

# University of Minnesota Law School Scholarship Repository

---

Minnesota Journal of International Law

---

2013

## Future War, Future Law

Eric Talbot Jensen

Follow this and additional works at: <https://scholarship.law.umn.edu/mjil>



Part of the [Law Commons](#)

---

### Recommended Citation

Talbot Jensen, Eric, "Future War, Future Law" (2013). *Minnesota Journal of International Law*. 290.  
<https://scholarship.law.umn.edu/mjil/290>

This Article is brought to you for free and open access by the University of Minnesota Law School. It has been accepted for inclusion in Minnesota Journal of International Law collection by an authorized administrator of the Scholarship Repository. For more information, please contact [lenzx009@umn.edu](mailto:lenzx009@umn.edu).

## Keynote Article

### Future War, Future Law

Eric Talbot Jensen\*

#### ABSTRACT

*Advancing technology will dramatically affect the weapons and tactics of future armed conflict, including the “places” where conflicts are fought, the “actors” by whom they are fought, and the “means and methods” by which they are fought. These changes will stress even the fundamental principles of the law of armed conflict, or LOAC. While it is likely that the contemporary LOAC will be sufficient to regulate the majority of future conflicts, the international community must be willing to evolve the LOAC in an effort to ensure these future weapons and tactics remain under control of the law.*

*Though many of these advancing technologies are still in the early stages of development and design, the time to act is now. 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 face anticipated future threats, it will help ensure that advancing technologies comply with the foundational principles of the LOAC and future armed conflicts remain constrained by law.*

-----

I would like to express my gratitude to the *Minnesota Journal of International Law* for inviting me to this

---

\* Associate Professor, Brigham Young University Law School. The author wishes to express gratitude to the staff of the *Minnesota Journal of International Law* for having the foresight to organize a symposium on such an important issue and for editorial assistance on the article. The author also expresses gratitude to Allison Arnold and Aaron Worthen for invaluable research assistance. A video recording of this speech can be found on the *Minnesota Journal of International Law's* website, [http://www.minnjil.org/?page\\_id=913](http://www.minnjil.org/?page_id=913).

symposium, and really, for having this symposium. This is a very important subject and one which, if we do not engage on now, we will miss an opportunity to really have an impact on the future of the law of armed conflict.

In a recent address, Harold Koh, the State Department Legal Advisor, said “Increasingly, we find ourselves addressing twenty-first-century challenges with twentieth-century laws.”<sup>1</sup> Mr. Koh is not the only person to espouse this belief.<sup>2</sup> The twenty-first century challenges that Mr. Koh is referring to involve rapidly advancing technologies and changing tactics that are beginning to seriously challenge even the foundational principles of the Law of Armed Conflict, or LOAC.<sup>3</sup> I would like to spend the next few minutes discussing what I think are some waning factors in future armed conflicts and the resulting waning legal norms and then attempt a brief peek into the future factors that will emerge from advancing technologies and even posit some suggestions concerning emerging legal norms.

I do this with some trepidation. As Louise Doswald-Beck stated, “Any attempt to look into the future is fraught with difficulty and the likelihood that much of it will be wrong.”<sup>4</sup> However, I believe that we are currently at a point when we can see into the future of armed conflict and project, at least to some degree, the effect of advancing technologies on armed conflict and the governing LOAC. It is likely that the

---

1. Harold Hongju Koh, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1772 (2012).

2. See Rosa Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 745 (2004); P.W. Singer, Address at the United States Naval Academy William C. Stutt Ethics Lecture: Ethical Implications of Military Robotics (Mar. 25, 2009), [http://www.au.af.mil/au/awc/awcgate/navy/usna\\_singer\\_robot\\_ethics.pdf](http://www.au.af.mil/au/awc/awcgate/navy/usna_singer_robot_ethics.pdf).

3. See Koh, *supra* note 1, at 1772.

4. Louise Doswald-Beck, *Implementation of International Humanitarian Law in Future Wars*, in 71 NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 39, 39 (Michael N. Schmitt & Leslie C. Green eds., 1998); see also Stephen Peter Rosen, *The Future of War and the American Military*, HARV. MAG., May–June 2002, at 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 (Sept. 22, 2012), <http://www.nytimes.com/interactive/2012/09/23/opinion/sunday/the-new-world.html>.

contemporary LOAC will be sufficient to regulate the majority of future conflicts, but we must be willing and able to evolve the LOAC in an effort to ensure these future weapons and tactics remain under control of the law.

Our current situation is not unlike those who met at the Lateran Council of 1139.<sup>5</sup> Tradition has it that at the council, one of the issues raised was the new invention of the crossbow.<sup>6</sup> The crossbow caused alarm for several reasons. First, it allowed killing at a distance, which was not the traditional way of combat.<sup>7</sup> Secondly, it allowed a peasant who was properly trained to kill a knight.<sup>8</sup> This combination meant that a peasant, who was traditionally of little value as a fighter, could now kill a knight, an asset of great value and a major investment in training and equipment.<sup>9</sup>

Consequently, the Council outlawed the use of the crossbow, at least when Christians were fighting each other.<sup>10</sup> Of course, that legal prohibition hardly survived the vote that was taken to sustain it.<sup>11</sup> The important point this example makes is that as we contemplate future technologies and their linkage with the law, we have to take a practical view. We cannot assume that we can merely pronounce a developing weapon or tactic as illegal and expect universal compliance.<sup>12</sup> That is not the lesson history teaches us.<sup>13</sup>

---

5. See generally Harold E. Harris, *Modern Weapons and the Law of Land Warfare*, 12 MIL. L. & L. WAR REV. 7, 9 (1973).

6. Martin van Creveld, *The Clausewitzian Universe and the Law of War*, J. CONTEMP. HIST. 403, 416 (1991).

7. *Id.*

8. *Id.*

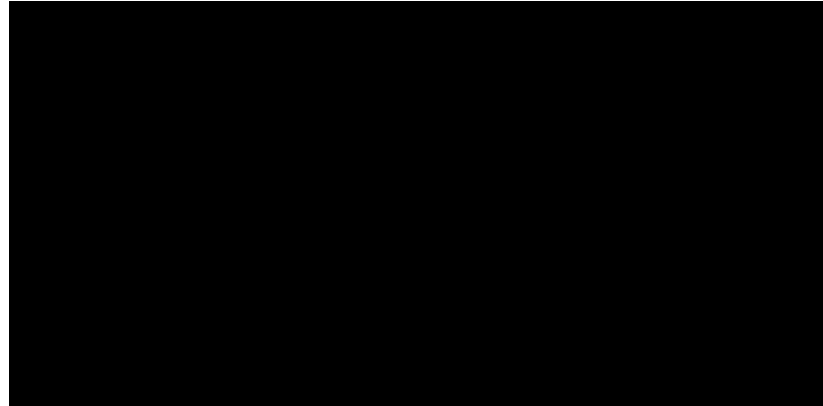
9. See *id.* ("The story of the early firearms which, by enabling a commoner to kill a knight from afar, threatened the continued existence of the medieval world, is well known.")

10. Harris, *supra* note 5, at 9; Donna Marie Verchio, *Just Say No? The SIRS Project: Well-Intentioned, But Unnecessary and Superfluous*, 51 A.F. L. REV. 183, 187 (2001).

11. See W.T. Mallison, Jr., *The Laws of War and the Juridical Control of Weapons of Mass Destruction in General and Limited Wars*, 36 GEO. WASH. L. REV. 308, 316 (1967) (discussing the continued use of the crossbow after the ban).

12. *Id.*

13. Vericho, *supra* note 10, at 187 ("The situation at that point in history is the same we observe today—no weapon has been effectively restricted or eliminated by international regulation.")



For convenience of my analysis, I will focus on the “places” where conflicts are fought, the “actors” by whom they are fought, and the “means and methods” by which they are fought. I remind you that predicting the future is not a promising line of work, and I do this hesitantly. My guess is that many of you will take issue with my characterization of what the future holds. However, I hope that even if you disagree with me, you will see the value of having the discussion and engaging on the issue of evolving the law of war in order to maintain its relevance in your version of the future.

Lest I be misunderstood, I am certainly not saying that these principles of law are no longer binding or useful in any situations throughout the world. Undoubtedly, advancing technologies which test these laws will emerge gradually and unequally among the international community. The majority of the current LOAC will continue to apply to most armed conflicts for the foreseeable future, but as technologies continue to advance, particularly among the advanced nations of the world, the LOAC will need to evolve to keep pace with innovation.

## I. PLACES

# Places

## Air, Land, Sea

Throughout history, armed conflict has taken place in “breathable air” zones—the land, the surface of the ocean, and recently the air above the land.<sup>14</sup> As the LOAC developed, these breathable air zones were concurrently being divided into areas of sovereign control,<sup>15</sup> with the exception of the high seas and the commons, such as the poles.<sup>16</sup> The effect of this was that the LOAC developed around rules governing sovereign territory and was based on presumptions about where armed conflict would occur.<sup>17</sup> These presumptions are now losing their applicability, requiring the international community to

14. See David Alexander, *Pentagon to Treat Cyberspace as “Operational Domain”*, REUTERS, July 14, 2011, available at <http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714> (identifying the “air, land and sea” as traditional areas of operational domain for the military).

15. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 707–09 (2012).

16. See generally Ron Purver, *Security and Arms Control at the Poles* 39 INT'L J. 888, 888–92 (1984) (discussing historical examples of the use of the poles for military purposes and noting that military operations in the poles were eventually banned for all countries in the first article of the Antarctic Treaty).

17. See Singer, *supra* note 2 at 14–16 (noting that “going to war” has meant the same thing for 5,000 years and the changing nature of law raises legal questions never before considered).

reconsider the validity of many LOAC provisions.<sup>18</sup>

#### A. WANING FACTORS

### Waning Factors

Breathable Air Zones

Geographic Boundaries

State Centric System

Consent

Time/Temporal Limits

I will not discuss each of my proposed waning factors, but several deserve specific mention. As I mentioned a moment ago, one of the most important waning factors in future conflict is the limitation to breathable air zones.<sup>19</sup> As I will discuss later concerning “actors,” the limitation of operating in breathable air zones is swiftly disappearing.<sup>20</sup> Miniaturization and robotics are opening areas to use that have previously not been available.<sup>21</sup> We will soon not think of the ability to breath as a limitation on our ability to operate. As technology increases, military planners will not feel constrained by human restrictions, but will find other tools that can function equally

---

18. *Id.* at 16 (suggesting one reason the LOAC needs to be reconsidered is that modern enemies know the laws and are using them to their advantage).

19. Alexander, *supra* note 14.

20. *Id.* (discussing the increased need for protection from cyber-attacks and suggesting the United States has suffered \$1 trillion in economic losses as a result of past cyber-attacks).

21. Jon Cartwright, *Rise of the Robots and the Future of War*, THE OBSERVER (Nov. 20, 2010), <http://www.guardian.co.uk/technology/2010/nov/21/military-robots-autonomous-machines> (discussing the increasing role of robots in warfare and how technological developments will likely change warfare).

well in these areas that lack breathable oxygen.<sup>22</sup>

Just as advancing technologies have opened access to new areas, existing geographic boundaries are beginning to feel pressure from scientific innovation. Armed conflict has for centuries been based on the Westphalian style demarcation of boundaries.<sup>23</sup> Crossing the boundary with your army was a sign that armed conflict had begun.<sup>24</sup> People on one side of the boundary generally associated themselves with one group of fighters and people on the other side with the other group.<sup>25</sup> This perspective on geographic boundaries is diminishing.<sup>26</sup> Individuals do not necessarily limit themselves or their emotional or patriotic attachments by the geographic boundaries which surround them.<sup>27</sup> Other means of association, such as global social networking, are lessening the perceived binding nature of geographic affiliations.<sup>28</sup>

Speaking of Westphalia, the system of state supremacy instituted by the post-Westphalian peace is quickly eroding.<sup>29</sup> States find their sovereignty threatened both politically and

---

22. Nick Hopkins, *Militarisation of Cyberspace: How the Global Power Struggle Moved Online*, THE GUARDIAN (Apr. 16, 2012), <http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle> (discussing an assertion made by the head of the US Military, General Martin Dempsey, that the United States needed to fully include space and cyberspace operations along with its traditional air-land-sea operations).

23. See generally PHILIP C. BOBBITT, *THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY* 75–143, 501–538 (2002) (detailing historical armed conflicts and describing how boundaries factored into the conflicts).

24. See Saikrishna Prakash, *Unleashing the Dogs of War: What the Constitution Means by “Declare War”*, 93 CORN. L. REV. 45, 67–77 (November 2007).

25. See Koh, *supra* note 1, at 1772 (suggesting the traditional actors in wars were blocs of countries, but the actors in future conflicts will likely be “networks of actors connected in countless tangible and intangible ways”).

26. *Id.*; Frederic Megret, *War and the Vanishing Battlefield*, 9 LOY. U. CHI. INT'L L. REV. 131, 131–33 (2011) (discussing the classic notion of a battlefield and its diminishing relevance in modern conflicts).

27. See Singer, *supra* note 2, at 11 (discussing a fundraiser held by college students at Swarthmore to take a stand against genocide in Darfur in which the proceeds were used to enter negotiations to rent drones to deploy to Sudan).

28. See Koh, *supra* note 1, at 1771–72 (“[W]e live in an age not divided by a Berlin Wall but linked by a World Wide Web.”).

29. See generally Bobbitt, *supra* note 7, at 283–342, 667–807 (discussing how the development of the market-state and increasing number of global problems such as AIDS, environmental issues, and the changing landscape of war are eroding traditional notions of state sovereignty).



territorially by a number of emerging forces, supra- and supranational in nature.<sup>30</sup> It used to be that States were the final speaker on issues considered incident to sovereignty, such as the internal and external use of force, domestic policing, treatment of citizens, and relations with peers.<sup>31</sup> State-centricity as the sole way of viewing the world is waning and being overtaken by other views that have much more traction today.<sup>32</sup> I am not arguing that the state system is going away, but that its exclusivity—and possibly its supremacy in relation to certain previously sovereign prerogatives—is evaporating.

Finally, just a word about consent; much has been said lately about consent as the basis for extraterritorial military actions. The United States continues to rely—at least in part—on consent for its prosecution of the war on terror in countries such as Yemen and Pakistan.<sup>33</sup> The question remains unanswered as to whether, if that consent were removed, the United States would cease military operations it could justify under a self-defense argument.<sup>34</sup> I believe that the U.S. is setting a precedent that will inevitably weaken the doctrine of consent and, coupled with the weakening of geographic borders, allow future military actions under various self-defense theories that will dramatically weaken the need for consent.

---

30. *Id.*

31. See Oscar Schachter, *The Decline of the Nation-State and its Implications for International Law*, 36 COLUM. J. TRANSNAT'L L. 7, 7–8 (1998).

32. *Id.* (discussing the abundance of scholarship produced by economists, businessmen, political scientists, and journalists that suggests the state-centric model is on the decline).

33. Greg Miller, *Yemen's Leader Says He Approves All Drone Strikes*, WASH. POST, Sept. 30, 2012, at A3; Adam Entous, Siobhan Gorman & Evan Perez, *U.S. Unease Over Drone Strikes*, WALL ST. J. (Sept. 26, 2012), <http://online.wsj.com/article/SB10000872396390444100404577641520858011452.html>.

34. Entous, Gorman & Perez, *supra* note 33 (noting the United States believes it has broad authority to defend itself against those who planned the attacks of September 11, 2001).

## B. WANING LAW

Waning Law

LOAC Bifurcation

Declaration of War

Sovereignty

Neutrality

In bello/ad bellum

Conflict Termination

The waning of these (and other) factors will impact the law and particularly the LOAC. As geographic boundaries lose meaning and the primacy of states wanes, a number of particular LOAC principles will face increasing attack.

The bifurcation of the LOAC between international armed conflicts, or IACs, and non-international armed conflicts, or NIACs, is already under fire.<sup>35</sup> The International Committee of the Red Cross, or ICRC,<sup>36</sup> as well as international tribunals<sup>37</sup>

35. Jensen, *supra* note 15, at 702–706.

36. See Jakob Kellenberger, ICRC President, Address at the Sixtieth Anniversary of the Geneva Conventions: Sixty Years of the Geneva Conventions: Learning from the Past to Better Face the Future (Aug. 12, 2009), <http://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-president-120809.htm>; Jakob Kellenberger, ICRC President, Address at the Follow-Up Meeting to the Sixtieth Anniversary of the Geneva Conventions: Strengthening Legal Protection for Victims of Armed Conflicts (Sept. 21, 2010), <http://www.icrc.org/eng/resources/documents/statement/ihl-development-statement-210910.htm>.

37. In addition to the quote beginning Section V, the *Tadić* Appellate Court also argued that “[i]f international law, while of course duly safeguarding the legitimate interests of States, must gradually turn to the protection of human beings, it is only natural that the [bifurcation between

and renowned scholars<sup>38</sup> have all argued that the LOAC bifurcation has lost its usefulness. In a powerful quote by the International Criminal Tribunal for the Former Yugoslavia (ICTY), the Court stated “What is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife.”<sup>39</sup> The division of the binding nature of LOAC principles, those that apply to NIACs and those that apply to IACs, is quickly becoming obsolete.<sup>40</sup>

Little needs to be said about the declaration of war, a now antiquated idea.<sup>41</sup> As Robert Turner has written, “Although conflicts between and among states continue, no state has issued a formal declaration of war [since the 1948 Arab-Israeli War].”<sup>42</sup> Similarly, the idea that conflicts terminate with a formal agreement on cessation of hostilities also lacks currency.<sup>43</sup> It is hard to imagine the United States signing a peace accord with the various iterations of al-Qaeda to signify the formal end to that conflict.<sup>44</sup>

---

IAC and NIAC] should gradually lose its weight.” Prosecutor v Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 97 (Int’l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

38. See Emily Crawford, *Unequal Before the Law: The Case for the Elimination of the Distinction between International and Non-International Armed Conflicts*, 20 LEIDEN J. INT’L L. 441, 483–84 (2007); Avril McDonald, *The Year in Review*, 2 Y.B. INT’L HUMANITARIAN L. 113, 121 (1998) (“With the increase in the number of internal and internationalised armed conflicts is coming greater recognition that a strict division of conflicts into internal and international is scarcely possible, if it ever was.”); see also Michael Reisman, Remarks at a Panel on the Application of Humanitarian Law in Noninternational Armed Conflicts (Apr. 18, 1991), in 85 AM. SOC’Y INT’L L. PROC. 83, 85 (suggesting a bifurcated system serves as “a sweeping exclusion device that permits the bulk of armed conflict to evade full international regulation”); Michael N. Schmitt, Yoram Dinstein & Charles H.B. Garraway, *The Manual on the Law of Non-International Armed Conflict: With Commentary*, INT’L INST. HUMANITARIAN L. (2006), <http://www.ihl.org/ihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf> (suggesting that laws addressing the growing problems created by NIACs need to be developed).

39. Prosecutor v Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 119 (Int’l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

40. See *supra* notes 35–39 and accompanying text.

41. ROBERT F. TURNER, *THE WAR POWERS RESOLUTION: ITS IMPLEMENTATION IN THEORY AND PRACTICE* 25 (1983).

42. *Id.*

43. Brooks, *supra* note 2, at 725–729 (noting the erosion of temporal restrictions on some international conflicts).

44. *Id.* at 726 (suggesting a peace accord between the United States and al-Qaeda is unlikely for several reasons, including the nature of the “war on

While technically not a part of the LOAC, the distinction between the applicability of the *jus ad bellum*, or the law of going to war, and the *jus in bello*, or the LOAC, is also on the wane.<sup>45</sup> Current technologies such as cyber warfare have led many to discuss the difficulty of determining when states are actually in armed conflict.<sup>46</sup> Future technologies will make that an even more difficult distinction to make as the idea of crossing a border to signal hostilities becomes increasingly anachronistic.<sup>47</sup>

Finally for this section, the law of neutrality will also become less and less applicable as geographic boundaries become more porous and states struggle to maintain the monopoly of violence. The soon-to-be-published “Tallinn Manual on the International Law Applicable to Cyber Warfare,”<sup>48</sup> in which I participated, struggled to apply the doctrines of neutrality to cyber warfare and acknowledged that the current rules need to evolve to deal effectively with future technologies.<sup>49</sup>

---

terrorism” and fact that al-Qaeda is not a state and as such may not be able to enter a formal peace agreement).

45. Eyal Benvenisti, *Rethinking the Divide Between Jus ad Bellum and Jus in Bello in Warfare Against Nonstate Actors*, 34 YALE J. INT'L L. 541, 541–42 (2009).

46. Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, in 87 INT'L L. STUD. 59, 71–72 (Raul A. “Pete” Pedrozo & Daria P. Wollschlager eds., 2011).

47. See *id.*; Megret, *supra* note 26, at 132 (noting that the notion of the traditional “battlefield” is disappearing).

48. THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 214 (Michael N. Schmitt ed.) (forthcoming March 2013).

49. *Id.* at 212, see generally Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815, 838–841 (2012).

## C. EMERGING FACTORS

## Emerging Factors

Space

Seabed

Poles

Moon

Cyber

Information

The lack of limitation to breathable air zones will move armed conflict to areas where it is currently not occurring.<sup>50</sup> Future armed conflicts will occur without respect to national borders, on the seabed, under the ground, and in space.<sup>51</sup> It will also occur across the newly recognized domain of cyberspace.<sup>52</sup> And it will occur in all of these places simultaneously.

The United States has already demonstrated in its “Global War on Terror” that the LOAC is not well prepared to regulate an armed conflict against a transnational non-state terrorist actor who does not associate itself with geographic boundaries.<sup>53</sup> The waning geographic affiliation and increasing global social affiliation which will be discussed more later will create transnational linkages between previously unconnected people

---

50. See Hopkins, *supra* note 22.

51. *Id.*

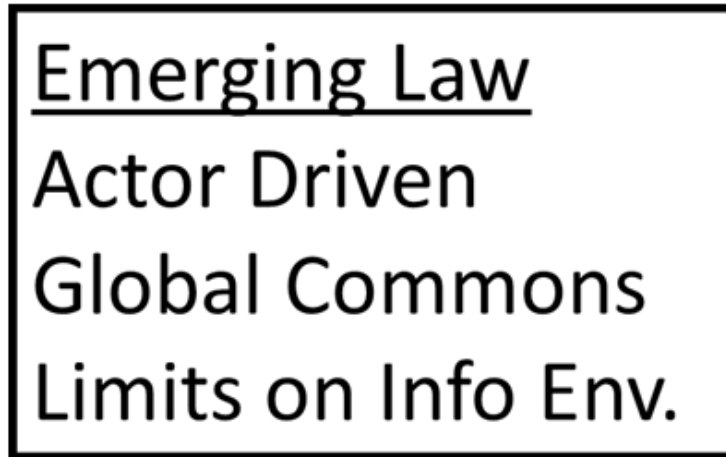
52. Alexander, *supra* note 14.

53. Megret, *supra* note 26, 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).

will make identifying the battlefield extremely difficult. Mackubin Owens has written that “multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields.”<sup>54</sup>

Few of these areas have seen armed conflict to this point.<sup>55</sup> And perhaps that will continue. However, as technology advances and these areas become available for weaponization, or at least for the placement of sensors, the temptation to militarize these areas will be irresistible.<sup>56</sup>

#### D. EMERGING LAW



Many of these individual domains just discussed are regulated by a treaty regime. For example, the Outer Space Treaty discourages military activities in space.<sup>57</sup> There is also a treaty which prohibits the use of nuclear weapons on the ocean floor or seabed.<sup>58</sup> These international agreements will become

54. Mackubin Thomas Owens, *Reflections on Future War*, 61 NAVAL WAR C. REV. 61, 71 (2008).

55. See Hopkins, *supra* note 22 (suggesting more sophisticated tools of cyber-warfare exist but have rarely been used).

56. *Id.* (suggesting the potential to conduct future military operations in space and cyberspace).

57. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies arts. 3-4, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 201.

58. Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and Ocean Floor and in the Subsoil Thereof, Feb. 11, 1971, 23 U.S.T. 701, 955 U.N.T.S. 115.

more and more difficult to apply and to comply with.<sup>59</sup>

Even if states continue to regard these rules as binding in the face of the transformation of geographic boundaries, these agreements still serve only to bind states.<sup>60</sup> The continuing diversification of actors in armed conflict will force states to consider whether they should remain militarily outside of these areas while non-state actors begin to operate within;<sup>61</sup> states will reconsider their legal obligations and take actions to establish control in these currently unmilitarized areas.<sup>62</sup> Laws might form to authorize states to exclude non-state actors from operating in these areas.<sup>63</sup> A new regime established around the global commons, ensuring state access but allowing states to enforce exclusion to non-state actors, could develop.<sup>64</sup>

Many possibilities exist for resolution here, but the new legal answer will revolve around actors, rather than geographic boundaries. The commons will be accessible by certain actors, rather than open to all.

This focus on actors and their impact on the places where armed conflict will occur in the future provides an excellent transition to the next area of emphasis—actors in future armed conflict.

---

59. See Doswald-Beck, *supra* note 4 (“In the light of such developments, States cannot continue to simply assume that the present scope of application of humanitarian law treaties suffices.”).

60. See *id.* (“Recent attempts by the government of Colombia to indicate clearly that the new treaty banning antipersonnel mines applies to non-State entities ran into difficulties when certain Western governments could not accept the proposition that such entities might have responsibilities under international law.”).

61. Mégret, *supra* note 26, at 145, 148-151.

62. See *id.* at 149, 151 (“However, it is not only ‘transnational terrorists’ who fundamentally change the nature of the battlefield, but also the states that chose to follow them on that terrain, effectively fighting ‘a war’ as if it unfolded on a ‘global battlefield.’ . . . [H]umanitarians have been tempted to extend the scope of the battlefield to make sure that as much violence as possible falls under its constraints.”).

63. See Wolff Heintchel von Heinegg, *Current Legal Issues in Maritime Operations*, 80 INT’L L. STUD. 207, 216 for precedent on exclusion zones in the context of, and questionable legality, under traditional LOAC.

64. See *id.*

## II. ACTORS

<p><b><u>Actors</u></b></p> <p>Combatants</p> <p>Civilians</p> <p>    Direct Participation in Hostilities</p> <p>Terrorists</p> <p>    Organized Armed Groups</p> <p>    Narco Terrorists</p>
---

The Geneva Conventions and Additional Protocols categorize everyone in armed conflict as either combatants or civilians.<sup>65</sup> The United States continues to assert that there is a small category of individuals who exist in the twilight between these two categories, most recently known as “unprivileged belligerents.”<sup>66</sup> Within the category of civilians are individuals who forfeit their protections by taking a “direct part in hostilities.”<sup>67</sup> As the post 9-11 “War on Terror” has progressed, this category has been understood to include organized armed groups<sup>68</sup> (e.g. terrorist organizations). There is much we could

65. Geneva Convention Relative to the Treatment of Prisoners of War, arts. 3, 4, 6, Aug. 12, 1949, U.S.T. 3316, 75 U.N.T.S. 135; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 50, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

66. See *In re Guantanamo Bay Detainee Litigation*, Respondents’ Memorandum Regarding the Government’s Detention Authority Relative to Detainees Held at Guantanamo Bay, *In Re: Guantanamo Bay Detainee Litigation*, NO. 08-0442 (D.D.C., filed March 13, 2009); *Prosecuting Terrorists; Civilian and Military Trials for GTMO and Beyond: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. 47 (2009) (statement of Michael J. Edney, Counsel, Gibson, Dunn & Crutcher, LLP).

67. Protocol I, *supra* note 65, art. 51.

68. Nils Melzer, Int’l Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 90 INT’L REV. RED CROSS 991, 1006-09



say about these categorizations, but the waters on these issues will get deeper and murkier.

#### A. WANING FACTORS

### Waning Factors

State vs. State

Combatant

Citizenship Loyalties

Reciprocity

Attribution

Rule of Law

State Monopolization of Force

As mentioned previously, the LOAC was formulated largely based on a Westphalian model of state sovereignty.<sup>69</sup> Principles such as reciprocity<sup>70</sup> and the state's monopolization of force<sup>71</sup> were foundational principles which undergird the LOAC, especially the provisions applying to actors on the battlefield. However, the notion of a battlefield populated by only organized state militaries who comply with all aspects of the LOAC is not what future battlefields will be like, if they ever were like that.<sup>72</sup> Modern battlefields are fluid and ill-defined spaces where the actors are seldom clearly identified<sup>73</sup>

---

(2008), available at <http://www.icrc.org/eng/resources/documents/article/review/review-872-p991.htm>.

69. See generally BOBBITT, *supra* note 23, at 75–143, 501–538.

70. See Doswald-Beck, *supra* note 4, at 41 (“[R]eciprocity did become important with the introduction of new rules in treaties, namely, the international law rule that parties need to be bound by the treaties in question.”).

71. Jensen, *supra* note 15, at 708, 715.

72. Kellenberger, *supra* note 36.

73. Sean Watts, *Law-of-War Perfidy* (unpublished manuscript) (on file with author.).

and often not even present at the place of attack.<sup>74</sup>

The vast majority of the armed conflicts in recent decades have not been between states, but between states and non-state actors or between two groups of non-state actors.<sup>75</sup> Advancing technologies will make this phenomena even more pronounced.<sup>76</sup> The ability of non-state actors to exert state-level violence combined with the diminishing association of individuals and groups to states will result in the waning of many factors currently prevalent in armed conflict.<sup>77</sup>

A result of the decreasing number of armed conflicts between states is that fewer and fewer conflicts occur between “combatants” and more and more involve some form of “fighters,” whether those be organized armed groups, narco-terrorists, or individuals who are directly participating in hostilities.<sup>78</sup> The changing nature of participants in armed conflict should cause a reassessment of the applicability of the current LOAC paradigm. This process has already begun with the ICRC’s issuance of the Interpretive Guidance on Direct Participation in Hostilities.<sup>79</sup> This tacit acceptance that the current understanding that the LOAC needs updated is a harbinger of things to come. Future armed conflict will undoubtedly increase the difficulty of defining actors on the battlefield.<sup>80</sup> The differentiation between fighters and non-fighters will become even more blurred as global technologies allow linkages and associations among people not contemplated in 1949 or 1977.<sup>81</sup>

In addition to the categorization of participants in armed

---

74. Megert, *supra* note 26, at 154 (“[T]his will cover crimes committed outside actual battle zones but that nonetheless display a strong element of connection to them.”).

75. Themnér, Lotta Themnér & Peter Wallensteen, 2012. *Armed Conflicts by Type, 1946-2011*, 49(4) JOURNAL OF PEACE RESEARCH 565, 566, 568 (2012), available at [http://www.per.uu.se/digitalAssets/122/122552\\_conflict\\_type\\_2011.pdf](http://www.per.uu.se/digitalAssets/122/122552_conflict_type_2011.pdf).

76. See Watts, *supra* note 46, at 61 (“Second, and related, CNA will produce a significantly expanded cast of players, creating a complex and uncontrollable multipolar environment comprising far more States and non-State actors pursuing far more disparate interests than in previous security settings. CNA are unprecedented conflict levelers.”).

77. See *id.* at 62, 73, 76 (“Either one accepts a real threat to the positive jus ad bellum’s claim to law, or one accepts very real threats to States’ security as a trade-off for preserving legal idealism.”).

78. See Jensen, *supra* note 15; Crawford, *supra* note 38, at 442.

79. See Melzer, *supra* note 68.

80. See Mégret, *supra* note 26, at 138; Watts, *supra* note 46.

81. See Mégret, *supra* note 26, at 138; Brooks, *supra* note 2, at 677.

conflict, the ability to attribute actions in armed conflict to specific actors is being significantly undermined through the use of advancing technologies. Cyber operations are a good example of this difficulty. The difficulty of attributing cyber actions has been well documented.<sup>82</sup> The ability to hide one's identity or appear to be someone else is more problematic with stand-off weapons such as cyber weapons. Future weapons will continue to make attribution difficult, forcing the international community to reevaluate the approach to attribution.

#### B. WANING LAW

### Waning Law

Combatants/Civilians

Responsible Command

Armed Attack

Status Based Targeting

Distinction

The increasing conflation of fighters and civilians will devalue the legal distinctions between combatant and civilian as categories that determine protections from targeting.<sup>83</sup> To the extent that the legal classification is useful in current armed conflicts, its utility will decrease as asymmetrical disadvantages force non-state fighters to seek anonymity while taking part in hostilities.<sup>84</sup>

The results of this conflation will undermine the current regime of status-based targeting and instead require most targeting decisions to be based on conduct.<sup>85</sup> Recent conflicts in

82. Collin Allan, *Attribution Issues in Cyberspace*, CHI.-KENT J. INT'L & COMP. L. (forthcoming May 2013).

83. Brooks *supra* note 2, at 730-31, 761.

84. See Watts, *supra* note 46, at 72-73.

85. See Brooks, *supra* note 2, at 706, 756-57 ("Thus, for instance, one's

Iraq and Afghanistan have already verified this emerging trend.<sup>86</sup> Status-based targeting will only be applicable to a very limited number of circumstances and will force states to look for other means of determining targets.<sup>87</sup>

The inability to meaningfully differentiate between actors on the battlefield will have a detrimental effect on the bedrock principle of distinction.<sup>88</sup> As states suffer devastating effects from non-attributable sources, the pressure for an evolved understanding of the principle of distinction will be great. For example, protecting a nation's critical infrastructure from computer attack<sup>89</sup> may be so important that attribution (and even individualized distinction) may become a casualty of the need to prevent significant social harm.<sup>90</sup>

---

status as a 'lawful combatant' under the Geneva Conventions hinges, as a threshold matter, not on one's substantive actions but on certain questions of form: whether one is under responsible command, whether one wears 'a fixed distinctive sign recognizable at a distance,' and whether one carries arms openly. . . . Status as a lawful combatant should not hinge on whether a person is 'commanded by a person responsible for his subordinates,' has a 'fixed distinctive sign recognizable at a distance' (e.g, a uniform or other sign by which combatants can be visually distinguished from civilians), or whether she 'carr[ies] arms openly.'").

86. *Id.* passim.

87. See Watts, *supra* note 46 ; Mégret, *supra* note 26.

88. See Mégret, *supra* note 26.

89. See Sean M. Condon, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. & TECH. 403, 421 (2007).

90. See *id.*

## C. EMERGING FACTORS

Emerging Factors

Robotics

Human “Tools”

Social Networks

Corporate Armies

“New Arms” Dealers

Cultural Uncertainty

Global Criminal Enter.

Arms/Actors Ebay

Lawfare

At the sixty-year commemoration of the Geneva Conventions, then-President of the ICRC, Jakob Kellenberger, stated that “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.”<sup>91</sup>

I divide my remarks in this area into two subcategories:

---

91. Jakob Kellenberger, President, Int’l Red Cross, Sixty Years of the Geneva Conventions and the Decades Ahead at the Conference on the Challenges for IHL posed by New Threats, New Actors and New Means and Methods of War, ICRC (Sept. 11, 2009), <http://www.icrc.org/eng/resources/documents/statement/geneva-convention-statement-091109.htm>.

emerging factors concerning influences on “existing actors” and emerging factors concerning “new actors.” I will begin with the latter category.

This Article has already alluded to the break-down of geographic boundaries and the resulting traditional associations. Modern and future social networking capabilities will allow instantaneous linkages between individuals and groups from across the globe. These “instantaneous transnational communities of interest” mean that, as Jeffrey Walker argues, “[i]t’s simply no longer necessary to have a state sponsor for an interested group of people to effect changes within the international community.”<sup>92</sup> Anthony Lake describes how these instantaneous transnational communities of interest use “technology 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.”<sup>93</sup> Philip Bobbitt has written, “The internet enabled the aggregation of dissatisfied and malevolent persons into global networks.”<sup>94</sup>

Social networking’s effects on armed conflict have already been demonstrated during the Arab Spring.<sup>95</sup> The future effects of this phenomenon will undoubtedly increase over time. Audrey Kurth Cronin draws the analogy between social networking and the *levée en masse*. She argues that it allows cyber mobilization of people across the entire globe on issues of common ideology.<sup>96</sup> The result of this expanding social networking linkage is that people will begin to view themselves less as Americans or Germans or Iranians and more as members of global ideologies created, maintained, and mobilized through social media.<sup>97</sup> The resulting cultural

---

92. 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, 329330329-30 (2001).

93. Walker, *supra* note 92, at 330 (quoting ANTHONY LAKE, SIX NIGHTMARES: REAL THREATS IN A DANGEROUS WORLD AND HOW AMERICA CAN MEET THEM 281–82 (2000)).

94. Philip C. Bobbitt, *Inter Arma Enim Non Silent Leges, View of Law and War*, 45 SUFFOLK U. L. REV. 253, 259 (2012).

95. George Griffin, *Egypt's Uprising: Tracking the Social Media Factor*, PBS.ORG (Apr. 20, 2011), [http://www.pbs.org/newshour/updates/middle\\_east/jan-june11/revsocial\\_04-19.html](http://www.pbs.org/newshour/updates/middle_east/jan-june11/revsocial_04-19.html).

96. Audrey Kurth Cronin, *Cyber-Mobilization: the New Levée en Masse*, 36 PARAMETERS 77 passim (2006).

97. See Michigan State University News, *Civilian Cyber-Warriors Not*

uncertainty will provide a means and incentive for like-minded individuals to connect and interact on areas of agreement that are not determined by geographic borders or national affiliation.

These groups will use social networks to recruit, gather resources, provide financial support, collect and pass intelligence, and create and transmit plans of action including attacks. The communications will occur far from where the effects of the communications will eventually be felt, but could conceivably have significant effects on ongoing armed conflicts.

A current example of a developing trend is the computer activist group known as “Anonymous.”<sup>98</sup> In addition to state-affiliated hacking groups and their documented participation in armed conflict,<sup>99</sup> hacktivists, who have organized themselves around a social theme or ideology, such as the members of Anonymous, have also started to take part in armed conflict.<sup>100</sup>

While many of the participants are conscious of the influence of social networking on armed conflict, advancing technology will increase the likelihood that individuals and groups will become unwitting “direct participants.” As will be discussed later, the use of future technologies such as virology and nanotechnology will allow attackers to increase the reach of their weapons by using the civilian population to propagate their weapons.<sup>101</sup> A DNA-coded virus will eventually reach its target after harmlessly passing through the population.<sup>102</sup>

Cyber attackers will use the same methodology. As with

---

*Driven by Patriotism*, MICH. ST. U. RES. (Sept. 10, 2012), <http://research.msu.edu/tags/cyber-warriors>.

98. *Anonymous*, N.Y. TIMES (Mar. 8, 2012), [http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous\\_internet\\_group/index.html](http://topics.nytimes.com/top/reference/timestopics/organizations/a/anonymous_internet_group/index.html).

99. Collin Allan, *supra* note 82; David E. Hoffman, *The New Virology: From Stuxnet to Biobombs, The Future of War by Other Means*, 185 FOREIGN POL'Y 78, 80 (2011), available at [http://www.foreignpolicy.com/articles/2011/02/22/the\\_new\\_virology?print=yes&hidecomments=yes&page=full](http://www.foreignpolicy.com/articles/2011/02/22/the_new_virology?print=yes&hidecomments=yes&page=full).

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

101. *Id.*

102. Andrew Hessel, Marc Goodman & Steven Kotler, *Hacking the President's DNA*, ATLANTIC MAG. (Nov. 2012), <http://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/>.

STUXNET,<sup>103</sup> malware will be fashioned to spread broadly through the internet but only cause damage to specific systems in a precision targeted attack.<sup>104</sup> For this to work, individual civilians and their computer systems will be a vital, though unwitting, part of the attack. Similarly, hacktivists, such as the members of Anonymous, participate along a spectrum of activity. Some may be writers of harmful code; others may be coordinators of the attack. Still others may simply leave their computers on, allowing those running the malware to slave their computers and put them to a nefarious use. In this way, they may become unwitting participants. However, to the individual or state being attacked, there will be almost no timely way of ascertaining the difference. Nations will struggle to deal with how to classify and then respond to such individuals, especially when the groups are extremely large and geographically dispersed.<sup>105</sup>

In addition to influences on actors, future technologies will create wholly new actors that are either a limited part, or not part at all, of the current paradigm.<sup>106</sup> These new actors will nonetheless emerge as important factors in future armed conflict. These include those who deal in new types of weapons—referred to as “new arms” dealers—global criminal enterprises, corporate armies and robots or autonomous weapon systems.

Advancing technology will provide a wide array of new weapons, many of which do not require state financing and organization to produce or market. In addition to computer hacktivists, bio engineers who are creating viruses and other DNA-linked tools are springing up around the world.<sup>107</sup> There is already a very lucrative market for cyber “arms.” It is

---

103. See *Factbox: What is Stuxnet*, REUTERS (Sept. 24, 2010), <http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924>.

104. 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 passim (March 2012).

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

106. See Watts, *supra* note 46.

107. Hanno Charisius, Richard Friebe & Sascha, & Karberg, *Becoming Biohackers: Learning the Game*, BBC FUTURE (Jan. 22, 2013), <http://www.bbc.com/future/story/20130122-how-we-became-biohackers-part-1>.



sourced almost exclusively by non-state actors.<sup>108</sup> A similar market for biological and genetic weapons will undoubtedly emerge.<sup>109</sup> Many of these individuals or groups will see this as a business, not as dealing in weapons. Nevertheless, in some instances, they will produce, transport, and even sometimes unleash these new types of weapons on the targets.

In addition to these relatively unorganized groups, a number of highly organized armed groups will emerge on the future battlefield. These include corporate armies, including private security companies (PSCs), and global criminal enterprises.<sup>110</sup> Recent events in Algeria<sup>111</sup> are making corporations rethink their reliance on state forces for protection of multi-billion dollar complexes. Corporate assets will continue to exist in unstable areas and even in areas of armed conflict. Businesses whose annual revenue exceeds that of the gross domestic product of the country in which they have assets are unlikely to continue to rely on state forces or police for protection if such protection fails. Rather, they will hire private security companies or raise their own armies to ensure the safety of their personnel and assets. ExxonMobil in Indonesia and Talisman Energy in Sudan have already “hired” and/or controlled national military forces to protect their business interests.<sup>112</sup> As armed conflicts ebb and flow, these corporate armies will inevitably become involved in armed conflicts, stressing the current application of the LOAC.<sup>113</sup> Corporate

---

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

109. See Charisius, *supra* note 107; Hessel, *supra* note 102.

110. See generally FROM MERCENARIES TO MARKET: THE RISE AND REGULATION OF PRIVATE MILITARY COMPANIES (Simon Chesterman & Chia Lehnhardt eds., 2007).

111. Aomar Ouali & Paul Schemm, *Al-Qaida-linked Militants Seize BP Complex in Algeria, Take Hostages Over Mali Intervention*, YAHOO! NEWS, Jan. 16, 2013, <http://news.yahoo.com/al-qaida-linked-militants-seize-bp-complex-algeria-185156149.html>.

112. Jonathan Horlick et al., *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 *Developments in the Law, International Criminal Law*, 114 HARV. L. REV. 1943, 2025, 2029–30 (2001).

113. See generally FROM MERCENARIES TO MARKET, *supra* note 110; Eric Talbot Jensen, *Combatant Status: Is it Time for Intermediate Levels of Recognition for Partial Compliance*, 46 VA. J. INT'L L. 214 (2005); Christopher J. Mandernach, *Warriors Without Law: Embracing a Spectrum of Status for Military Actors*, 7 APPALACHIAN J.L. 137 (2007). Christopher J.

armies have already been implicated in “unlawful taking of property, forced labor, displacement of populations, severe damage to the environment, and the manufacture and trading of prohibited weapons.”<sup>114</sup> This trend will increase in the future.

Another emerging factor is the role played by global criminal enterprises. These would include organizations such as the narco-traffickers operating in Mexico and other parts of Central and South America.<sup>115</sup> Reports place the number of armed fighters supporting the narco-trafficking in Mexico alone at over 100,000.<sup>116</sup> This army is substantially larger than the armies involved in most recent armed conflicts.

Global criminal enterprises are also involved in other illegal activity, including money laundering, arms smuggling, counterfeiting, and the sex trade.<sup>117</sup> Criminal enterprises often have links to armed conflict because of the goods or services that they offer.<sup>118</sup> As demand for their goods increases, the number of criminal enterprises will only increase.

We have just heard a truly superb discussion on robotics and autonomous weapon systems.<sup>119</sup> I will just add a few comments of my own. I will revisit these weapons under the category of means and methods of warfare, but to the extent that robots or other similar weapons systems become autonomous, they must also be considered as actors. We have

---

114. 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 Int'l Comm. of the Red Cross, *Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises Under International Humanitarian Law* 24 (2006); Erik Mose et al., *Corporate Criminal Liability and the Rwandan Genocide*, 6 J. INT'L CRIM. JUST. 947, 973–974 (2008).

115. Carina Bergal, Note, *The Mexican Drug War: The case for a Non-International Armed Conflict Classification*, 34 FORDHAM INT'L L.J. 1042, 1066–72 (2011).

116. *Id.* at 1066.

117. John Evans, *Criminal Networks, Criminal Enterprises*, UNIV. B. C., INT'L CTR. FOR CRIMINAL LAW REFORM, at 2, <http://www.icclr.law.ubc.ca/publications/reports/netwks94.pdf> (last visited Feb. 24, 2013).

118. *Id.*

119. To review these discussions, please see other Articles in 22 MINN. J. INT'L L. (Summer 2013), as well as some articles found in 23 MINN. J. INT'L L. (forthcoming Winter 2014). To see video recordings of the discussions that took place at the 2013 Symposium, please see the *Minnesota Journal of International Law's* website, [http://www.minnjil.org/?page\\_id=913](http://www.minnjil.org/?page_id=913).

discussed both the Department of Defense's recently issued Directive titled "Autonomy in Weapon Systems,"<sup>120</sup> which says "autonomous 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,"<sup>121</sup> and the Human Rights Watch report<sup>122</sup> calling for a multilateral treaty that would "prohibit the development, production and use of fully autonomous weapons."<sup>123</sup> My personal prognostication is that fully autonomous weapon systems will absolutely make their way onto the battlefield and eventually become the predominant actors. Having been in combat, I believe that controlled and regulated use of autonomous weapons systems can provide more reliable responses in many cases than relying on human senses and decision making. I am firmly convinced it is not a matter of "if," but "when."

#### D. EMERGING LAW

### Emerging Law Merger of Status and Conduct Discrimination

We could spend much more time discussing the emerging factors that will affect the actors in future armed conflict, but let's move to a discussion of the emerging law. I will highlight two points that I think are important to this discussion: the first is the merging of status and conduct by actors, and the second is the effects on the principle of discrimination.

---

120. DEP'T OF DEF., DIRECTIVE NO. 3000.09, AUTONOMY IN WEAPON SYSTEMS (Nov. 21, 2012). This Directive followed a DoD Defense Science Board Task Force Report issued in July of 2012. DEP'T OF DEF. DEF. SCI. BOARD, THE ROLE OF AUTONOMY IN DOD SYSTEMS (July 2012), *available at* <http://www.fas.org/irp/agency/dod/dsb/autonomy.pdf>.

121. DEP'T OF DEF., DIRECTIVE NO. 3000.09, AUTONOMY IN WEAPON SYSTEMS (Nov. 21, 2012).

122. 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](http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf).

123. *Id.* at 5, 46.

As alluded to previously, individuals are targeted based on either their status as combatants or fighters or on their inappropriate conduct as civilians. Emerging technologies and tactics will make states want to blur these distinctions. For example, the members of “Anonymous” who are preventing the military leadership from communicating to subordinates are likely taking a direct part in hostilities and are therefore targetable. However, if the attack is generated by thousands of slaved computers, some owned by witting participants, others by unwitting participants, what are the targeting options for the target state? Further, is the civilian recreational hacker who develops the malware or establishes the botnet targetable?

In the area of virology, is the designer of the DNA-linked virus targetable, even if he or she is just selling it to a customer? It is unclear if that individual would be a direct participant, especially if he did not know the eventual target of the viral attack. What about an organization who sells such DNA-linked viruses to the highest bidder? What about the completely unwitting carrier of the virus who is about to enter the auditorium where the President is about to speak and doesn't know that she is going to infect the President with the lethal virus?<sup>124</sup>

Transnational social networking communities present similar problems. As individuals pass along vital information, including attack plans, do they become targetable? Their counterparts in a geographically contained kinetic conflict would be. Does the fact that these interactions occur thousands of miles from the intended event and the originating group make a targeting difference?

Transitioning now to the principle of discrimination, the LOAC requires attackers to discriminate in the attack.<sup>125</sup> We could have a long discussion about what the word “attack” means with respect to these new technologies, but I will delay that to discuss the impact of new actors on the principle of discrimination. Much has already been said about the need for human discretion in the attack as it relates to autonomous weapon systems. I will add my own thoughts just to say that the requirement is that the attack is discriminate, not that a human make the decision as to whether to conduct the attack

---

124. Hessel, *supra* note 102.

125. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51, *supra* note 25, 1125 U.N.T.S. at 29.

2013]

*FUTURE WAR, FUTURE LAW*

309

or not.

We are making and using computer malware that is making the ultimate decision on discrimination in the attack. Stuxnet had been programmed to and was presumably acting on its own when it identified the computer controlling the centrifuges and then conducted the “attack” on that computer. Emerging weapon systems will increasingly be making those decisions through automated or natural processes that are based on controlled circumstances. To the extent that our current interpretation of discrimination is bothered by that, we may have to evolve that LOAC understanding. I think it is clear that autonomous weapons on the battlefield will increase, and the autonomy of those weapon systems will also increase. To the extent that we need to adjust the current understanding of discrimination in the attack, the LOAC needs to be responsive and evolve in order to ensure that these “actors” act responsibly.

### III. MEANS AND METHODS

## Means & Methods

Heat, Blast, and Fragmentation

Information Operations

Non-Lethal Weapons

Cyber Operations

Nuclear Weapons

Moving now to means and methods of warfare, since the development of gunpowder, modern conflicts have been characterized by heat, blast, and fragmentation. We have recently included some innovative means of conflict including numerous non-lethal weapon systems which have proven to be

very effective. You will also note that I have cyber operations in the category of existing means and methods, though I do not believe that states have even begun to tap into the potential cyber operations presents.

#### A. WANING FACTORS

Waning Factors  
Attack  
Heat, Blast and Fragmentation  
Limited Dispersion of Weapons

Despite the fact that all of these means and methods will continue to be a vital part of future armed conflicts, they will not maintain the role they currently have. For example, while most weapons will still likely use heat, blast, and fragmentation as the primary source of injury, the proportion of such weapons that are produced and used in any armed conflict will steadily decrease. As other weapons that use advanced technology enter the arsenal, they will provide more options to the commander and will better suit his needs. For example, if a commander had access to a DNA-linked virus that would effectively kill an enemy leader, he could avoid all the LOAC concerns such as proportionality and distinction that would be part of a targeting analysis using heat, blast, and fragmentation weapons such as a missile.

Similarly, the idea of an “attack” will wane in the face of new weapons. The meaning of attack is defined in API as “acts of violence against the adversary, whether in offence or in defence.”<sup>126</sup> This definition is mired in the armed conflict of heat, blast, and fragmentation which was characterized by violence. However, such a definition is not clear enough to adequately address the weapons of the future. Is a cyber-attack an act of violence? What about infecting someone with a virus? Certainly the victim of the DNA-linked virus is attacked, but what about the intermediate carrier who is merely infected but

---

126. *Id.* art. 49, at 25.

has no effects?

The important point this raises is that if infecting a host carrier (or a thousand host carriers) with a DNA-linked virus that has no physical effects is not an attack, the majority of the LOAC principles would not apply to that action and would not limit a commander's ability to conduct such an action. A similar analysis applies to cyber actions. Cyber operations that merely cause inconvenience are likely not attacks and can therefore potentially be targeted at civilians.<sup>127</sup> Given the underlying purposes of the LOAC, it is unlikely that this understanding of "attack" can survive these new weapon systems and will have to evolve to provide the protections expected from the LOAC.

One of the characteristics of heat, blast, and fragmentation weapons was a limited dispersal. The military has computer programs which model the blast radius of weapons to assist commanders in making a correct proportionality analysis. The limited dispersion of the weapon system is not an exact science, but it is generally discernible. This may not be true of many future weapon systems.

Stuxnet again provides an interesting perspective on this topic. Despite its creators' apparent best attempts, the malware made it onto computers that it was not intended to infect.<sup>128</sup> Though it did not have negative effects on those computers,<sup>129</sup> its dispersal was still not tightly controlled. Similar problems will occur with other future weapons systems. The inability to project the actual dispersal of some future weapons will make this a waning principle in the conduct of future armed conflict.

---

127. See THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 18, at 91–95, 133.

128. See Holger Stark, *Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War*, SPEIGEL ONLINE, Aug. 8, 2011, <http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html>.

129. Richmond, *supra* note 104, at 860–61.

## B. WANING LAW

Waning Law

“Armed Conflict”

“Use of Force”

Military Objective

Arms Control

Proportionality

Military Necessity

Unnecessary Suffering

I anticipate that my list of waning law will be quite controversial, but remember that I am not necessarily saying that these principles will disappear. My argument is that they will wane as we currently know them. For example, though it is not a LOAC principle, consider for a minute the *jus ad bellum* principle of “use of force” as used in the UN Charter. This is applicable here because presumably a use of force would be governed by the LOAC. What level of cyber operation equates to a “use of force?” There are differing views, though I think the predominant view now is the effects test initially set out by Michael Schmitt. However, like the previous discussion of “attack,” these legal terms need to evolve to maintain their currency and ability to regulate future armed conflict.

Similarly, the LOAC defining principle of “armed conflict” will wane as well. The LOAC is not triggered until there is an armed conflict. Traditionally, this required some level of hostilities.<sup>130</sup> In an era of bloodless weapons, as Blake and

130. See generally Commentary, Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 22–23 (Jean S. Pictet ed., 1960),



Imburgia call them,<sup>131</sup> is the trigger of “armed conflict” going to be clear enough to regulate conflict? When is a cyber-operation “armed?” Or the dispersion of nanobots? Or the spreading of GENOMIC altering viruses?

These weapons will also make us reconsider time-honored LOAC principles such as military objective, unnecessary suffering, and proportionality. For example, one of the potentially unanticipated consequences of Stuxnet is that it has the possibility of being reengineered and reused.<sup>132</sup> Bernhard Langner who first discovered Stuxnet 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. . . . 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.”<sup>133</sup>

The possibility of reengineering raises an interesting question about the proportionality analysis for commanders. With heat, blast, and fragmentation weapons, commanders did not have to concern themselves with the potential of the weapon being reused. However, with cyber malware such as Stuxnet, or with a DNA-linked virus, or with a genetic mutation, the malware, or virus or mutation remain and can be reengineered, reused and resold, potentially leading to significant impacts, including death and injury, on civilians who were never even implicated in the original attack. Must the commander consider this potentiality as he does his proportionality analysis prior to using the weapon? I think the LOAC does not yet provide a clear answer for that question. To the extent that experts have opinions, I have found them to differ widely.

Finally, another waning legal norm is arms control. Arms

---

available at <http://www.icrc.org/ihl.nsf/COM/375-590007?OpenDocument>.

131. 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 (2010).

132. See 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>.

133. David E. Hoffman, *supra* note 42 (quoting Ralph Langer, the German industrial control systems security expert who discovered Stuxnet).

control has been an effective means of limiting states in the production and use of certain weapons, such as chemical<sup>134</sup> or biological agents,<sup>135</sup> as well as nuclear weapons.<sup>136</sup> However, these international agreements have legally bound states but do not reach non-state actors. In an age where many new means and methods of warfare are not controlled or controllable by states, but can be created in an individual's garage<sup>137</sup> or office, arms control agreements lose much of their value. Until the international community finds a way to get individuals to agree to weapons controls and voluntarily comply, arms control agreements will have limited utility for many future weapon systems.

---

134. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, *opened for signature* Jan. 13, 1993, 3 U.N.T.S. 1974.

135. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, *opened for signature* Apr. 10, 1982, *available at* <http://www.icrc.org/ihl.nsf/FULL/450?OpenDocument>.

136. Treaty on the Non-Proliferation of Nuclear Weapons, *opened for signature* July 1, 1968, 21 U.S.T. 483 (entered into force Mar. 5, 1970).

137. 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&\\_r=0](http://www.nytimes.com/2011/10/30/magazine/how-ready-are-we-for-bioterrorism.html?pagewanted=all&_r=0).

## C. EMERGING FACTORS

Emerging Factors

Cyber Conflict

Miniaturization

Latent Attacks

Controlled Reality

Nanotechnology

Directed Energy

Robotics

U.S. Deputy Defense Secretary William J. Lynn III recently stated that “few weapons in the history of warfare, once created, have gone unused.”<sup>138</sup> This quote reinforces the point demonstrated by the Lateran Council that once a weapon or technology that can be weaponized is developed, it almost inevitably ends up on the battlefield. Specific arms control regimes have had some success in this area, but the general rule is that technology drives weapon development and those developed are eventually used in warfare.

I will start with cyber conflict. While cyber technology is not really new, its future uses leave it squarely in the category of emerging factors. The potential uses, and dangers, of cyber technology are only beginning to be understood. Cyber capabilities were viewed by top national security professionals and policymakers as the most dangerous of emerging capabilities in a recent survey conducted by *Foreign Policy*.<sup>139</sup>

138. John D. Banusiewicz, *Lynn Outlines New Cybersecurity Effort*, FED. INFO. & NEWS DISPATCH, INC., June 16, 2011.

139. See *The FP Survey: The Future of War*, FOREIGN POL’Y, Mar./Apr. 2012, [http://www.foreignpolicy.com/articles/2012/02/27/The\\_Future\\_of\\_War?print=ye](http://www.foreignpolicy.com/articles/2012/02/27/The_Future_of_War?print=ye)

Of course, the general availability of cyber means of armed conflict is part of what causes the concern. Many nations, including both China and the United States, have institutionalized their cyber forces.<sup>140</sup> A recent estimate suggests that 140 nations already have or are actively building cyber capabilities within their military.<sup>141</sup> The recent malware packages known as Stuxnet, Flame, and Red October aptly illustrate that states are already using cyber space to conduct military activities that cause harm, similar to kinetic operations.<sup>142</sup>

Additionally, non-state actors and even individuals have access to cyber weapons. Symantec estimates that Stuxnet could be created by as few as five to ten highly trained computer technicians in as little as six months.<sup>143</sup> Non-state actors have been known to develop sophisticated malware that cause great damage.<sup>144</sup>

---

s&hidecomments=yes&page=full (ranking cyberwarfare at a 4.6 on a 1-7 scale, 1 being the largest threat and 7 being the least threat); Micah Zenko, *The Future of War*, FOREIGN POL'Y, Mar./Apr. 2011, [http://www.foreignpolicy.com/articles/2011/02/22/the\\_future\\_of\\_war](http://www.foreignpolicy.com/articles/2011/02/22/the_future_of_war). (Mar./Apr.

140. See 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>; 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>; Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 96 (2009).

141. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU SCI. & TECH. L. REV. 249, 249 (2010).

142. See *STUXNET Malware Analysis Paper*, CODEPROJECT (Sep. 11, 2011), <http://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper> (explaining Stuxnet was created to sabotage Iran's nuclear program); *Full Analysis of Flame's Command and Control Servers*, SECURELIST (Sep. 17, 2012), [http://www.securelist.com/en/blog/750/Full\\_Analysis\\_of\\_Flame\\_s\\_Command\\_Control\\_servers](http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers) (explaining Flame malware, the advanced cyber-espionage tool, was a large scale campaign targeting several countries in the Middle East); *Red October Computer Virus Found*, TELEGRAPH (Jan. 14, 2013), <http://www.telegraph.co.uk/technology/news/9800946/Red-October-computer-virus-found.html> (explaining Red October focused targeting countries in eastern Europe).

143. Josh Halliday, *STUXNET Worm is the Work of a National Government Agency*, THE GUARDIAN, Sept. 24, 2010, <http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency>.

144. See David Kleinbard & Richard Richtmyer, *U.S. Catches 'Love' Virus: Quickly Spreading Virus Disables Multimedia Files, Spawns Copycats*, CNNMONEY, May 5, 2000, <http://money.cnn.com/2000/05/05>

Moving on to nanotechnology, it is “the understanding and control of matter at the nanoscale, at dimensions between approximately 1 and 100 nanometers, where unique phenomena enable novel applications.”<sup>145</sup> Nanotechnology has already proven its value.<sup>146</sup> For example, “a nanoparticle . . . has shown 100 percent effectiveness in eradicating the hepatitis C virus in laboratory testing.”<sup>147</sup> The U.S. Government Accountability Office reported:

From fiscal years 2006 to 2010, the National Science and Technology Council (NSTC) reported more than a doubling of National Nanotechnology Initiative (NNI) 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 nanotechnology funding over the same period, ending at about 5 percent in 2010.<sup>148</sup>

And the United States is not alone. China and Russia are also “openly investing significant amounts of money in nanotechnology.”<sup>149</sup>

As with other innovations, nanotechnology is well on its way to being at the forefront of military operations. Between

/technology/loveyou/ (describing how the “I Love You” virus swept through banks, securities firms, and Web companies causing damage).

145. *What it is and How it Works*, NAT’L NANOTECHNOLOGY INST., <http://nano.gov/nanotech-101> (last visited Feb. 6, 2013).

146. 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](http://articles.washingtonpost.com/2012-11-19/national/35505658_1_steam-nanoparticles-water) (“It shows you could make steam in an arctic environment.”).

147. Dexter Johnson, *Nanoparticle Completely Eradicates Hepatitis C Virus*, IEEE 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](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); see also “Nanorobot” Can be Programmed to Target Different Diseases, PHYS.ORG, July 16, 2012, <http://phys.org/news/2012-07-nanorobot-diseases.html> (explaining the programmable nature of the nanoparticle makes it useful against cancer and other viral infections).

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

149. See Blake & Imburgia, *supra* note 131, at 180.

2001 and 2006, the Department of Defense spent over \$1.2 Billion on nanotechnology research.<sup>150</sup> Blake and Imburgia argue that nanotechnology will significantly affect future weapons and warfare. They write:

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.<sup>151</sup>

Nanotechnology will also eventually produce more powerful and efficient bombs, and result in miniature nuclear weapons.<sup>152</sup> It will lead to the creation of microscopic nanobots that can act as sensors to gather information or as weapons to attack humans.<sup>153</sup> The results of nanotechnology will be

---

150. Josh Wolfe & Dan van den Bergh, *Nanotech Takes on Homeland Terror*, FORBES.COM, Aug. 14, 2006, [http://www.forbes.com/2006/08/11/nanotech-terror-cepheid-homeland-in\\_jw\\_0811soapbox\\_inl.html](http://www.forbes.com/2006/08/11/nanotech-terror-cepheid-homeland-in_jw_0811soapbox_inl.html).

151. See Blake & Imburgia, *supra* note 131, at 180.

152. *Military Uses of Nanotechnology: The Future of War*, THENANOAGE.COM, <http://www.thenanoage.com/military.htm> (last visited Feb. 7, 2013).7, 2013).

153. Scientists and the University of California, Berkeley, are already working on the Micromechanical Flying Insect Project; see *Micromechanical Flying Insect*, U.C. BERKELEY, <http://robotics.eecs.berkeley.edu/~ronf/mfi.html/index.html> (last visited Feb. 7, 2013) (describing the goal of micromechanical flying insect project is to develop a 25 mm device capable of sustained autonomous flight); *Nanotech Weaponry*, CENTER FOR RESPONSIBLE NANOTECHNOLOGY (Feb. 12, 2004), [http://www.crnano.typepad.com/crnblog/2004/02/nanotech\\_weapon.html](http://www.crnano.typepad.com/crnblog/2004/02/nanotech_weapon.html) (explaining molecular manufacturing could lead to a weapon capable of seeking and injecting toxin into unprotected humans); Caroline Perry, *Mass-Production Sends Robot Insects Flying*, LIVE SCI., Apr. 18, 2012,

2013]

*FUTURE WAR, FUTURE LAW*

319

weapons that are smaller, more mobile, and more potent; sensors that are quicker and more accurate, and platforms with greater range, effect, and lethality.

In addition to the means of warfare I have discussed, let me also discuss a method of attack—the method of latent attack. A latent attack is when a weapon of some kind is placed in position, but will not be triggered until sometime in the future. The attack may be triggered by a signal sent by the weapon's creator or even by the victim's own actions. Though possible with viruses and nanotechnology delivery systems, the classic latent attack is done via computer malware.<sup>154</sup> The application of this form of emerging warfare as it relates to sales of weapons or military equipment is significant.

To illustrate, assume the United State sells F-16 aircraft to other countries, some of which the United States is not sure will remain allies. As a precautionary measure, the aircraft engineers embed some code in the targeting system that prevents that aircraft from targeting United States aircrafts. Such a valuable capability and tactic raises interesting legal issues which I will discuss next.

#### D. EMERGING LAW

### Emerging Law

Effects

Precautions such as reverberation

Distinction

Discrimination

Emerging technology will require emerging law. There are

---

<http://www.livescience.com/19773-mini-robot-production-nsf-ria.html> (stating a new technology will soon allow clones of robotic insects to be mass produced).

154. The Los Alamos National Laboratory in New Mexico, responsible for maintaining America's arsenal of nuclear weapons, discovered its computer systems contained Chinese-made network switches which are used to manage data traffic on computer networks. See Steve Stecklow, *U.S. Nuclear Lab Removes Chinese Tech Over Security Fears*, REUTERS, Jan. 7, 2013, <http://www.reuters.com/article/2013/01/07/us-huawei-alamos-idUSBRE90608B20130107>.

two particular areas of emerging law that I will discuss and both need to evolve in order to keep pace with advancing technologies. The first emerging area of law is the principles of distinction and discrimination.

Article 48 of API states the foundational LOAC principle of distinction: belligerents may “direct their operations only against military objectives.”<sup>155</sup> API Article 51, paragraph 2 reinforces that norm: “The civilian population as such, as well as individual civilians, shall not be the object of attack.”<sup>156</sup> In contrast, the principle of discrimination, or the prohibition on indiscriminate attacks, comes from API Article 51.4, and prohibits attacks which are “not directed at a specific military object” and “those which employ a method or means of combat which cannot be directed at a specific military objective” or “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.”<sup>157</sup> The principle of discrimination is considered “an implementation of the principle of distinction.”<sup>158</sup>

Future weapons present options that are difficult to analyze under the existing law. For example, assume that the United States wants to kill a foreign enemy leader and chooses to do so by way of a DNA-linked virus. In order to get the virus into the vicinity of the enemy leader, a covert operator spreads the virus liberally in the area where the covert operator frequents. The virus will infect thousands of civilians but will only have a lethal effect on the enemy leader. I remind you, first of all, that these restrictions only apply to “attacks.” Analyzing the law, one might argue that API Article 51.4(c) would preclude the attack because it was “of a nature to strike military objectives (the enemy leader) and civilians or civilian objects without distinction.” However, one might equally make the argument that the attack did not “strike” civilians; it merely used or inconvenienced civilians. The attack ultimately discriminated when it finally exercised its lethal payload on the

---

155. See Protocol I, *supra* note 65, art. 48.

156. See *id.* art. 51.2.

157. See *id.* art. 51.4.

158. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 43 (Cambridge Univ. Press 2005), available at <http://www.icrc.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng>.



enemy leader. Is infecting the general populace a violation of distinction even though the virus is absolutely discriminating in the attack?

Jeremy Richmond made a similar analysis of the Stuxnet computer malware and concluded that had it been used during armed conflict, it would have complied with the LOAC despite its general dispersion.<sup>159</sup> Further clarity in this area of emerging technology will provide guidance to states as future technologies develop and continue to be used.

I have already introduced the idea of precautions and the potential impact of re-engineering as a factor in the commander's proportionality analysis. API Article 57 requires that commanders do "everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects"<sup>160</sup> 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."<sup>161</sup>

Does that mean that a commander cannot choose to use a weapon that can potentially be re-engineered and used again against civilians? Or does it mean that he has to weigh the likelihood of it being re-engineered and the likelihood of it being used against civilians? Or does it mean that he has to do everything feasible to prevent it from being re-engineered without having to consider the potential effects if it is?

Currently, the law is unclear as to the application of the proportionality standard to this analysis. This is another area where, as technology advances, the law should advance as well.

#### IV. CONCLUSION

Let me now conclude with a quote from David Ignatius. He stated:

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

---

159. See Richmond, *supra* 104, at 894.

160. See Protocol I, *supra* note 65, art. 57.2(a)(i).

161. See *id.* art. 57.2(a)(ii)

are needed for targets and targeters alike.<sup>162</sup>

I would add that it is not just people living in combat zones, but potentially people anywhere in the world are in the cross hairs of deadly weapons.

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 a future situation. As the LOAC evolves to face anticipated future threats, it will help ensure that advancing technologies comply with the foundational principles of the LOAC and future armed conflicts remain constrained by law.

---

162. David Ignatius, *Dazzling New Weapons Require New Rules for War*, WASH. POST, Nov. 11, 2010; see generally Gary Marchant, Douglas Sylvester & Kenneth W. Abbott, *Nanotechnology Regulation: The United States Approach*, in NEW GLOBAL FRONTIERS IN REGULATION: THE AGE OF NANOTECHNOLOGY 189 (Graeme Hodge et al. eds., 2007); 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., forthcoming); Kenneth W. Abbott, Gary E. Marchant, & Douglas J. Sylvester, *A Framework Convention for Nanotechnology*, 36 ENVTL. L. REP. 10931 (2006); Gary E. Marchant, Douglas J. Sylvester & Kenneth W. Abbott, *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, 28 UCLA J. ENVTL. L. & POL'Y. 123 (2010).

