WHY THE HURRY TO REGULATE AUTONOMOUS WEAPON SYSTEMS–BUT NOT CYBER-WEAPONS?

*Kenneth Anderson**

I. INTRODUCTION

Debates over the international legal regulation of autonomous weapon systems (AWS) range in their proposals from a total, preemptive ban to regulation under the existing process of legal weapons review as found in the law of armed conflict (LOAC).[1] Debates over the proper mechanism by which to undertake such regulation range in their proposals from a brand new treaty by which to enact a ban on such weapons, to an unfolding emergence of shared norms among states and their militaries under the processes of LOAC legal weapons review, with the possibility of some new treaty codifying those norms remaining an open question for the present time.[2] At the diplomatic level, agitation for some form of treaty has resulted in informal expert meetings at the United Nations (U.N.) in Geneva at Germany's invitation to discuss how a possible new Protocol to the existing Convention on Certain Conventional Weapons (CCW) might enshrine, in international law (for states that become party to such a protocol a ban) or else some other form of regulation short of a complete ban.[3]

The intervention offered by this brief paper is limited merely to asking two questions: (1) why the urgency to create an international treaty regime to regulate what are thus far merely hypothetical AWS?; and (2) why the urgency to create a new treaty regime for AWS (whatever its content, total ban or less sweeping regulation), given that in sharp contrast to AWS, cyber-weapons *actually* exist; have *actually* been used as weapons; and are *in fact* proliferating rapidly? Yet for all that, states show little or no appetite, as they do with AWS, to take up treaty

---

*Kenneth Anderson is professor of law at Washington College of Law, American University, Washington D.C. (kanders@wcl.american.edu). He thanks his frequent co-author on autonomous weapon systems issues, Matthew C. Waxman, for discussion of ideas in this paper, though all errors are Professor Anderson's alone. Thanks also to Duncan Hollis, all those at Temple University Beasley School of Law who helped organize its meeting on emerging weapon systems, and the participants in the meeting.

1. *See* Mary Wareham, Human Rights Watch Coordinator, Campaign to Stop Killer Robots, Statement to the UN General Assembly First Committee on Disarmament and International Security (Oct. 16, 2015) (transcript available at http://www.stopkillerrobots.org/wp-content /uploads/2015/10/KRC_StatementUNGA1_16Oct2015.pdf) (advocating for a ban on autonomous weapons); Kenneth Anderson et al., *Adapting the Law of Armed Conflict to Autonomous Weapon Systems*, 90 INT'L L. STUD. 386, 398–406 (2014) (arguing for regulation under LOAC).

2. *See, e.g.*, Anderson et al., *supra* note 1, at 398–406 (asserting that without a new treaty any new weapon system must still comply in its design and usage with LOAC and discussing the regulation of AWS under LOAC).

3. *See 2015 Meeting of Experts on Laws*, THE UNITED NATIONS OFFICE AT GENEVA, http://www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument (last visited April 9, 2016).

negotiations to address the risks that cyber-weapons and cyber-warfare pose today, in the here and now.[4]

The appetite to take up one, yet not the other is curious and puzzling. This paper examines some possible reasons for this dissimilarity of response to emerging weapon technologies. It does so mostly by comparing features of AWS and cyber-weapons and drawing certain (provisional, not proven) conclusions—takeaways—about what these features imply should be done regarding regulation by international legal processes at this point in each technology's development.

The discussion opens, however, by briefly describing what kinds of weapon systems the article means under the term "AWS;" it is a definitional prior of the paper as to what technology is under discussion here. It also seems useful to clarify two additional normative and factual priors that I bring to the table with respect to AWS and their possible regulation, so as not to confuse them with comparative discussion of AWS and cyber-weapons. One is a brief statement of my view of the normative status of AWS, as such, in the conduct of hostilities. The other is my view as to whether the weapons under discussion are, or could meaningfully be, genuinely autonomous: what does "autonomous" mean in the context of weapon systems and, indeed, does it mean anything coherent at all?

II. THREE PRIORS ABOUT AWS

A. What Kinds of Systems Are at Issue in Today's Debates Over AWS and What Is Special About Them With Regards to LOAC Weapons Review?

The weapon systems that are (or ought to be) at the center of today's debates over the regulation of autonomy do not include every weapon that might, in some abstract sense, be thought of as able to act without an immediate human action to trigger its firing. In a purely abstract way, for example, "dumb" anti-personnel landmines might be understood as "autonomous," in the minimal sense that once emplaced, they will explode in reaction to some trigger, such as a footfall, potentially long after their emplacement.[5]

In the meaning of this paper, however — and indeed, in informed discussion today — these kinds of passive systems are not regarded or debated "autonomous weapons," principally because they do not "target" or, more exactly, they do not "undertake" to target anything at all.[6] The legal regulation of such passive, automatic weapons (which include weapons other than landmines) might range from requiring restrictions on their battlefield use to outlawing them altogether as inherently indiscriminate. Whatever one's view of that, in the context of this discussion, there is nothing in their capabilities and limitations as weapons that

4. Jordan Peagler, *The Stuxnet Attack: A New Form of Warfare and the (In)applicability of Current International Law*, ARIZ. J. INT'L & COMP. L., 399, 428–29 (2014).

5. Mary A. Ferrer, *Affirming Our Common Humanity: Regulating Landmines to Protect Civilians and Children in the Developing World*, 20 HASTINGS INT'L & COMP. L. REV. 135 (1996).

6. *See id*. at 156–57, 159.

poses any special challenge to the law of weapons and legal weapons review.

By contrast, the weapon systems that matter in this discussion are those that are capable of "undertaking to target" in more than merely a passive, abstractly reactive way. That does not, by itself, make them legal systems, or systems that can be used lawfully in every battlefield environment.[7] But it does define them as AWS for purposes of this discussion because they incorporate artificial intelligence (AI).[8] The present and future capabilities of AI to *undertake* targeting in the meaning of the Department of Defense (DoD) definition of "full autonomy,"[9] — to *make* a target selection and to *undertake* to engage it with a weapon — which might or might not be sufficiently robust for any given system to comply with LOAC requirements in given environments and uses, raises questions about capabilities that do not arise with respect to passive, merely abstractly autonomous systems, such as landmines.[10]

These questions are old as far as the law of weapons is concerned, but the technology is, or at least appears to be, progressing so as to render the perennial legal questions about weapons new and unique. The AI in these systems, in combination with other elements of the technology, does raise new and unique questions with respect to their promise as well as their possible risks. The core concern about them (shared by *everyone* in the AWS debate, irrespective of whether they favor some radical, preemptive ban or instead believe they can be regulated through LOAC weapons reviews of particular systems) is not the concern exemplified by landmines, viz., they fail tests of discrimination because, in the relevant legal sense, they merely react, do not meaningfully target, and in the requisite legal sense cannot be "aimed."[11]

The fundamental weapons law concern, rather, is that such systems potentially over-promise their AI capabilities to undertake lawful targeting (as always, with respect to the particular uses and battlefield environments for which

---

7. *See* Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L SEC. J. 11 (Feb. 5, 2013, 2:07 PM), http://harvardnsj.org/wp-content/uploads/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf ("The inability of the weapon systems to distinguish bears on the legality of their use in particular circumstances . . . .").

8. *See* Kelly Cass, *Autonomous Weapons and Accountability: Seeking Solutions in the Law of War*, 48 LOY. L.A. L. REV. 1017, 1025 (2015) ("The legal fear associated with fully autonomous weapons is that, due to the robot's evolved reasoning, humans will not be able to predict the robot's actions.").

9. *See* U.S. DEP'T OF DEF., DIRECTIVE 3000.09, AUTONOMY IN WEAPON SYSTEMS 13–14 (2012) [hereinafter DOD DIRECTIVE 3000.09] (defining autonomous weapon systems); *see also* Cass, *supra* note 8, at 1024 (providing a description of fully autonomous robots).

10. *See* Cass, *supra* note 8, at 1025 (indicating that the legal fear of fully autonomous weapons stems from the fact that humans cannot always predict the weapons' effects).

11. *See* Paul J. Lightfoot, *The Landmine Review Conference: Will the Revised Landmine Protocol Protect Civilians?*, 18 FORDHAM INT'L L.J. 1526, 1530 (1995) ("Because landmines do not explode until their victims approach, a mine cannot be aimed at a specific target . . . .") (footnote omitted).

they are designed and in which they are used).[12] Put in the more general language of design in social robotics (not just weapons) these systems potentially over-elicit trust and reliance by their human users (planners of operations, operators in the field, and other human actors) beyond what they are capable of delivering in a given situation within the requirements of law.[13]

AWS in the sense of something new and unique by reason of their AI capabilities do not exist yet, it is widely agreed, at least not in the sense of the DoD definition of a "fully autonomous" weapon that, once engaged, is able to select its own targets and engage them without further human intervention.[14] Systems that in a more limited sense do exist, such as Israel's Iron Dome missle defense system[15] against rockets and missiles, or U.S. ship protection systems[16] against missile attacks (without which, it bears noting, a naval vessel and all souls aboard might be sent to the bottom in the opening naval engagement).[17] Yet for all the automation, even autonomy, they are still limited insofar as they remain "human-on-the-loop" systems—those characterized by the presence of a human operator who, in principle, can intervene to override the system's automated operation.[18]

Since these "really-existing, really-deployed" systems are designed as defenses against threats typically moving at beyond-human cognitive response speeds, they of necessity might be on-the-loop rather than in-the-loop systems—and the human operator truly "on" the system only in a limited, more decorative

---

12. *See* Michael N. Schmitt & Jeffrey S. Thurnher, *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 243–44 (2013) (discussing when autonomous weapons might be legally used on a battlefield).

13. *See* Rebecca Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 CARDOZO L. REV. 1837, 1860, 1862 (2015) (discussing the problem that humans can place too much faith in computers and explaining that even robots such as Roomba cleaning robots are autonomous).

14. *See* Schmitt & Thurnher, *supra* note 12, at 266 ("Despite potential advances in artificial intelligence, autonomous weapons systems will be unlikely to be capable of performing such subjective evaluations for the foreseeable future."); *see also* DOD DIRECTIVE 3000.09, *supra* note 9, at 13–14 (defining autonomous weapon system).

15. *See Israel Defense Forces: Iron Dome Missile Defense System*, JEWISH VIRTUAL LIBR., http://www.jewishvirtuallibrary.org/jsource/Peace/IronDome.html (last visited Apr. 11, 2016) (explaining that the Iron Dome ,missile defense system is a response to the threats that Israel faces from rockets and mortar shells fired by Palestinian terrorists in Gaza).

16. *See USS Benfold Receives First Install of Shipboard Protection System*, U.S. NAVY (Feb. 5, 2008), http://www.navy.mil/submit/display.asp?story_id=34778 (explaining that the shipboard protection system uses radar and cameras in order to identify and engage threats from high-speed seaborne craft).

17. *See, e.g.*, Schmitt & Thurnher, *supra* note 12, at 236; *MK 15 – Phalanx Close-In Weapons System (CIWS)*, U.S. NAVY (Nov. 15, 2013), http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2; John Pike, *MK 15 Phalanx Close-In Weapons System (CIWS)*, FED'N AM. SCIENTISTS (Jan. 9, 2003), http://fas.org/man/dod-101/sys/ship/weaps/mk-15.htm (describing a defense system that can automatically engage anti-ship missiles).

18. *See* William C. Marra & Sonia K. McNeil, *Understanding "The Loop": Regulating the Next Generation of War Machines*, 36 HARV. J. L. & PUB. POL'Y 1139 (2013) (explaining the loop system).

than real, way.[19] Even so, the limits of these systems' capabilities (including the cognitive limits of the on-the-loop operator, as well as the limits of the battlefield environments in which they can lawfully be used) have been evaluated systematically under the process of legal weapons review for years, at least with regards to such systems fielded by the United States or Israel.[20] In that regard, at least some weapon systems, in at least some battlefield environments, and at least for some combat uses, can be characterized as "fully autonomous" in practical operational terms (despite the person "on-the-loop").[21] This is, of course, because of the faster-than-human speeds with which they necessarily select and engage targets.[22] The legality of their use in the environments for which these types of "fully autonomous" weapons were designed and fielded is not seriously at issue.[23]

Given the actual facts of existing, arguably "autonomous" weapons, and the acceptance of their legality as well as acceptance of the process of assessing their legality under the existing law of weapons,[24] there would seem to be a heavy burden on those desiring some radical break with the existing law of weapons and its processes. What exactly in the overall, existing framework of legal weapon reviews requires such radical changes to the existing law of weapon reviews? Radical, that is, in the sense of either demanding a categorical ban on the whole category of supposedly autonomous weapons, or else insistence that new, fundamental requirements of law be grafted — vivisected, more accurately — onto LOAC ("meaningful human control," to start with) that are not already part of LOAC's fundamental principles of military necessity, discrimination, proportionality, and humanity.[25]

It is almost certainly true that the technical requirements of legal weapons

---

19. *See* Schmitt, *supra* note 7, at 13 ("[A] man in the loop is not a panacea during situations in which it may be difficult to distinguish civilians and civilian objects from combatants and military objectives.").

20. *See id*. at 4 ("U.S. forces have operated two human-supervised autonomous systems for many years . . . .").

21. *See* Schmitt & Thurnher, *supra* note 12, at 280 (indicating that humans are never really out of the loop).

22. *See* HUMAN RIGHTS WATCH & INT'L HUMAN RIGHTS CLINIC HARV. L. SCHOOL, LOSING HUMANITY: THE CASE AGAINST HUMAN ROBOTS 19 (2012), https://www.hrw.org/sites /default/files/reports/arms1112ForUpload_0_0.pdf (indicating fully autonomous weapons could process more information and faster than humans could); *see also* Schmitt & Thurnher, *supra* note 12, at 239 (indicating future computing capabilities of autonomous weapons will be much faster than today's military systems).

23. *See* Schmitt & Thurnhur, *supra* note 12, at 243–44 (describing how guns can be used both lawfully and unlawfully). As Schmitt and Thurner note, human targeting officers in U.S. forces sometimes employ sophisticated software programming to estimate likely collateral damage from the employment of a particular munition in particular circumstances, given assumptions about a variety of factors. *Id*. at 267.

24. *See id*. at 243 ("There is universal consensus that the law of armed conflict applies to autonomous weapon systems.").

25. *See* Schmitt & Thurnhur, *supra* note 12, at 280 ("Virtually every rule of the law of armed conflict reflects a balancing by States of two seminal factors—military necessity and humanitarian concerns.").

review will need (indeed might already stand in need of) adjustment to take adequate account of the performance of complex, software driven systems as well as methods of its evaluation;[26] incorporation of reliability engineering and performance/error standards measured, for example, in risk-probability terms that are not necessarily those used by military lawyers;[27] and other changes in process such as ensuring that legal weapons review is incorporated into the design requirements of the system from the outset.[28] But such evolutionary changes in legal weapons review, changing as technology advances, is nothing new in LOAC.[29] Granted that increasingly robust AI incorporated into weapon systems raises new and unique issues, it remains opaque what in the process of weapons review has shown itself to be inherently incapable of adapting and responding to change, specifically, changes in technology.

This definitional discussion of AWS and the question of what makes it special so as to supposedly require whole new ways of dealing with it has been expressed at greater length than the three remaining "priors" (below). This is on account of its centrality in the debate over whether there is anything special about AWS that would require the relatively immediate (even before the real emergence of such AWS) elaboration of new international law based on radical new norms–including by comparison to cyber-weapons and cyber-warfare.[30]

B. Normative: Rejecting the Call for a Total, Preemptive Ban on AWS, or a New Fundamental Principle of Meaningful Human Control for AWS

To state plainly my own normative views up front, I believe that calls for a total, preemptive ban by international NGO advocacy groups – the Stop Killer Robots campaign,[31] notably–are a serious mistake. A moral mistake, moreover, because such a ban would take away the possibility of utilizing technological advances (that, to be sure, might or might not come about) that might have many important benefits–improved compliance with LOAC, and lessened harm on the battlefield for both civilians and combatants. We have an affirmative moral obligation to try and wring out of advancing automation, robotic, and AI technologies whatever net benefits might be had. While those and other arguments against a total, preemptive ban will not be discussed further here, and in-depth discussion regarding those arguments can be found in another writing of mine, along with co-authors Matthew C. Waxman and Daniel Reisner.[32]

---

26. *See id*. at 270–76.

27. *See, e.g*., *id*. at 261 (stating that armies are required to select the means of warfare likely to cause the least harm to civilians and civilian objects without sacrificing military advantage).

28. Schmitt, *supra* note 7, at 28.

29. *See generally* Darren M. Stewart, *New Technology and the Law of Armed Conflict*, 87 INT'L L. STUD. 271, 284 (2011).

30. *See generally* Anderson et al., *supra* note 1.

31. *Learn*, CAMPAIGN TO STOP KILLER ROBOTS, https://www.stopkillerrobots.org/learn/ (last visited April 9, 2016).

32. *See* Anderson et al., *supra* note 1.

Similarly, for reasons explained elsewhere as well, I regard current calls to insert a new standard of "meaningful human control" with respect to AWS[33] to be either redundant, because any consequences of the concept are already part of LOAC, or else gravely inconsistent with the existing fundamental principles of LOAC.[34] If the proposed meaningful human control principle is to mean anything not already part of LOAC's four fundamental principles,[35] it would have to be because it requires something on the front end of targeting–viz., some human involvement, often justified by reference to inherent human dignity, expressed in a prohibition against being targeted entirely by a machine.[36] But this creates the possibility, and very likely near certainty, of grave inconsistency with LOAC's fundamental principles. Those fundamental principles are not solely about the protection of dignity, but rather focus on the protection of human beings on the battlefield by deliberate reference to the *effects* of weapons and every other means or methods of war. The focus of these principles is not to create some (quite possibly) new and inconsistent principle insisting, without regard for consequences, that targeting must involve a "who" and not just a "what," irrespective of what is likely to produce most discriminating and least harmful effects.[37]

---

33. For examples of those who have proposed an additional requirement of "meaningful human control" to the existing laws of war on autonomous weapons, see Bonnie Docherty, *Taking on "Killer Robots,"* JUSTSECURITY.ORG (May 23, 2014), http://justsecurity.org/10732/guest-post-killer-robots/; Jonathan Fowler, *UN Talks to Tackle Potential Killer Machines*, TIMES OF ISRAEL (May 13, 2014), http://www.timesofisrael.com/un-talks-to-tackle-potential-killer-machines/; Steve Goose, Director of the Arms Division of Human Rights Watch, Statement To the Convention on Conventional Weapons Informal Meeting of Experts on Lethal Autonomous Weapons Systems (May 13, 2014) (transcript available at http://www.hrw.org/news/2014/05/13/statement-convention-conventional-weapons-informal-meeting-experts-lethal-autonomous); *Killer Robots: UK Government Policy on Fully Autonomous Weapons*, ARTICLE 36 (Apr. 19, 2013), http://www.article36.org/weapons-review/killer-robots-uk-government-policy-on-fully-autonomous-weapons-2/; *Memorandum for delegates at the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS)*, ARTICLE 36 (May 13-16, 2014), http://www.article36.org/wp-content/uploads/2014/05/A36-CCW-May-2014.pdf.

34. Anderson et al., *supra* note 1, at 396–97.

35. GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 251–86 (2010) [hereinafter SOLIS]. The four listed principles are distinction, military necessity, unnecessary suffering, and proportionality. *Id*.

36. *See Mind the Gap: The Lack of Accountability for Killer Robots*, HUM. RTS. WATCH (Apr. 8, 2015), https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots (arguing against autonomous weapons both through the argument that the decision to kill a human being should not be left to a machine as well as the argument that AWS escape accountability).

37. *See* Schmitt, *supra* note 7, at 24; *see also* JUDGE ADVOCATE GENERAL, U.S. A.F., AFI51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES 3.1.1, 3.1.2 (2011) (providing technical legal guidance for the legal review of weapon systems, specifying the scope of legal review of weapons to encompass both specific treaty rules and customary law rules regarding the use of the weapon, and considering, even in the absence of an express prohibition, whether the weapon is of a nature to inflict superfluous injury or unnecessary suffering upon

C. "Autonomy" is Not Categorical, but is Instead a Matter of Degrees of Automation/Autonomy, and is a Matter of Autonomy With Respect to Particular Functions and Not Necessarily the Weapon System as a Whole

The debate over "autonomy" and what it means in AWS has been seriously distorted by the view that autonomy is a categorical attribute of a weapon system. It is not autonomous, or it can be semi-autonomous, or it can be fully autonomous– to use the DoD definition, which has been widely adopted by many in the AWS debate, including many in the ban campaign generally, who call for bans on "fully autonomous weapons."[38] The categorical, essentially "is" or "is not" definition is fundamentally flawed in three ways. First, it puts the analytic attention on the machine and its capabilities, as though it were somehow independent of human beings – the human beings who designed and programmed it, and the human beings who, in the case of a weapon system, determine the criteria, with greater or lesser specificity, for its target selection and the conditions of its engagement.

Second, the categorical definition treats the weapon system, the machine, as autonomous or not,[39] rather than recognizing that the "system" is always a human-machine dyad, and as a consequence, the degree of autonomy is a matter of the degree of human involvement, including at what stage that human involvement takes place.[40] Autonomy is incremental in relation to a human role that is always present, if only in the background by reason of a human designer and programmer.

Third, the categorical definition–and even a definition of autonomy in weapons that recognizes its incremental relationship to human roles in the weapon system–fails to take account of the likelihood that parts of the system, in any given design or general programming, or in any particular configuration for particular operations with particular criteria, might be more or less autonomous, independent of human involvement, with respect to one function but not others.[41] The weapon system, for example, might be autonomous with regard to targeting missiles in the air, but not so with regard to targeting human beings. It might be autonomous with regards to targeting and engagement in clear weather, but not with regards to storms or rain. The target engagement process might be autonomous, in the sense that the weapon might be guided by heat-seeking or GPS technology without direct human monitoring or intervention once fired–while the target selection process

---

combatants and whether it has the capability of being directed against specific military objectives —or if it does not, if it is of a nature that it could result in an effect on military objectives and civilians, or cause an effect on civilian objects, without distinction).

38. DOD DIRECTIVE 3000.09, *supra* note 9.

39. *Id*.

40. Paul Scharre & Michael C. Horowitz, *An Introduction to Autonomy in Weapon Systems*, 6 (CTR. FOR A NEW AM. SEC., Working Paper No. 021015, 2015), http://www.cnas.org/sites/default/files/publications-pdf/Ethical%20Autonomy%20Working%20Paper_021015_v02.pdf; *see also* Schmitt, *supra* note 7 ("[A]ll autonomous systems are supervised by human operators at some level . . . .").

41. *See* Schmitt, *supra* note 7, at 5–7 (discussing the idea that a fully autonomous system is never completely human free, either the system designer or an operator would at least have to program the system to function pursuant to specified parameters).

might require that a human being select what target lists, on which the machine will draw, are relevant to the operation in the first place. Calling something an "autonomous" weapon requires a further question, "autonomous" with respect to what function or activity?

More fundamentally, as David Mindell[42] points out in his recent book, *Our Robots, Ourselves: Robotics and the Myths of Autonomy* (Viking 2015),

> automation changes the type of human involvement required and transforms but does not eliminate it. For any apparently autonomous system, we can always find the wrapper of human control that makes it useful . . . . Every operator, when controlling his or her machine, interacts with designers and programmers who are still present inside it – perhaps through design and coding done many years before . . . . How a system is designed, by whom, ad for what purpose shapes its abilities and its relationships with the people who use it.[43]

With respect to AWS, particularly concerning accountability for its effects in some battlefield environment, the fundamental issue is not whether there is an "autonomous" machine–there is not, as Mindell says.[44] It is a question of whether our judgment as to what constitutes accountability under LOAC for the use of weapons can be satisfied in a given circumstance by human roles consisting of all or some of the system's designers and programmers.[45]

This is *not* to say that the machine is autonomous because speed of response means that a human operator likely will not be able to override it in real time–but instead that operators in battlefield engagement must necessarily rely on the machine performing without malfunction, and more crucially, on the humans who made it ready for its use. Whether that reliance is sufficient to establish accountability in the sense of the laws of war or military discipline in any given circumstance is open to debate. But it bears noting that human accountability, put onto any individual person, in any military organization is always defined, and frankly limited, by intense specialization of function and the elaborate division of

---

42. David A. Mindell is the Dibner Professor of the History of Engineering and Manufacturing, amongst other titles, at the Massachusetts Institute of Technology. *See David A. Mindell*, MASSACHUSETTS INSTITUTE OF TECHNOLOGY ENGINEERING SYSTEMS DIVISION (last visited Apr. 20, 2016), https://esd.mit.edu/Faculty_Pages/mindell/mindell.htm.

43. DAVID A. MINDELL, OUR ROBOTS, OURSELVES: ROBOTICS AND THE MYTHS OF AUTONOMY 5 (2015).

44. *Id*.

45. The roles in question relate to those determining its configurations and limits for use in particular environments as well as those putting into it intelligence information gathered quite apart from the machine or its programmers or operators to give it the basis for target selection. The roles also relate to those establishing the relationship between machine's specified selection and targeting limitations and the operation's rules of engagement. Finally, the question concerns the roles of commanders and operators using it in a given battlefield environment, including their training in its use and understanding of its capabilities and limitations, and including as well the possibility that the operationally necessary speed of response might mean that, in practical terms, they must let the machine perform as others have set it up to do. *See generally* Schmitt, *supra* note 7.

labor among humans.[46] War is an irreducibly social activity, conducted by irreducibly "corporate" actors, with the aim of making the whole greater than the sum of the parts.

The commander on the field, the pilot in the aircraft, the sailors firing the missile to a point hundreds of miles away–every one of these people depends on the quite fallible performance of other specialized individuals of whom they will frequently have no knowledge, and vice-versa.[47] The supposedly autonomous weapon system introduces no truly new element in that regard. Autonomous actions of the machine in target selection and engagement apparently leave no identifiable, individual human beings who bear real accountability for failures or mistakes, innocent or negligent—but the same is true of any complex military bureaucracy with specialized functions. The division of labor, distributing functions beyond single actors, whether human or machine, is by definition the fragmentation of responsibility.

These considerations raise serious challenges to the meaningfulness of arguments regarding bans and regulations that are premised on categorical definitions of autonomy, which ignore the system's relation to humans. Proponents of the regulatory concept of a requirement of "meaningful human control" that can slide higher or lower depending on circumstances such as the nature of the battlefield, and so on, believe that they have captured this idea of a human-machine dyad–what Mindell calls "situated autonomy."[48] What these proponents fail to acknowledge, however, is that anything relevant in the concept of "meaningful human control," including one that that takes into account a sliding scale of greater or lesser human involvement, is already captured by LOAC principles insofar as the concept looks to *effects* of weapons on the battlefield.[49] And any concept of meaningful human control that imposes new fundamental requirements as a *prior* condition of targeting, whether by a machine or anything or anyone else, independent of effects, is simply morally mistaken and deeply inconsistent with LOAC.[50]

---

46. *See* Women's International League for Peace and Freedom, *Fully Autonomous Weapons*, REACHING CRITICAL WILL, http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/7972-fully-autonomous-weapons (showing that that pinpointing accountability onto a specific individual may be nearly impossible given the nature of AWS).

47. Kenneth Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems*, HOOVER INSTITUTION, (Feb. 27, 2015), http://www.hoover.org/research/comparing-strategic-and-legal-features-cyberwar-drone-warfare-and-autonomous-weapon-systems (describing standoff systems — where the operators can be physically removed from the weapon).

48. MINDELL, *supra* note 43, at 9–10.

49. *See supra* text accompanying notes 33–35.

50. *See* SOLIS, *supra* note 35, at 251–86 (discussing the four core principles of LOAC and how they are effects focused).

III. COMPARING AWS AND CYBER-WEAPONS

A. From "Priors" to Comparisons of Weapons

The foregoing considerations discussed as priors, framing concepts about the nature of AWS, might seem a lengthy preamble to getting to the questions that this article aims to address–why a hurry to create new international law for AWS, but not a similar hurry with respect to cyber-weapons and cyber-warfare? Without the background discussion, however, the paramount questions of whether, when, or how to regulate AWS through international law mechanisms risks distortion by the misconception of an AWS as merely a machine in isolation. In reality, AWS is a dynamic human-machine dyad in which autonomy is neither static nor an attribute of the machine as such. Therefore, we now turn to the question of what comparisons can be made between AWS and cyber, armed with a more adequate understanding of what AWS means.

B. A List of Comparisons Between AWS and Cyber-Weapons

Cyber-weapons and cyber-warfare (cyber-weapons, for convenience) of course are like AWS in that they have many evolving features. The comparisons made below will not remain stable over time, as technology changes. Below, then, is a list of similarities and differences.

The starting point of comparison is that cyber-weapons *do* exist, *have* been used, and indeed are rapidly proliferating across state arsenals.[51] By contrast, AWS are still (in the relevant sense set out earlier in this discussion) a technology of the future, not a weapon of today. Cyber-weapons are an "actually existing" weapon in a way that AWS are not.

Both AWS and cyber-weapons offer the possibility of being "remote" or "standoff" systems.[52] The operator of the system in each case might be far away from the place of the attack, perhaps even a continent away.[53] It is true that an AWS, for example, might be used by a combatant as a weapon system in the same place where that person, unit, ship, aircraft, etc., is engaged in combat, but the features of autonomy might mean that it can operate in certain circumstances independently of the human operator, even if the human operator is standing next to it–in those specifically autonomous functions (selecting targets and firing its weapons) to whatever degree permitted by its capabilities and programming.[54]

---

51. *See* Gordon Corera, *Rapid escalation of the cyber-arms race*, BBC, (Apr. 29, 2015), http://www.bbc.com/news/uk-32493516 (discussing the growth of a potential cyber arms race); *see generally* Daniel Cohen & Aviv Rotbart, *The Proliferation of Weapons in Cyberspace,* 5 MILITARY AND STRATEGIC AFFAIRS 59 (May 2013).

52. Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems*, *supra* note 47. "Remote" and "Standoff" systems are synonymous, and refer to weapons systems at a remote distance from the place attacked, potentially far away from any conventional military theater of operations. *Id*.

53. *Id*.

54. *See* Schmitt, *supra* note 7, at 3–7 (discussing autonomous functions of AWS).

Autonomous operation in this way is also a form of this remoteness.

AWS is kinetic in its operation, while cyber-weapons are not.[55] However, this might not be true in all circumstances. Cyber-weapons might well have kinetic effects, at least indirectly through their actions on an adversary's cyber-controlled systems.[56] But broadly speaking, AWS act kinetically in the physical world directly, while cyber-weapons act in the cyber-sphere, though with the possibility of causing serious (at the margin potentially catastrophic) harm to physical infrastructure such as power grids, water systems and many interrelated systems, as well as harm to network systems such as financial markets, banking or government records or ledgers, or even the ability to access or operate them.[57]

Although we describe these weapons systems as "autonomous," in important ways cyber-weapons might often be even more "autonomous" in their behavior than AWS. The cyber-weapon might necessarily act in ways that, in software terms, meet the understanding of "autonomous," even the special definition of autonomy in weapons–pre-programmed, yet able to adapt its behavior to engage in its own target selection and target engagement.[58] AWS is not unique in regard to having the possibility of adaptive learning systems.

AWS are not self-replicating or self-propagating machines.[59] They do not create or re-create themselves, reproduce their physical selves, science fiction novels aside.[60] Cyber-weapons, by contrast, might be engineered to do so, depending on the design of the weapon.[61] As with biological viruses or reproducing pathogens, they might spread (by design or through unanticipated consequences) in unpredictable and potentially uncontrollable ways.[62]

Cyber-weapons are systems that target an adversary's command, control, and communications.[63] They might also be programmed to attack logistical targets,

---

55. *See* Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems, supra* note 47 (comparing AWS and cyber-weapons).

56. *See* Scott D. Applegate, *The Dawn of Kinetic Cyber*, 2013 5TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 2 (K. Podins, J. Stinssen & M. Maybaum eds., 2013), https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf (stating that kinetic cyber refers to a class that can cause direct or indirect damage or harm).

57. *Id*. at 2, 9.

58. *See* Eric Messinger, *Is it Possible to Ban Autonomous Weapons in Cyberwar?* JUST SECURITY, (Jan. 15, 2015), https://www.justsecurity.org/19119/ban-autonomous-weapons-cyberwar/ (discussing how the likely targets of cyber warfare will be run by autonomous systems).

59. *See* DOD DIRECTIVE 3000.09, *supra* note 9, at 13 (defining AWS as needing human activation and operation prior to working).

60. *Id*.

61. *See* Y.M. YUFIK, NETWORK SCIENCE AND CYBER SECURITY 76 (Robinson E. Pino, ed., June 14, 2014) (discussing how cyber-weapons can self-regulate and self-propagate).

62. *See* P. W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, 47 CASE W. RES. J. INT'L L. 79, 80 (2015), http://scholarlycommons.law.case.edu/jil/vol47/iss1/10/ (discussing a prior cyber-weapon that globally spread uncontrollably to unintended targets).

63. *See The Department of Defense Cyber Strategy*, DEP'T OF DEF. 7 (April 2015),

such as an adversary's civilian infrastructure systems, but their most direct use in conflict is against these classic military targets.[64] AWS might be designed or programmed to target any of these directly and kinetically, to be sure–but AWS might also be programmed to attack a wide variety of other military or civilian targets in the physical world, including buildings or other physical targets that are not connected to cyberspace, and so cannot be attacked with a cyber-weapon.

AWS and cyber-weapons are similar in that each relies on complex systems, and inherently non-transparent software engineering,[65] in which assessment of the systems' capabilities and limitations on the basis of its actual programming will inevitably become more difficult as the weapon passes from the hands of its designers into the hands of users, whether they are those programming its specific rules of engagement for a specific operation, or whether they are the actual human operators of the system during the engagement itself. Moreover, where the programming is not only complex, but also features machine learning, probabilistic or stochastic programming, or similar AI features, it is possible that either a cyber-weapon or an AWS might result in unpredictable, non-deterministic behavior.

Both AWS and cyber-weapons can be designed to make attribution of an attack difficult.[66] This is a consequence of remoteness, complexity, and other features.[67] That said, at least at present, cyber-weapons present far greater problems of difficulty in attributing an attack than AWS (or AWS projected to exist one day), if only because AWS operate in the physical world.[68] But both AWS and cyber-weapons have characteristics that make them useful in covert, unacknowledged, and "hybrid warfare" operations.[69]

Both AWS and cyber-weapons rely fundamentally on technologies that are, or will be, ubiquitous in the civilian world.[70] In neither case are their fundamental technologies special to "weapons."[71] This is true for AWS with respect to the three features usually taken to define a "robot" or "robotic machine" in the human social

---

http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (discussing cyber strategy against cyber threats targeted by adversaries).

64. *See id*. at 2 (discussing expected cyber attacks against infrastructure and military networks).

65. Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems*, *supra* note 47 (detailing how AWS and cyber-weapons rely on both civilian and military networks).

66. *Id*.

67. *Id*.

68. *See* Corinne Iozzio, *The 10 Most Mysterious Cyber Crimes*, PC MAG, (Sept. 26, 2008), http://www.pcmag.com/article2/0,2817,2331225,00.asp (discussing ten major unsolved cybercrimes).

69. *See* Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems, supra* note 47 (mentioning that the shared remoteness aspect of both weapons systems makes them difficult to detect and allows the possibility of unattributable attacks).

70. *Id*.

71. *Id*.

world: sensors by which to "map" and "situate" itself in the physical world; AI computing capabilities; and physical mechanisms by which the machine can move and act directly in the physical world.[72] These are essentially the same technologies that will enable genuinely self-driving cars, for example, and many other emerging robotic technologies.[73] As for cyber-weapons, the overlaps of the technologies are a fact of life now; the ubiquitous and embedded nature of cyber-based systems for so many facets of life is a core reason why cyber-warfare has become possible.[74] The overlap of cyber with national defense and civilian life is also one of the reasons that it is difficult to disentangle "cyber-security" in a civilian sense from "cyber-weapon" in a military or national security one.[75]

It is, and probably always will be, easier to devise, design, and deploy both AWS and cyber-weapons that are indiscriminate rather than discriminate.[76] This is true of most weapons, but it is especially so in the case of complex, technologically cutting-edge weapons.[77] In the case of cyber-weapons, attempting to make a weapon discriminating (including in ways that go beyond simply its LOAC meaning) might mean significantly greater efforts, expenditure of limited human capital resources, and money, not just in creating software–but also the intelligence gathering in order to determine the nature of the system to be attacked, in part, but also (if discrimination is desired) in order to know how the attack can be limited, if it can be. In the case of cyber-weapons, parties might not want to invest in the uncertain and costly attempt to make the weapon discriminate, if it even can be done (and can be determined that it has been done in advance). In the case of AWS, precision and discrimination are functions of enabling greater precision in each of the robotic functions–sensors, cognitive computational capabilities, and mechanical actions–and it is already much easier to design and field systems that do not embrace advancing technologies that give greater precision but require much more difficult and expensive engineering and production.[78] But it is also true that advances in the precision of weapons that might translate into increased discrimination on the battlefield is almost certainly only available through

72. *See Robotics: Facts*, IDAHO PUBLIC TELEVISION, http://idahoptv.org/sciencetrek/topics/robots/facts.cfm (last visited Mar. 21, 2016) (discussing the basic definition, history, and components of a robot).

73. ROBERT O. WORK & SHAWN BRIMLEY, 20YY: PREPARING FOR WAR IN THE ROBOTIC AGE 25 (2014).

74. *See* Anderson, *supra* note 48 (explaining how the digital infrastructure of military and civilian life has perpetuated cyber-warfare).

75. *Id*.

76. *See* Kenneth Anderson & Matthew Waxman, *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*, THE HOOVER INSTITUTION, 2013, http://www.hoover.org/sites/default/files/uploads/documents/Anderson-Waxman_LawAndEthics_r2_FINAL.pdf (explaining that indiscriminate systems are much easier to design and build).

77. *Id*.

78. *See Robotics: Facts*, *supra* note 72 (describing the parts and their functions of AI); Anderson & Waxman, *supra* note 76 (explaining that discriminate AWS require more precision in engineering).

advances in robotics, automation, and machine programming.[79] If an actor cares about discrimination and reducing battlefield harms, technological advance in precision is the only real possibility.

It might be the case–though not always or necessarily–that advances in technology to make AWS more precise and discriminating in its effects will tend to be "general" advances in the precision and discrimination of robot as a whole system. These advances are, perhaps, more likely to constitute general advances for the machine's abilities, applicable to other tasks. It might also be the case, however, that much of the programming of a cyber-weapon to increase its precision and discrimination is entirely unique to a particular target and operation, and not usefully, or at least not easily, transferable to the software of other cyber-weapons with entirely different targets and systems. I have some hesitation about this hypothesis, however.

AWS and cyber-weapons differ in the extent of the advanced technical and industrial base required to create and produce them, as well what they require to successfully field and maintain them.[80] Existing weapons that are arguably a form of AWS–shipboard systems such as the Aegis Weapon System, for example–are highly complex, computerized systems.[81] AWS, as it actually emerges, is not likely to be less complex, expensive, and dependent upon a strong military-industrial base. Although there is much discussion about an arms race and the proliferation of weaponized Unmanned Aerial Vehicle (UAV) systems,[82] it remains true that UAVs in the full military sense, such as the Predator or Reaper, require a sophisticated industrial base, not only to design and produce them–but also to maintain and operate them.[83] There are "drones" and there are "drones," in other words.

While leading states are capable of producing and fielding weaponized UAVs–China, Russia, the big NATO states, Japan, South Korea, etc.[84]–large-scale military UAVs such as Predators or Reapers will not often, if ever, be found in the hands of non-state actors, if they could even operate them successfully.[85] Moreover, most of the benefit of Predators, Reapers, and other large military UAVs is found in their sensor capabilities for gathering intelligence through persistent surveillance, not the ability to fire a weapon, which involve whole other

79. *Id*.

80. Anderson, *supra* note 48 (describing how the element of control differs between AWS and cyber-weapons).

81. *See AEGIS Weapon System Mk 7*, MILITARY, GLOBALSECURITY.ORG, http://www.globalsecurity.org/military/systems/ship/systems/aegis-core.htm (last visited Apr. 16, 2016) (discussing the complexity of the Aegis Weapon System and its autonomous capabilities).

82. *See* Nicholas West, *Global Drone Arms Race Spreading Quickly*, ACTIVIST POST, (Aug. 22, 2011), http://www.activistpost.com/2011/08/drone-arms-race-heats-up-worlds-first.html (discussing the global arms race surrounding drones to take the example of a related significantly automated if not necessarily autonomous system, given that AWS of the requisite kind are not yet fielded).

83. *Id*.

84. *Id*.

85. *See* Anderson, *supra* note 50 (noting the difficulty for non-State actors to use AWS).

technological capabilities from the physical sensors themselves to the cognitive processing capability to gather information out of their feeds.[86] These considerations will be true in many analogous ways for AWS as they gradually emerge. By contrast, however, cyber-weapons–particularly ones that are not concerned with discrimination–can be created by small teams of software designers or even by individuals, by States or by non-State actors.[87]

IV. "WHAT'S THE HURRY TO CREATE INTERNATIONAL LAW TO REGULATE AWS, BUT NOT CYBER-WEAPONS?"

A. Hypotheses About the Rush to Regulate, Not Firm Conclusions

What might be gleaned from these comparisons of AWS and cyber-weapons, with respect to the apparent urgency many in the international community seem to share of the need to create new international law to govern AWS, but not cyber-weapons? Here are several possibilities–more hypotheses than conclusions, that should be noted.

Cyber-weapons are a far more prevalent national security concern today than AWS.[88] Cyber-weapons will continue to evolve and advance, and in that sense they are still an "emerging" military technology–but, by comparison to AWS, they are already solidly part of the equation of security and conflict today, for the United States as well as for others.[89] AWS, by contrast, though arguably in existence in the form of the limited defensive weapons today–shipboard defense, for example, or Israel's Iron Dome missle defense system,[90] discussed earlier–are still a matter of the future and require significant advances in technology.

That future will gradually draw nearer, by incremental advances in the multiple technologies that AWS systems require, to be sure. The neat conceptual distinctions used to define AWS in the abstract today (machines capable of autonomously selecting/engaging its own targets) will not turn out to describe usefully the continuum of weapons automation over time, or the other distinctions

86. West, *supra* note 80.

87. *See* Peirluigi Peganini, *The Rise of Cyber Weapons and Relative Impact on Cyberspace*, INFOSEC INSTITUTE, (Oct. 5, 2012) http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/ (discussing the ability of States as well as individuals to create and use cyber-weapons).

88. *See* Anderson, *supra* note 50 (arguing cyber-weapons are more dangerous than AWS because of large-scale effects on real people).

89. *See* Danny Vinik, *America's secret arsenal*, POLITICO (Dec. 9, 2015, 4:57 AM), http://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331 (discussing the rapid growth of cyber-weapons and their uses).

90. *MK 15 – Phalanx Close-In Weapons System (CIWS)*, U.S. NAVY (Nov. 15, 2013), http://www. navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2; Niv Elis, *Iron Dome: Defense at bargain price*, THE JERUSALEM POST (Mar. 28, 2012), http://www.inss.org.il/uploadImages/systemFiles/Iron%20Dome—%20Defense%20at%20bargain%20prices 253012041.pdf; *see also* Schmitt & Thurnher, *supra* note 12, at 235–36.

discussed earlier about the nature of machine autonomy.[91] There are short to medium predictions[92] that will probably turn out to be broadly correct about the capabilities of the technologies that will power AWS in that time frame. But the actual systems themselves, their actual battlefield capabilities and limitations, remain speculative.

The destructive capabilities of cyber-weapons, as they exist today, are far greater than those of AWS, which after all are still essentially in the future.[93] From the standpoint of risk and threat, in other words, it is remarkably strange that attention for a sweeping and essentially unenforceable ban on AWS, or even international treaty regulation of AWS in advance of even having specific technologies to regulate, is relatively large, while calls for similar treaty regulation for cyber is not. (Why this might be is deferred to the next section of this discussion.)

Even if AWS *were* available today, however, so that a direct comparison of the destructive capabilities of such weapons were possible, cyber-weapons would still likely be capable of far greater harm than AWS, because of such properties as self-propagation and the possibility of uncontrollable effects.[94] Science fiction aside, AWS might be more capable of greater precision and discrimination on the battlefield than existing ordinary weapons; any particular AWS might turn out to be less capable in those terms, and hence more destructive than anticipated. But even so, AWS are still battlefield weapon systems, physically present in this battlefield, and not simultaneously replicable across many battlefields in short order as a result of its programming alone.[95] AWS are a physical, kinetic battlefield weapon system–and, unlike some cyber systems, not one with potentially uncontrollable effects beyond any particular battlefield.[96]

It is possible a sophisticated military could deploy AWS in large numbers—especially if it could be produced cheaply and without regard to the requirements of LOAC—causing severe harm to civilians. However, the harm caused by AWS is unlikely to be greater than a military without AWS who is indifferent to the laws of war. Militaries using area bombardment or other indiscriminate means of attack with great kinetic power and no target discrimination already cause significant damage.

Those new to the AWS debates often mistakenly believe that the strategic

---

91. *See, e.g.*, DOD DIRECTIVE 3000.09, *supra* note 9.

92. Many experts have predicted that AWS will become the norm on the battlefield, but the expected timeline for that to happen is about twenty years. *See* Luke Muehlhauser, *When Will AI be Created?*, MACH. INTELLIGENCE RESEARCH INST. (May 15, 2013), https://intelligence.org/2013/05/15/when-will-ai-be-created/ (describing the varying predictions of the development of AI).

93. *See* Messinger *supra*, note 56 (discussing the capabilities of cyber-weapons).

94. *See* David Raymond et al., *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*, NATO (2013), https://ccdcoe.org/cycon/2013/proceedings/d1r2s6_raymond.pdf (discussing dangers of self-propagation and ways to limit it).

95. *See* Anderson, *supra* note 1, at 388 (noting AWS are battlefield systems).

96. *See* Schmitt, *supra* note 7, at 7 (noting AWS will not go rogue).

military reason for developing AWS capabilities is as force multipliers, large numbers of robotic troops controlled by a relatively small group of human soldiers.[97] The reality is that destruction (or military operations indifferent to destruction or collateral harms) can be achieved with far easier, cheaper, and long-existing technologies.[98] One of the main reasons to develop AWS is speed. Speed can be utilized either offensively to win an engagement, or defensively to respond to an adversary's attack faster and prevent potentially disastrous harm. Another primary factor motivating the development of AWS is that it can be operated remotely, thus protecting one's own forces by removing them from the actual battlefield.[99] Lastly, the promise of increased precision motivates the development of AWS because it has the potential to significantly reduce unnecessary battlefield harms.[100] Of these reasons for the making the extraordinary investments in military robotics required to create and field AWS that can perform unique battlefield tasks or perform them in a uniquely valuable way, the only one that has emerged so far is AWS to address the increasing speed and tempo of certain kinds of battle — countering missiles and rockets.[101]

Cyber-weapons are far more likely to have effects, whether by direct targeting directly or collaterally, on civilians and civilian objects than AWS, and in many cases cyber-attacks are likely to have effects in many different places connected by their cyber-links.[102] With physical machines such as AWS, it is hard to see how they have similar effects that might reach far beyond particular battlefields where they are physically present. Moreover, cyber-technologies serve both civilian and military infrastructure in ways that are today deeply intertwined and likely to grow only more so.[103] In that case, whether cyber-attacks take place in the course of a purely cyber-war; or whether they take place as acts of cyber-warfare embedded within a larger conventional armed conflict; or whether they are aimed directly at civilian infrastructure or are simply collateral effects of attacks on other targets, civilian infrastructure of many kinds is highly vulnerable in cyber-warfare in ways that is not likely to be true for AWS, if only because of the fact of physical machine embodiment.[104] The potential for serious harm as things stand today is,

97. *See March of the robots*, THE ECONOMIST (June 2, 2012), http://www.economist.com /node/21556103 (discussing many robots that are used in tandem with humans, instead of as replacements).

98. *See Civilians Killed & Wounded*, WATSON INST. INT'L PUB. AFFAIRS (Mar. 2015), http: //watson.brown.edu/costsofwar/costs/human/civilians (noting most deaths in war come from malnutrition and poor health care, rather than weapons).

99. *See* Michael W. Lewis, *Drones and the Boundaries of the Battlefield*, 47 TEX. INT'L L. J. 294, 296 (Spring 2012) (discussing the benefits of developing AWS).

100. *Id*.

101. *See* Elis, *supra* note 90 (discussing the effectiveness of Israel's Iron Dome system, and AWS).

102. *See* Peganini, *supra* note 87.

103. *See id*. (asserting that vulnerable connections between systems are one of the main risk factors for the population in handling cyber-weapons).

104. *See id*. ("Different from what leads to a conventional attack, a cyber attack can be conducted in a silent way in times of peace and this leads to having to consider the extremely

and is likely to remain into the future, higher by orders of magnitude for cyber-warfare by comparison to the destructive capabilities likely to be true of even advanced and widespread AWS.

IV. SO WHERE IS THE "BAN KILLER APPS" CAMPAIGN?

A. Why No Agitation to Ban Killer Apps?

If the foregoing hypotheses are at least approximately correct about differences in the potential harms as things stand today with respect to cyber-weapons and AWS, then the question posed by this article seems unavoidable. Why does there not seem to be anything resembling a concerted push to create sweeping new international legal regimes to outlaw cyber-weapons? Where is the "Ban Killer Apps" NGO advocacy campaign, demanding a sweeping, total ban on the use, possession, transfer, or development of cyber-weapons–all the features found in today's Stop Killer Robots campaign?[105]

It will not do to say there is no campaign because there is no real way to make it work, given the nature of cyber. It is not at all obvious that the same is not true of the robotics technologies that are poised to enter the world of ordinary social life as they simultaneously enter the world of weapons and national security. They are essentially the same technologies applied in mildly different directions.[106] States are quite capable of pursuing AWS technologies in secret, and capable of signing onto international treaties while secretly pursuing these technologies.[107]

B. Proliferation and Self-Replication

Moreover, cyber-weapons should raise far greater proliferation concerns. They are a far more cost-effective weapon, given that cyber-weapons do not require the same techno-industrial base to design and produce them.[108] Given that they provide almost certainly greater destructive leverage and bang for the buck, because of the ability to attack so many soft civilian targets in so many different places at once; and given and the low barriers to entry compared to AWS, at least if a party is indifferent to engineering for discrimination and precision in cyber-targeting.[109] Beyond proliferation, by comparison to AWS, cyber-weapons should also raise fears of the digital equivalent of biological warfare–self-replicating cyber-weapons that, entirely unlike physical AWS machines, might have genuinely

---

insidious threat that requires a high level of alertness.").

105. *See Ban 'Killer Robots' Before It's Too Late*, HUMAN RIGHTS WATCH (Nov. 19, 2012), https://www.hrw.org/news/2012/11/19/ban-killer-robots-its-too-late (discussing the reasons for advocating against AWS).

106. *See* Anderson, *Comparing The Strategic and Legal Features of Cyberwar, Drone Warfare, and Autonomous Weapons Systems*, *supra* note 47 (comparing the similarities of AWS and cyber-weapons).

107. *See* Peganini, *supra* note 87 (noting the United States admits cyberspace is an area for warfare, but is secretive about its programs).

108. *See* Peganini, *supra*, note 87.

109. *See id*. (discussing cost effectiveness of cyber-weapons).

uncontrollable effects.[110]

Yet there is not an international advocacy campaign nor is there anything like the excitement and agitation, the intense interest, evinced by states and their diplomatic representatives in the U.N. two years ago, or the intense interest by U.N. officials themselves.[111] There does not appear, in my perception of the comparison of the two weapon types, to be anything like the sense of urgency in the demand for new instruments of international law to govern cyber-weapons that there appears to be in the case of AWS.

C. A Cautious Approach to Cyber Through State-to-State Discussions, Informal Discussions Not Part of Treaty Processes, and Allowing the Emergence of Best Practice and Common Standards Among State

It is true that concerns over cyber-warfare have resulted in an explosion of writing academic and policy venues.[112] The concerns about cyber-war and cyber-warfare have resulted in one major expert effort to propose a coherent legal approach within LOAC to address cyber-warfare.[113] This is, of course, the *Tallinn Manual*, for which the eminent LOAC scholar Michael Schmitt served as reporter and drafter of the book-length report.[114] It is acknowledged to be a very significant effort; the Tallinn process is now coming up with version two, taking into account the great number of responses and comments on it.[115]

It is possible that continued evolution of the *Tallinn Manual* might eventually result in either a treaty setting out its terms as international law or (it seems to me less likely) claims in the future that the *Tallinn Manual* (or certain of its parts) has become customary international law. Yet still the question of this paper persists–why no significant agitation by States or international advocacy NGOs for immediate and sweeping international treaty law, given the relative magnitude of the threats, particularly by comparison to the as-yet infant–embryonic, even–technologies of AWS?

It is noteworthy that alongside the informal, unofficial expert group meetings that gave birth to the *Tallinn Manual*, there has been discussion and debate within and among some important states.[116] The U.S. government, specifically, the Obama

---

110. *See* Raymond et al., *supra* note 94 (noting the potential negative effects of cyber-weapons).

111. Chairperson of the Meeting of Experts, UN Convention on Certain Conventional Weapons, Report of the 2014 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS) ¶ 20, http://www.unog.ch/80256EDD006B8954/% 28%20httpAssets%29 /350D9ABED1AFA515C1257CF30047A8C7/$file/Report_Advan cedVersion_10June.pdf.

112. *See, e.g.*, INT'L GROUP OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEFENSE CENTRE OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

113. *Id*.

114. *Id*.

115. *Id*.

116. *See, e.g.*, *The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited

administration, has given some speeches and statements of policy and some carefully phrased (i.e., revisable) statements of its legal views.[117] Additionally, there have been important efforts to establish "best practices" promulgated by and for States, and attempts to describe what might fall under "cyber-security" versus "cyber-war and cyber-warfare."[118] In my view, and by comparison to today's discussions of AWS, therefore, states appear to be very cautious and hesitant to initiate discussions that aim at binding treaties at this stage.[119] States are far more interested in discussions conceived around more modest efforts to develop state practice and flexibility with respect to evolving technologies, and allow broader forms of inter-state agreement to emerge.[120]

One wonders–well, I wonder, just in case the point has not been driven home enough–why the same approach does not appear to hold, or anyway hold with the same caution, for creating grand treaty regimes with respect to AWS.

D. Speculative Hypotheses About the Lack of Agitation for an Immediate, Sweeping Cyber-Warfare Treaty, By Comparison to AWS

The relatively broader ability by many States today to create and use cyber-weapons–their far lower barriers to entry, by comparison to AWS–causes States to evaluate realistically their own concrete interests in possibly possessing such weapons, for both defensive and offensive purposes.[121] By contrast, the much higher barriers to entry at this point in time for AWS mean that only a handful of States are in a position to develop and field these weapons as the technologies gradually emerge and mature.[122] One possible consequence is that, at this stage, a great many other States perceive an interest in restraining those few players with the technological capabilities of developing AWS at this stage. One motivation might be so that at least some of the "have-nots" have time and breathing-space to catch up and become "haves." For others, restraining the United States as the hegemonic actor in the world is reason enough. For still others, rent-seeking[123] by using the threat of creating international law in exchange for other benefits might be a possibility.

For some States, internal politics might drive the government's position to

---

Apr. 18, 2016).

117. *Id*.

118. *See*, *e.g*., John Haller et al., *Best Practices for National Security: Building a National Computer Security Incident Management Capability*, (June 2010), http://resources.sei.cmu.edu /asset_files/SpecialReport/2010_003_001_15137.pdf.

119. *See*, *e.g*., *id*.

120. *See*, *e.g*., *id*.

121. *See* Peganini, *supra* note 87 (explaining that the United States is not the only nation investing in cyber warfare capabilities).

122. *Id*.

123. Rent-seeking is the use of a company, organization or individual's resources to obtain economic gain from others without reciprocating any benefits to society through wealth creation. *Rent-seeking*, INVESTOPEDIA, http://www.investopedia.com/terms/r/rentseeking.asp (last visited Apr. 18, 2016).

take up the cause of AWS rather than cyber-warfare. For example, perhaps in some Western European countries, internal social movements that provide support to international NGO advocates, combined with relative indifference on the part of such governments to external security concerns (given the U.S. security guarantee through NATO),[124] leads to an embrace of a treaty ban (or a functional ban through severe regulation) on AWS. This embrace, it should be said, need not be a rational government decision taken by comparing the risks and possible benefits of AWS to the risks and threats (already) posed by cyber-warfare. On the contrary, a government that perceives no external risk to its own security might simply be being willing to follow, without much attention to the actual content or implications of policy, whatever internal social movements and civil society organizations have embraced because they, in turn, merely follow without much reflection or consideration whatever international NGO advocates happen to have settled on as the cause de jour. In other words, governments in that happy, risk-free position might just as easily have embraced agitation for a sweeping, immediate treaty on cyber-warfare–but they did not because Human Rights Watch settled on AWS rather than cyber-warfare.[125]

The fact that there are already really-existing cyber-weapons, indeed a flood of them, and the fact that cyber-weapons have already been used, forces States to grapple with the gritty detailed facts, known and unknown, about such systems, both one's own and those of potential or actual adversaries.[126] It forces States, and any expert advisers inside States' respective Ministries of Defense, to think realistically both as to what the content of a meaningful treaty, addressed to actually-existing, though rapidly evolving, cyber-weapons technologies, would actually be able to say, as well as the very real knowledge with respect to existing technologies that enforcement would be essentially unachievable. The fact of actual technologies tends to concentrate the mind of the State with respect to what a treaty would actually mean, and how it would be likely to hamper most precisely those states that might agitate for it.

By contrast, the fact that AWS at this point in its technological development remains in the abstract and in the future (even if it is approaching incrementally and gradually)[127] allows the debate over AWS and how an international law regime would be conceived and articulated to remain at the level of sweeping, abstract, and categorical principles. Such abstraction favors, of course, advocates of a ban, or advocates of regulation stringent enough that it could easily be interpreted as endorsing a ban.[128] Indeed, the fact that AWS is not on the table in concrete

124. NATO, *Collective Defense –Article 5*, (last updated Mar. 22, 2016) http://www.nato.int/cps/en/natohq/topics_110496.htm.

125. *Autonomous Weapons Systems: Five Key Human Rights Issues For Consideration*, AMNESTY INTERNATIONAL (2015), https://www.amnesty.org/en/documents/act30/1401/2015/en/ [hereinafter AMNESTY INTERNATIONAL].

126. *See*, *e.g.*, Peganini, *supra* note 87.

127. Schmitt, *supra* note 7.

128. *Id*.

technologies that can be evaluated with respect to their particular capabilities practically means that any treaty at this stage must consist of sweeping abstract principles, rather than concrete rules that arise from the experience of actual weapon systems and their particular technological possibilities and limitations.[129]

The complexities of distinguishing between cyber-security and cyber-war, between criminal acts and acts of war, within the context of difficult and ambiguous attribution–and the fact that states already *know* this to be the case in cyber–have made States aware of the great difficulties in defining exactly what one proposes to regulate and what those regulations might mean in a binding, permanent treaty.[130] This leads, to some extent at least, a preference by States to allow State practice to emerge and to reserve debates over new treaty law as a matter for the future, following the emergence (if, of course, it does emerge) of reasonably broad agreement over best practices, with regards to technologies in their particular capabilities and limitations.[131] AWS debates, at least at this stage, seem inclined through a sense of moral and legal urgency, to bypass that process and proceed directly or nearly directly to codification in one form or another.[132] This seems to me an enormous legal policy mistake.

5. States committed to LOAC might decide that the long-run development of stable rules for cyber-weapons–forms of regulation that are most likely to having staying power–is most likely to emerge by letting the existing legal processes of legal weapons review in LOAC/international humanitarian law (IHL) provide evaluations of individual cyber-weapon systems by leading States, at least those that actually perform legal weapons reviews. These are the concrete bases out of which *might* emerge the bases of common standards among States. These reviews begin, of course, with the fundamental principles of LOAC/IHL–as the whole body of law does–but then descend into the granular features of design, performance, reliability engineering, and so on in order to assess not merely the lawfulness of the weapon, but far more importantly, the environments and uses to which it can lawfully be put in conflict.[133]

It should be added—as Matthew Waxman, a professor at Columbia Law specializing in in national security law and international law, and I have often stressed in past writing—that the emergence of best practices and shared norms among leading states, whether in cyber-weapons or in AWS, can only happen if leading states are willing to share enough information to allow standards to become "common" among them.[134]

---

129. *Id*.
130. *Id*.
131. AMNESTY INTERNATIONAL, *supra* note 125.
132. *See*, *e.g*., Schmitt, *supra* note 7.
133. AMNESTY INTERNATIONAL, *supra* note 125.
134. Anderson & Waxman, *supra* note 76.

VI. CONCLUSION

What has been offered in this article by way of explanation for why AWS rather than cyber-warfare or cyber-weapons as the object of agitation for sweeping, immediate international law consists of hypotheses, provisional explanations, rather than firm conclusions supported by scads of evidence. It is hard to produce evidence with regards to counter-factuals that are counter-factuals in no small part because AWS is not yet on hand technologically with any great specificity or granularity as to particular systems, and so assessing its nature is necessarily speculative at this stage. Assessment of cyber-weapons–though the weapons are quite real technologies–is also speculative, though for a different reason, viz., that they are national security secrets of many different countries.[135] The underlying features of the programming, as well as concrete information about the use of cyber-weapons to date, is not reliably known, at least not so as to include a wide sample of leading, technologically active states.

Nonetheless, if this paper has no other take-away, there is something politically provocative and important to be explained about the gap in enthusiasm for immediate creation of international law between the two. Part of the gap, I believe, does indeed depend upon the sort of speculative hypotheses that the latter half of this article offers in comparing cyber-weapons and AWS. But another part of the gap, I believe, arises from conceptual confusions and misconceptions about the nature of autonomy in robotic technology and AI generally that are addressed in the first half of the paper.

There is an opportunity here to assist in at least possible establishment of reasonably stable rules (capable of evolving as well) with regards to AWS. It is, however and somewhat paradoxically, participation that consists, at least as far as the creation of new international law, new treaty law, is concerned, a matter of holding back rather than rushing in. The reflexive desire to start drafting international law, rather than letting informal State-to-State processes take their course, with far greater attention paid to the granular features of actual AWS and their technologies as they emerge, is not likely to lead straight-away to the total ban treaty sought by some that might, tragically, leave the technology and the benefits that it might one day offer in reducing the harms of conflict still-born. Still-born, moreover, without deterring in the least development, secretly or otherwise, of such weapons by the world's less scrupulous States, and with little or no pressure to address discrimination and precision by such States.

But the reach straight-away to establishing (in advance of actual weapons and the technology undergirding them that can be evaluated by the processes of legal weapons review in LOAC) a supposed "regulatory" treaty regime under the CCW would almost certainly be an exercise in futility that, worse, might permanently derail the attempt to come up with stable rules for addressing systems possessed of increasingly sophisticated forms of machine autonomy. Futility in that it would necessarily consist of abstract statements of principle, because there would be as

135. *Id*.

yet no actual technology or experience with the weapon that would allow for the concrete formulation of treaty rules grounded in experience. The conditions for genuinely useful and effective regulation of AWS would, in my view, be something that is many years down the road, and following on the cautious development of State-to-State standards among friends and allies, and cautious outreach to other states on the basis that the discussions are entirely provisional and are not part of an effort to create an international law regime–at the first sign of which States would treat what they say as hedged against the protection of their interests. Best practices and shared standards do not emerge from that kind of discussion.

A stable regime for regulating AWS, including the evolution of the technology, would require something that international treaty processes cannot provide in the first instance–the experience of States in developing the technologies, developing weapons, and developing a base of experience in both the technology and legal issues arising from the intense particularity and granularity of weapons reviews to come to common standards for regulation based on actual experience. Calls for international discussions, informal or otherwise, as part of treaty or treaty review processes, is by many years premature.