience applied to the battlespace, for example. But convergence of technologies will inevitably create entirely new – and surprising – weapons. The future of war is then significantly different than can currently be projected. Consider, for example, warfighters that are enhanced both neurologically and genetically. They may not eat or sleep for long periods of time. They may be stronger and faster than the Olympians of today. Will such future warfighters be considered "human"? Will they consider themselves to be "human"?

Governance & management

Given the emerging technologies discussed above, some Council participants expressed an interest in governance or management of the technologies themselves (though not stopping it as that is likely to be

impossible). Consider, for example, pilots in Las Vegas firing weapons from UAVs (unmanned aerial vehicles) in Afghanistan. Who is responsible if and when the weapon creates collateral damage? There are more categories of personnel on the battlefield today than ever before: NGOs, security apparati, journalists, bounty hunters (effectively a mercenary army). Perhaps what should be studied is not necessarily the law, but means to manage technology and conflict, perhaps through cultural models and experiential training ("soft law" models of technology management). Note also that the assumption that technology can be understood, and reacted to quickly enough to be managed, is testable, and is not necessarily accepted by all students of technology.

The Council suggested that one goal might be simply to raise concerns about the implications for civil society early in the military technology development process. Currently, no one is taking responsibility for addressing these issues. One example comes from the routine iris scans that are being done to identify people in Afghanistan. Such technologies certainly provide one mechanism that would, in civil society, reduce privacy and enhance security. Will it, and other technologies such as insect size surveillance robots, lead toward a security state? The flow of military tech into civil society is going to be significant, but nobody is looking at that pattern of migration. This is a huge gap.

Lessons Learned and Future Suggestions

"There is nothing new under the sun, but somehow it's different."

Laws of armed conflict

One of the most divisive issues among the Council members concerned the comprehensiveness, relevance, and applicability of the existing legal framework and ethical principles in terms of their ability to address the issues of 21st century conflict. On one hand, many participants felt that the underlying framework of the laws of armed conflict is sound and that, at least for now, technology is not a game-changer. Others disagreed, indicating that human enhancement, in particular, is not sufficiently addressed by LOAC. Moreover, concern was expressed with regard to becoming complacent with existing legal frameworks as the world changes. Still others took a more pragmatic view, suggesting that the laws themselves are not only fairly static, but also not easy to change. Instead, they continued, what needs to be addressed today is the interpretation of the laws as they stand. As an example *ad bellum,* consider whether a cyber-attack can be equivalent to an armed attack? As an example *in bello*: Can a robot distinguish between a combatant and a civilian? Moreover, under what circumstances should unmanned systems be used? Not be used? In sum, the creative tension could be characterized as one of deeper and more extensive interpretation of new technological developments within the existing conceptual framework of law and morality, versus a conviction that that framework itself was increasingly threatened with obsolescence in the face of new military technologies. While general agreement was reached on the need to stay proactive, there remained a variety of positions on the question of whether LOAC were currently adequate. While it was apparent that the existing legal structure was not completely inadequate, and had a number of significant strengths, it was also felt by some that that aspects of the legal structure may have to be reassessed or reconsidered as time and technology marches on, probably on a case by case basis.

Research Methods

The group expressed interest in ongoing research toward developing an observational science of LOAC. Perhaps the most immediate realization among the Council participants was the lack of an appropriate analytical approach or framework, one that would allow them to think better about emerging technologies at various scales. Thus, the closing sessions of the Chautauqua Council turned to identifying additional research methods to aid future work.

Reflective equilibrium

The first such method is an existing approach to future studies. "Reflective equilibrium" begins with social contract thinking as interpreted by John Rawls in *A Theory of Justice*. The researcher imagines a situation in which social institutions and laws do not exist. The underlying assumption is that reasonable, well-informed people are blinded to their own circumstances within existing institutions. The research then asks, in the absence of existing norms, what would a reasonable individual create in terms of social institutions and legal regimes? The reflective equilibrium construct, as compared to current standards, provides the researcher with specific proposals regarding what might be changed in existing institutions.

Comprehensive matrix

The second research method involves the development of a large, comprehensive matrix that draws together all of the topics of the discussion and organizes it. For example, the identified themes could be mapped to the associated problems by labeling columns with specific technologies and rows with ethical principles. This example is depicted in Table 3. An alternative labeling scheme for the rows might be arms control dimensions: treaties, from legally-binding international accords through softer national law to policy.

Table 3. Example research matrix

5 Cardinal Principles	RPVs	UUVs	AUAVs	…	Prosthetics	Pharma	…	Crime	Espionage	Eternal conflict
Jus ad bellum										
Just cause										
Last resort										
SIUS*										
Necessity										
Proportionality										
Distinction										
Command responsibility										
	Robotics				Enhancements			Cyber		

*SIUS = Superfluous injury and unnecessary suffering

Complexity theory

The lens of complexity might be a means to analyze this area. If the cycle time of tech change is coupled to the cycle time of legal change, then the law can keep up, at least incrementally. But if technology advances faster, then the law will never catch up and there will always be dysfunction. This leads to complexity as a framing device. The fact that technology is not always used in the manner it was intended adds another level of abstraction and further points to complexity theory as an appropriate framework.

Moreover, there is coevolution in and among systems: distinct technologies interact in ways that are difficult to predict, and could become unstable. Thus it is important to consider not only first order, but also second- and third-order impacts. This approach is explicated in Allenby and Sarewitz, *The Techno-Human Condition.*

Research challenges

Other challenges were identified in conjunction with the development of research approaches, most of which are best addressed by individual researchers. For example, a discussion emerged with respect to where the issues of ethical use of military technologies actually arise: with the technology itself or society. That is, does technology per se present the full panoply of ethical and legal challenges? Or does its use? Others took a wider view, stating that issues emerged in the three states of design, manufacture *and* use, with additional complication added when troops in the field adapt tools for novel and unintended purposes.

An alternative view might look at relationships between technologies and actors or institutions: how does emerging tech relate to the state, how does technology relate to non-state actors, etc. Moreover, when viewed systemically, will instabilities arise? Will there be surprising secondary and tertiary effects? In the midst of conflict, how should states balance the need to deploy technology rapidly with the need to monitor its impacts (perhaps via slow and more controlled releases)? Is such control of technology systems even possible, or does it depend on the granularity with which the technology is being addressed?

Questions of scale were also posed. That is, should the focus be on the individual warfighter being hit with a Taser, or on armies fighting wars (the wars impact/kill a lot more people) – or is it a case by case situation based on the questions posed and the subsequent analysis. Where should the balance lie? Similarly, there is a tension between whether to study individual technologies (or artifacts), which is relatively simple from a research standpoint, and looking at the issues systemically, which is much more difficult. Identifying the best practices is likely to be an ongoing process. Looking at individual technologies would result in one analysis, but that would not capture the larger outcomes that result from converging technologies becoming embedded in social and military systems.

Conclusion

There are three primary perspectives on war:

- pacifism, the belief that war is never just;
- realism, the belief that any attempt to apply ethics to warfare is futile; and
- just war theory, the position that some wars are indeed justified and can be conducted according to ethical standards.

The Chautauqua Council, however, took one step back and made only one assumption: That, given historical experience, armed conflict of some form will continue. Given that starting point, it then asked two important questions: (1) Regardless of any legal or ethical framework, if observed objectively, what norms of conflict do diverse cultures practice? (2) Even though the existing laws of war continue to be refined and expanded, are they keeping pace with the conduct of war in a complex global context of rapidly-coevolving technologies? Both questions taken together form the core of a critical research agenda which is, to date, inadequately addressed.

This inaugural Council meeting highlighted a number of issues that require ongoing consideration. Among these is the need for constant and active review of the LOAC in light of emergent scenarios. Human enhancement, in particular, is an emerging technology that could expose voids or disparities in the

laws of war. Another major issue highlighted by the Council was that of ambiguous terminology. This is a serious point because a definitional change can render an act illegal when it previously was not and vice versa, and sloppy and inadequate analysis can arise when assumptions embedded in common terms become obsolete.

In terms of research, the Council noted a lack of appropriate analytical methods for considering the laws of war and emerging technologies at various scales. However, members concluded the workshop with a number of ideas that can be refined as research progresses.

Technology and armed conflict are inseparable. However, just as technological advancement imparts a military advantage to its owner; it simultaneously renders old norms obsolete and can destabilize social institutions – include the laws of armed conflict themselves. Thus this Council represented the first of potentially many collaborative meetings meant to identify gaps in current knowledge and set an agenda for future research. The ultimate goal is to produce intelligence that can enhance long term military and national security, and enable enhanced social stability and prosperity, nationally and globally in the 21st century.

ASU LINCOLN CENTER for APPLIED ETHICS
ARIZONA STATE UNIVERSITY

Appendix A

SUMMARY DOCUMENT: LAWS OF WAR

I. Sources of behavior regarding state conflict
   a. Western cultural and ethical morays
   b. Laws of War as philosophical and theological constructs
   c. Legal obligations such as customary international law, treaties, applicable domestic law,

II. Categories of Laws of War
   a. *Jus ad bellum:* when is it just to start a war (traditional)
   b. *Jus in bello:* how is it just to fight a war (traditional)
   c. *Jus post bellum:* what is a just resolution after war (cf Kant)

III. *Jus ad bellum*
   a. Just cause (self-defense, or other-defense)
   b. Right intention (St. Augustine)
   c. Public declaration by proper authority
   d. Last resort
   e. Probability of success
   f. Proportionality

IV. *Jus in bello*
   a. Treatment of external entities
      i. Military necessity/military objective
      ii. Discrimination (or distinction) between legitimate and non-legitimate targets
         1. intentional targeting of protected persons is prohibited
         2. Non-combatant immunity/hors de combat (enemy personnel who are "out of combat")
      iii. Doctrine of Double Effect: where collateral effects will occur, combat action may still be taken provided that it is otherwise permissible; that the combat and not the collateral effect is the one intended; that the collateral effect is not the means to achieve the combat effect; and that the combat benefits outweigh the collateral impacts.
      iv. Proportionality (only proportionate force employed, and only against legitimate targets)
      v. Principle of unnecessary suffering or humanity: primarily means and methods of warfare
         1. Prohibition on weapons that are *per se* intended or calculated to cause unnecessary suffering;
         2. Prohibition on use of otherwise lawful weapons in ways that cause unnecessary suffering
         3. Prohibition on means *mala in se* (evil in themselves); e.g., mass rape as weapon
   b. Treatment of internal entities
      i. Follow external rules, since this owed to internal public in whose name war is being conducted
      ii. Respect domestic human rights (cf Rwandan genocide, Holocaust)
      iii. Respect rights of state's military personnel
   c. Supreme emergency exemption (country that is victim of aggression, if on verge of defeat and humanitarian disaster at hands of aggressor, may set aside *jus in bello* (e.g., WWII UK prepared to

use poison gas on Nazi invaders, and initiated bombing of German cities to avoid invasion) (nowhere written into international law)

V. *Jus post bellum*
   a. Newly evolving domain of just war theory
   b. Appropriate termination of war increases changes of productive peace; inappropriate termination increases chances of future conflict (e.g., Treaty of Versailles).
   c. Issues: compensation, discrimination, sanctions, rehabilitation, management of war crimes
   d. Is regime change acceptable?

VI. *Jus contra bellum*
   a. Aims at absolute renunciation of aggressive war (fairly modern; cf: "The War to End All Wars")
      i. Eighth Assembly of League of Nations; Kellogg-Briand Pact of 1928 (The Treaty for the Renunciation of War, it remains in force today and has become customary international law. *Note that it does not limit force in self- or other-defense.)*
      ii. UN Charter Article 2(4): bans "the threat or use of force".

VII. Sources of theory of just war
   a. Philosophical and theological
      i. Control of conduct during conflict has a long tradition in many cultures (ancient Babylon, China, India, Old Testament, Koran)
      ii. Concern over when wars should be fought has similar history (ancient Egyptians, Sumerians, Hittites, Greeks, Romans, among others)
      iii. Notable contributions by Aristotle, Cicero, Aquinas, Grotius (1583-1645; his book, *On the Law of War and Peace*, often considered starting point for modern law of war).
      iv. Hague Conventions of 1899 and 1907 (primarily focused on avoidance of war, weapons)
      v. Geneva Conventions: four treaties (1864, 1906, 1929, 1949) and three additional protocols (1977, 1977, 2005) (generally deal with standards for the humanitarian treatment of the victims of war; considered customary international law).
      vi. Other treaties governing means of war:
         1. 1925 Geneva Protocol prohibits use in war of asphyxiating, poisonous, or other gases
         2. 1993 Chemical Weapons convention prohibits production, stockpiling, and use of chemical weapons, even as part of otherwise legitimate retaliation
         3. 1954 Hague Cultural Property Convention (protects cultural property)
         4. 1925 Geneva Protocol also prohibits biological weapons; 1972 Biological Weapons convention prohibits production, manufacture, stockpiling, and use even in otherwise legitimate retaliation
         5. 1980 Certain Convention Weapons Convention, based on principles of unnecessary suffering or indiscriminate effects, restricts or prohibits:
            a. Non-detectable fragments (Protocol I)
            b. Mines, booby traps, and similar devices (Protocol II)
            c. Incendiaries (Protocol III)
            d. Laser weapons (Protocol IV)
            e. Explosive remnants of war (Protocol V)

VIII. US has ratified Hague and Geneva Conventions; not ratified Protocols I and II of the Geneva Convention; ratified 1980 CCW with reservations, declarations, and understandings.

IX. Major alternative perspectives to Laws of War

a. Realist: war is arena where nation must do what it takes to win (e.g., Hobbes, Thucydides [esp. Athenians at Melos: join us or die], Machiavelli). Realists do not recognize moral or ethical controls on the state and therefore reject International Humanitarian Law and the laws of armed conflict. In their view, states have interests, but not ethical obligations, and certainly not obligations derived from one cultural framework.
    i. Descriptive realism (this is factually how states act)
    ii. Prescriptive realism (this is how they should act)
b. Pacifist: Like realists, pacifists reject IHL and LOAC, but on the grounds that warfare itself is unethical, thereby rendering any laws and norms that address it obsolete (and even unethical, to the extent that such rules make conflict more likely by appearing to make it less harmful).
    i. Religious ("turn the other cheek" in Christianity)
    ii. Secular
        1. Wars violate human flourishing
        2. Benefits of war never outweigh costs
        3. Rule-based: war violates duties of morality, justice

Principle Sources: Brian Orend, *The Morality of War* (Broadview Press: Peterborough, Ontario, Canada, 2006); LTC Jeff Bovarnick, et al, *Law of War Deskbook* (International and Operational Law Department, The Judge Advocate General's School, U. S. Army, Charlottesville, Va, 2010).

Appendix B

CHAUTAUQUA COUNCIL ATTENDEES

(with bios)

Brad Allenby (ASU, Chair).

> Dr. Braden R. Allenby is currently Lincoln Professor of Engineering and Ethics, and Professor of Civil, Environmental and Sustainable Engineering, and of Law, at Arizona State University, where he is also the Founding Chair of the Consortium for Emerging Technology, Military Operations, and National Security, established in 2009, and Founding Director of the Center for Earth Systems Engineering and Management. He is a Fellow of the American Association for the Advancement of Science; a U. S. Naval Academy Stockdale Fellow for 2009/2010; an AT&T Industrial Ecology Fellow for 2008/2009; a Batten Fellow in Residence at the University of Virginia's Darden Graduate School of Business Administration; a Fellow of the British Royal Society for the Arts, Manufactures & Commerce; and was a Templeton Research Fellow in 2008/2010. Dr. Allenby has written extensively on emerging technologies, sustainable engineering, industrial ecology, and earth systems engineering and management.

George Lucas (U. S. Naval Postgraduate School, Co-chair).

> Dr. George Lucas is Class of 1984 Distinguished Chair in Ethics in the Vice Admiral James B. Stockdale Center for Ethical Leadership at the United States Naval Academy (Annapolis), and Professor of Ethics and Public Policy at the Graduate School of Public Policy at the Naval Postgraduate School (Monterey, CA). Dr. Lucas has authored and edited numerous books, book reviews, and scholarly articles on the topics of philosophy, military ethics, and national security. Dr. Lucas is co-editor (with Capt. Rick Rubel, U.S. Navy, retired) of the textbook, Ethics and the Military Profession: the Moral Foundations of Leadership, and a companion volume, Case Studies in Military Ethics, both published by Pearson Education (New York, 2004). These texts are used in core courses devoted to ethical leadership at the United States Naval Academy, the United States Air Force Academy, and at Naval ROTC units at over 57 colleges and universities throughout the nation.

Carolyn Mattick (ASU, Chair Assistant).

> Ms. Carolyn Mattick is currently pursuing a Ph.D. in Environmental Engineering at Arizona State University. She has written on the role of energy in society and engineering education. She teaches an annual workshop on ethics for professional engineers.

Fritz Allhoff (Western Michigan).

> Dr. Fritz Allhoff is an Assistant Professor in the Philosophy Department at Western Michigan University, as well as a Senior Research Fellow at the Australian National University's Centre for Applied Philosophy and Public Ethics. His primary research interests are in ethical theory, applied ethics, and philosophy of biology. In applied ethics, his two most extensive research programs are on the moral permissibility of interrogational torture and on ethical issues surrounding emerging technologies, especially nanotechnologies. He has authored and edited a number of peer-reviewed articles and books in these areas.

Ron Arkin (Ga Tech).

> Dr. Ronald C. Arkin is Associate Dean for Research and Space Planning, Regents' Professor, and Director of the Mobile Robot Laboratory at the Georgia Institute of Technology College of Computing. His research interests include behavior-based reactive control and action-oriented perception for mobile robots and unmanned aerial vehicles, hybrid deliberative/reactive software architectures, robot survivability, multiagent robotic systems, biorobotics, human-robot interaction, robot ethics, and learning in autonomous systems. His numerous publications in these areas include a book entitled *Governing Lethal Behavior in Autonomous Robots* published by Chapman-Hall (Taylor & Francis) in 2009. Dr. Arkin has formerly served as a board member for several committees on robots in society and robot ethics, and currently serves on the Board of Governors of the IEEE Society on Social Implications of Technology.

Charli Carpenter (Univ of Mass).

> Dr. Charli Carpenter is an Associate Professor in the Department of Political Science at University of Massachusetts-Amherst. Her teaching and research interests include national security ethics, the laws of war, transnational advocacy networks, gender and political violence, war crimes, comparative genocide studies, humanitarian affairs and the role of information technology in human security. She has a particular interest in the gap between intentions and outcomes among advocates of human security. She has published three books and numerous journal articles and has served as a consultant for the United Nations. Dr. Carpenter's current research focuses on global agenda-setting, investigating why certain issues but not others end up on the human security agenda. With funding from the National Science Foundation, she is directing a project on Transnational Advocacy Networks.

Andrew Carswell (International Committee for the Red Cross).

> Mr. Andrew Carswell currently serves as delegate to the US and Canadian Armed Forces for the International Committee of the Red Cross (ICRC). He holds a Master's degree in international humanitarian law from the University of Geneva and the Graduate Institute of International Studies. Since 2006, he has been employed by the ICRC as advisor for its Unit for Relations with Arms Carriers in Geneva, and as Regional Delegate to the Armed Forces of Southern Africa and the Indian Ocean in Pretoria. Prior to joining ICRC, he served as a legal officer in the Canadian Forces Office of the Judge Advocate General, specializing in military prosecutions as well as operational and international law.

Ron Lehman (Director, Center for Global Security Research, Lawrence Livermore Nat'l Lab).

> Dr. Ronald F. Lehman is Director of the Center for Global Security Research at Lawrence Livermore National Laboratory, Chairman of the Governing Board of the International Science and Technology Center, and Vice Chair of the Defense Department's Threat Reduction Advisory Committee. Ron co-chaired the National Academy of Sciences' study on the future of Cooperative Threat Reduction. Ron was Director of the U.S. Arms Control and Disarmament Agency from 1989 to 1993 Previously, Ron served in the Defense Department as Assistant Secretary for International Security Policy, in the State Department as Ambassador and U.S. Chief Negotiator on Strategic Offensive Arms (START I), in the White House as Deputy Assistant to the President for National Security Affairs, on the National Security Council staff, in the Pentagon as Deputy Assistant Secretary, on the Senate Armed Services Committee staff, and in the United States Army. In past years, he served on the Presidential Advisory Board on Proliferation Policy, on the State Department's International Security Advisory Board, and co-

chaired the Policy Advisory Group on nonproliferation for the Senate Foreign Relations Committee.

Herbert Lin (NRC).

Dr. Herbert Lin is chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (Cryptography's Role in Securing the Information Society), a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (Realizing the Potential of C4I: Fundamental Challenges), a 2007 study on cybersecurity research (Toward a Safer and More Secure Cyberspace), a 2009 study on offensive information warfare (Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities), and a 2010 study on cyber deterrence (Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy). Currently, he is study director of a project on the ethics of emerging technologies with military applications. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Patrick Lin (Cal Poly).

Patrick Lin, Ph.D. is the director of the Ethics + Emerging Sciences Group, based at California Polytechnic State University, San Luis Obispo. He has published several books and papers in the field of technology ethics, especially the areas of military technologies, robotics, human enhancement, and nanotechnology, and including a new edited volume *Robot Ethics* (MIT Press, 2012). Currently, he is an associate professor in Cal Poly's philosophy department, an affiliate scholar at Stanford Law School's Center for Internet and Society, and an adjunct senior research fellow at Australia's Centre for Applied Philosophy and Public Ethics (CAPPE). Dr. Lin also serves on the executive board of the Consortium for Emerging Technologies, Military Operations, and National Security (CETMONS). Previously, he was an ethics fellow at the US Naval Academy and a post-doctoral associate at Dartmouth College. His research has been supported by the National Science Foundation, the Office of Naval Research, the Greenwall Foundation, and others.

Rick O'Meara (Brig Gen, JAG, retired).

Dr. Richard M. O'Meara is a retired Brigadier General (USA) and trial attorney who teaches human rights, security issues, and international law in the Division of Global Affairs, Rutgers University. He is a former resident fellow at the Stockdale Center for Ethical Leadership, US Naval Academy and has taught governance and rule of law issues in such diverse locations as Cambodia, Rwanda, Chad, Philippines, Guinea, Sierra Leone, Slovenia, Moldova, Ukraine, Bosnia- Herzegovina, Peru, El Salvador and Iraq.

Paul Robinson (University of Ottawa).

Paul Robinson is currently a professor at the Graduate School of Public and International Affairs at the University of Ottawa. He holds an MA in Russian and Eastern European Studies from the University of Toronto and a D. Phil. in Modern History from the University of Oxford. Prior to his graduate studies, he served as a regular officer in the British Army Intelligence Corps from 1989 to 1994, and as a reserve officer in the Canadian Forces from 1994 to 1996. He also worked as a media research executive in Moscow in 1995. Having published six books, he has also

written widely for the international press on political issues. His research focuses generally on military affairs. In recent years, he has worked on Russian history, military history, defense policy, and military ethics.

Mark Steinbeck (International Committee for the Red Cross).

Dr. Mark Steinbeck is the Medical Advisor and Delegate for the International Committee of the Red Cross (ICRC) at its Regional Delegation for the United States and Canada; he previously held this position between 2006 and 2008. Prior to returning to Washington DC in 2011, Mark was based in Geneva, Switzerland as the Health Advisor on the effects of weapons for the Arms Unit within the Legal Division of the ICRC. Dr. Steinbeck has worked for the ICRC since 1998 in various contexts including Afghanistan, India, Nepal and Bhutan, and in various roles including surgeon, relief / humanitarian assistance coordinator and detention team doctor. He is an Australian citizen with a medical degree and surgical qualification; he also has a law degree. Prior to working in the humanitarian field, he worked as a doctor in Australia and England, and as a commercial lawyer in Australia.

ASU LINCOLN CENTER for APPLIED ETHICS
ARIZONA STATE UNIVERSITY

Appendix C

2012 CHAUTAUQUA COUNCIL: FINAL AGENDA

	Morning session **9 am to 12 pm**	**Afternoon session** **2 pm to 5 pm**
Day 1: Sunday, July 29	Participants arrive	Introduction: Welcome, agenda, and goals: Brad Allenby
Day 2: Monday, July 30	Overview of laws of war: George Lucas Overview of contextual trends: Privatization of war, responsibility to protect, combat versus policing roles, rise of non-state actors and democratization of weapon technologies, etc: Brad Allenby	Introduction to cyber conflict issues: Patrick Lin
Day 3: Tuesday, July 31	Introduction to robotics technologies: Ron Arkin	Introduction to non-lethal military and security technologies and issues: Fritz Allhoff
Day 4: Wednesday, Aug 1	Overview of scenario planning approach	No session. Develop research questions on your own.
Day 5: Thursday, Aug 2	Brainstorming session on questions for future research	Scenario planning for contextual trends; consideration of ethical, legal, and governance implications of scenarios
Day 6: Friday, Aug 3	Future considerations: Emerging technologies and research topics	Reflection on workshop outcomes and suggestions for future meetings
Day 7: Saturday, Aug 4	Panel presentations to Chautauqua audience: feedback and critique from audience	No session. Free time for recreation.
Day 8: Sunday, August 5, 2012	Participants depart	

ASU LINCOLN CENTER for APPLIED ETHICS
ARIZONA STATE UNIVERSITY

Appendix D

QUESTIONS PRESENTED TO CHAUTAUQUA PUBLIC AUDIENCE AUGUST 4, 2012

Ethical Questions from Workshop on Laws of Armed Conflict and Emerging Technologies

1. If we have rules of warfare/conflict, why can't we just make a rule that says, "No war"? Isn't the best law of war simply not to have them?

2. Assuming that war is an inherently human endeavor, do wars need to be "fair"? Isn't "just war" an oxymoron?

3. Does modern technology make the use of force too tempting an option for world leaders?

4. If it is the horror of war that makes us avoid it, why should we attempt to make it less horrible? ("An ethical war is a short one, so use the most violence?")

5. Has increasing reliance on new military technologies helped to insulate the public from the consequences of war?

Appendix E

QUESTIONS POSED BY CHAUTAUQUA PUBLIC AUDIENCE AUGUST 4, 2012

1. What is the meat of the matter? What technologies did you discuss? What were your conclusions?
2. Why don't combatants fire on the government and civilians? Why are laws protecting those people respected and not others?
3. Where is the woman's perspective on the panel and the discussion in a larger context?
4. How are you going to report your conclusions?
5. Have you addressed land mines? What did you decide?
6. Computers and drones can be hacked. How will that affect war and the norms of war in the future?
7. Shouldn't we be thinking about putting the genie back in the bottle rather than continuing the testosterone race (the technological imperative)? This question applies to current/old technology (land mines) as well as emerging tech.
8. Can the panel marshal the laws of war? To minimize the advent of war? Should this be your goal?
9. What is the impact of war on the environment?
10. I'd like to learn more about the laws of war and underlying philosophy. Are there any books I can read?
11. This panel is very timely, but it's about a world that's gone. The nation-state has eroded; engagements are fought by PMCs, etc. It would be easy to set up an island of hackers and direct their efforts at crashing an economy (an undervalued currency is a good way to weaken your enemy).
12. It seems there is a hegemony regarding certain technologies: drones in non-combat zones; nuclear weapons are used by the US but denied to others (asymmetrical ethics).
13. What are the ethics associated with the sale and use of military tech for law enforcement? The inquirer knows of people who have brain damage as a result from being hit by bean bags fired from guns while the military industrial complex profits from sales of weapons to law enforcement.