Michigan Journal of International Law

Volume 35 | Issue 2

2014

The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots

Eric Talbot Jensen
Bringham Young University Law School

ARTICLES

THE FUTURE OF THE LAW OF ARMED CONFLICT: OSTRICHES, BUTTERFLIES, AND NANOBOTS

*Eric Talbot Jensen**

INTRODUCTION

Increasingly, we find ourselves addressing twenty-first century challenges with twentieth-century laws.[1]

As Louise Doswald-Beck correctly stated in her 1998 article, "[a]ny attempt to look into the future is fraught with difficulty and the likelihood

* Associate Professor, Brigham Young University Law School. The author spent twenty years in the U.S. military, including five as a Cavalry officer and the rest as a JAG officer, including deployments to Bosnia, Macedonia, Kosovo, and Iraq. His last job in the U.S. Army was as the Chief of International Law. He would like to thank the faculty of Brigham Young University Law School for their assistance as well as attendees at the Rocky Mountain Junior Scholars Forum. Additionally, Allison Arnold, Matthew Hadfield, Rebecca Hansen, SueAnn Johnson, Rachel LeCheminant, Brigham Udall, and Aaron Worthen provided excellent research and review assistance.

1. Harold Hongju Koh, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1772 (2012); *see also Al-Bihani v. Obama*, 590 F.3d 866, 882 (D.C. Cir. 2010) (Brown, J., concurring) ("War is a challenge to law, and the law must adjust. It must recognize that the old wineskins of international law, domestic criminal procedure, or other prior frameworks are ill-suited to the bitter wine of this new warfare. We can no longer afford diffidence. This war has placed us not just at, but already past the leading edge of a new and frightening paradigm, one that demands new rules be written. Falling back on the comfort of prior practices supplies only illusory comfort.").

that much of it will be wrong."[2] This, in part, accounts for the military axiom that a nation is always preparing to fight the last war. In a study about future war, military historian and theorist Thomas Mackubin writes that research has shown "the United States has suffered a major strategic surprise on the average of once a decade since 1940."[3]

If this inherent lag is true about the tactics and strategy of fighting wars, it is even more true concerning the law governing the fighting of wars. Michael Reisman writes that, "[b]ecause modern specialists in violence constantly seek new and unexpected ways of defeating adversaries, the codified body of the law of armed conflict always lags at least a generation behind."[4] This law lag was recently illustrated by those who have argued for new laws to govern the post–9/11 armed conflict paradigm.[5]

The historical fact that the law of armed conflict (LOAC) has always lagged behind current methods of warfare does not mean that it always must. This Article will argue that the underlying assumption that law must be reactive is not an intrinsic reality inherent in effective armed conflict governance. Rather, just as military practitioners work steadily to predict new threats and defend against them, LOAC practitioners need to focus on the future of armed conflict and attempt to be proactive in evolving the law to meet future needs.

In a recent article in *The Atlantic*, authors Andrew Hessel, Marc Goodman, and Steven Kotler propose a hypothetical in the year 2016 where an anonymous web personality known as Cap'n Capsid posts a competition to deliver a specific virus that, unbeknownst to the competitors, is linked to the DNA of the President of the United States. The virus eventually makes its way to Samantha, a sophomore majoring in govern-

---

2. Louise Doswald-Beck, *Implementation of International Humanitarian Law in Future Wars*, *in* 71 INT'L L. STUD., THE LAW OF ARMED CONFLICT: INTO THE NEXT MILLENNIUM 39, 39 (1998); Stephen Peter Rosen, *The Future of War and the American Military*, HARV. MAG., May-June 2002, at 29, 29 ("The people who run the American military have to be futurists, whether they want to be or not. The process of developing and building new weapons takes decades, as does the process of recruiting and training new military officers. As a result, when taking such steps, leaders are making statements, implicitly or explicitly, about what they think will be useful many years in the future."). Despite the difficulty, it is a vital requirement of militaries and one in which plenty of people are still willing to engage. *See* Frank Jacobs & Parag Khanna, *The New World*, N.Y. TIMES (Sep. 22, 2012), www.nytimes.com/interactive/2012/09/23/opinion/sunday/the-new-world.html.

3. Mackubin Thomas Owens, *Reflections on Future War*, NAVAL WAR C. REV., Summer 2008, at 61, 64.

4. W. Michael Reisman, Rasul v. Bush*: A Failure to Apply International Law*, 2 J. INT'L CRIM. JUST. 973, 973 (2004).

5. *See* NEW WARS, NEW LAWS? APPLYING THE LAWS OF WAR IN 21ST CENTURY CONFLICTS (David Wippman & Matthew Evangelista eds., 2005); Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675 (2004); Geoffrey S. Corn, *Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VAND. J. TRANSNAT'L L. 295 (2007); Roy S. Schondorf, *Extra-State Armed Conflicts: Is There a Need for a New Legal Regime?*, 37 N.Y.U. J. INT'L L. & POL. 1 (2004); Robert D. Sloane, *Prologue to a Voluntarist War Convention*, 106 MICH. L. REV. 443 (2007).

ment at Harvard University, who ingests it and comes down with the flu. Given her symptoms, she quickly spreads billions of virus particles, infecting many of her college friends who also get flu-like symptoms, but nothing very harmful.

> This would change when the virus crossed paths with cells containing a very specific DNA sequence, a sequence that would act as a molecular key to unlock secondary functions that were not so benign. This secondary sequence would trigger a fast-acting neurodestructive disease that produced memory loss and, eventually, death. The only person in the world with this DNA sequence was the president of the United States, who was scheduled to speak at Harvard's Kennedy School of Government later that week. Sure, thousands of people on campus would be sniffling, but the Secret Service probably wouldn't think anything was amiss. It was December, after all—cold-and-flu season.[6]

This scenario may sound more like science fiction than like something you would read in a law review article. However, events like this seem inevitable as the technology of war progresses. Such events raise numerous legal issues both about the law of going to war, or *jus ad bellum*, and the LOAC, or *jus in bello*. Would this be considered a "use of force" in violation of the U.N. Charter?[7] In relation to *jus ad bellum*, would it be considered an "armed attack," giving the United States the right to exercise self-defense?[8] How would these answers be affected if Cap'n Capsid were not a state actor, but a terrorist or an individual acting on his own? With respect to the *jus in bello*, was this an attack, triggering the LOAC? If so, did it violate the principles of distinction or discrimination?[9] Is a genetically coded virus a lawful weapon?

---

6. Andrew Hessel, Marc Goodman & Steven Kotler, *Hacking the President's DNA*, The Atlantic (Oct. 24, 2012, 10:42 AM), http://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/.

7. U.N. Charter art. 2, para. 4. Article 2, paragraph 4 has become the accepted paradigm restricting the use of force among states. Actions that amount to a threat or use of force are considered a violation of international law. However, the international community has very different views on what the language actually means and the Charter contains no definitions.

8. U.N. Charter art. 51. The definition of armed attack is controversial. There is no agreed definition of what equates to an armed attack. Despite this lack of clarity, states seem to agree that not all armed military actions equate to an armed attack. The ICJ confirmed this in the Nicaragua case when it decided that Nicaragua's provision of arms to the opposition in El Salvador was not an armed attack. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 195 (June 27). Additionally, there are unresolved questions about the application of new technologies, such as cyber operations, to armed attack. It is still unclear what level of offensive cyber operations against a state will constitute an armed attack.

9. *See infra*, section II.C.2.b. The principle of distinction requires militaries to distinguish between civilians and combatants in the attack. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

Technological development in each of the areas highlighted in the scenario mentioned above is proceeding quickly, and not just in the United States but also amongst nations throughout the world. While much of the development is currently for peaceful purposes, there is no doubt that many, if not all, of these advances will be weaponized over time. Historically, few technologies throughout history that can be weaponized have not been.[10]

P.W. Singer, known scholar on advancing technologies and the law, has recently written,

> Are we going to let the fact that these [new technologies] look like science fiction, sound like science fiction, feel like science fiction, keep us in denial that these are battlefield reality? Are we going to be like a previous generation that looked at another science fiction-like technology, the atomic bomb? The name "atomic bomb" and the concept come from an H.G. Wells short story. Indeed, the very concept of the nuclear chain reaction also came from that same sci-fi short story. Are we going to be like that past generation that looked at this stuff and said, "We don't have to wrestle with all the moral, social, and ethical issues that come out of it until after Pandora's box is open?"[11]

Pandora's box is opening as new technologies are being developed. They will inevitably shape the future battlefield, affecting where conflicts are fought, by whom they are fought, and the means and methods used to fight.

The premise of this Article is that we are at a point in history where we can see into the future of armed conflict and discern some obvious points where future technologies and developments are going to stress the current LOAC. While the current LOAC will be sufficient to regulate the majority of future conflicts, we must respond to these discernible issues by anticipating how to evolve the LOAC in an effort to bring these future weapons under control of the law, rather than have them used with devastating effect before the lagging law can react.

Part I of this article will argue that the LOAC plays a vital signaling role in warfare that is especially needed at this time of technological innovation. Like these changing technologies, the LOAC must also evolve to face the new challenges of future armed conflict. Part II will project armed conflict into the future in three main categories—places, actors, and means and methods—and analyze how advancing technologies and techniques

---

The principle of discrimination requires each specific attack, including each weapon system, to be able to differentiate in the attack and only attack intended targets. *Id.*, art. 57.

10. John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort*, U.S. DEP'T OF ST. (June 16, 2011), http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/news/newsarticle.aspx?id=64349.

11. P.W. Singer, Ethical Implications of Military Robotics, The 2009 William C. Stutt Ethics Lecture, United States Naval Academy (Mar. 25, 2009), *available at* http://www.au.af.mil/au/awc/awcgate/navy/usna_singer_robot_ethics.pdf.

will call into question the current LOAC's ability to adequately regulate armed conflict. This Part will identify specific principles of the LOAC, the effectiveness of which will wane in the face of state practice, and suggest emerging concepts that will allow the LOAC to evolve and maintain its relevance and virulence in armed conflict. The Article will then conclude.

I. Ostriches or Butterflies

Warfare has always been an evolving concept. Throughout history, it has constantly been shaped and altered by the exigencies of nations and the moral sentiments of the global community. Yet, the paramount force behind this continual military evolution is not economic, social, or moral; rather, the greatest controlling factor has been the ever-changing limitations of wartime technology. . . . For centuries, nations have searched for and sought ways to utilize technological advancements to overcome material deficiencies.[12]

We have all heard or read about how, when faced with danger or adversity, the ostrich buries its head in the sand, hoping the bad thing will pass and leave it unharmed. While this is a myth,[13] it is also a powerful metaphor to describe a possible reaction to a threat. Compare that mythical reaction of the ostrich with the theory of the "coevolutionary arms race"[14] in plants and animals, where a change in the genetic composition of one species is in response to a genetic change in another.[15] For example, over time, the Heliconius butterfly has co-evolved with the passion vine through a series of changes and counter-changes that now link the two inextricably together. As the passion vine developed toxins to protect itself from overfeeding, the Heliconius developed the ability to internalize the toxin and then use it as a defense against its own predators. Similarly, while the Heliconius feeds on the passion vine, it also fertilizes the vine, ensuring the vine's survival.[16]

The natural phenomenon of the co-evolutionary arms race between species is instructive in considering the LOAC and its relationship with

12. Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. Nat'l Ass'n Admin. L. Judiciary 602, 603 (2011).

13. Karl S. Kruszelnicki, *Ostrich Head in Sand*, ABC Science (Nov. 2, 2006), http://www.abc.net.au/science/articles/2006/11/02/1777947.htm.

14. Richard Dawkins & John R. Krebs, *Arms Races Between and Within Species*, 205 Proc. Royal Soc'y London, Series B, Biological Sciences 489 (1979); Interview with Charles Riley Nelson, Professor, Department of Biology, Brigham Young University, in Provo, Utah (Dec. 20, 2012).

15. Paul R. Ehrlich & Peter H. Raven, *Butterflies and Plants: A Study in Coevolution*, 18 Evolution 586 (1964); Daniel H. Janzen, *When is it Coevolution?*, 34 Evolution 611 (1980); John N. Thompson, *Concepts of Coevolution*, 4 Trends Ecology & Evolution 179 (1989).

16. Interview with Charles Riley Nelson, Professor, Department of Biology, Brigham Young University, in Provo, Utah (Dec. 20, 2012) (explaining coevolutionary analysis using the example of the Heliconius and passion vine); *see also* Lawrence E. Gilbert, *The Coevolution of a Butterfly and a Vine*, 247 Sci. Am., Aug. 1982, at 110 (describing how species of Heliconius and passion vine have influenced each other's evolution).

advancing technology. In response to advancing technologies that will undoubtedly affect the conduct of hostilities on the future battlefield, the LOAC can play the role of the ostrich and stick its head in the sand by saying that the current rules are sufficient and all technologies must mold themselves to current rules or not be used. Alternatively, the LOAC can play the role of the butterfly and respond to future developments (or even anticipate them) and adapt or evolve sufficiently to regulate these developments in a meaningful way.

A. *Evolution*

Predicting the future is very difficult,[17] and fraught with the potential for serious error. Hence, the law of armed conflict has been mostly reactive throughout its history. The Fourth Geneva Convention of 1949[18] concerning the protection of civilians during armed conflicts did not come about until after the devastating attacks on civilians that occurred in World War II.[19] Likewise, the Additional Protocols of 1977[20] did not extend protections to victims of non-international armed conflict until decades of lobbying by the International Committee of the Red Cross (ICRC).[21]

The ICRC is engaged in a similar work now. During the recent sixty-year commemoration of the 1949 Geneva Conventions, the ICRC reported on a number of concerns looking at current and future armed conflicts where the law may need to evolve in order to address the needs of victims of armed conflict.[22] Most of these suggestions are based on reactions to current conflicts, but they clearly denote that the international community cannot take the "ostrich's" approach to impending problems. If the law is going to maintain its relevance and ability to adequately regu-

17. Katie Drummond, *Defense Whiz to Pentagon: Your Predictions are Destined to Fail*, WIRED (Oct. 28, 2011, 2:54 PM), http://www.wired.com/dangerroom/2011/10/danzig-military-predictions/ ("The U.S. government has a perfectly awful track record of predicting future events. And there's a good reason why, says the chairman of an influential think tank: it's friggin' impossible.").

18. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention].

19. See *Civilians protected under international humanitarian law*, INT'L COMM. RED CROSS (Oct. 29, 2010), http://www.icrc.org/eng/war-and-law/protected-persons/civilians/overview-civilians-protected.htm.

20. Protocol I, *supra* note 9, art. 43, para. 2; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol II].

21. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 693–94 (2012).

22. Jakob Kellenberger, President, Int'l Comm. Red Cross, Sixty Years of the Geneva Conventions: Learning from the Past to Better Face the Future, Address at Ceremony to celebrate the 60th anniversary of the Geneva Conventions, (Aug. 12, 2009), *available at* http://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-president-120809.htm.

late armed conflict, it must take the "butterfly's" approach and be adaptive and able to evolve in the face of difficulties.[23]

Employing the ostrich's approach and failing to infuse flexibility and adaptability into the LOAC will lead to an increase in the recent phenomenon known as lawfare, or "the use of law as a weapon of war."[24] Recent examples of this phenomenon abound[25] and many LOAC scholars argue that the current LOAC regime in fact encourages non-compliance and incentivizes fighters to use the LOAC as a shield to give them an advantage when fighting LOAC-compliant forces.[26]

---

23. *See* Kenneth Anderson & Matthew Waxman, *Law and Ethics for Robot Soldiers*, POL'Y REV. (Dec. 1, 2012), http://www.hoover.org/publications/policy-review/article/135336 (making a similar argument very effectively with respect to autonomous weapon systems); Louise Arbour, *10 Conflicts to Watch in 2013*, FOREIGN POLICY (Dec. 27, 2012), http://www.foreignpolicy.com/articles/2012/12/27/10_conflicts_to_watch_in_2013 (pointing to the principles of distinction between civilians and combatants and collateral damage from advanced technology as two pressures on the LOAC). *But see* Brad Allenby & Carolyn Mattick, *Why We Need New Rules of War*, SLATE (Nov. 12, 2012), http://www.slate.com/articles/technology/future_tense/2012/11/drones_cyberconflict_and_other_military_technologies_require_we_rewrite.html.

24. *See* Charles J. Dunlap, Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, HARVARD PROGRAM ON NATIONAL SECURITY AND HUMAN RIGHTS, WORKSHOP PAPERS: "HUMANITARIAN CHALLENGES IN MILITARY INTERVENTION" 4, 5 (2001), *available at* http://www.ksg.harvard.edu/cchrp/Web%20Working%20Papers/Use%20of%20Force/Dunlap2001.pdf; MICHAEL N. SCHMITT, THE IMPACT OF HIGH AND LOW-TECH WARFARE ON THE PRINCIPLE OF DISTINCTION, HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, INT'L HUMANITARIAN LAW RESEARCH INITIATIVE BRIEFING PAPER, 1, 7 (November 2003), *reprinted in* INTERNATIONAL HUMANITARIAN LAW AND THE 21ST CENTURY'S CONFLICTS: CHANGES AND CHALLENGES (Roberta Arnold & Pierre-Antoine Hildbrand eds., 2005).

25. The recent war in Iraq illustrates many examples. Tony Perry & Rick Loomis, *Mosque Targeted in Fallouja Fighting*, L.A. TIMES (Apr. 27, 2004), http://articles.latimes.com/print/2004/apr/27/world/fg-fallouja27 (attacking from protected places and using them as weapons storage sites); *Coalition Forces Continue Advance Toward Baghdad*, CNN (Mar. 24, 2003), http://transcripts.cnn.com/TRANSCRIPTS/0303/24/se.17.html (fighting without wearing a proper uniform); *The Rules of War are Foreign to Saddam*, OTTAWA CITIZEN, Mar. 25, 2003, *available at* LEXIS, Nexis Library, CURNWS File (using human shields to protect military targets); David Blair, *Human Shields Disillusioned with Saddam, Leave Iraq after Dubious Postings*, NATIONAL POST (Canada), Mar. 4, 2003, at A1, *available at* LEXIS, Nexis Library, CURNWS File (same); David B. Rivkin, Jr. & Lee A. Casey, *Leashing the Dogs of War*, NAT'L INT. (Sept. 1, 2003), http://nationalinterest.org/article/leashing-the-dogs-of-war-1120) (using protected symbols to gain military advantage); *South Korean Hostage Beheaded in Iraq*, TORONTO STAR, June 23, 2004, *available at* LEXIS, Nexis Library, CURNWS File (murdering prisoners or others who deserve protection); *see also* Michael Sirak, *Legal Armed Conflict*, JANE'S DEF. WKLY, Jan. 14, 2004, at 27 (listing a number of violations of the law of war committed by Iraqi military and paramilitary forces). In each of these cases, an inferior force used the superior force's commitment to adhere to the law of war to their tactical advantage.

26. *See, e.g.*, Dunlap, *supra* note 24, at 6 ("[T]here is disturbing evidence that the rule of law is being hijacked into just another way of fighting (lawfare), to the detriment of humanitarian values as well as the law itself."); Owens, *supra* note 3, at 70 ("Thus these enemies will try to leverage 'lawfare,' the use of the rules of warfare against the United States (while ignoring these rules themselves), by, for example, taking refuge among the civilian population in an attempt to maximize civilian casualties. In turn, adversaries employing complex

Much of the recent lawfare discussion has centered on backward military opponents or non-state actors who need to use lawfare to overcome asymmetric disadvantages.[27] However, a static and inflexible LOAC will incentivize even developed and powerful nations to use the law as a tool, rather than as a regulator. The Chinese already write of "three warfares" including "legal warfare," which is defined as "arguing that one's own side is obeying the law, criticizing the other side for violating the law, and making arguments for one's own side in cases where there are also violations of the law."[28] This Chinese view portrays the law generally "as a means of enforcing societal (and state) control of the population."[29] Presumably, this would apply to both domestic and international law.

China is, of course, not alone in potentially using lawfare to gain an edge through future technologies. The United States has come under heavy criticism recently for its use of drones in fighting transnational terrorism.[30] Though U.S. and Chinese perspectives on the law may be different,[31] the danger of a static and inflexible approach to the LOAC as future technologies emerge is equally applicable to developed and undeveloped,

---

irregular warfare will take advantage of the fact that such casualties are magnified by the proliferation of media assets on the battlefield."); Jason Vest, *Fourth-Generation Warfare*, THE ATLANTIC (Dec. 1, 2001), http://www.theatlantic.com/magazine/archive/2001/12/fourth-generation-warfare/302368/ (discussing Fourth-generation Warfare which includes a recognition of asymmetric operations "in which a vast mismatch exists between the resources and philosophies of the combatants, and in which the emphasis is on bypassing an opposing military force and striking directly at cultural, political, or population targets").

27. The Council on Foreign Relations has defined lawfare as "a strategy of using or misusing law as a substitute for traditional military means to achieve military objectives." *See* Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F.L. REV. 1, 78 (2005); *Lawfare, the Latest in Assymetries*, COUNCIL ON FOREIGN REL. (Mar. 18, 2003), http://www.cfr.org/publication.html?id=5772.

28. Dean Cheng, *Winning Without Fighting: Chinese Legal Warfare*, HERITAGE FOUND. (May 21, 2012) http://www.heritage.org/research/reports/2012/05/winning-without-fighting-chinese-legal-warfare.

29. *Id.* The report also states "[n]o strong tradition that held the law as a means of constraining authority itself ever developed in China." *Id.* at 3.

30. Chris Jenks, *Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict*, 85 N.D. L. REV. 649, 651 (2010); Thomas Michael McDonnell, *Sow What You Reap? Using Predator and Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Islamic Terrorists*, 44 GEO. WASH. INT'L L. REV. 243, 246–47 (2012); Owen Bowcott, *UN to Examine UK and US Drone Strikes*, GUARDIAN (Jan. 23, 2013), http://www.guardian.co.uk/world/2013/jan/24/un-examine-uk-afghanistan-drone-strikes; Owen Bowcott, *UN to Investigate Civilian Deaths from U.S. Drone Strikes*, GUARDIAN (Oct. 25, 2012), http://www.guardian.co.uk/world/2012/oct/25/un-inquiry-us-drone-strikes; *see* Robert P. Barnidge, Jr., *A Qualified Defense of American Drone Attacks in Northwest Pakistan Under International Humanitarian Law*, 30 B.U. INT'L L.J. 409 (2012).

31. *See* Cheng, *supra* note 28, at 6 ("The most important strategic difference between [the United States and China] is that there is little evidence that Chinese analysts and decision-makers see legal warfare as a misuse of the law. Given the much more instrumentalist view of the law in Chinese history, the idea that the law would be employed toward a given end (in support of higher military and national goals) would be consistent with Chinese culture but problematic, if not antithetical, from the Western perspective.").

Western and non-Western nations. The international community needs to take the butterfly's approach and not that of the ostrich. It is only through being proactive and recognizing the pressures that future developments will have on the LOAC (such as where conflicts are fought, by whom they are fought, and the means and methods used to fight) that the LOAC can evolve to avoid increasing lawfare and maintain its role as regulator on the conduct of armed conflict.

B. *Signaling*

The analogy of the ostrich and the butterfly is useful to illustrate the fate of non-evolving principles in the face of a changing technological environment. Indeed, the fate of organisms is often based on their ability to understand environmental signals that are occurring around them. In this way, the analogy would seem to argue that taking a reactive approach to changing circumstances would be sufficient, especially if the reaction comes quickly. In other words, the law need not be proactive, as this Article argues, but can remain reactive, particularly if the international community decreases the reaction time and makes changes quickly in response to technological developments.

This argument might appear to be especially true in the case of international law generally, and the LOAC specifically, since they are so heavily dependent on state practice and preferences. These areas of the law develop based mainly on consensual agreements between states and also on the activities of states, particularly when done through a sense of legal obligation. These twin sources of international law are complemented by other general principles of law recognized by civilized nations such as equity, judicial decisions, and the teachings of the most highly qualified publicists.[32] As technologies develop, states will have time to consider their potential application to armed conflict and then deliberate on the best way to apply the law to changing circumstances. If nothing else, this approach will certainly maintain the maximum freedom to maneuver for states that are developing new technologies.

This approach would continue millennia of LOAC formulation where custom ripened over time. Increasing the speed with which actions ripen

---

32. See Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993 [hereinafter ICJ Statute], which states:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

into customary international law would also be beneficial. However, relying solely on quick reaction to technological developments ignores the vital signaling role that the LOAC plays in the development of state practice.

The signaling value of the LOAC is clear from the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (GPI). Article 36 of GPI, titled "New weapons," states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[33]

This article requires every state that is contemplating developing a new technology or weaponizing an existing technology to ensure that such development complies with the LOAC. In other words, the LOAC signals to states what is permissible and what is not even at the stage of study and development of new weapons.[34]

U.S. practice in this area is very clear. Even prior to GPI coming into effect, the United States required such a review,[35] and it is now codified in Department of Defense Directive 5000.01, which states:

> The acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements (for arms control agreements, see DoD Directive 2060.1 (Reference (lm), customary international law, and the law of armed conflict (also known as the laws and customs of war). An attorney authorized to conduct such legal reviews in the Department shall conduct the legal review of the intended acquisition of weapons or weapons systems.[36]

Each military service has an attorney designated to do such reviews.[37]

---

33. Protocol I, *supra* note 9, art. 36; *cf.* Duncan Blake & Joseph S. Imburgia, "*Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons"*, 66 A.F. L. Rev. 157, 159, 161 (2010) (discussing the application of legal reviews to certain future and developing weapons).

34. Neil Davison, *How International Law Adapts to New Weapons and Technologies of Warfare*, Intercross Blog (Dec. 4, 2012), http://intercrossblog.icrc.org/blog/how-international-law-adapts-new-weapons-and-technologies-warfare.

35. Geoffrey S. Corn, et al., The Law of Armed Conflict: An Operational Approach 203 (2012).

36. Dept. of Def. Directive 5000.01, The Defense Acquisition System ¶ E1.1.15 (D.O.D. 2003) (Certified Current as of Nov. 20, 2007), *available at* http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

37. For an example of a weapon review, see Corn, et al., *supra* note 35, at 228–31 (2012).

This requirement would clearly apply to all new and developing technologies that states may be considering. In such cases, the proposed weapon or means or method of warfare would be reviewed by a legal adviser who would determine its legality under the current law. In many cases, this review might be quite easy. However, it is here that Harold Koh's quote from the beginning of this Article[38] is most relevant. The legal adviser performing the review will look to the current LOAC for signals as to the legality of a proposed weapon, but that may prove difficult if the existing law does not adequately apply to the future weapon. In the absence of apparently applicable law, each legal adviser or nation is left to a discretionary decision that may lead to uneven application of LOAC constraints.

In addition to the legal review at the research and development stage, the law also requires a legal review at the point the weapon is employed. Article 82 of the same Protocol, titled "Legal Advisers in Armed Forces," states:

> The High Contracting Parties at all times, and the Parties to the conflict in time of armed conflict, shall ensure that legal advisers are available, when necessary, to advise military commanders at the appropriate level on the application of the Conventions and this Protocol and on the *appropriate* instruction to be given to the armed forces on this subject.[39]

It is clear from this provision that an otherwise lawful weapon can be employed in an unlawful way. Additionally, advanced technologies might provide tactical options that otherwise do not exist. In each case, the legal adviser must be available to the commander to provide legal advice, but the legal adviser will be looking to the LOAC for signals as to how to apply the LOAC in that specific situation. If the law is not specific to that potential employment or tactic, the legal adviser must be able to extrapolate existing rules to new technologies.

The recent development and deployment of cyber weapons demonstrates that applying existing rules to new technologies will present difficulties. Over the past decade, numerous statements and articles have been written on the application of the law to cyber operations, often coming out with different conclusions. Some have argued that existing law is sufficiently flexible to respond to new technologies such as cyber capabilities,[40]

38. Koh, *supra* note 1 ("Increasingly, we find ourselves addressing twenty-first century challenges with twentieth-century laws.").

39. Protocol I, *supra* note 9, art. 86 (emphasis added).

40. Michael N. Schmitt, *IHL Challenges Series—Part III on New Technologies*, Intercross (June 17, 2013), http://intercrossblog.icrc.org/blog/ihl-challenges-series-part-iii-new-technologies; *cf.* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 Int'l Rev. Red Cross 533 (2012).

while others argue that a whole new set of rules should be written to provide proper guidance.[41]

In response to this ongoing debate, a group of international LOAC experts embarked on a three-year process to determine how the LOAC applied to cyber operations.[42] Headed by Michael N. Schmitt, a renowned cyber scholar,[43] the experts found that they had to interpret or evolve the law in certain areas for it to sufficiently provide guidance to cyber operators. For example, most of the experts determined that the traditional definition of "attack" was insufficient to determine when the LOAC applied to cyber activities. Instead, a cyber action that affected the functionality of a cyber system might also be considered an attack.[44]

This example is representative of similar difficulties that will occur as new technologies are developed and used. For example, in the scenario quoted from *The Atlantic* at the beginning of this article, would the employing of the virus in the proposed way violate the principle of distinction, even though it was absolutely discriminating in the attack? Similar issues will be raised below.

There is no doubt that legal advisers have been extrapolating rules to new technologies throughout history. But as will be shown below, the kinds of technological advances in weapons and tactics will be unprecedented over the next few decades, applying tremendous stresses on the LOAC. Because of the important signaling role the LOAC plays in providing guidance to states and their legal advisers, particularly during research and development, the international community needs to begin now to analyze these future weapons and tactics and proactively provide guidance on the application of the LOAC to future armed conflict.

II. The Future of the Law Of Armed Conflict

The nature of armed conflict, and of the causes and consequences of such conflict, is continuing to evolve. IHL must evolve too.[45]

Jakob Kellenberger's statement above, as the president of the ICRC, reflects the fundamental need to evolve IHL to the changing nature of armed conflict. The ICRC's approach is not in disagreement with that of

41. Alireza Miryousefi & Hossein Gharibi, *View from Iran: World Needs Rules on Cyberattacks*, Christian Science Monitor (Feb. 14, 2013), http://www.csmonitor.com/Commentary/Opinion/2013/0214/View-from-Iran-World-needs-rules-on-cyberattacks-video; Jody R. Westby, *We Need New Rules for Cyber Warfare*, N.Y. Times (Mar. 1, 2013), http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagment-for-cyberwar.

42. The Tallinn Manual on the International Law Applicable to Cyber Warfare 1 (Michael N. Schmitt ed., 2013) [hereinafter Tallinn Manual]. Note that the author was one of the participants in the formulation of the Manual.

43. *Michael N. Schmitt: Faculty Profile*, U.S. Naval War C., https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx (last visited Mar. 9, 2014).

44. Tallinn Manual, *supra* note 42, at 156–159.

45. Kellenberger, *supra* note 22.

the International Court of Justice (ICJ), as stated in the 1996 Nuclear Weapons Advisory Opinion:

> However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present, and those of the future.[46]

The assumption that the "intrinsically humanitarian character of the legal principles" of the LOAC applies to future forms of warfare does not mean that the principles cannot evolve. Rather, the decision by the ICJ that the new technology of nuclear weapons continued to be regulated by the LOAC demonstrates that the ICJ views the law as adaptive to new weapon systems even on LOAC's core fundamental principles.

Many commentators have discussed the need for change in various aspects of the laws applicable to the initiation and continuation of armed conflict,[47] including the division of international law into *jus ad bellum* and

---

46. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 259, ¶ 86 (July 8).

47. *See* Brooks, *supra* note 5, at 684 ("In the long run, the old categories and rules need to be replaced by a radically different system that better reflects the changed nature of twenty-first century conflict and threat."); Interview with Peter W. Singer, Senior Fellow, the Brookings Institute, *available at* http://www.abc.net.au/lateline/content/2012/s3442876.htm ("I think the way to think about this is that when we look at the laws of war that are set for—that are supposed to guide us today, they date from a year when the most important invention was the 45 RPM vinyl record player. We don't listen to music on vinyl record players anymore. I'm guessing a lot of the audience might never have listened to music on a vinyl record player anymore. And yet, the laws of war from that year, we still try and apply today. And so it doesn't mean that the laws of war, you know, you need to throw them out, but it does mean that they're having a real hard time."); *see also* Sylvain Charat, *Three Weapons to Fight Terror*, WASH. TIMES (Sept. 9, 2004), http://www.washingtontimes.com/news/2004/sep/8/20040908-085545-9034r/. Judge George H. Aldrich identified "those aspects of the law that are most in need of further development in the early years of the next century" for international armed conflicts as:

> (1) entitlement of those who take up arms to combatant and prisoner-of-war status;
>
> (2) protection of noncombatants from the effects of hostilities; and
>
> (3) compliance mechanisms, including external scrutiny, repression and punishment of offenses, and the right of reprisal; and
>
> in other armed conflicts—
>
> (1) the extent of regulation by international law when those conflicts are noninternational; and
>
> (2) the applicability of international law when those conflicts are partly international and partly noninternational.

jus in bello,[48] evolution of law to accommodate potential need for preemptive self-defense,[49] the bifurcation of the LOAC between international armed conflicts and non-international armed conflicts,[50] the application of the law to state and non-state actors,[51] and the geographic applicability and limitations of the LOAC to the "active conflict zone,"[52] to name just a few. P.W. Singer framed the question nicely when he asked, "[h]ow do we catch up our twentieth century laws of war that are so old right now they qualify for Medicare to these twenty-first century technologies?"[53]

The prescriptions for solving the current problem include calls for specific adjustments to discrete areas of the current LOAC, but Rosa Brooks has argued for "a radical reconceptualization of national security law and the international law of armed conflict."[54] If catching the law up to current technologies, strategies, and tactics requires a "radical reconceptualization" of the LOAC, it certainly behooves the international community to be proactive in anticipating the future evolution of the LOAC to accommodate changes in future armed conflict.

The next Part of this article will briefly analyze elements of the future battlefield, focusing on "places," or where conflicts are fought; "actors," or by whom they are fought; and "means and methods," or how they are fought. The purpose of the analysis is to highlight areas of the LOAC that will struggle to deal with the future changes that are likely to occur, and to

---

George H. Aldrich, *The Hague Peace Conferences: The Laws of War on Land*, 94 AM. J. INT'L L. 42, 42 (2000).

48. Nathaniel Berman, *Privileging Combat? Contemporary Conflict and the Legal Construction of War*, 43 COLUM. J. TRANSNAT'L L. 1 (2004); Sean D. Murphy, *Protean Jus ad Bellum*, 27 BERKELEY J. INT'L L. 22 (2009); Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE J. INT'L L. 47 (2009).

49. W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AM. J. INT'L L. 82 (2003).

50. Brooks, *supra* note 5, at 711–14; Jensen, *supra* note 21; Francisco Forrest Martin, *Using International Human Rights Law for Establishing a Unified Use of Force Rule in the Law of Armed Conflict*, 64 SASK. L. REV. 347 (2001); Gabor Rona, *Legal Frameworks to Combat Terrorism: An Abundant Inventory of Existing Tools*, 5 CHI. J. INT'L L. 499 (2005).

51. Kenneth Watkin, *Canada/United States Military Interoperability and Humanitarian Law Issues: Land Mines, Terrorism, Military Objectives, and Targeted Killing*, 15 DUKE J. COMP. & -INT'L L. 281, 281 (2005) ("The conduct of military operations at the commencement of the 21st century has also shone a bright spotlight on traditional tensions in humanitarian law, such as the application of that law to conflicts between state and non-state actors.").

52. Jennifer C. Daskal, *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone*, 161 U. PA. L. REV. 1165, 1212; Frédéric Mégret, *War and the Vanishing Battlefield*, 9 LOY. U. CHI. INT'L L. REV. 131 (2011).

53. Singer, *supra* note 11.

54. Brooks, *supra* note 5, at 747. The author further states that "it is becoming more and more difficult to know how to characterize, as a matter of law, the kinds of threats that increasingly face the U.S. and other nations, and it is therefore becoming harder and harder to determine the appropriate legal responses to these threats. The old categories have lost their analytical and moral underpinnings, but we have not yet found alternative paradigms to replace them." *Id.* at 744.

begin a discussion on how the LOAC needs to evolve to maintain its ability to regulate armed conflict in the future.

A. *Places*

The traditional paradigm of armed conflict assumes that at any given time, it will be readily apparent where the armed conflict is taking place, and where it is not. To put it another way, the traditional paradigm assumes clear spatial boundaries between zones of war and zones of peace.[55]

For the entire history of mankind, armed conflict has been confined to breathable air zones—the land, the surface of the ocean, and recently the air above the land in which land-based aircraft can fly. Additionally, the post-Westphalian system was built on the foundation of state sovereignty and the clear demarcation and control of borders.[56] Armed conflicts occurred within specific spatial and temporal limits. As a result, the laws governing armed conflict have been built around certain presumptions about where armed conflict will occur. In the future, these presumptions will no longer be true. The LOAC will have to adjust to account for the emerging factors affecting where armed conflicts take place.

1. Emerging Factors

As technology advances, armed conflict will no longer be restricted to breathable air zones. Instead, it will occur without respect to national borders, underground, on the seabed, in space and on celestial bodies such as the moon, and across the newly recognized domain of cyberspace.[57]

a. Global Conflict

The phenomena of global conflict has already begun to stress the LOAC[58] as the United States has struggled to confront a transnational non-state terrorist actor that does not associate itself with geographic boundaries. As will be discussed in Subsection B, the ability to communicate globally through social media will likely produce organized (armed) groups that will not be bound by geographic boundaries and as such will not see themselves as representing a specific geographic collective. Rather, the boundaries will revolve around affiliations, interests, and ideologies. As Mack Owens has written:

> Thus multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields; unavoidable urban battles and unavoidable collateral damage exploited by the

55. *Id.* at 720.

56. Jensen, *supra* note 21, at 707–09.

57. *See* David Alexander, *Pentagon to Treat Cyberspace as "Operational Domain"*, REUTERS (Jul. 14, 2011), http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

58. Mégret, *supra* note 52, at 132 (arguing that the "death of the battlefield significantly complicates the waging of war and may well herald the end of the laws of war as a way to regulate violence").

> adversary's strategic communication; and highly vulnerable rear areas. On such battlefields, friends and enemies are commingled, and there is a constant battle for the loyalty of the population.[59]

This issue is amply illustrated through the U.S. practice of drone strikes on terrorists associated with al-Qaeda but not located in Afghanistan.[60] The focused outcry about U.S. reliance on authorities granted by the law of armed conflict even though outside the geographic confines of the recognized battlefield[61] highlights the current paradigm's assumptions about the LOAC's applications to territory. As global communications allow participants in armed conflict to be more widely dispersed across the world, it is unlikely that states will allow themselves to be attacked by transnational actors because they are not located within a specific geographic region that has been designated as the "battlefield."

b. Seabed

Currently the seabed and even non-surface waters have seen very little armed conflict.[62] Submarine vessels have engaged surface vessels but there has been almost no conflict between submarines and none from the seabed. This is likely to change dramatically with technological improvements. For example, China has developed submersibles that can reach 99.8 percent of world's seabed.[63] As more and more underwater vehicles become unmanned, the need for breathable air dissipates. Underwater drones will almost certainly become armed and underwater engagements will quickly follow.

Similarly, the seabed will likely become militarized, once the need for air is erased. Not only could sensors be used to track surface and subsurface traffic, but also armaments will likely soon follow and the seabed will become another area where states will employ weapons systems.

---

59. Owens, *supra* note 3, at 71.

60. Cora Currier, *Everything We Know So Far About Drone Strikes*, ProPublica (Jan. 22, 2013), http://www.propublica.org/article/everything-we-know-so-far-about-drone-strikes.

61. Daskal, *supra* note 52.

62. Two treaties provide limitations on certain military activities on the sea bed. *See* Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space, and Under Water, Aug. 5, 1963, T.I.A.S. No. 5433, 480 U.N.T.S. 43; Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof, Feb. 11, 1971, 23 U.S.T. 701, 955 U.N.T.S. 115 [hereinafter Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed]. These agreements, however, only apply to nuclear weapons and do not limit the transport or use of nuclear weapons in the waters above the seabed.

63. Gordon G. Chang, *China Explores the Seabed Near America*, World Aff. (July 25, 2011), http://www.worldaffairsjournal.org/blog/gordon-g-chang/china-explores-seabed-near-america.

c. Subterranean

Similar to the seabed, the ability to place weapons systems underground and employ them effectively against an enemy is beginning to develop.[64] Not only is it almost certain that underground weapons will attack surface targets, but it is also clear that they could be used to create surface effects through underground explosions and other means of manipulation. This will probably include the creation of earthquakes, tsunamis, and other surface effects that will severely affect an enemy. This portion of the earth is currently not weaponized,[65] but it will be in the future.

d. Space and Celestial Bodies

Space and the free use of space have become vital to the functioning of the modern military. In fact, "[a] Government Accountability Office report . . . showed major Defense space acquisition programs 'have increased by about $11.6 billion'—321 percent—from initial estimates for fiscal years 2011 through 2016."[66]

U.S. Air Force Gen. William Shelton, who is the head of Space Command, recently stated that "[o]ur assured access to space and cyberspace is foundational to today's military operations and to our ability to project power whenever and wherever needed across the planet."[67] Similarly, Army Lt. Gen. Richard Formica stated, "If the Army wants to shoot, move or communicate, it needs space."[68] Formica added that because of the Army's dependency on these systems, they "have to be defended."[69]

These quotes refer mostly to the use of satellites, but despite current legal restrictions, it is very likely that the use of the moon and potentially other celestial bodies will soon follow.[70] Space systems such as satellites

---

64. *See* Geoff Manaugh, *Drone Landscapes, Intelligent Geotextiles, Geographic Countermeasures*, BLDG BLOG (Jan. 11, 2012), http://bldgblog.blogspot.com/2012/01/drone-landscapes-intelligent.html.

65. *See* Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed, *supra* note 62.

66. Walter Pincus, *Hearings Show Our Dependence on Military Space Technology*, WASH. POST (Mar. 26, 2012), http://articles.washingtonpost.com/2012-03-26/world/35448260_1_military-space-space-command-aehf.

67. *Id.*

68. *Id.*

69. *Id.*

70. The 1967 Outer Space Treaty limits military activities in outer space. Article IV states:

> States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military per-

can be defended and attacked both from space and from the ground. Both China and the United States have conducted recent anti-satellite operations and established that both have that capability.[71] Space has already begun to be weaponized[72] and that trend will continue and increase in speed and lethality.

e. Cyberspace

Much has already been written about cyberspace. The Chinese have created a separate department of their military to handle the military aspects of cyberspace.[73] The United States recently created Cyber Command to specifically plan and control U.S. military cyber operations.[74] Army General Keith Alexander not only commands Cyber Command but also heads the National Security Agency.[75] Currently, 140 nations either already have or are actively building cyber capabilities within their military,[76] with Brazil being one of the most recent to make that decision.[77]

> sonnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

71. Amy Chang, *Indigenous Weapons Development in China's Military Modernization*, U.S.-China Econ. & Sec. Rev. Commission (Apr. 5, 2012), http://www.uscc.gov/researchpapers/2012/China-Indigenous-Military-Developments-Final-Draft-03-April2012.pdf; Angela Webb, *Joint Effort Made Satellite Success Possible*, Free Republic (Feb. 26, 2008), http://www.freerepublic.com/focus/f-news/1976747/posts; *Concern Over China's Missile Test*, BBC News (Jan. 19, 2007), http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm.

72. Blake & Imburgia, *supra* note 33, 173–76; Jameson W. Crockett, *Space Warfare in the Here and Now: The Rules of Engagement for U.S. Weaponized Satellites in the Current Legal Space Regime*, 77 J. Air L. & Com. 671 (2012).

73. Tania Branigan, *Chinese Army to Target Cyber War Threat*, The Guardian (July 22, 2010), http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department.

74. Andrew Gray, *Pentagon Approves Creation of Cyber Command*, Reuters (June 23, 2009), http://www.reuters.com/article/2009/06/24/us-usa-pentagon-cyber-idUSTRE55M78920090624.

75. *Biography: Director of the NSA/CSS*, Nat'l Sec. Agency, http://www.nsa.gov/about/leadership/bio_alexander.shtml (last visited Mar. 9, 2014).

76. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU Sci. & Tech. L. Rev. 249, 249 (2010); Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. Rev. 65, 96 (2009).

77. Pedro Ozores, *Eyeing Major Events, Brazil to Form Body to Fight Cyber Attacks*, BNAmericas (Dec. 28, 2012), http://www.bnamericas.com/news/technology/eyeing-major-events-brazil-to-form-body-to-fight-cyber-attacks.

Recent revelations concerning Stuxnet[78] and Flame[79] make it clear that nations are already using cyberspace to conduct military activities that cause harm similar to kinetic operations. Nations are also stealing technologies and trade secrets through cyber operations.[80] These cyber thefts have not yet been equated with an attack but may be so treated in the future as the seriousness of the thefts continues and increases. Cyberspace has certainly been militarized by states and will continue to be so, and on an increasing basis.[81]

One of the most important aspects of cyberspace is that, unlike the weaponization of space or the seabed, it does not require a nation to conduct "military" activities in cyberspace. There are numerous examples of private hackers, organized groups, and business organizations using the Internet to do great harm to both private and public entities.[82] The accessibility of the militarization of cyberspace makes it somewhat unique in the future of armed conflict, which will be discussed below.

Most important for this discussion is the lack of boundaries in cyberspace. While the computer used to conduct the "attack" must be in one geographic location and work through a server in a specific geographic location, the lethal electrons will traverse many nations in their path to the requested destination. Further, to this point, states have been unwilling to take responsibility for cyber "attacks" that emanate from within their geographic boundaries,[83] leaving only criminal process as the means of seeking redress for non-state-actor-sponsored attacks, a process that has seldom proven successful.[84]

2. Emerging Law

The emerging factors discussed above will create stress on the current underpinnings and general principles of the LOAC. Fundamental ideas, such as territorial sovereignty, upon which the state-centric LOAC is based, will diminish in importance. The current doctrine of neutrality will

78. Amr Thabet, *Stuxnet Malware Analysis Paper,* CODEPROJECT (Sept. 9, 2011), http://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper.

79. *Full Analysis of Flame's Command and Control Servers*, SECURELIST (Sept. 17, 2012, 1:00 PM), http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers.

80. *See, e.g.*, Peter Foster, *China Chief Suspect in Major Cyber Attack*, DAILY TELEGRAPH (Aug. 3, 2011), http://www.telegraph.co.uk/technology/news/8679658/China-chief-suspect-in-major-cyber-attack.html.

81. Noah Shachtman, *DARPA Looks to Make Cyberwar Routine with Secret "Plan X"*, WIRED, (Aug. 21, 2012), http://www.wired.com/dangerroom/2012/08/plan-x/.

82. Mathew J. Schwartz, *Anonymous Attacks North Korea, Denies Targeting South*, INFO. WEEK (June 25, 2013), http://www.informationweek.com/security/attacks/anonymous-attacks-north-korea-denies-tar/240157253; *Global Network of Hackers Steal $45 Million from ATMs*, CNBC (May 10, 2013), http://www.cnbc.com/id/100726799.

83. *See, e.g.*, *The Cyber Raiders Hitting Estonia*, BBC NEWS, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665195.stm.

84. *See, e.g.*, Clifford J. Levy, *What's Russian for 'Hacker'?*, N.Y. TIMES (Oct. 21, 2007), http://www.nytimes.com/2007/10/21/weekinreview/21levy.html?pagewanted=all&_r=0.

be impossible to apply. Certain specific international agreements that impact the LOAC will likely be ignored or abrogated as technological capabilities increase. As these stresses develop, the LOAC will need to adjust to maintain its relevance to future armed conflicts.

a. Territorial Sovereignty

Since the inauguration of the Westphalian system, one of the indicia of statehood is a designated territory. This was memorialized in the Montevideo Convention[85] and has been part of recent discussions on statehood in both Kosovo[86] and Palestine.[87] Assumed in this attachment of territory to statehood is the authority and obligation to control that territory, including the use of force within designated borders and the use of force from within designated borders that will have effects outside the territory.[88]

It is this assumption that led to the bifurcation of the LOAC into rules governing international armed conflicts (IACs) and separate rules governing non-international armed conflicts (NIACs).[89] When the United States was faced with conducting an armed conflict with a transnational actor after the terrorist attacks of 9/11, it struggled to apply the appropriate rules.[90] It seems clear that applying the NIAC rules to a transnational armed conflict was clearly outside the meaning of the Geneva Conventions as originally signed.[91] Despite this, the U.S. Supreme Court eventually determined that certain LOAC provisions formed a minimum set of rights that applied to all armed conflicts, regardless of unbounded geography.[92]

It is almost certain that armed conflicts in the future will continue to be carried out by organized groups who will be found outside a limited geographic scope. To the extent that the LOAC would prevent the applica-

85. Montevideo Convention on the Rights and Duties of States, Dec. 26, 1933, 49 Stat. 3097, 165 LNTS 19.

86. William Thomas Worster, *Law, Politics, and the Conception of the State in State Recognition Theory*, 27 B.U. Int'l L.J. 115 (2009).

87. John Quigley, The Statehood of Palestine: International Law in the Middle East Conflict 209–11 (2010).

88. *See* Philip Bobbitt, The Shield of Achilles: War, Peace, and the Course of History 81–90, 96–118 (2002); Frederic Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 Penn. St. Int'l L. Rev. 433, 443 (2006) (citing sixteenth-century writer Bodin as defining sovereignty as "the absolute and perpetual power of the commonwealth resting in the hands of the state").

89. *See generally* Jensen, *supra* note 21; James G. Stewart, *Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict*, 85 Int'l Rev. Red Cross 313 (2003), *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/5PYAXX/$File/irrc_850_Stewart.pdf (describing the history of the development of the Geneva Conventions).

90. Jensen, *supra* note 21, at 685–88.

91. Anthony Cullen, The Concept of Non-International Armed Conflict in International Humanitarian Law 36–39 (2010).

92. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 628–32 (2006).

tion of force in accordance with current U.S. practice, a reinterpretation of the LOAC will be necessary. Additionally, the specific application of LOAC provisions, such as non-movement of security detainees,[93] would need to be reinterpreted in light of transnational groups during armed conflict.

Future conflicts will also raise questions about the ability of states to control the use of force from within their territory during armed conflicts in the same way as they currently do. For example, even now, during peacetime, nations have claimed that they cannot be responsible for cyber activities that emanate from within their borders.[94] The obligation to prevent transboundary harm that was clearly articulated in the Trail Smelter Arbitration,[95] and made applicable to situations of armed conflict in the Corfu Channel case,[96] has not prevented states from disclaiming responsibility for cyber actions from within their borders during armed conflict.[97]

As will be discussed below, the globalization of social networking will allow linkages between people of many different nationalities who might take forceful actions during armed conflict. These individuals will be acting not as citizens of any particular country but as members of transnational ideological groupings, and nations will find these individuals difficult to control. While the inability of a state to control all the actions of its individual residents is not new, the capability for those residents to readily harness state-level violence, such as cyber tools, and then direct that state-level violence across boundaries is relatively new and will only become more possible with technological advances.

The transnational nature of fighters and the decreasing ability of states to control the emanation of state-level violence from within their sovereign territory will likely frustrate the current understanding of the application of the LOAC. The idea of a geographically limited conflict is difficult to maintain when organized (social networking) groups are using state-level violence from multiple (neutral) states across the world.[98]

---

93. Geneva Convention, *supra* note 18, art. 49.

94. Shashank Bengali, Ken Dilanian & Alexandra Zavis, *Chinese Cyber Attack Disclosures*, L.A. Times (June 5, 2013),http://timelines.latimes.com/la-fg-china-cyber-disclosures-timeline/; *see also*, *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, Intelligence & Nat'l Sec. Alliance 8 (Sept. 2011), https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf.

95. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1965–66 (1941).

96. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

97. *See* John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. Times (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

98. *See* Mathew J. Schwartz, *Anonymous Takes Down North Korean Websites*, InformationWeek (Apr. 16, 2013), http://www.informationweek.com/security/attacks/anonymous-takes-down-north-korean-websit/240152985 (describing the hacktivist group Anonymous's disruption of North Korean websites).

b. Neutrality

As implied above, the doctrine of neutrality will also come under pressure in future conflicts where the geography of the battlefield is less confined. States that are not participants in armed conflict and that wish to maintain their neutrality will find it difficult to effectively do so when individuals' actions from within their geographic borders will involve state-level violence. For example, assume a citizen of a neutral country decides to conduct a cyber attack against one of the belligerent countries. To maintain its neutrality, the neutral country must prevent such attacks.[99] Alternatively, the attacked country may use self-help to stop the attacks. This is not new.[100] However, what is new is the level of violence that individuals can readily muster and the global scale of organization and reach of these individual participants.

When individuals from eighty neutral countries can organize themselves to attack simultaneously and instantaneously with state-level violence at different targets in the belligerent state, the doctrine of neutrality and a belligerent's ability to respond become almost meaningless. The belligerent state may not have time to determine the neutral state's willingness or ability to intervene or stop the attack. Under the current LOAC doctrine of neutrality, such activities would likely lead to the belligerent declaring the neutral as a hostile party to the conflict.[101]

Additionally, when an individual launches a cyber attack, the malware will inevitably flow through the infrastructure of neutral states. Under Article 8 of Hague V, "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[102] This provision is one of the very few codified provisions in the LOAC that refer to neutrality and electronic communications. Yet, when considering Article 8 specifically, the group of experts who wrote the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) could not agree on its specific applicability to cyber operations.[103] The experts did agree that the provisions of the LOAC applicable to neutrality were difficult to apply in the context of cyber war and "need to be interpreted."[104] This approach by the Tallinn

99. Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 5, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention (V)].

100. *See* U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, ch. 7.3 (2007) [hereinafter COMMANDER'S HANDBOOK]; R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT'L L. 82, 89 (1938); Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825 (2012).

101. *See* COMMANDER'S HANDBOOK, *supra* note 100, at ch. 7.2.

102. Hague Convention (V), *supra* note 99, art. 8.

103. TALLINN MANUAL, *supra* note 42.

104. *Id.*; *see generally* Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L. J. 815 (2012).

Manual should signal to the international community the need to look more closely at the LOAC, at least within the context of cyberspace, and acknowledge that review and revision is necessary.

c. International Agreements

Finally, though not strictly a matter of the LOAC, there are numerous international agreements that affect the militarization of specific areas and the application of the LOAC to activities in these areas. For example, the Outer Space Treaty limits some military activities in space but has no specific provision prohibiting the use of conventional weapons (or for example, lasers) in outer space that may be used against targets in orbit, on celestial bodies, or on the Earth.[105]

Other treaties[106] also limit or affect the use of Earth's "places" for military purposes. However, these agreements, to the extent that states will continue to follow them in the future, serve only to limit states. As will be discussed below, the actors of armed conflict are going to dramatically change and increase, including a significant variety of non-state entities that will have no legal obligations under these international agreements and may or may not be effectively constrained by states. As emphasized below, the LOAC will have to reach out to these other actors to regulate Earth's "places" during future armed conflict.

B. *Actors*

The potential range of 'new actors' whose actions have repercussions at the international level is of course vast. While many of these 'new actors' have in fact been around for some time, they have called into question—and will continue to call into question—some of the more traditional assumptions on which the international legal system is based.[107]

From the very beginnings of human conflict, fighters have created rules to govern their war-like conduct.[108] As argued by Krauss and Lacey,

105. *See* Ricky J. Lee, *The Jus Ad Bellum In Spatialis: The Exact Content and Practical Implications of the Law on the Use of Force in Outer Space*, 29 J. SPACE L. 93, 95–98 (2003); *see also* P.J. Blount, *Limits on Space Weapons: Incorporating the Law of War into the Corpus Juris Spatialis*, Int'l Austronautical Fed'n, IAC-08.E8.3.5 (2008); Deborah Housen-Couriel, *Disruption of Satellites ad Bellum and in Bello: Launching a New Paradigm of Convergence*, 45 ISR. L. REV. 431 (2012).

106. *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3; Treaty on the Prohibition of the Emplacement of Nuclear Weapons on the Sea-Bed, *supra* note 62.

107. Kellenberger, *supra* note 22.

108. *See* William C. Bradford, *Barbarians at the Gates: A Post-September 11th Proposal to Rationalize the Laws of War*, 73 MISS. L.J. 639, 641 n.12, 697–710 (2004); Gregory P. Noone, *The History and Evolution of the Law of War Prior to World War II*, 47 NAVAL L. REV. 176, 182–85 (2000); Thomas C. Wingfield, *Chivalry in the Use of Force*, 32 U. TOL. L. REV. 111, 114 (2001).

these were rules "written by the utilitarians for the warriors."[109] While the quality and content of these rules ebbed and flowed over time, this progression resulted in a definition of a combatant as an agent for a state that provided authorities for individuals to take part in otherwise illegal conduct (such as killing others) so long as that conduct was in compliance with rules established by the state.[110] Because these rules were initially based on reciprocal application, they established strict qualifications for who could act with this impunity—rules that were codified in the 1899/1907 Hague Convention[111] and in greater detail in the 1949 Geneva Convention for the Protection of Prisoners of War.[112]

Concurrently, the LOAC has developed rules for the treatment of those not acting as fighters but as the victims of armed conflict. The treatment has moved from a point where non-fighters were treated as the spoils of war,[113] to a time when non-fighters were considered part of the targetable enemy,[114] to the current paradigm where militaries are strictly prohibited from targeting civilians,[115] so long as they do not "take a direct part in hostilities."[116]

As a result of these provisions, actors on the battlefield are divided into either combatants or civilians and, in fact, are defined in relation to each other. As Article 50 of GPI states, "A civilian is any person who does not belong to one of the categories of persons referred to in Article 4A(1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol."[117] This clean division between two types of battlefield actors is among the current LOAC principles that will be stressed in future armed conflict.

1. Emerging Factors

The seemingly clear bifurcation between combatants and civilians that was established in 1949 was already eroding in the armed conflicts leading up to the 1970s, causing the ICRC to recommend relaxing the require-

109. Eric S. Krauss & Michael O. Lacey, *Utilitarian vs. Humanitarian: The Battle Over the Law of War*, PARAMETERS, Summer 2002, at 73, 73.

110. Jensen, *supra* note 21, at 710–11.

111. Regulations Concerning the Laws and Customs of War on Land, annex to Convention (IV) Respecting the Laws and Customs of War on Land art. 1, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument [hereinafter Hague Regulations].

112. *See* Geneva Convention, *supra* note 18, at art. 4.

113. 3 THE GENEVA CONVENTIONS OF 12 AUGUST 1949: COMMENTARY, GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 45 (Jean S. Pictet ed., 1960), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-III.pdf [hereinafter Geneva Conventions Commentary].

114. FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD arts. 15-25 (1863), *available at* http://www.icrc.org/ihl.nsf/FULL/110?OpenDocument.

115. Protocol I, *supra* note 9, arts. 51.2, 52.1.

116. *Id.* at art. 51.3.

117. *Id.* at art. 50.1.

ments for qualification of a combatant which was then codified in GPI.[118] Recent armed conflicts have demonstrated the difficulty of determining when a civilian takes "a direct part in hostilities."[119]

Future armed conflict will undoubtedly increase the consternation over defining actors on the battlefield. The differentiation between civilians and combatants will become more blurred as global technologies allow linkages and associations among people that were not possible in 1949 or 1977. The following sections analyze emerging factors that will stress LOAC understandings of civilians, organized armed groups, and combatants.

a. Civilians

The current LOAC is clear that "the civilian population as such, as well as individual civilians, shall not be the object of attack . . . unless and for such time as they take a direct part in hostilities."[120] Despite the seeming clarity of the rule, applying the rule to civilians on the future battlefield is surprisingly difficult.[121] This rule will be discussed in two parts below, the first dealing with the prohibition on attacking civilians and the second on the meaning of direct participation in hostilities.

i. Prohibition on Attacking Civilians

Future technologies, such as the virology discussed in the scenario at the beginning of this Article, will be enhanced or facilitated by using the civilian population to either spread or host the eventual weapon. Attackers who use viruses or nanotechnologies or genetic mutators will find their attacks facilitated by using the civilian population to propagate their weapons. The nanobot will be released generally into the population and then trigger its payload based on finding the correct DNA sequence or other similar marker.

Cyber attackers will find the same methodologies useful. They will create malware that spreads broadly throughout civilian systems until it finds the specific computer system it is designed to attack and then conduct its attack. The details on these means and methods will be discussed in greater detail below, but the important aspect of these attacks for this section is that they are facilitated or hosted by civilians or civilian objects.

These types of systems are unlike prior chemical or biological weapons because they do not necessarily have deleterious effects on the host and certainly don't take full effect on the host, but rather save their full

118. *Id.* at art. 44.3. Although there is no official statement on this point, it appears that this provision is one of the reasons that the United States has not ratified Protocol I. *See* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions,* 2 Am. U. J. Int'l L. & Pol'y 419 (1987).

119. Protocol I, *supra* note 9, art. 51.3.

120. *Id.* at arts. 51.2, 51.3.

121. *See* R. George Wright, *Combating Civilian Casualties: Rules and Balancing in the Developing Law of War*, 38 Wake Forest L. Rev. 129, 129–36 (2003).

effect for the target. Thus, the civilian or civilian object can facilitate the attack without feeling much, if any, of the effects. This approach to disseminating a weapon system will stress the LOAC as future technologies continue to develop.

ii. Direct Participation in Hostilities

Not all civilians enjoy complete protection from being attacked. As GPI states, civilians forfeit their protection from attack if they take a direct part in hostilities.[122] The actual meaning of these words and their practical application on the battlefield has been a matter of great debate.[123] In response to the debate, the ICRC issued its "Interpretive Guidance on the Notion of Direct Participation in Hostilities"[124] (DPH Guidance), which was intended to provide guidance on what actions by civilians rose to the level of direct participation. While this publication is not without controversy[125] and certainly does not purport to be a statement of the law, it provides an interesting basis for analysis.

The DPH Guidance lays out three cumulative criteria for a civilian to be directly participating.[126] The first is that there must be a certain threshold of harm.[127] The harm should "adversely affect the military operations or military capacity of a party to an armed conflict, or . . . inflict death, injury or destruction on persons or objects protected against direct attack."[128] The second criterion is that there must be direct causation.[129] The act must be designed to directly cause harm, or part of a concrete and coordinated military operation of which the act constitutes an integral part.[130] Finally, there must be a belligerent nexus between the act and the conflict.[131] In other words, the act must be designed to directly cause the required threshold of harm in support of a party to the conflict.[132]

However "direct participation" is defined, future weapons systems and tactics will likely increase the number of civilians who become actors on the battlefield, either intentionally or otherwise. Some examples follow.

---

122. Protocol I, *supra* note 9, art. 51.3.

123. Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 90 INT'L REV. RED CROSS 991, 993–94 (2008), *available at* http://www.icrc.org/eng/assets/files/other/irrc-872-reports-documents.pdf.

124. *Id.* at 1006–09.

125. Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641 (2010).

126. Melzer, *supra* note 123, at 1016.

127. *Id.*

128. *Id.*

129. *Id.* at 1019.

130. *Id.* at 1019–25.

131. *Id.* at 1025.

132. *Id.* at 1026.

a) Tools

In the scenario from *The Atlantic* at the beginning of this Article, Samantha has no idea that she is playing a role in the attack on the President of the United States. She is undoubtedly an innocent instrumentality or tool in the attack plan. Nevertheless, she is a key component of the attack and her ingestion of the virus and subsequent spreading of the virus is vital to the operation. Is she directly participating in hostilities though she has no intention of taking part? Does her lack of intention make targeting her any less vital?

Many other future means and methods of warfare will use civilians as tools in the attack as well, including genomics and nanotechnologies. Cyber operations already struggle with this issue.[133] The use of civilians as tools to facilitate advanced technological attacks requires a reconsideration of the rules on direct participation.

b) Transnational Communities of Interest

The rise of social networking and its ability to instantaneously link together individuals and groups from across the globe is just beginning to be explored as a social phenomenon. Negative aspects of this global linkage are already being felt across various levels of society, including the business world.[134]

Jeffrey Walker has termed these groups "instantaneous transnational communities of interest" and argues that "It's simply no longer necessary to have a state sponsor for an interested group of people to effect changes within the international community."[135] Anthony Lake, former National Security Advisor to President Clinton, described these instantaneous transnational communities of interest as "technology enabling local groups to forge vast alliances across borders, and . . . a whole host of new actors challenging, confronting, and sometimes competing with governments on turf that was once their exclusive domain."[136]

Social networking's effects on armed conflict have also already begun to surface[137] and will only increase over time. As Philip Bobbitt has writ-

133. Tallinn Manual, *supra* note 42, at 119–20; Collin Allan, *Attribution Issues in Cyberspace*, 13 Chi.-Kent J. Int'l & Comp. L. 55, 57 (2013).

134. Bob Hayes & Kathleen Kotwica, Trend Research: Crisis Management at the Speed of the Internet, Security Executive Council (2013), *available at* https://www.securityexecutivecouncil.com/secstore/index.php?main_page=product_info&cPath=77_66&products_id=361.

135. Jeffrey K. Walker, *Thomas P. Keenan Memorial Lecture: The Demise of the Nation-State, the Dawn of New Paradigm Warfare, and a Future Profession of Arms*, 51 A.F. L. Rev. 323, 329–30 (2001).

136. *Id.* at 133, 330 (citing Anthony Lake, 6 Nightmares 281–82 (2000)).

137. *See* George Griffin, *Egypt's Uprising: Tracking the Social Media Factor*, PBS (Apr. 20, 2011), http://www.pbs.org/newshour/updates/middle_east/jan-june11/revsocial_04-19.html.

ten, "The internet enabled the aggregation of dissatisfied and malevolent persons into global networks."[138]

Audrey Kurth Cronin likens social networking to the *levée en masse* and argues that it allows cyber mobilization of people across the entire globe on issues of common ideology.[139] She writes:

> The evolving character of communications today is altering the patterns of popular mobilization, including both the means of participation and the ends for which wars are fought. . . Today's mobilization may not be producing masses of soldiers, sweeping across the European continent, but it is effecting an underground uprising whose remarkable effects are being played out on the battlefield every day.[140]

As social networking continues to embed itself as a societal norm, people will begin to view themselves less as Americans, or Germans, or Iranians, and more as members of global ideologies created, maintained, and mobilized over social media.[141]

Through social media, individuals will be able to recruit, provide financial support, collect intelligence, pass strategies and information, forward ideas and instructions for munitions, create and solidify plans of action, and coordinate attacks. These events will occur far from any existing battlefield but will have profound and immediate effects on hostilities, creating a global group of direct participants who will meet the legal criteria for targeting.

c) Hacktivists

The role of hacktivists has already been demonstrated in conflicts between Russia and Estonia[142] and between Russia and Georgia.[143] Though there has been no evidence to date to attribute these actions to states, David Hoffman argues that "States like China and Russia now encourage groups of freelance hackers to do their dirty work, allowing plausible deniability."[144]

Additionally, other groups of hacktivists, which are clearly not state-sponsored or state-aligned, have been able to apply state-level force and create significant effects in armed conflicts. For example, the global collec-

---

138. Philip C. Bobbitt, Inter Arma Enim Non Silent Leges, 45 SUFFOLK U. L. REV. 253, 259 (2012).

139. *See, e.g.*, Audrey Kurth Cronin, *Cyber-Mobilization: The New* Levée en Masse, PARAMETERS, Summer 2006, at 77, 77.

140. *Id.* at 84–85.

141. *See* Thomas J. Holt & Max Kilger, *Examining Willingness to Attack Critical Infrastructure Online and Offline*, 58 CRIME & DELINQUENCY 798 (2012).

142. Allan, *supra* note 133, at 59.

143. *Id.*

144. David E. Hoffman, *The New Virology: From Stuxnet to Biobombs, the Future of War by Other Means*, FOREIGN POL'Y, Mar.-Apr. 2011, *available at* http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology.

tive "Anonymous" has engaged in activities against states during armed conflict with the intent to influence government behavior.[145]

Because hacktivists participate along a spectrum of activities with varying associations, it is very difficult to determine each individual's level of participation. Unless the collective work of a hacktivist group rises to the level of an organized armed group (see below), it is difficult to treat it as a collective when making targeting determinations. Many individuals, though part of the organization, may just be tools (see above) on any specific operation.

In addition to groups, individuals often act alone in this capacity and can also cause great damage. One of the first monumental "hacks" in the United States was the "solar sunrise," which ended up being the work of three individuals—a man in Israel and two teenagers in California.[146]

Hacktivism is unique to computer operations, but civilian activism is not. As the world progresses toward future armed conflict, activists and activist groups in other areas will certainly coalesce. Genomics and nanotechnology will have their own Cap'n Capsid and the international community will have to figure out how to deal with them under the LOAC.

d) "Arms" Dealers

As is discussed below in Section II(C), a wide variety of new means and methods of warfare will emerge as future technologies develop. Similar to computer malware from the hacktivists of the prior section and bioengineers from the scenario at the beginning of this article, some of these new technologies will not be limited to development by states. Some will be developed and marketed by individuals, organized groups, criminal organizations, and corporations. There is already a large market for cyber "arms" that is very lucrative and is sourced almost exclusively by non-state actors.[147]

Some of these arms dealers may also be users of the arms, which will make their legal classification simpler; but many will not be users, but mere producers. For them, this will be a business opportunity, just as it is for many contemporary arms dealers who deal in traditional arms. However, the spread of technology and the needs of future armed conflict will open this line of work to a much broader and previously innocuous group of individuals. At some point, do these creators of modern arms become

145. *See* Jana Winter & Jeremy A. Kaplan, *Communications Blackout Doesn't Deter Hackers Targeting Syrian Regime*, Fox News (Nov. 30, 2012), http://www.foxnews.com/tech/2012/11/30/hackers-declare-war-on-syria/#ixzz2Ht69GA1J.

146. Kevin Poulsen, *Solar Sunrise Hacker 'Analyzer' Escapes Jail*, The Register (June 15, 2001), http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/. The FBI made a documentary about the hacks. Fed. Bureau of Investigation, *Solar Sunrise Documentary*, Security Tube, http://www.securitytube.net/video/189 (last visited Mar. 9, 2014).

147. *See* Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, Business Week (July 20, 2011), http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html.

participants in the conflict? If not, can they assume that they can continue to take these actions with relative impunity?

e) Nongovernmental Organizations

Nongovernmental organizations (NGOs) deserve mention here also. Though they are unlikely to become actors on the future battlefield, they are expanding their participation in international governance.[148] One need only look at their efforts in the area of anti-personnel landmines to see how significant an effect NGOs can have in the formulation and alteration of the LOAC.[149] It seems likely that the trend of greater influence by NGOs will increase and that as the international community struggles to evolve the LOAC in response to future places, actors, and means and methods of warfare, NGOs will have a seat at the table. Their involvement in law formulation may provide a vehicle for the incorporation of each NGO's individual agenda, whatever that may be. While this may or may not result in positive effects on LOAC development, the point is that NGOs' role is increasing which is likely to lead to different results than in the past.

b. Organized "Armed" Groups

One of the great clarifications urged by the DPH Guidance is the recognition that civilians often form themselves into organized armed groups and that membership in these groups should result, to varying degrees, in a forfeiture of civilian protections.[150] These groups, in many varieties, are likely to increase in future armed conflict. Some examples are discussed below.

i. Non-traditional "Armed" Groups

One of the most important potential changes to the idea of organized armed groups in the future is what it means to be armed. In the discussion above, transnational communities of interest and hacktivist groups were treated as individuals who might directly participate in hostilities. This was based on a more traditional view of "armed," meaning kinetic, weapons. However, many future technologies will produce, as in the scenario at the beginning of this article, weapons or things that can be used as weapons that are very different than the traditional view of "arms."

For example, is "Anonymous" an organized armed group? It possesses state-level force with its ability to infiltrate and affect governmental (and corporate) computer systems. Would a transnational community of interest that has gathered DNA samples on world leaders and is willing to

148. Steve Charnovitz, *Two Centuries of Participation: NGOs and International Governance*, 18 MICH. J. INT'L L. 183, 183 (1997).

149. Walker, *supra* note 135, at 330.

150. For example, the ICRC's DPH Guidance allows for targeting based on membership in an organized armed group when combined with a continuous combat function within the organization. Melzer, *supra* note 123, at 1006–09.

sell them to the highest bidder be an organized armed group? Or a group of individuals who work together to build a virus that will transport a genomic mutator? Or a transnational group of concerned scientists who publish openly nanotechnology processes or offer their services so everyone can enjoy the benefits of nanotechnology?

The future is likely to present numerous groups of varying composition and intent that do not possess traditional arms, but control or create the means to do great harm. These groups will stress the current application of targeting law, including the determination of lawful targets (as will be discussed below), even with the clarification of organized armed groups.

ii. Traditional "Armed" Groups

In addition to the non-traditional armed groups, the types and activities of more traditional armed groups will also expand. Four examples are discussed briefly below.

a) Private Security Companies

Much has been written recently concerning the use of private contractors, and particularly private security companies (PSC).[151] The use of contractors in current military operations has added pressures to the definition of actors on the battlefield.[152] Private contractors are involved in providing a wide array of services[153] and according to the ICRC, the trend of militaries outsourcing traditional military functions to private contractors is "likely to increase in the years ahead."[154]

---

151. John R. Crook, *Contemporary Practice of the United States Relating to International Law: International Law and non-State Actors: United States Supports Conclusion of Code of Conduct for Security Companies*, 105 Am. J. Int'l L. 156 (2011); Daniel P. Ridlon, *Contractors or Illegal Combatants? The Status of Armed Contractors in Iraq*, 62 A.F. L. Rev. 199 (2008).

152. From Mercenaries to Market: The Rise and Regulation of Private Military Companies (Simon Chesterman & Chia Lehnardt eds., 2007); Eric Talbot Jensen, *Combatant Status: It is Time for Intermediate Levels of Recognition for Partial Compliance*, 46 Va. J. Int'l L. 214 (2005); Christopher J. Mandernach, *Warrior Without Law: Embracing a Spectrum of Status for Military Actors*, 7 Appalachian J. L. 137 (2007).

153. Greg Miller & Julie Tate, *CIA's Global Response Staff Emerging From the Shadows After Incidents in Libya and Pakistan*, Wash. Post, Dec. 26, 2012, *available at* http://articles.washingtonpost.com/2012-12-26/world/36015677_1_security-for-cia-officers-cia-compound-benghazi; Craig Whitlock, *U.S Expands Secret Intelligence Operations in Africa*, Wash. Post (June 13, 2012), http://articles.washingtonpost.com/2012-06-13/world/35462541_1_burkina-faso-air-bases-sahara.

154. Kellenberger, *supra* note 22.

In response to abuses,[155] good work is already being done in this area[156] and more will continue to be done. However, this work is unlikely to constrain how these groups are used in the future. Governments will continue to hire PSCs to provide security to people and places on the battlefield. Even if not intentionally, the PSCs will continue to find themselves in the midst of situations requiring the use of force. It is quite possible that at some future point, some states will contract out their entire state armed forces and designate them as combatants representing the state. If this occurs, significant businesses will arise whose purpose is to provide state forces for hire. These groups of fighters, though likely compliant with the LOAC, will also be loyal to their paymaster rather than a specific state.

b) Corporate Participation and Armies

In addition to private armies for hire, corporations will do even more to provide their own security, especially in regions of instability. ExxonMobil in Indonesia and Talisman Energy in Sudan have already "hired" and controlled national military forces to protect their business interests.[157] Past corporate involvement in armed conflict includes "unlawful taking of property, forced labor, displacement of populations, severe damage to the environment, and the manufacture and trading of prohibited weapons."[158] Recent events where corporate assets were attacked and employees held hostage[159] would increase and cause corporations to reconsider their protective posture.

---

155. Press Release, Federal Bureau of Investigation, Academi/Blackwater Charged and Enters Deferred Prosecution Agreement (Aug. 7, 2012), *available at* http://www.fbi.gov/charlotte/press-releases/2012/academi-blackwater-charged-and-enters-deferred-prosecution-agreement.

156. *See, e.g.*, Jennifer K. Elsea, Cong. Research Serv., R40991, Private Security Contractors in Iraq and Afghanistan: Legal Issues (2010); Rep. of the Working Group on the Use of Mercenaries As a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, Human Rights Council 15th Sess., U.N. Doc. A/HRC/15/25 (July 2, 2010), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/151/55/PDF/G1015155.pdf?OpenElement.

157. Jonathan Horlick, Joe Cyr, Scott Reynolds & Andrew Behrman, *American and Canadian Civil Actions Alleging Human Rights Violations Abroad by Oil and Gas Companies*, 45 Alta. L. Rev. 653, 657–58 (2008); *see also* Note, *Corporate Liability for Violations of International Human Rights Law*, 114 Harv. L. Rev. 2025 (2001).

158. Regis Bismuth, *Mapping a Responsibility of Corporations for Violations of International Humanitarian Law Sailing Between International and Domestic Legal Orders*, 38 Denv. J. Int'l L. & Pol'y 203, 204 (2010); *see also* ICRC, Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises Under International Humanitarian Law 24 (2006); Erik Mose, *Corporate Criminal Liability and the Rwandan Genocide*, 6 J. Int'l Crim. Just. 973, 974 (2008).

159. Aomar Ouali & Paul Schemm, *Desert Drama: Islamists Take Hostages in Algeria*, Associated Press (Jan. 16, 2013), http://hosted2.ap.org/APDEFAULT/3d281c11a96b4ad082fe88aa0db04305/Article_2013-01-16-Algeria-Kidnapping/id-1b29673dae1745f686acac504f96c598.

Many corporations have far greater resources than the states in which they operate. The search for profit will drive them to protect their assets in areas where governments cannot control the territory. In many cases, this territory will be contested and in an area already enflamed by internal armed conflict. These corporate armies will be tasked with protecting corporate assets, employees, and resources, but will find themselves involved in the armed conflicts raging about them.

c) Global Criminal Enterprises

Another group that could also be discussed under "Organized Armed Groups" below is global criminal enterprises, such as the various organized narcotics organizations operating in Mexico and other parts of Central and South America. Reports place the number of armed fighters in Mexico alone at over 100,000,[160] a number much larger than in most recent armed conflicts.

In addition to narcotics organizations, global criminal enterprises are involved in counterfeiting, money laundering, arms smuggling, and the sex trade to name just a few.[161] Many of these criminal enterprises have links to armed conflict and even contain factions within their business whose role is to conduct military-type tasks necessary for the business enterprise. However, all of these global organizations are likely to appear on future battlefields in order to conduct their business.

d) State Paramilitaries

The large-scale operation of armed drones by the CIA portends a shift in the use of paramilitary organizations in the future. While the CIA has, from its inception, been involved in covert operations that resulted in military-type activities, the scale and openness of current operations is qualitatively different.[162] There is very little difference between the drone strikes conducted by the U.S. military and those done by the CIA, except perhaps in their regulation by the LOAC.[163]

These activities by the United States will likely set an example for other countries that also have similar agencies and will begin to use them more openly in similar ways. Future armed conflicts will undoubtedly involve intelligence and other paramilitary agencies operating openly and using military weapons and tactics.

---

160. Carina Bergal, *The Mexican Drug War: The Case For A Non-International Armed Conflict Classification*, 34 FORDHAM INT'L L.J. 1042, 1066 (2011).

161. JOHN EVANS, CRIMINAL NETWORKS, CRIMINAL ENTERPRISES 2 (1994) *available at* http://www.icclr.law.ubc.ca/publications/reports/netwks94.pdf.

162. *See* Richard M. Pious, *White House Decisionmaking Involving Paramilitary Forces*, J. NAT'L SEC. L & POL'Y (Jan. 24, 2012), http://jnslp.com/2012/01/24/white-house-decision-making-involving-paramilitary-forces/.

163. *See US: Transfer CIA Drone Strikes to Military Ensure Intelligence Agency Abides by International Law*, HUMAN RIGHTS WATCH (Apr. 20, 2012), http://www.hrw.org/news/2012/04/20/us-transfer-cia-drone-strikes-military.

c. State Forces

Significant changes will occur in future armed conflict even to recognized state forces. The changing methods of warfare will undermine the traditional criteria for combatants, and the incorporation of autonomous weapons into regular armed forces will diminish the role of humans in targeting decisions.

i. Combatant's Traditional Criteria

Article 1 of the Annex to Hague Convention (IV) respecting the Laws and Customs of War on Land states that:

> The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:
>
> 1. To be commanded by a person responsible for his subordinates;
> 2. To have a fixed distinctive emblem recognizable at a distance;
> 3. To carry arms openly; and
> 4. To conduct their operations in accordance with the laws and customs of war.
>
> In countries where militia or volunteer corps constitute the army, or form part of it, they are included under the denomination "army."[164]

These qualifications for militias are repeated in the GPI.[165] Though textually limited to militias and volunteer corps who are working with a party to

---

164. Hague Regulations, *supra* note 111, art. 1.

165. Article 4 states:

> Art 4. A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:
>
> (1) Members of the armed forces of a Party to the conflict, as well as members of militias or volunteer corps forming part of such armed forces.
>
> (2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfil the following conditions:
>
> (a) that of being commanded by a person responsible for his subordinates;
>
> (b) that of having a fixed distinctive sign recognizable at a distance;
>
> (c) that of carrying arms openly;
>
> (d) that of conducting their operations in accordance with the laws and customs of war.

See Geneva Convention, *supra* note 18, at art. 4.

the conflict, the common understanding is that state forces will also meet these criteria.[166] The difficulty with "armed groups" and these criteria has been alluded to above, but it also exists with traditional state forces.

States (and other organized groups) are employing weapons from great distances where the uniform of the targeter is indiscernible by the eventual target. The eventual target of malware launched from the National Security Agency in Maryland will be completely unaware of whether the person who launched the malware was wearing a uniform or civilian clothes. The development and employment of viruses or genomic mutators will likely be done far from the active battlefield.

Even if created and employed by uniformed personnel, when the virus, nanobot, or computer malware reaches its intended target, it will contain no marking that notifies the victim of the identity of the attacker. In fact, in many of these future weapons systems, anonymity is vital to the success of the operation. As future technologies develop, the issue of "having a fixed distinctive sign recognizable at a distance [and] . . . carrying arms openly"[167] will pressure the LOAC to account for modern armed conflict practices.

ii. Autonomous Weapon Systems

Autonomous weapons have become a very important discussion in the area of the law governing future weapons systems. They include robots, unarmed and armed unmanned aerial and underwater vehicles,[168] auto-response systems such as armed unmanned sentry stations,[169] and a host of other developing weapon systems. The systems will be discussed in greater detail below as means and methods, but they are raised here because the more autonomous they become, the more like "actors" they appear.

---

166. According to 3 GENEVA CONVENTIONS COMMENTARY, *supra* note 113, at 52:

> The drafters of the 1949 Convention, like those of the Hague Convention, considered that it was unnecessary to specify the sign which members of armed forces should have for purposes of recognition. It is the duty of each State to take steps so that members of its armed forces can be immediately recognized as such and to see to it that they are easily distinguishable from members of the enemy armed forces or from civilians. The Convention does not provide for any reciprocal notification of uniforms or insignia, but merely assumes that such items will be well known and that there can be no room for doubt.

167. Hague Regulations, *supra* note 111, art. 1.

168. Damien Gayle, *Rise of the Machine: Autonomous Killer Robots 'Could Be Developed in 20 Years'*, DAILY MAIL (Nov. 20, 2012), http://www.dailymail.co.uk/sciencetech/article-2235680/Rise-Machines-Autonomous-killer-robots-developed-20-years.html; *Marlin,* LOCKHEED MARTIN, http://www.lockheedmartin.com/us/products/marlin.html (last visited Mar. 9, 2014).

169. Jonathan D. Moreno, *Robot Soldiers Will Be a Reality—And a Threat*, WALL STREET J. (May 11, 2012), http://online.wsj.com/article/SB10001424052702304203604577396282717616136.html.

The military use of robots will sufficiently illustrate the point. It is clear that the general use of robots in armed conflict is increasing.[170] According to Peter Singer, a well-known expert on the issue of robotics and armed conflict,[171] "besides the U.S., there are 43 other nations that are also building, buying and using military robotics today."[172] Remotely controlled armed robots entered action in Iraq in summer of 2007.[173] This is a trend that will clearly continue. A report that the "Joint Forces Command drew up in 2005 . . . suggested autonomous robots on the battlefield will be the norm within 20 years,"[174] and a recent report written by the U.S. Department of Defense (DoD), titled *Unmanned Systems Integrated Roadmap FY2011-2036*, stated that it "envisions unmanned systems seamlessly operating with manned systems while gradually reducing the degree of human control and decision making required for the unmanned portion of the force structure."[175]

It appears the intent is to increase the autonomy with which these weapon systems will function, causing Singer to point out that robotics is "changing not just the 'how' [of warfare] but the 'who.'"[176] Future robots may use "brain-machine interface technologies" or "whole brain emulation."[177] The potentially autonomous nature of robots means that they will become actors on the battlefield, as well as means and methods of warfare.

Singer describes this dramatically changing advance in robotic technology as a revolution:

> Carrying forward, that means that our [robotic] systems . . . will be a billion times more powerful than today within 25 years. I'm not saying a billion in a sort of amorphous, meaningless, Austin-Powers' one billion. I mean literally take the power of those systems and multiply them times 1 with 9 zeros behind it. What that means is that the kind of things people used to talk about only at science

170. John Markoff, *U.S. Aims for Robots to Earn Their Stripes on the Battlefield*, INT'L HERALD TRIBUNE (Nov. 27, 2010), at 1.

171. Singer is currently the director of the 21st Century Security and Intelligence and a senior fellow in foreign policy at Brookings. He has authored numerous articles and books on future weapons, with particular emphasis on robotics. *See* Peter W. Singer, BROOKINGS, http://www.brookings.edu/experts/singerp (last visited Mar. 9, 2014).

172. Steve Kanigher, *Author Talks about Military Robotics and the Changing Face of War*, LAS VEGAS SUN (Mar. 17, 2011), http://www.lasvegassun.com/news/2011/mar/17/military-robotics-and-changing-face-war/.

173. Stew Magnuson, *Gun Toting Robots See Action in Iraq*, NAT'L DEF. MAG. (Sept. 2007), http://www.nationaldefensemagazine.org/archive/2007/September/Pages/RifleToting4435.aspx.

174. P.W. Singer, *In the Loop? Armed Robots and the Future of War*, DEF. INDUSTRY DAILY (Jan. 28, 2009, 20:09), http://www.defenseindustrydaily.com/In-the-Loop-Armed-Robots-and-the-Future-of-War-05267/.

175. U.S. DEP'T OF DEF., UNMANNED SYSTEMS INTEGRATED ROADMAP FY2011-2036, 3 (2011), *available at* http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf.

176. Singer, *supra* note 11, at 10.

177. Moreno, *supra* note 169.

> fiction conventions like Comic-Con now need to be talked about by people like us, need to be talked about by people in the halls of power, need to be talked about in the Pentagon. We are experiencing a robots revolution.[178]

In response to these advances, the DoD recently issued a Directive titled "Autonomy in Weapon Systems"[179] that applies to the "design, development, acquisition, testing, fielding, and employment of autonomous and semi-autonomous weapon systems, including guided munitions that can independently select and discriminate targets."[180] The Directive states that "It is DoD policy that . . . [a]utonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[181]

In the same week the DoD Directive was issued, Human Rights Watch issued a report[182] calling for a multilateral treaty that would "prohibit the development, production and use of fully autonomous weapons."[183] The Directive and Report have sparked a great deal of discussion,[184] much of which has revolved around the ability of an autonomous weapon to make decisions as required by the LOAC.[185]

---

178. Singer, *supra* note 11.

179. Dept. of Def., Directive, 3000.09, Autonomy in Weapon Systems (D.O.D. 2012). The Directive followed a DoD Defense Science Board Task Force Report on "The Role of Autonomy in DoD Systems" that was issued in July of 2012. DoD Defense Science Board, The Role of Autonomy in DoD Systems (2012), *available at* http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf.

180. Dept. of Def., Directive, 3000.09, Autonomy in Weapon Systems ¶ 2a(2), (D.O.D. 2012). The Directive "[d]oes not apply to autonomous and semi-autonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g. laser- or wire-guided munitions); mines; or unexploded explosive ordnance." *Id.* ¶ 2b.

181. *Id.* ¶ 4a.

182. Human Rights Watch, Losing Humanity: The Case Against Killer Robots (2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf.

183. *Id.* at 46.

184. *See, e.g.*, Kenneth Anderson, *Readings: Autonomous Weapon Systems and Their Regulation*, Lawfare: Hard Nat'l Sec. Choices (Dec. 11, 2012, 6:26 PM), http://www.lawfareblog.com/2012/12/readings-autonomous-weapon-systems-and-their-regulation/; Kenneth Anderson, *Autonomous Weapon Systems and Their Regulation—A Flurry of Activity*, The Volokh Conspiracy (Dec. 12, 2012, 9:32 PM), http://www.volokh.com/2012/12/12/autonomous-weapon-systems-and-their-regulation-a-flurry-of-activity/; Jordana Mishory, *Carter: Human Input Required For Autonomous Weapon Systems*, Unmanned Systems Alert (Nov. 28, 2012) http://unmannedsystemsalert.com/Unmanned-Systems-General/Public-Content/carter-human-input-required-for-autonomous-weapon-systems/menu-id-1004.html?S=LI#%21; Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to Critics*, Harv. Nat'l. Sec. J. (Feb. 5, 2013), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf.

185. Spencer Ackerman, *Pentagon: A Human Will Always Decide When a Robot Kills You*, Wired (Nov. 26, 2012, 6:12 PM), www.wired.com/dangerroom/2012/11/human-robot-kill.

Despite the DoD Directive, the international community must recognize that at some point, fully autonomous weapon systems will likely inhabit the battlefield (and may eventually become the predominant players) and will be making decisions that we now think of as requiring human intervention.[186] This will stress our current understanding and application of the LOAC, and force an evolution in how we apply LOAC principles.

2. Emerging Law

The section above has touched only briefly on some of the emerging factors regarding actors on the battlefield that will place stresses on the LOAC in future armed conflicts. Anticipating these emerging factors, the law will need to evolve to respond to technological developments and signal appropriate regulation.

a. Attack

The proscription dealing with civilians is against making them the object of "attack." The meaning of attack is defined in GPI as "acts of violence against the adversary, whether in offence or in defence."[187] The strict reading of this treaty language is that civilians are only protected from acts of violence. As clearly argued by Paul Walker, most cyber activities will not reach the threshold of an attack,[188] meaning they are not proscribed. Cyber (and other) activities that cause mere inconvenience are legitimate, even when directed at the civilian population.[189] This argument will arise again below under means and methods of warfare because there are any number of potential or future weapons that will likely fall under the threshold of an "act of violence." If so, as a matter of targeting, civilians are not protected from these activities that do not amount to an attack.

For example, recalling the scenario from the beginning of the article, it is unclear whether the voluntary ingestion of a pill or even the inhalation of a nanobot would be considered an attack. Likewise, it is unclear that infection with a flu-like virus or even a viral gene alteration that had no effect on an individual would be considered an attack. Therefore, under the current LOAC, such activities may be permitted.

One might argue that Article 51 of GPI requires that "the civilian population and individual civilians shall enjoy general protection against dangers arising from military operations,"[190] and "military operations" is a category much broader than "attacks." However, even Article 51 only pro-

186. Anderson & Waxman, *supra* note 23.

187. Protocol I, *supra* note 9, at art. 49.1.

188. Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SEC. L. BRIEF 33 (2011), *available at* http://digitalcommons.wcl.american.edu/nslb/vol1/iss1/3.

189. TALLINN MANUAL, *supra* note 42.

190. Protocol I, *supra* note 9, art. 51.1.

tects civilians against "dangers," a term that is not clearly defined and might not include flu-like symptoms. Similarly, Article 57.1 states that "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[191] The commentary defines military operations as "any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat,"[192] but does not explain what it means to "spare" the population or define "constant care."[193]

With the future development of weapons that will undoubtedly fit below the attack threshold of "acts of violence," it will be important to clarify the LOAC as it pertains to targeting of civilians as actors in armed conflict. If the LOAC is designed to protect civilians from the effects of armed conflict, more detail is necessary here.

b. Status and Conduct

Targeters justify attacking individuals based on either their status or their conduct. Combatants are targetable simply based on their status. The LOAC also allows targeting of members of the military wing or an organized armed group based on their status as members.[194] Almost all others are targetable based solely on their conduct. In other words, the normal civilian has to do something to bring himself within the crosshairs of a targeter. As discussed above, future technologies will cause us to rethink how we currently understand both status and conduct.

Beginning with civilians, under the current DPH Guidance, it is unlikely that Samantha in the scenario that begins this article would be targetable. She is an unknowing facilitator of a uniquely lethal virus. Perhaps the virus could be targeted with lethal force, effectively amounting to the targeting of Samantha, but one can imagine a different scenario where Samantha might, instead of walking to the place where the U.S. President would be speaking, merely prepare food that was going to be served at a luncheon or package flowers that were going to be delivered to the White House. Does she become targetable once she has ingested the virus and remain targetable for the life of the virus, potentially for the rest of her life? The current LOAC does not seem to contemplate such a reading. One could argue that she does not directly participate at any point in her life (though she carries the virus) until she plans on coming into direct contact with the President, but the burden on targeters to maintain awareness of her until she decides to take direct part is overly burdensome, par-

191. *Id.* art. 57.1.

192. Int'l Comm. of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 680 (Sandoz et al. eds., 1987) [hereinafter Red Cross Commentary].

193. For a discussion on this issue relative to cyber operations, see Tallinn Manual, *supra* note 42; Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 Int'l L. Stud. 198, 202 (2013).

194. *See, e.g.*, Melzer, *supra* note 123, at 1036.

ticularly once she has inadvertently passed the virus to others who now also presumably carry the threatening virus.

Similar difficulties arise from social networking and transnational communities of interest. As civilians attach themselves to causes, and then work through social media to forward that cause, do they become targetable? For example, are the tens of thousands of individuals targetable who forward a message trying to garner support for a rebel group? What if they are seeking information that might help the rebel group attack opposing forces?

In a variation on the same theme, can a state mobilize its citizens to accomplish national security goals through social media and not forfeit their protected status? Chris Ford proposes that the federal government use social networking methods to involve U.S. citizens "into a nation-wide program designed to address discrete security issues."[195] Would this make the citizens targetable?

Similarly with hacktivists, could Georgia have targeted the Russian hacktivists who were degrading the government's ability to exercise command and control of their military forces? Whatever response Georgia would have contemplated would certainly be bound by the principle of proportionate response, but even the authority to target the hacktivists is unclear under the current application of the LOAC.

This prospect of using civilians as unwitting tools is an area where the LOAC is not fully developed. Many of the answers to these questions are undoubtedly fact-specific, but the use of these future technologies will force the international community to reconsider its application of LOAC immunity.

The same questions exist concerning civilian property. Collin Allan has highlighted the difficulties of the computer system that has been taken over remotely and acts as part of the attack but whose owner has not made any affirmative decision to participate in the attack.[196] Perhaps that civilian property is transformed into a military objective, but if so, that would potentially implicate hundreds of thousands of computers that have been incorporated into powerful botnets and used for nefarious purposes.[197]

This status and conduct difficulty will also be magnified as new "armed" groups, including PSCs, corporate armies, and paramilitaries, become more prominent on the battlefield. Presumably, the Taliban could target a member of the CIA who was flying an armed drone with the intent of attacking members of the Taliban, based on his conduct. Since the CIA now has a continuing program of targeting with armed drones, is the entire CIA (or even the portion who work with the drones) targetable

195. Christopher M. Ford, *Twitter, Facebook and Ten Red Balloons: Social Network Problem Solving and Homeland Security*, 7 HOMELAND SECURITY AFF. J. 1, 1–2 (2011), *available at* http://www.hsaj.org/?article=7.1.3.

196. Allan, *supra* note 133, at 78–81.

197. *See* Pierre Thomas & Jack Cloherty, *FBI, Facebook Team Up to Fight 'Butterfly Botnet'*, ABC NEWS (Dec. 12, 2012), http://abcnews.go.com/Technology/butterfly-botnet-targets-11-million-including-computer-users/story?id=17947276.

based on status, not conduct? Similar analysis would apply to PSCs or corporate armies.

In addition to the question of lawfully targeting corporate armies or PSCs, there is an issue of how the LOAC should respond to their increasing presence on the battlefield. Many will argue that holding to the current LOAC, which does not authorize them to participate with any status on the battlefield, is the right way to proceed. But the realities of future armed conflict and the prevalence of these actors may lead to a different conclusion.

And finally, in the area of status and conduct there is the traditional requirement of marking or wearing a uniform and carrying arms openly. This is an area that is ripe for LOAC evolution. Both Sean Watts[198] and Rosa Brooks[199] have written convincingly, challenging the value of the traditional requirements that combatants "have a fixed distinctive emblem recognizable at a distance," and "carry arms openly"[200] as being "detach[ed] from reality."[201] In an age where an ever-increasing number of weapons are initiated, launched, or activated from a time and place distant from the victim, wearing uniforms and carrying your weapon openly seems of little value.[202]

Does it really matter to the victim if the individual launching the computer malware from his office in Maryland is wearing a uniform or not? Would it be much more meaningful if the malware itself was "marked" as coming from the United States? When the President collapses from ingesting the virus created in the scenario that begins this Article, would it do more to protect innocent victims of the armed conflict from the United States' retaliation if the virus was somehow marked or if Cap'n Capsid was wearing a uniform while he took his actions in sending the virus to Samantha?

Each cruise missile launched by the United States is marked with a U.S. flag, though it is unlikely that anyone will ever see the flag as it flies toward its target. But the idea of marking the weapon may set the pattern for future "over the horizon" or "shoot and forget" weapons. One of the intents in originally requiring combatants to wear uniforms was to make clear that the attacker represented a sovereign. Accomplishing this with viruses, genomics, nanotechnology, and cyber attacks will force the international community to reexamine the traditional criteria for combatants.

c. "Human" Discretion

Much of the legal consternation over robotics and other autonomous weapons systems is the discomfort with non-human decision making in

198. Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391 (2010).

199. Brooks, *supra* note 5.

200. Hague Regulations, *supra* note 111, art. 1.

201. Watts, *supra* note 198, at 446.

202. Brooks, *supra* note 5, at 756–57.

armed conflict, or the "human-out-of-the-loop" weapons. The Human Rights Watch Report referenced above categorized autonomous weapons into three categories:

- HUMAN-IN-THE-LOOP WEAPONS: Robots that can select targets and deliver force only with a human command;
- HUMAN-ON-THE-LOOP WEAPONS: Robots that can select targets and deliver force under the oversight of a human operator who can override the robots' actions; and
- HUMAN-OUT-OF-THE-LOOP WEAPONS: Robots that are capable of selecting targets and delivering force without any human input or interaction.[203]

Currently, it is unclear what having a human "in the loop" actually means[204] and whether it will result in fewer targeting mistakes.[205] What does seem to be clear is that having a human in the loop just makes the communication link between the robot and human the vulnerability.[206]

Despite this discomfort with a lack of legal precedent, technology continues to push forward, attempting to make robots more and more capable of independent decision making. Dyke Weatherington, DoD Deputy Director of Unmanned Warfare said, "I don't see any program going down that path (yet). There are legal and ethical issues, and I just don't think either the department or the technology is ready to do that."[207] Dr. Arkin, Director of the Mobile Robot Laboratory at Georgia Technical College, says that robots "will not have the full moral reasoning capabilities of humans, but I believe robots can—and this is hypothesis—perform better than humans."[208] There is certainly an argument to be made that a robot that is not subject to the emotions of the situation, dependence on inaccuracies and limitations of human sensory perception, and driven to make decisions based on frail human survivability will "perform better" and be less likely to engage an inappropriate target.

---

203. HUMAN RIGHTS WATCH, *supra* note 182.

204. Singer, *supra* note 174.

205. *See id.*

206. *Id.*

207. Tara McKelvey, *Human Input at an End as Killer Robots do the Thinking*, THE AUSTRALIAN (May 21, 2012) at 1. For a discussion of the ethical issues, see Ken Anderson, *An Ethical Turing Test For Autonomous Artificial Agents*, CONCURRING OPS. (Feb. 17, 2012, 11:47 AM), http://www.concurringopinions.com/archives/2012/02/an-ethical-turing-test-for-autonomous-artificial-agents.html.

208. Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 279–80 (2011) (listing several reasons why autonomous robots may be able to outperform humans under combat conditions including: the ability to act conservatively, they can be used in a self-sacrificing manner if needed and appropriate without reservation by a commanding officer, and they can be designed without emotions that cloud their judgment); McKelvey, *supra* note 207; *Cry Havoc, and Let Slip the Highly Ethical Robots of War*, THE AM. PROSPECT (Aug. 9, 2011), http://prospect.org/article/cry-havoc-and-let-slip-highly-ethical-robots-war.

Autonomous weapons on the battlefield will increase and the autonomy of those weapon systems will also increase, raising serious questions about how the LOAC can deal with these issues.[209] As Jonathan Moreno has noted, "The various international agreements about weapons and warfare do not cover the convergence of neuroscience and robotic engineering."[210]

At what point do we determine that we have sufficiently programmed a weapon system such that it can legally respond to external information and stimuli in order to make a lethal decision? If the weapon acts incorrectly and unlawfully kills someone, who is responsible? Do we put the system on trial, its designer, its programmer, the soldier who set it up, or the commander who determined it could be used in that situation? As Vik Kanwar writes when reviewing Singer's *Wired for War*:

> From the point of view of the international lawyer, the concern is not asymmetry of protection, but rather that one side might be shielded from legal consequences. For a series of partially coherent reasons, the "human element" is seen as "indispensible": for providing judgment, restraint, and ultimately responsibility for decisions.[211]

All of these questions, and many more, raise legal issues that are as yet unresolved but will need to be resolved as technology propels us toward the greater use of autonomous weapons. It is unlikely that the international community will respond to Human Rights Watch's call for an international agreement to ban autonomous weapons. History does not support that idea.[212] Therefore, the international community needs to begin now to think of how the LOAC must evolve to respond.[213]

C. *Means and Methods*

"Few weapons in the history of warfare, once created, have gone unused."

U.S. Deputy Defense Secretary William J. Lynn III[214]

The quote above by William Lynn highlights the need to evolve the LOAC to regulate new technologies. Once developed, weaponized technologies almost inevitably find their way onto the battlefield. In the few instances where the technologies have not been used, or at least used in a

209. Anderson & Waxman, *supra* note 23.

210. Moreno, *supra* note 169.

211. Vik Kanwar, *Review Essay: Post-Human Humanitarian Law: The Law of War in the Age of Robotic Weapons*, 2 HARV. NAT'L SEC. J. 616, 620 (2011).

212. *See* Banusiewicz, *supra* note 10.

213. Anderson and Waxman make this argument very effectively concerning autonomous weapons in their article, *Law and Ethics for Robot Soldiers*. Anderson & Waxman, *supra*, note 23.

214. Banusiewicz, *supra* note 10.

limited fashion, it has been largely based on legal restrictions.[215] The means and methods discussed below will also require the international community to consider whether the current LOAC is sufficient to adequately regulate their use, and where not, consider what evolutions to the LOAC are necessary.

1. Emerging Factors

Weapons technology is always advancing. The means of conducting hostilities and the methods for employment of those means will continue to develop at an incredible pace over the next few decades. Many of these future technologies, some of which are discussed below,[216] will spring from peaceful advances that greatly benefit the world at large, but when weaponized, create difficult regulatory and response problems.[217]

a. Means

The means of armed conflict generally refers to the weapon used to engage a target, whether that weapon is a rifle fired by a fighter, an explosive round fired from an artillery tube, or a bomb dropped from an aircraft. Research continues to develop weapons that are more lethal, more accurate, more survivable, and less expensive. Future weapons will develop in response to perceived needs by the military, constrained by the LOAC. This section is certainly not comprehensive, but will discuss some

215. *See, e.g.*, Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 (entered into force Mar. 5, 1970); Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, S. Treaty Doc. No.103-21, 1974 U.N.T.S. 3 [hereinafter Chemical Weapons Convention].

216. There is no way to adequately describe even a small number of the new technologies that will become a common part of future armed conflicts. *See* Blake & Imburgia, *supra* note 33, at 162–63; David Axe, *Military Must Prep Now for 'Mutant' Future, Researchers Warn*, WIRED (Dec. 31, 2012, 6:30 AM), http://www.wired.com/dangerroom/2012/12/pentagon-prepare-mutant-future/; Patrick Lin, *Could Human Enhancement Turn Soldiers Into Weapons That Violate International Law? Yes*, THE ATLANTIC, (Jan. 4, 2013), http://www.theatlantic.com/technology/print/2013/01/could-human-enhancement-turn-soldiers-into-weapons-that-violate-international-law-yes/266732/; Anna Mulrine, *Unmanned Drone Attacks and Shape-shifting Robots: War's Remote-control Future*, CHRISTIAN SCI. MONITOR (Oct. 22, 2011), http://www.csmonitor.com/USA/Military/2011/1022/Unmanned-drone-attacks-and-shape-shifting-robots-War-s-remote-control-future; Noah Schachtman, *DARPA's Magic Plan: 'Battlefield Illusions' To Mess With Enemy Minds*, WIRED (Feb. 14, 2012), http://www.wired.com/dangerroom/2012/02/darpa-magic/; Noah Schachtman, *Suicide Drones, Mini Blimps and 3D Printers: Inside the New Army Arsenal*, WIRED (Nov. 21, 2012), http://www.wired.com/dangerroom/2012/11/new-army-arsenal/; Mark Tutton, *The Future of War: Far-out Battle Tech*, CNN (Dec. 16, 2011), http://www.cnn.com/2011/12/15/tech/innovation/darpa-future-war/index.html.

217. Hoffman, *supra* note 144, at 78 ("Both cyber and bio threats are embedded in great leaps of technological progress that we would not want to give up, enabling rapid communications, dramatic productivity gains, new drugs and vaccines, richer harvests, and more. But both can also be used to harm and destroy. And both pose a particularly difficult strategic quandary: A hallmark of cyber and bio attacks is their ability to defy deterrence and elude defenses.").

of the new weapons technologies that are being developed or researched to highlight some of the areas where the LOAC will need to evolve.

i. Drones

Drones are a quickly developing technology, and their use has been widely documented.[218] In addition to the armed drones so often the topic of discussion in the media,[219] the United States is using unmanned, unmarked turboprop aircraft in places like Africa to "record full-motion video, track infrared heat patterns, and vacuum up radio and cellphone signals."[220] Drones are now a component of local law enforcement and the U.S. Federal Aviation Administration is going to pass laws regulating the use of domestic airspace for drones,[221] in anticipation of a dramatic increase in drone space requests.

As the technology continues to develop, not only would drone capabilities increase, but also drone size will significantly decrease. The United States is currently designing drones as small as caterpillars and moths that replicate flight mechanics so they can "hide in plain sight."[222] Eventually, drones will be measured in terms of nanometers and be capable of travel through the human body.[223]

In addition to decreasing the size of drones, the technology to arm these microscopic drones continues to increase. Through innovative weapons technologies,[224] genomics,[225] and other miniaturization advances, future nanodrones will be lethal and pervasive, amongst the population generally and continuously transmitting data back to the drone's controllers. Singer describes them as a "game changer" on the level with the atomic bomb.[226]

---

218. Peter Bergen & Katherine Tiedemann, *Washington's Phantom War: The Effects of the U.S. Drone Program in Pakistan*, Foreign Aff., July-Aug. 2011, at 12, 13 (2011)*; see also*, Tony Rock, *Yesterday's Laws, Tomorrow's Technology: The Laws of War and Unmanned Warfare*, 24 N.Y. Int'l L. Rev. 39, 42 (2011) (talking about the use of drones and its legal implications).

219. Bergen & Tiedemann, *supra* note 218, at 17.

220. Whitlock, *supra* note 153.

221. Wells C. Bennett, *Unmanned at Any Speed: Bringing Drones into Our National Airspace*, Brookings (Dec. 14, 2012), http://www.brookings.edu/research/papers/2012/12/14-drones-bennett.

222. Elisabeth Bumiller & Thom Shanker, *War Evolves With Drones, Some Tiny as Bugs*, N.Y. Times (June 20, 2011), at A1, *available at* http://www.nytimes.com/2011/06/20/world/20drones.html?pagewanted=all.

223. *See* Blake & Imburgia, *supra* note 33, at 180.

224. Mike Hanlon, *Recoilless Technology Provides Killer App for UAVs*, Gizmag (Dec. 11, 2006), http://www.gizmag.com/go/6590/.

225. See *infra* Part II.C.1.a.vii.

226. Interview with Peter W. Singer, *supra* note 47 ("I think the way to think about [unmanned drones] is they are a game-changer when it comes to both technology, but also war and the politics that surrounds war. This is an invention that's on the level of gunpowder or the computer or the steam engine, the atomic bomb. It's a game changer.").

Technology will also make drones accessible to many more actors than states. Currently, "for about $1,000, you can build your own version of the Raven drone."[227] General access to miniaturized drones will soon follow. Eventually, a disgruntled adversary or disaffected civilian will not need Samantha to carry the virus to the President, but a microdrone with the ability to inject the virus into the President's system.

ii. Cyber

In recent surveys by *Foreign Policy*, cyber capabilities were viewed as the most dangerous of emerging capabilities.[228] Like drones, cyber operations have been written about extensively,[229] including the new Tallinn Manual, which gives guidance on the application of LOAC to cyber operations in armed conflict.[230] As mentioned above, many nations are developing cyber capabilities,[231] and some speculate that cyber operations will become such a part of future conflict that "eventually, the Cyber Force will need to become a separate military branch because of cyberspace's international use as a battlefield that directly affects households, corporations, universities, governments, military, and critical infrastructures."[232]

The increasing prevalence and complexity of cyber weapons is without dispute. The Stuxnet[233] malware "infected about 100,000 computers worldwide, including more than 60,000 in Iran, more than 10,000 in Indo-

227. Singer, *supra* note 11.

228. Elizabeth Dickinson, *The Future of War*, FOREIGN POL'Y, Mar.-Apr. 2011, at 64, *available at* http://www.foreignpolicy.com/articles/2011/02/22/the_future_of_war (describing that out of sixty-two top professionals, policymakers, and thinkers in the military world, twenty-four reported drones and other unmanned technologies to be the most innovative in the last decade but the highest response for the most dangerous innovation was cyberwarfare). In the 2012 survey, of seventy-six top professionals, policymakers, and thinkers in the military world, twenty-four (the majority by ten) thought that cyber operations was the area where the Chinese were catching up with U.S capabilities the fastest. Margaret Slattery, *The Future of War*, FOREIGN POL'Y, Mar.-Apr. 2012, at 78, *available at* http://www.foreignpolicy.com/articles/2012/02/27/The_Future_of_War?print=yes&hidecomments=yes&page=full.

229. COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell, eds., 2002); Eric Talbot Jensen, *Unexpected Consequences From Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145 (2003), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987553; Michael N. Schmitt, *The Principle of Distinction in 21st Century Warfare,* 2 YALE HUM. RTS. & DEV. L.J. 143 (1999); Watts, *supra* note 198, at 392; Sean Watts, Cyber Perfidy and the Law of War (unpublished manuscript)(on file with author).

230. TALLINN MANUAL *supra* note 42, at 75–202.

231. See *supra* Part II.A.1.e.

232. Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 318 (2008).

233. *See generally* Thabet, *supra* note 78.

nesia and more than 5,000 in India;"[234] the recent Flame malware[235] "exceeds all other known cyber menaces to date" according to Kapersky Lab and CrySys Lab which discovered the malware.[236]

One of the great allures of cyber weapons is their bloodless nature,[237] but ethicists worry about the impact of that on armed conflict. "With cyberweapons, a war theoretically could be waged without casualties or political risk, so their attractiveness is great—maybe so irresistible that nations are tempted to use them before such aggression is justified."[238]

Another aspect of cyber means of armed conflict is its ready access to non-state actors. Individual hackers have been known to develop sophisticated malware and cause great damage.[239] Particularly in cyber operations, one of the great dangers is reengineering or copycats.[240] As reported by David Hoffman,

> Langner [who first discovered the Stuxnet malware] warns that such malware can proliferate in unexpected ways: "Stuxnet's attack code, available on the Internet, provides an excellent blueprint and jump-start for developing a new generation of cyber warfare weapons." He added, "Unlike bombs, missiles, and guns, cyber weapons can be copied. The proliferation of cyber weapons cannot be controlled. Stuxnet-inspired weapons and weapon technology will soon be in the hands of rogue nation states, terrorists, organized crime, and legions of leisure hackers."[241]

---

234. Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE INT'L (Aug. 8, 2011, 3:04 PM), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html. Admittedly, Stuxnet was governed by the *jus ad bellum*, but similar malware will undoubtedly be used during armed conflict in the future. For an analysis of Stuxnet under the *jus in bello*, see Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842 (2012).

235. *See generally Full Analysis of Flame's Command and Control Servers*, *supra* note 79.

236. *Flame Virus Update: UK Servers Used to Control Malware*, INT'L BUS. TIMES NEWS (June 6, 2012, 1:10 PM), http://www.ibtimes.co.uk/articles/349195/20120606/flame-update-servers-shut-down.htm.

237. Blake & Imburgia, *supra* note 33, at 181–83.

238. Patrick Lin, Fritz Allhoff & Neil Rowe, *Is it Possible to Wage a Just Cyberwar?*, THE ATLANTIC (June 5, 2012, 11:24 AM), http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/.

239. David Kleinbard & Richard Richtmyer, *U.S. Catches 'Love' Virus: Quickly Spreading Virus Disables Multimedia Files, Spawns Copycats*, CNNMONEY (May 5, 2000, 11:33 PM), http://money.cnn.com/2000/05/05/technology/loveyou/.

240. Mark Clayton, *From the Man Who Discovered Stuxnet, Dire Warnings One Year Later*, CHRISTIAN SCI. MONITOR (Sept. 22, 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.

241. Hoffman, *supra* note 144.

iii. Robots

Again, the use of robots has been well documented, along with many of the issues they create.[242] Though the use of robotics has not progressed as far as that of drones and cyber operations, their use is increasing in armed conflict. As noted by Singer,

> When the U.S. military went into Iraq in 2003, it had only a handful of robotic planes, commonly called "drones" but more accurately known as "unmanned aerial systems." Today, we have more than 7,000 of these systems in the air, ranging from 48-foot-long Predators to micro-aerial vehicles that a single soldier can carry in a backpack. The invasion force used zero "unmanned ground vehicles," but now we have more than 12,000, such as the lawnmower-size Packbot and Talon, which help find and defuse deadly roadside bombs.[243]

Singer further argues that "literally thousands of Americans are alive today because of [ground and air robotic systems]. They offer precision on the battlefield never imagined before, as well as remove many dangers to our forces."[244]

Robots will be used for both lethal and less than lethal operations. Bobby Chesney speculates on the potential use of robots in capturing as opposed to killing enemies on the battlefield. He admits this possibility is "far-fetched" now, but says he "would not be surprised to learn that a robotic descent/secure/ascent technology already is in development."[245]

Retired Army Colonel Thomas Adams argues that "Future Robotic weapons 'will be too fast, too small, too numerous and will create an environment too complex for humans to direct.' . . . Innovations with robots 'are rapidly taking us to a place where we may not want to go, but probably are unable to avoid.'"[246] Testing and development continue[247] as robots take a more active role in hostilities.

---

242. *See generally* PETER W. SINGER, WIRED FOR WAR (2009).

243. P. W. Singer, *We. Robot*, SLATE (May 19, 2010), http://www.slate.com/articles/news_and_politics/war_stories/2010/05/we_robot.html; *see also* Bumiller & Shanker, *supra* note 222.

244. Steve Kanigher, *Author Talks About Military Robotics and the Changing Face of War*, LAS VEGAS SUN (Mar. 17, 2011, 2:01 AM), http://www.lasvegassun.com/news/2011/mar/17/military-robotics-and-changing-face-war/ (quoting Singer).

245. Robert Chesney, *Robot Rendition: Will There One Day Be Machines That Capture Rather Than Kill?*, LAWFARE: HARD NAT'L SEC. CHOICES (Aug. 10, 2012, 5:41 PM), http://www.lawfareblog.com/2012/08/robot-rendition-will-there-one-day-be-machines-that-capture-rather-than-kill/.

246. *Robots on Battlefield: Robotic Weapons Might be the Way of the Future, But They Raise Ethical Questions About the Nature of Warfare*, TOWNSVILLE BULL. (Austr.), Sept. 18, 2009, at 210.

247. Peter Finn, *A Future for Drones: Automated Killing*, WASH. POST (Sept. 19, 2011), http://articles.washingtonpost.com/2011-09-19/national/35273383_1_drones-human-target-military-base.

iv. Nanotechnology

Nanotechnology is "the understanding and control of matter at the nanoscale, at dimensions between approximately 1 and 100 nanometers, where unique phenomena enable novel applications."[248] As stated by Lieutenant Commander Thomas Vandermolen, "Nanoscience is in its infancy" and its "true practical potential is still being discovered."[249] It has already "exploded from a relatively obscure and narrow technical field to a scientific, economic and public phenomenon."[250]

The United States has embraced nanotechnology development. The National Nanotechnology Initiative is a federal interagency activity that was established in 2000. It is managed by the National Science and Technology Council and its goal is to "expedite[ ] the discovery, development and deployment of nanoscale science and technology to serve the public good, through a program of coordinated research and development aligned with the missions of the participating agencies."[251] Nanotechnology has already yielded amazing results[252] including "a nanoparticle that has shown 100 percent effectiveness in eradicating the hepatitis C virus in laboratory testing."[253]

Because of its potential and its infancy, the U.S. Government has passed legislation concerning nanotechnology, creating a National Nanotechnology Program (NNP) and a National Nanotechnology Coordination Office (NNCO).[254] The responsibilities of the NNCO are to

> (1) establish the goals, priorities, and metrics for evaluation for federal nanotechnology research, development, and other activities;

---

248. *Frequently Asked Questions*, NAT'L NANOTECHNOLOGY INITIATIVE, http://nano.gov/nanotech-101/nanotechnology-facts (last visited Mar. 9, 2014).

249. Thomas D. Vandermolen, *Molecular Nanotechnology and National Security*, AIR & SPACE POWER J. (Fall 2006), http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/apj06/fal06/vandermolen.html.

250. Kenneth W. Abbot, Douglas S. Sylvester & Gary E. Marchant, *Transnational Regulation of Nanotechnology: Reality or Romanticism?*, *in* INTERNATIONAL HANDBOOK ON REGULATING NANOTECHNOLOGIES (Edward Elgar ed. 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1424697.

251. *NNI Vision, Goals, and Objectives*, NAT'L NANOTECHNOLOGY INITIATIVE, http://www.nano.gov/about-nni/what/vision-goals (last visited Mar. 9, 2014).

252. *See* David Brown, *Making Steam Without Boiling Water, Thanks to Nanoparticles*, WASH. POST (Nov. 19, 2012), http://articles.washingtonpost.com/2012-11-19/national/35505658_1_steam-nanoparticles-water.

253. Dexter Johnson, *Nanoparticle Completely Eradicates Hepatitis C Virus*, SPECTRUM (July 17, 2012), http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/nanoparticle-completely-eradicates-hepatitis-c-virus?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IeeeSpectrumSemiconductors+%28IEEE+Spectrum%3A+Semiconductors%29; *accord "Nanorobot" Can be Programmed to Target Different Diseases*, PHYS.ORG (July 16, 2012), http://phys.org/news/2012-07-nanorobot-diseases.html.

254. 15 U.S.C. § 7501 (2006).

(2) invest in federal research and development programs in nanotechnology and related sciences to achieve those goals; and

(3) provide for interagency coordination of federal nanotechnology research, development, and other activities undertaken pursuant to the Program.[255]

The legislation does not mention military uses of nanotechnology, but it does task the NNP with "ensuring that ethical, legal, environmental, and other appropriate societal concerns, including the potential use of nanotechnology in enhancing human intelligence and in developing artificial intelligence which exceeds human capacity, are considered during the development of nanotechnology."[256]

Nanotechnology research is booming. The U.S. Government Accountability Office reports that:

> From fiscal years 2006 to 2010, the National Science and Technology Council reported more than a doubling of National Nanotechnology Initiative member agencies' funding for nanotechnology environmental, health, and safety (EHS) research—from approximately $38 million to $90 million. Reported EHS research funding also rose as a percentage of total na-

255. 15 U.S.C. § 7501(a) (2006).

256. 15 U.S.C. § 7501(b)(10) (2006). In response to concerns about the ethics of nanotechnology, the President's Council of Advisors on Science and Technology, in its report of April 2008 on nanotechnology, concluded:

> [T]here are no ethical concerns that are unique to nanotechnology today. That is not to say that nanotechnology does not warrant careful ethical evaluation. As with all new science and technology development, all stakeholders have a shared responsibility to carefully evaluate the ethical, legal, and societal implications raised by novel science and technology developments. However, the[re is] . . . no apparent need at this time to reinvent fundamental ethical principles or fields, or to develop novel approaches to assessing societal impacts with respect to nanotechnology.

PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., NATIONAL NANOTECHNOLOGY INITIATIVE: SECOND ASSESSMENT AND RECOMMENDATIONS OF THE NNAP (2008), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST-NNAP-NNI-Assessment-2008.pdf. Marchant, et al. have written:

> More recently, codes of conduct have emerged at the forefront of discussions to restrict the use of genetic engineering to create new biological weapons. Although there are concerns that unenforceable codes of conduct will not provide strong enough assurances against the creation of new genetically engineered biological weapons, they may play an important bridging role in providing some initial protection and governance until more formal legal instruments can be negotiated and implemented. In the same way, codes of conduct may play a similar transitional role in establishing agreed-upon principles for the military use of robots.

Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 307 (2011).

> notechnology funding over the same period, ending at about 5 percent in 2010.[257]

In addition to the United States, countries like China and Russia are also "openly investing significant amounts of money in nanotechnology."[258]

The potential benefits of nanotechnology for military purposes have quickly become apparent. As early as 2006, Forbes reported:

> The Department of Defense has spent over $1.2 billion on nanotechnology research through the National Nanotech Initiative since 2001. The DOD believed in nano long before the term was mainstream. According to Lux Research, the DOD has given grants totaling $195 million to 809 nanotech-based companies starting as early as 1988. Over the past ten years, the number of nanotech grants has increased tenfold.[259]

Blake and Imburgia believe that nanotechnology will have a profound effect on both means and methods of warfare:

> Scientists believe nanotechnology can be used to develop controlled and discriminate biological and nerve agents; invisible, intelligence gathering devices that can be used for covert activities almost anywhere in the world; and artificial viruses that can enter into the human body without the individual's knowledge. So called "nanoweapons" have the potential to create more intense laser technologies as well as self-guiding bullets that can direct themselves to a target based on artificial intelligence. Some experts also believe nanotechnology possesses the potential to attack buildings as a "swarm of nanoscale robots programmed only to disrupt the electrical and chemical systems in a building," thus avoiding the collateral damage a kinetic strike on that same building would cause.[260]

Nanotechnology also has the:

> potential to drastically enhance military operations and safety as well as homeland security. Advances in lightweight, nanoscale-engineered materials will protect soldiers on the battlefield from bullets and shrapnel while giving them extreme mobility. In case of injury, engineered bandages with embedded antimicrobial na-

257. *US Government Accountability Office Releases Report on Nanotechnology EHS Research Performance*, NANOWERK NEWS (June 22, 2012), http://www.nanowerk.com/news2/newsid=25691.php.

258. Blake & Imburgia, *supra* note 33, at 180.

259. Josh Wolfe & Dan van den Bergh, *Nanotech Takes on Homeland Terror*, FORBES (Aug. 14, 2006, 6:00 AM), http://www.forbes.com/2006/08/11/nanotech-terror-cepheid-homeland-in_jw_0811soapbox_inl.html.

260. Blake & Imburgia, *supra* note 33, at 180 (citations omitted).

> noparticles will stop deep bleeding in a matter of minutes and keep the wound free from infection.[261]

Recently, French scientists "report[ed] the first attempt to control the combustion and the detonation properties of a high explosive through its structure."[262]

Nanotechnology is likely to improve the strength and longevity of machinery,[263] advance stealth technology,[264] allow the creation of more powerful and efficient bombs,[265] and result in miniature nuclear weapons.[266] It will eventually allow for the creation of microscopic nanobots that can be controlled and used as sensors to gather information or as weapons to carry lethal toxins or genomic alterers into the bodies of humans.[267]

Nanotechnology is a development with almost unlimited applications to future armed conflict. It will make weapons smaller, more mobile, and more potent. It will provide easier, quicker, and more accurate means of collecting information. It will allow greater range, effect, and lethality. For actors with the technology, it has the potential to completely change armed conflict as we know it.

v. Directed Energy

Directed energy weapons include lasers of various magnitude, microwave and millimeter-wave weapons. These weapon systems are based on relatively new technology and almost all are still in the early stages of development. Despite this, in a report by the U.S. Defense Science Board dealing with directed energy,[268] the co-chairs lament the lack of focus on what they term a "transformational 'game changer'."[269] Though the DoD

261. Wolfe & van den Bergh, *supra* note 259.

262. *Military Nanotechnology: High Precision Explosives Through Nanoscale Structuring*, NANOWERK NEWS (June 5, 2008), http://www.nanowerk.com/spotlight/spotid=5956.php.

263. *Benefits and Applications*, NAT'L NANOTECHNOLOGY INITIATIVE, http://nano.gov/you/nanotechnology-benefits (last visited Mar. 9, 2014).

264. Clay Dillow, *Carbon Nanotube Stealth Paint Could Make Any Object Ultra-Black*, POPSCI (Dec. 6, 2011, 12:15 PM), http://www.popsci.com/technology/article/2011-12/paint-imbued-carbon-nanotubes-could-make-any-object-absorb-broad-spectrum-light.

265. Adrian Blomfield, *Russian Army 'Tests the Father of All Bombs'*, TELEGRAPH (Sept. 12, 2007, 12:01 AM), http://www.telegraph.co.uk/news/worldnews/1562936/Russian-army-tests-the-father-of-all-bombs.html.

266. *Military Uses of Nanotechnology: The Future of War*, THENANOAGE.COM, http://www.thenanoage.com/military.htm (last visited Mar. 9, 2014).

267. Scientists and the University of California, Berkeley, are already working on the Micromechanical Flying Insect Project. *Micromechanical Flying Insect*, U. CAL. BERKELEY, http://robotics.eecs.berkeley.edu/~ronf/mfi.html/index.html (last visited Mar. 9, 2014); *Nanotech Weaponry*, CENTER FOR RESPONSIBLE NANOTECHNOLOGY (Feb. 12, 2004), http://www.crnano.typepad.com/crnblog/2004/02/nanotech_weapon.html; Caroline Perry, *Mass-Production Sends Robot Insects Flying*, LIVE SCI. (Apr. 18, 2012, 5:51 PM), http://www.livescience.com/19773-mini-robot-production-nsf-ria.html.

268. DEF. SCI. BD. TASK FORCE, DIRECTED ENERGY WEAPONS (2007), *available at* http://www.acq.osd.mil/dsb/reports/ADA476320.pdf.

269. *Id.* at vii.

is working on a number of potential systems, "years of investment have not resulted in any currently high-operational laser capability."[270] There are a number of functioning systems such as the Airborne Laser and the Advanced Tactical Laser,[271] but these systems have not proven to be effective battlefield weapons to this point,[272] though the Navy recently shot down a drone with ship-mounted laser.[273]

Despite these recent setbacks, directed energy weapons of various types are likely to be deployed in future armed conflicts. They will be used as maritime, airborne, land-based, and space-based systems. They will be used both as lethal and non-lethal variants.[274]

vi. Biological Agents

Biological agents have rarely appeared in armed conflict since the early twentieth century.[275] However, "[s]ince 2001, senior members of both the Obama and Bush administrations, who have reviewed classified intelligence, have consistently placed biodefense at or near the top of the national-security agenda."[276] A 2008 report on the use of weapons of mass destruction, including biological agents, believes that "a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013" and that "terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon."[277] Though such an attack has not materialized, the concern about such capability is still valid as evidenced by the fact that the FBI has recently established a Biological Countermeasures Unit that monitors the growing Do-It-Yourself Biology

---

270. *Id.*

271. Blake & Imburgia, *supra* note 33, at 177.

272. DEF. SCI. BD. TASK FORCE, *supra* note 268, at 21–29.

273. Spencer Ackerman, *Watch the Navy's New Ship-Mounted Laser Shoot Cannon Kill a Drone*, WIRED (Apr. 8, 2013), http://www.wired.com/dangerroom/2013/04/laser-warfare-system/.

274. *See generally* DEF. SCI. BD. TASK FORCE, *supra* note 268; Fritz Allhof, *Why Does International Law Restrict Nonlethal Weapons More Than Deadly Ones?*, SLATE (Nov. 13, 2012), http://www.slate.com/articles/technology/future_tense/2012/11/nonlethal_weapons_and_the_law_of_war.html.

275. 137 nations are parties to the Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65 [hereinafter Gas Protocol], and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, T.I.A.S. No. 8062; *see* Stefan Riedel, *Biological Warfare and Bioterrorism: A Historical Review*, 17 BAYLOR U. MED. CENTER PROCEEDINGS 400 (2004).

276. Wil S. Hylton, *How Ready are We for Bioterrorism?*, N.Y. TIMES (Oct. 26, 2011), http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all.

277. BOB GRAHAM ET AL., WORLD AT RISK: THE REPORT OF THE COMMISSION ON THE PREVENTION OF WMD PROLIFERATION AND TERRORISM, xv (2008), *available at* http://www.absa.org/leg/WorldAtRisk.pdf.

(DIYbio) movement.[278] The general consensus is that although the United States has made progress in its biodefenses, we are far from being adequately prepared.[279]

Recent advances in laboratory technology have allowed access to these horrific weapons to a much more general audience. Brett Giroir, former Director at the Defense Advanced Research Projects Agency (DARPA) argues that

> [w]hat took me three weeks in a sophisticated laboratory in a top-tier medical school 20 years ago, with millions of dollars in equipment, can essentially be done by a relatively unsophisticated technician. . . . A person at a graduate-school level has all the tools and technologies to implement a sophisticated program to create a bioweapon.[280]

Michael Daly writes that "there is already information in public databases that could be used to generate highly pathogenic biological warfare agents,"[281] and "biohacker communities have popped up around the globe, with hundreds of do-it-yourself biologists testing their experimental prowess."[282]

In addition to increased access, the methods of contamination make biological agents catastrophically dangerous. As Wil Hylton argues,

> The specter of a biological attack is difficult for almost anyone to imagine. It makes of the most mundane object, death: a doorknob, a handshake, a breath can become poison. Like a nuclear bomb, the biological weapon threatens such a spectacle of horror—skin boiling with smallpox pustules, eyes blackened with anthrax lesions, the rotting bodies of bubonic plagues—that it can seem the province of fantasy or nightmare or, worse, political manipulation.[283]

---

278. *See* Todd Kuiken, *DIYbio: Low Risk, High Potential*, THE SCIENTIST (Mar. 1, 2013), http://www.the-scientist.com/?articles.view/articleNo/34443/title/DIYbio—Low-Risk—High-Potential/; *On Guard Against WMD*, FBI (Feb. 21, 2012), http://www.fbi.gov/news/stories/2012/february/wmd_022112.

279. Wil S. Hylton, *How Ready are We for Bioterrorism?*, N.Y. TIMES, (Oct. 26, 2011), http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all.

280. *Id.*

281. Michael J. Daly, *The Emerging Impact of Genomics on the Development of Biological Weapons: Threats and Benefits Posed by Engineered Extremophiles*, 21 CLINICS IN LABORATORY MED. 620, 621 (2001), *available at* http://www.usuhs.mil/pat/deinococcus/FrontPage_DR_Web_work/Pages/Lab_info/Daly_papers/clinicsLabMedicineVol21No3.pdf.

282. Hanno Charisius et al., *Becoming Biohackers: Learning the Game*, BBC FUTURE (Jan. 22, 2013), http://www.bbc.com/future/story/20130122-how-we-became-biohackers-part-1.

283. Hylton, *supra* note 276.

In combination with advances in nanotechnology, biological agents become even more deadly. As Immanuel has written, "the application of nanobiotechnology for engineering biological weapons opens pathways for an entirely new class of biology based nanoweapons. They could be self-replication or non-replicating, remotely operable and extremely destructive."[284]

Biological agents also pose some unique problems for deterrence and interdiction. Graham Allison, the founding Dean of Harvard's John F. Kennedy School of Government and a leading expert on nuclear proliferation, argues that biological terrorism presents some problems even more difficult than nuclear terrorism:

> Nuclear terrorism is a preventable catastrophe, and the reason it's preventable is because the material to make a nuclear bomb can't be made by terrorists. But in the bio case—oh, my God! Can I prevent terrorists from getting into their hands anthrax or other pathogens? No! Even our best efforts can't do that. I think the amazing thing is that one hasn't seen more bioterrorism, given the relative ease of making a bioweapon and the relative difficulty of defending.[285]

The combination of increasing accessibility, the difficulty of detection and interdiction, and the potentially catastrophic nature of biological weapons makes them a very appealing weapon for not only terrorists, but also for nation-states. Despite current legal prohibitions, biological weapons will remain a possible (and likely) weapon in armed conflict.

vii. Genomics

Genomics is the "study of genes and their function."[286] The rapid advances in genomics[287] have had a multitude of benefits for modern medicine and science in general. The costs are rapidly decreasing and accessibility rapidly increasing.

> A couple of decades ago, it took three years to learn how to clone and sequence a gene, and you earned a PhD in the process. Now, thanks to ready-made kits you can do the same in less than three days . . . [T]he cost of sequencing DNA has plummeted, from

284. Gifty Immanuel, *Biotechnology by Bioterrorism: Implications for Clinical Medicine, Biotechnology*, 12 BIOTECHNOLOGY 1, 4 (2007), *available at* http://www.eolss.net/Sample-Chapters/C17/E6-58-11-18.pdf.

285. Hylton, *supra* note 276 (quoting Graham Allison).

286. *Definition of Genomics*, MEDICINENET.COM, http://www.medterms.com/script/main/art.asp?articlekey=23242 (last visited Mar. 9, 2014).

287. Hoffman, *supra* note 144, at 78 ("One thing is certain: The technology for probing and manipulating life at the genetic level is accelerating. . . . But the inquiry itself highlighted the rapid pace of change in manipulating biology. Will rogue scientists eventually learn how to use the same techniques for evil?").

> about $100,000 for reading a million letters, or base pairs, of DNA code in 2001, to around 10 cents today.[288]

However, calls for controls on genetic research and development are increasing.[289]

Some scientists and concerned advocates argue for caution and restraint because "vulnerability arises from the relative ease with which this digital genetic code can be accessed, translated, and incorporated into conventional genetic technologies."[290] Machi and McNeill state that:

> In today's market it costs just a few thousand dollars to design a custom DNA sequence, order it from a manufacturer, and within a few weeks receive the DNA in the mail. Since select agents are currently not defined by their DNA sequences, terrorists can actually order subsets of select agent DNA and assemble them to create entire pathogens.[291]

They similarly estimate that "by 2020 malefactors will have the ability to manipulate genomes in order to engineer new bioterrorism weapons."[292]

The range of nefarious possibilities through the use of genes is very broad. As proposed at the beginning of this article, stealth viruses could be introduced covertly through agricultural infestation or nanobots into the genomes of a given population, and then triggered later by a signal.[293] "Bionanobots might be designed that, when ingested from the air by humans, would assay DNA codes and self-destruct in an appropriate place (probably the brain) in those persons whose codes had been program-

---

288. Charisius et al., *supra* note 282.

289. *See* Brian Vastag, *Environmental Groups Call for Tighter Regulation of 'Extreme Genetic Engineering,'* WASH. POST (Mar. 13, 2012), http://articles.washingtonpost.com/2012-03-13/national/35447443_1_synthetic-biology-environmental-groups-synthetic-organisms.

290. Daly, *supra* note 281, at 620; *see also* Anthony C. Littrell, *Biological Weapons of Mass Destruction: The Present and Future Threat*, CONFRONTING TERRORISM, 2002, at 339, *available at* http://digitalcorpora.org/corp/nps/files/govdocs1/065/065912.pdf; Melinda Willis, *Dangers of Genetically Engineered Weapons*, ABC NEWS (Oct. 5, 2011), http://abcnews.go.com/Health/story?id=117204&page=1#.T-3ze44zzbx.

291. Ethel Machi & Jena Baker McNeil, *New Technologies, Future Weapons: Gene Sequencing and Synthetic Biology*, HOMELAND SECURITY 2020, at 1 (Aug. 24 2010), *available at* http://thf_media.s3.amazonaws.com/2010/pdf/wm2986.pdf.

292. *Id.*; according to Paul Hansen's review, Jeffery Lockwood's book, *Six-Legged Soldiers*, describes how insects have been used in war over the last 100,000 years and suggests some possibilities for genomics and insects in the future. Paul Hansen, *Six-Legged Soldiers: Using Insects as Weapons of War by Jeffery A. Lockwood*, 13 J. MILITARY & STRATEGIC STUD. 140 (2009), *available at* http://jmss.org/jmss/index.php/jmss/article/viewFile/375/395. Lockwood also details "the possibility of future human-made genomic infused mosquito weapons in North America," specifically "the potential of insects to be used in future conflicts; terrorist attacks with crop destroying beetles, fireflies as natural guardians against biological attack, or cyborgs used for bomb detection based on the body of a cockroach as the ultimate indestructible and mobile platform." *Id.*

293. Mae-Wan Ho, *GM & Bio-Weapons in the Post-Genomics Era*, INSTITUTE OF SCIENCE IN SOCIETY (Apr. 30, 2002), http://www.i-sis.org.uk/gmbiopost.php.

med."[294] The genomic material could be designed to cause a wide array of results "including death, incapacitation, [and] neurological impairment."[295]

Some domestic legal restrictions are beginning to appear.[296] But the field of genomics and its potential weaponization is still new and difficult to accurately project or regulate. Even with this limited amount of information, it raises some important impacts on the LOAC that will be discussed below.

b. Methods

The method of targeting is most often a matter of tactics where the commander decides how and when to employ a weapon system. Commanders and individuals must not only concern themselves with the weapon they are using, but also with the way in which they are using it. Advancing technology allows weapons to be employed in creative ways that raise interesting legal issues.

i. Latent Attacks

Perhaps one of the most feared methods of attack is the latent attack. This type of attack is characterized by the placing or embedding of some weapon in a place or position where it will not be triggered until signaled sometime in the future or activated by some future action. Some latent attacks may even be triggered by the victim himself. As mentioned above in relation to genomics and biological weapons, latent attacks are a fertile area for development of stealth viruses and similar weapons. "The concept of a stealth virus is a cryptic viral infection that covertly enters human cells (genomes) and then remains dormant for an extended time. However, a signal by an external stimulus could later trigger the virus to activate and cause disease."[297] The unique aspect of this is that the viral genetic material might be implanted into the victim far in advance by a nanobot and potentially never activated or only activated upon some signal by the attacker or some other event, either triggered by an unknowing third party or the victim himself.

---

294. John L. Petersen & Dennis M. Egan, *Small Security: Nanotechnology and Future Defense*, 8 DEF. HORIZONS, Mar. 2002, at 1, 3, *available at* http://www.carlisle.army.mil/DIME/documents/DH08.pdf.

295. Neil Davison, *Biochemical Weapons: Lethality, Technology, Development, and Policy*, BRADFORD NON-LETHAL WEAPONS RESEARCH PROJECTS (May 8, 2004), http://www.brad.ac.uk/acad/nlw/research_reports/docs/biochemical_weapons_May04.pdf (quoting J. Petro, et al., *Biotechnology: Impact on Biological Warfare and Biodefense*, 1 BIOSECURITY AND BIOTERRORISM: BIODEFENSE STRATEGY, PRACTICE, AND SCIENCE 161, 168 (2003)).

296. Charisius et al., *supra* note 282.

297. Michael J. Ainscough, *Next Generation Bioweapons: Genetic Engineering and Biological Warfare*, *in* THE GATHERING BIOLOGICAL WARFARE STORM 165, 176–77, 180 (Barry R. Schneider & Jim A. Davis eds., 2002), *available at* http://www.bibliotecapleyades.net/ciencia/ciencia_virus08.htm.

The method of implanting the attack far in advance of its likely use is not unique to biological agents and genomics. Latent computer attacks have already caused concern[298] and continue to grow in appeal. Consider the manufacture of computer components. It is certainly possible that manufacturers of computer materials could embed source code in the hardware of computer components that would trigger certain functions or operations by that computer at a future time.[299] Similarly, consider weapons or military equipment sales. As countries sell military hardware to other countries, it is entirely possible that latent code has been implanted that might affect its future function. For example, the United States sells F-16 aircraft to numerous countries around the world. It seems not only plausible, but perhaps irresponsible to not implant in the computer functions of that aircraft some computer code that will not allow the F-16 to engage aircraft that it identifies as belonging to the United States.

The ability to perform latent attacks and keep them hidden until the appropriate time is a technological question, but it seems unlikely that if the potential for such actions exists, it would not be used extensively, even against current allies, as a hedge against changing political landscapes and alliances.

ii. Camouflage

It is clear that camouflaging soldiers or military equipment is a legitimate ruse of war and raises no LOAC issues generally.[300] However, future developments will allow camouflage in a different way than used before. Prior uses of camouflage included both blending in with the natural environment and mimicking other environments.[301] For example, dressing in a camouflaged uniform allowed soldiers to blend into their environment, but the nature of the uniform was known to opposing forces. Painting vehicles to match the anticipated terrain did not change the form of the vehicle.

New technologies will use electronic sensors to "project images of the surrounding environment back onto the outside of the vehicle enabling it to merge into the landscape and evade attack."[302] Use of this type of camouflage in cities or urban environments might actually project a tank to be a civilian object such as a car. Similar technology is being developed for individuals as well.[303]

---

298. Steve Stecklow, *U.S. Nuclear Lab Removes Chinese Tech Over Security Fears*, REUTERS (Jan. 7, 2013, 3:32 PM), http://www.reuters.com/article/2013/01/07/us-huawei-alamos-idUSBRE90608B20130107.

299. *Wary of Naked Force, Israel Eyes Cyberwar on Iran*, REUTERS, (Jul. 7, 2009), http://www.ynetnews.com/articles/0,7340,L-3742960,00.html.

300. Sean Watts, *Law-of-War Perfidy*, on file with author.

301. *Id.*

302. Sean Rayment, *Invisible Tanks Could Be On Battlefield Within Five Years*, TELEGRAPH (Jan. 9, 2011, 9:30 AM), http://www.telegraph.co.uk/news/uknews/defence/8247967/Invisible-tanks-could-be-on-battlefield-within-five-years.html.

303. *See, e.g.*, Charley Cameron, *Quantum Stealth Camouflage is a Hi-Tech Invisibility Cloak*, INHABITAT (Dec. 22, 2012), http://inhabitat.com/quantum-stealth-camouflage-is-a-hi-

Other forms of "camouflage" for modern weapons might include hiding specific computers or information through making it appear to be something else,[304] or piggybacking harmful malware or biological or genetic agents on useful or benign agents. These types of methods of attack, though not new in theory, will be much more prevalent because of the nature of new technologies and weapons in future armed conflict.

2. Emerging Law

Technologically advanced means and methods of warfare will change the way armed conflict occurs. As David Ignatius comments,

> The 'laws of war' may sound like an antiquated concept in this age of robo-weapons. But, in truth, a clear international legal regime has never been more needed: It is a fact of modern life that people in conflict zones live in the perpetual cross hairs of deadly weapons. Rules are needed for targets and targeters alike.[305]

The LOAC must respond by evolving in several specific but fundamental areas. The section below will outline some of the areas where adaptation is most needed.

a. Attack

As discussed above,[306] the LOAC provisions apply most completely and forcefully only to actions that are deemed an "attack." The meaning of attack is defined in GPI as "acts of violence against the adversary, whether in offence or in defence."[307] Many operations conducted with new technologies will not reach the threshold of an attack, meaning they are not proscribed. This has already been discussed with reference to cyber operations, but it equally applies to the other means and methods dis-

---

tech-invisibility-cloak/; Damien Gayle, *The Camouflage Fabric 'That Can Make Soldiers INVISIBLE'*, DAILY MAIL (Dec. 10, 2012), http://www.dailymail.co.uk/sciencetech/article-2245935/The-camouflage-fabric-make-soldiers-INVISIBLE-Company-claims-Pentagon-backing-miracle-material.html.

304. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773 (2012).

305. Gary Marchant et al., *Nanotechnology Regulation: The United States Approach*, *in* NEW GLOBAL FRONTIERS IN REGULATION: THE AGE OF NANOTECHNOLOGY 189 (Graeme Hodge et al. eds., 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1305256; Kenneth W. Abbot et al., *supra* note 245; Kenneth W. Abbott, et al., *A Framework Convention for Nanotechnology*, 36 ENVTL. L. REP. 10931 (2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=946777; Gary E. Marchant et al., *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, UCLA J. ENVTL. L. & POL'Y (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1483910; Gary E. Marchant et al., *Risk Management Principles for Nanotechnology*, 2 NANOETHICS 43 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1020104; David Ignatius, *Dazzling New Weapons Require New Rules for War*, WASH. POST (Nov. 11, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/10/AR2010111005500.html.

306. *See supra*, Part II.B.2.a.

307. Protocol I, *supra* note 9, art. 49.1.

cussed above. For example, the use of a nanobot to infiltrate an individual's body and collect data and then transmit that data to an adversary may seem more like espionage than an attack, despite its invasive nature. Similarly, the spreading of a gene[308] that creates an allergic sensitivity to pollen may have significant effect on a fighting force, but might not be termed an act of violence.

Perhaps more vexing with respect to the LOAC definition of attack is its inability to clearly demarcate the temporal limitations on actions. Recalling the example at the beginning of this article, when does the attack occur? Is it when the virus is sent to Samantha? Is it when Samantha ingests the virus? Does Samantha attack all of her friends, associates, and unwitting accomplices by spreading the virus through proximity? Does the attack occur when the first infected person, whether Samantha or someone who has caught the virus from her, enters an area where she is proximate to the President? What about when the President actually ingests the virus? Or is it not an attack until the virus actually begins to do its genetic work on the President? If an analogy to a mine or explosive is appropriate, the attack would not occur until the virus actual began to take effect in the President. That would mean that no proportionality analysis was necessary for such an attack, since there would be no collateral damage from that specific attack. Such a conclusion does not seem to support the purposes of the LOAC in protecting non-participants from the effects of armed conflict.

Similar scenarios can be created with most future weapons that have latent effects. Computer viruses may sit resident in computer systems until activated by the attacker or victim (or third party–see below). Swarms of microrobots may cross a nation's borders and take up residence at various critical points, awaiting the activation signal to commence their operations.[309] As advancing technologies are developed that might affect future

308. With respect specifically to genetic weapons, some commentators believe that all genetic weapons are already prohibited by the provisions of the 1925 Gas Protocol, Gas Protocol, *supra* note 275, and the 1972 Biological Weapons Convention which proscribes "microbial or other biological agents, or toxins[,]" Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *supra* note 277. For example, Louise Doswald-Beck, in a presentation on the application of the LOAC to future wars, stated:

> Mention must be made of a potential new method of warfare that is already prohibited in law but that could have horrific effects if developed, namely genetic weapons. The specter of this as well as of new and obviously preliminary developments in bio-technology has already motivated States to begin negotiations for the development of verification methods for the Biological Weapons Convention.

Louise Doswald-Beck, *supra* note 2, at 44. However, this position is not universally accepted. Additionally, even if states accepted that they were limited in the use of genetic weapons and honored their obligations, those arms control conventions do not bind non-state actors and certainly wouldn't be a deterrent to terrorist organizations.

309. This scenario could also cause some reflection on the adequacy of the *jus ad bellum* under the U.N. Charter.

conflict, the LOAC will need to be ready to not only proscribe illegal behavior, but also signal in advance what kinds of behavior are prohibited.

b. Distinction and Discrimination

Article 48 of GPI embodies the foundational LOAC principle of distinction and states that "belligerents may direct their operations only against military objectives."[310] This rule is complemented by Article 51, paragraph 2 which states that "the civilian population as such, as well as individual civilians, shall not be the object of attack."[311] This rule is considered to be customary international law and binding on all nations, whether parties to the Additional Protocols or not.[312]

Discrimination in the attack, or the prohibition on indiscriminate attacks, is "an implementation of the principle of distinction"[313] and is codified in GPI, Article 51.4.[314] As discussed above, these restrictions only apply to "attacks," but even if one takes a very broad view of what constitutes an attack, the LOAC still struggles to signal effectively in the case of future weapons. For example, in the virus scenario from the beginning of the article, it appears that the lethal aspect of the virus can be and is directed at a specific military objective, and therefore not indiscriminate. Article 51.4(c) might allow one to argue that the virus was not discriminate in the attack because it was "of a nature to strike military objectives [the President in this case] and civilians or civilian objects without distinction."[315] However, the argument might be made equally convincingly that the virus did not "strike" civilians; it merely used or inconvenienced civilians.

A similar analysis can be made with cyber operations. Some have already made the argument that as a result of the use of Stuxnet by the United States, "contemporary warfare will change fundamentally" if cyber warfare is not regulated by international agreement.[316] Speaking specifically about distinction and discrimination, Patrick Lin, Fritz Allhoff, and Neil Rowe write:

---

310. Protocol I, *supra* note 9, art. 48.

311. *Id.* art. 51.2.

312. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8); 1 Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law 3 (2005), *available at* http://www.icrc.org/eng/resources/documents/publication/pcustom.htm.

313. 1 Henckaerts & Doswald-Beck, *supra* note 312, at 43.

314. Protocol I, *supra* note 9, art. 51.4.("Indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.").

315. *Id.* art. 51.4.

316. Misha Glenny, *A Weapon We Can't Control*, N.Y. Times (June 14, 2012), http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html?_r=0.

> It is unclear how discriminatory cyberwarfare can be. If victims use fixed Internet addresses for their key infrastructure systems, and these could be found by an adversary, then they could be targeted precisely. However, victims are unlikely to be so cooperative. Therefore, effective cyberattacks need to search for targets and spread the attack, but as with biological viruses, this creates the risk of spreading to noncombatants: while noncombatants might not be targeted, there are also no safeguards to help avoid them. The Stuxnet worm in 2010 was intended to target Iranian nuclear processing facilities, but it spread far beyond intended targets. Although its damage was highly constrained, its quick, broad infection through vulnerabilities in the Microsoft Windows operating system was noticed and required upgrades to antivirus software worldwide, incurring a cost to nearly everyone. The worm also inspired clever ideas for new exploits currently being used, another cost to everyone.[317]

The apparent difficulties in applying the principles of distinction and discrimination[318] to potential uses of future weapons implies that an evolved LOAC would provide better protections to victims of armed conflicts.

c. Precautions and Re-engineering

Article 57 of the GPI is titled "Precautions in Attack"[319] and requires the commander or fighter to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects"[320] and "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[321]

During the ratification process for the Protocol, there was great debate about what the term "feasible" meant.[322] Ultimately, "feasible" was generally understood "to mean that which is practicable or practicably

317. Lin et al., *supra* note 238.

318. *See* TALLINN MANUAL, *supra* note 42, at 157; Jensen, *supra* note 193, at 213–14.

319. Protocol I, *supra* note 9, arts. 57.2(a)(i)–(ii), 58.

320. *Id.* art. 57.2(a)(i).

321. *Id.* art. 57.2(a)(ii).

322. 14 Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974-1977), at 199 (1978); Jensen, *supra* note 193, at 209.

possible, taking into account the circumstances ruling at the time."[323] This is the accepted standard when considering an attack.[324]

One of the interesting aspects of many future weapons systems that is different than historical weapon systems is the ability to re-engineer these weapons. Historically, when an attacker dropped a bomb on his adversary, he did not have to think of potential uses his adversary might make of that bomb. It was destroyed amidst the heat, blast, and fragmentation of the explosion. The same is not true of many future weapons. For example, when an attacker uses a virus or computer malware, the enemy can see those weapons, recover them, analyze their composition, and then re-create or re-engineer them and reuse that weapon. This would be equivalent to the United States, after using its new stealth aircraft in the fight against Saddam Hussein in Iraq, simply landing one of the aircraft at an Iraqi airport and inviting Saddam to give the aircraft to his scientists for analysis. Viruses, computer malware, genetic material, and many other future weapon systems do not self-destroy on impact. Re-engineering has already occurred in the case of computer malware[325] and will undoubtedly continue to do so with other modern and future weapon systems.

This raises the question of whether these new technologies lead to a requirement for commanders to consider the potential effects from re-engineering as part of their attack analysis. In other words, assume a commander has the following plan. He will release a swarm of microrobots, perhaps in the form of flies, that injects the general population with a deadly but limited toxin that will only become lethal when combined with a known vaccination usually given only to military. He knows that his toxin is very discriminate in the attack, but he also knows that some enterprising geneticist might come along and reengineer his virus to affect the population more generally, having lethal effect on millions instead of one. If his discreetly targeted toxin has the ability to be re-engineered and used to kill thousands or millions, must he consider that as part of his analysis when deploying the toxin?

d. Marking

The LOAC requirement of marking and its relation to future armed conflict has been addressed earlier in relation to actors on the battle-

323. Letter from Christopher Hulse, Ambassador from the U.K. to Switz., to the Swiss Gov't (Jan. 28, 1998), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (listing the United Kingdom's reservations and declarations to Additional Protocol I, and explaining in paragraph (b) that "[t]he United Kingdom understands the term 'feasible' as used in the Protocol to mean that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"); *see also* JOINT DOCTRINE & CONCEPTS CENT., THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT 81 n. 191 (2004) (suggesting the same interpretation for the word "feasible").

324. Jensen, *supra* note 193, at 209–11.

325. Hoffman, *supra* note 144, at 80; *see* Ted Samson, *Hackers Release Decrypted Stuxnet Code—But Don't Panic*, INFOWORLD (15 Feb. 2011), http://www.infoworld.com/t/malware/hackers-release-decrypted-stuxnet-code-dont-panic-685.

field.[326] The fundamental principle is that an attacker is required to distinguish himself in the attack.[327] Similar concerns exist with relation to means and methods. Even if the actors are distinguishing themselves, to what extent is there or should there be a requirement that the weapon be distinguishable? For example, in the virus scenario, the victim state could have taken precautions had it been able to distinguish Samantha's flu-like symptoms from a potentially deadly virus. As future weapons transform from "over the horizon" to "from everywhere," the LOAC will need to provide some way for the victim to identify the attacker.

One of the more obvious examples of this is brought about by advances in camouflage, discussed above. As both vehicles and individuals use advanced technology to look like the surrounding environs, it is likely that both vehicles and fighters will take on civilian aspects. A tank that is parked amongst civilian vehicles and takes on their visual attributes may cross the line between ruse and perfidy. Is a genetically linked virus, masquerading as the common flu, significantly different? Similar concerns may exist in cyber warfare.[328]

Conclusion

The rule of law is the civilian's best bulwark not only against his own government but against those who would hold him hostage to their political objectives by threatening him with violence.[329]

When Samantha and the others to whom she has already spread the virus enter the auditorium where the President will soon be speaking and carry with them the genetically targeted virus, they will be launching the LOAC on a course it is not currently prepared to travel. It is likely that many nations are on the brink of developing similar capabilities and they will undoubtedly be used in the future.

As Professor Bobbitt states above, the rule of law is vital to protecting the victims of armed conflict from the effects of armed conflict.[330] The LOAC's role as a signaling mechanism to states and other developers of future technologies that will appear on the battlefield is vital to continuing to limit hostilities with legal proscriptions. Future changes in the places, actors and means and methods of armed conflict will stress the LOAC's ability, as currently understood and applied, to sufficiently regulate that conflict.

Now is the time to act. In anticipation of these developments, the international community needs to recognize the gaps in the current LOAC and seek solutions in advance of the situation. As the LOAC evolves to

326. *See supra*, section II.B.1.c.i.

327. Protocol I, *supra* note 9, art. 44.3.

328. Lin et al., *supra* note 238.

329. Bobbitt, *supra* note 138, at 260.

330. *See id.*

face anticipated future threats, its signaling function will help ensure that advancing technologies comply with the foundational principles of the LOAC and that future armed conflicts remain constrained by law.