AMSTERDAM LAW FORUM
VU UNIVERSITY AMSTERDAM

Article

Legal and Ethical Precepts Governing Emerging Military Technologies: Research and Use

George R Lucas, Jr.[*]

Introduction

From the emergence and increasing use of unmanned or "remotely-piloted" vehicles to the advent of cyber war and conflict, the development of new and exotic military technologies has provoked fierce and divisive public debate regarding the ethical challenges posed by such technologies.[1] I have increasingly come to believe that the language of morality and ethics has served us poorly in this context, and presently serves to further confuse, rather than to clarify or enlighten us on how best to cope with the continuing development and deployment of seemingly-exotic new military technologies.

There are numerous reasons that justify this concern. Segments of the public involved in these discussions harbour distinctive and incompatible—and sometimes conceptually confused and unclear—notions of what "ethics" entail. From individual and culturally-determined intuitions regarding right conduct, through the achievement of beneficial outcomes, all the way to equating ethics merely to legal compliance, this results in frequent and virtually hopeless equivocation. Moreover, many scientists and engineers (not to mention military personnel) tend to view the wider public's concern with "ethics" as misplaced, and regard the invocation of "ethics" in these contexts as little more than a pretext for technologically and scientifically illiterate, fear-mongering, nay-saying Luddites who simply wish to impede the progress of science and technology.

Why insist on invoking fear and mistrust, and posing allegedly "moral" objections to the development and use of unmanned systems, instead of defining clear engineering design specifications and operational outcomes that incorporate the main ethical

[*] *Professor of Philosophy & Public Policy, Global Public Policy Academic Group, Naval Postgraduate School; Distinguished Chair in Ethics, Stockdale Center, U.S. Naval Academy*

[1] E.g., P. W. Singer, *Wired for War*, New York: Penguin Press, 2009; A. Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons*, London: Ashgate Press, 2009; G. R. Lucas, Jr., "'This is Not Your Father's War': Confronting the Moral Challenges of 'Unconventional' War," *Journal of National Security Law and Policy*, 2009-3-2: 331-342; and "Postmodern War," in *New Warriors and New Weapons: Ethics & Emerging Military Technologies*," a special issue of *Journal of Military Ethics* 2010-9-4: 289-298.

concerns? Why not require engineers and the military to design, build and operate to these standards, if they are able, and otherwise to desist, until they succeed? Why engage in a science-fiction debate over the future prospects for artificial machine intelligence that would incorporate analogues of human moral cognition, when what is required is far more feasible and less exotic: machines that function reliably, safely, and fully in conformance with applicable international laws—such as the law of armed conflict (LOAC) when operating in wartime.[2] And why insist that the advent of cyber conflict is a "game changer" that ushers in a new mode of unrestricted warfare, in which all the known laws and moral principles of armed conflict are rendered obsolete,[3] when what is required is merely appropriate analogical reasoning to determine how the known constraints extrapolate to these novel conditions?[4]

In this essay, I propose initial outlines of a framework for identifying and fostering productive debate over the acceptable ethical boundaries regarding novel technologies. First, I survey the state of discourse surrounding the ethics of autonomous weapon systems and cyber warfare. Next, I discuss how attempting to codify the emerging consensus on ethical boundaries for a given technology can focus the conversation on unsettled areas more effectively than vague moral discourse. Thirdly, I offer a set of Precepts for the development and operation of autonomous systems, and invite discussion on their accuracy and degree of comprehensiveness. Finally, I suggest how this methodology and many of these individual precepts apply toward the regulation and governance of other military technologies as well.

I. Ethical Debate over Novel Technologies

Three recent and prominent threads of discussion serve to illustrate the ethical debate over use and development of novel technologies: first, the "Arkin-Sharkey" debate over the proposed benefits and liabilities of "machine morality" as part of the larger, seemingly-relentless drive toward developing ever-greater degrees of autonomy in lethally-armed, unmanned systems;[5] second, the efforts on the part of members of the International Committee on Robot Arms Control (ICRAC), led by Peter Asaro, Robert Sparrow, and Noel Sharkey, to outlaw the future development of autonomous, lethally-armed unmanned systems under international law;[6] third, areas of emerging consensus or agreement among the contending stakeholders regarding the role of "ethics" in cyber warfare. This third debate centres on the development of cyber weapons and tactics, both those aimed indiscriminately at civilian personnel and "objects", such as vital civil infrastructure, as well as highly-discriminate cyber

[2] See G R Lucas, Jr., "Engineering, Ethics & Industry: the Moral Challenges of Lethal Autonomy," Ch. 10 in B. J. Strawser, ed., *Killing by Remote Control*, New York: Oxford University Press, 2013: 297-318.

[3] See R. Dipert, "The Ethics of Cyber Warfare," *Journal of Military Ethics* 2010-9-4, 384-410.

[4] G. R. Lucas, Jr., "Just War and Cyber Warfare," in *The Routledge Handbook of Ethics and War*, eds. Fritz Allhoff, Nicholas G. Evans, and Adam Henschke, Oxford: Routledge, 2013.

[5] See R. C. Arkin, "The Case for Ethical Autonomy in Unmanned Systems," *Journal of Military Ethics* 2010-9-4: 347-356; N. Sharkey, "Saying 'No!' to Lethal Autonomous Targeting," *Journal of Military Ethics* 2010-9-4: 299-314.

[6] See the ICRAC mission statement and list of personnel at http://icrac.net/who/.

weapons like "Stuxnet" and "Flame," which may be used in a pre-emptive or preventive fashion against perceived threats that have, as yet, resulted in no actual harm inflicted by the recipient of the cyber-attack.[7]

These three examples do not exhaust the all features of the wider debate over emerging military technologies, by any means. The increasing array of so-called "non-lethal" weapons, for example, involves questions about the use of such weapons on non-combatants, as well as the potential of such weapons to expand the rules of engagement for use of force, rather than lessening the destruction or loss of life as compared to the current regime.[8] Prospects for military uses of nanotechnology raise spectres of weapons and systems that might cause widespread and catastrophic collateral or environmental destruction.[9] And efforts to use biological, neurological, and pharmaceutical techniques to enhance the capabilities of human combatants themselves raise a host of ethical questions: from "informed consent" for their use, to determining the likely long-term health prospects for enhanced individuals following their military service, to the potentially undesirable social conflicts and transformations ("civilian blowback") that such techniques might inadvertently bring about.[10] For the present, however, I will stick to the three illustrations above since, collectively, they encompass a great deal of the public debate over military technology, and the lessons learned in response have a wider applicability to these other areas and topics as well.

First, the prospects for machine models of moral cognition constitute a fascinating, but as yet futuristic and highly speculative enterprise. The goal of developing working computational models of reasoning, including moral reasoning, is hardly impossible,

---

[7] The discovery and strategic implications of the Stuxnet worm, against the backdrop of three prior cyber conflicts in Estonia (2007), Syria (2007) and Georgia (2008), were given a preliminary and (at the time) incomplete summary in G. R. Lucas, Jr., "Permissible Preventive Cyber Warfare," in L. Floridi and M. Taddeo, eds. *Philosophy of Engineering and Technology* (UNESCO Conference on Ethics and Cyber Warfare, University of Hertfordshire, 1 July 2011). Dordrecht, NE: Springer Verlag, 2013. A subsequent and complete retrospective account of the project, "Operation Olympic Games," in which the Stuxnet worm and Flame espionage malware were a part, is provided in New York Times columnist D. E. Sanger's book, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Crown Publishers, 2012.

[8] See, for example, P. Kaurin, "With Fear and Trembling: An Ethical Framework for Nonlethal Weapons," *Journal of Military Ethics* 2010-9-1: 100-114.

[9] Accounts of the military uses of "smart dust" (nanoreceptors) and the possible environmental result of "grey slime," the potential impact of runaway "nano-viruses," and other nightmare scenarios from nanotechnology are outlined and discussed in F. Allhoff, P. Lin, J. Moor, & J. Weckert (Eds.), *Nanoethics: The ethical and social implications of nanotechnology,* Hoboken, NJ: John Wiley, 2007.

[10] An up-to-date account of enhancement technologies and their prospective military uses (and potential abuses) is provided in a 2012 Greenwall Foundation report, "Enhanced Warfighters: Risk, Ethics and Policy" by P. Lin, M. J. Mehlman, and K. Abney. Available from the California Polytechnic University's "Ethics + Emerging Sciences" working group at: http://ethics.calpoly.edu/Greenwall_report.pdf.

but the effort required will be formidable.[11] "Morality" and moral deliberation remain firmly in the domain of human experience for the foreseeable future. In any event, discussions of ethics and morality pertaining to unmanned systems at present are largely irrelevant. We neither want nor need our unmanned systems to "be ethical," let alone "more ethical" or "more humane" than human agents. We merely need them to be safe and reliable, to fulfil their programmable purposes without error or accident, and to have that programming designed to conform to relevant international law (LOAC) and specific rules of engagement (ROEs). With regard to legal compliance, machines should be able to pass what is defined below as the modified "Arkin test:" autonomous unmanned systems must be demonstrably capable of meeting or exceeding behavioural benchmarks set by human agents performing similar tasks under similar circumstances.[12]

Second, proposals at this juncture to "outlaw" research, development, design and manufacture of autonomous weapons systems seem at once premature, ill-timed, ill-informed—classic examples of "poor governance." Such proposals do not reflect the concerns of the majority of stakeholders who would be affected; they misstate, and would attempt to over-regulate relevant behaviours.[13] Ultimately, such regulatory statutes would prove unacceptable to and unenforceable against many of the relevant

[11] The degree of futuristic speculation involved in such efforts is indicated in the "Arkin-Sharkey" debate, cited above (n.5). For an account of the formidable challenges entailed, by a proponent of such efforts, see: R.C Arkin, *Governing Lethal Behavior in Autonomous Robots*, Taylor-Francis, 2009. For an account of current progress to date, see: R. Arkin, P. Ulam, and A. Wagner, "Moral Decision Making in Autonomous Systems: Enforcement, Moral Emotions, Dignity, Trust, and Deception." *Proceedings of the IEEE*, 2012-100-3: 571-589.

[12] This criterion—that robots comply as or more effectively with applicable constraints of LOAC on their use of force and doing of harm than human combatants under similar circumstances—constitutes what I have termed the "Arkin Test" for robot "morality" (although that is likewise somewhat misleading, as the criterion pertains straightforwardly to compliance with international law, not with the exhibiting of moral judgment). In this sense, the test for "morality" (i.e, for the limited ability to comply with legal restrictions on the use of force) is similar to the "Turing Test" for machine intelligence: we have satisfied the demand when machine behavior is indistinguishable from (let alone better than) human behavior in any given context. *See* G. R. Lucas, Jr., "Industrial Challenges of Military Robotics," *Journal of Military Ethics,* 2011-10-4: 274-295. For these parameters of design success, *see also* R. Sparrow, "Building a Better Warbot: Ethical Issues in the Design of Unmanned Systems for Military Applications," *Journal of Science and Engineering Ethics*, 2009-15: 169–187.

[13] In addition to proposals to outlaw armed or autonomous military robotic systems by ICRAC itself, see most recently the report from Human Rights Watch, "Losing Humanity: the Case Against Killer Robots" (2012): http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0.pdf. While unquestionably well-intentioned, the report is often poorly or incompletely informed regarding technical details, and highly misleading in many of its observations. Furthermore its proposal for states to collaborate in banning the further development and use of such technologies would not only prove unenforceable, but likely would impede other kinds of developments in robotics (such as the use of autonomous systems during natural disasters and humanitarian crises) that the authors themselves would not mean to prohibit. It is in such senses that these sorts of proposals represent "poor governance."

parties (especially among nations or organizations with little current regard for international law), and would thus serve merely to undermine respect for the rule of law in international relations. Machines themselves (lacking the requisite features of folk psychology, such as beliefs, intentions, and desires) by definition cannot themselves commit war crimes, nor could a machine be held accountable for its actions. Instead, a regulatory and criminal regime, respecting relative legal jurisdictions, already exists to hold accountable individuals and organizations who might engage in reckless and/or criminally negligent behaviour in the design, manufacture, and end use of unmanned systems of any sort.[14]

Lastly, in contrast to robotics, which has spawned tremendous ethical debate but little in the way of jurisprudence, discussions of the cyber domain have been carried out almost entirely within the jurisdiction of international law,[15] with very sparse comment from ethicists until quite recently.[16] Some have found the threat of grave "cyber Armageddon" of the sort predicted by Clarke and Brenner[17] somewhat exaggerated, and even denied that the genuine equivalent of armed conflict has or could likely occur within this domain—no one has yet been killed, nor objects harmed or destroyed, in a cyber-conflict.[18] What has transpired instead is an increase in "low-intensity" conflict, such as crime, espionage, and sabotage, which blurs the line between such conflict and war, resulting in cumulative harm greater or more concrete than damage caused by conventional war.[19] However, several recent conflicts, at least one of which ("Stuxnet") did cross the boundary defining an act of war, have

---

[14] G. E. Marchant, B. Allenby, R. Arkin, E. T. Barrett, J. Borenstein, L. M. Gaudet, O. Kittrie, P. Lin, G. R. Lucas, R. O'Meara, J. Silberman, "International Governance of Autonomous Military Robots," *Columbia Science and Technology Law Review* 2011-12: http://www.stlr.org/cite.cgi?volume=12&article=7.

[15] "The Tallinn Manual on the International Law Applicable to Cyber Warfare" (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012): https://www.ccdcoe.org/249.html. For reviews and discussions of the extensive literature on cyber conflict in international law and jurisprudence, see D. E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law and Policy*, 4 (2010): 87-102, and M. N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online*, 54 (2012): 13-37, http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/. Cyber conflict and international law is also the topic of a special issue of *U.S. Naval War College International Law Studies*, 2011-87.

[16] The first article by an ethicist pertaining to cyber warfare was R. Dipert, "The Ethics of Cyber Warfare," *Journal of Military Ethics* 2010-9-4, 384-410. Computer scientist N. C. Rowe began earlier to raise moral concerns about cyber weapons and strategy: N. C. Rowe: "War Crimes from Cyberweapons," *Journal of Information Warfare,* 2007-6-3: 15-25; "The Ethics of Cyberweapons in Warfare," *Journal of Techoethics* 2010-1-1: 20-31.

[17] R. A. Clark and R. K. *Knake, Cyber War: the Next Threat to National Security, and What to Do About It*, New York: HarperCollins, 2010; J. Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare,* New York: Penguin Books, 2011.

[18] T. Rid, "Cyber War will Not Take Place," *Journal of Strategic Studies*, 2011-35-1, 5-32.

[19] T. Rid, "Think Again: Cyberwar," and J. Arquilla, "Cyber War is Already Upon Us," *Foreign Policy* (March-April 2012): http://www.foreignpolicy.com/articles/2012/02/27/cyberwar; and http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

suggested the emergence of increasingly shared norms by which such conflict can be assessed, and perhaps constrained.[20]

II. Codification of Emergent Norms

The final comment above illustrates an approach to understanding and governing the future development and use of exotic military technologies first suggested by Professor Gary Marchant, et al: namely, that rather than a rush toward proposing unenforceable treaties or ineffectual "bright line" statutes of black-letter international law, what is required is a form of governance known as "soft law."[21] Professor Marchant and his co-authors invited those engaged in the development and use of such technologies, in the course of their activities, to reflect upon and observe what appear to them to be the boundaries of acceptable and unacceptable conduct, and to codify these by consensus and agreement as the principles of best practice in their fields.

In many of the areas outlined above, "emergent norms" regarding ethics, legal jurisdiction and compliance – and, perhaps most importantly, appropriate degrees of consent and accountability for all the stakeholders – that together constitute the hallmarks of "good governance," already have been largely established. What is urgently needed at this juncture is a clear summary of the results of the discussions and debates (as contained in the numerous citations above surveyed above which) that would, in turn, codify what we seem to have proposed or agreed upon in these matters, as distinguished from what requires still further deliberation and attention.

In the case of the debate over autonomous systems, for example, I would summarise the past several years of contentious debate in the following Precepts, defining good or best practices, and the limits of acceptable versus unacceptable practice. I have already undertaken this task in the realm of cyber conflict,[22] based upon reactions to the several internationally-acknowledged examples of cyber conflict that have recently occurred, from Estonia (2007) to Stuxnet/Operation "Olympic Flame" (2010). The point of these exercises is not to presume or pre-empt proper legislative authority, but

[20] See G. R. Lucas, Jr., "Permissible Preventive Cyber Warfare," in Floridi and Taddeo, 2013 supra note 3.

[21] Marchant, et al, *supra* note 14 at [PIN].

[22] G. R. Lucas, Jr., "Just War and Cyber Warfare," in Allhoff, Evans and Henschke eds. 2013 supra note 4. There I summarise from extant literature that use of a cyber weapon against an adversary is justified whenever there is a compelling reason for doing so, toward the resolution of which every reasonable effort has been expended with little likelihood of success and in which further delay will only make matters even worse. Resort to cyber conflict is only justified, moreover, when the weapon is directed purely at military targets, would inflict no more damage or loss of life on these than would be reasonably proportionate to the threat posed, and finally, which use would pose no threat of harm whatsoever to noncombatant lives or property. In other respects, as noted below, these Precepts of cyber conflict are similar to, or can be straightforwardly derived from, several of the Precepts regarding the development and use of unmanned systems discussed in this article, as noted below.

instead to focus future discussions upon whether such Precepts are correctly stated (and if not, to modify them accordingly), the extent to which they are in fact widely held, and finally, to identify areas of omission that must still be addressed. This seems to me a far more constructive enterprise at this point than further futile "hand-wringing" over the vague ambiguities moral discourse.

III. Precepts for use of Autonomous Systems

Law and moral discourse, famously, always lag technological innovations (especially, if not exclusively, in warfare) and their transformative impact on the cultures in which they arise. That does not mean that law and morality are irrelevant and must be cast aside, nor does it require that ethics always be portrayed as an impediment or obstacle to technological development. Rather it demands, as such developments always have, that human agents employ appropriate ingenuity in the framing of suitable metaphors, the drawing of the most appropriate analogies, and reasoning by extrapolation from the known to the unknown in the continuing quest to order and organise the perplexing opportunities and risks that innovation and change otherwise invariably pose. In that spirit, I offer these Precepts as the emerging consensus on the use of autonomous weapons systems.

III.1. The Principle of Mission Legality

A military mission that has been deemed legally permissible and morally justifiable on all other relevant grounds does not lose this status solely on the basis of a modification or change in the technological means used to carry it out (i.e., by removing the pilot from the cockpit of the airframe, or replacing the pilot with demonstrably-reliable software), unless the technology in question represents or employs weapons or methods already specifically proscribed under existing international Weapons Conventions, or in violation of the prohibitions in international humanitarian law against means or methods that inflict superfluous injury or unnecessary suffering (or otherwise judged to constitute means *mala in se*).[23]

[23] A recent proposal by a much respected ethicist, Wendell Wallach of Yale University, suggests that lethal autonomous systems, at least, should (like rape and biological weapons) be classified among the means and methods of warfare that are "evil in themselves" (mala in se). In that case, the argument regarding mission legality with respect to the use of that technology would be rendered moot. It is not at all clear or convincing, however, that the reasons adduced for this classification would prove compelling in the case of unmanned systems generally, both because the analogy between autonomous systems and the examples of means male in se above do not appear obvious, while the author's argument rests on the largely-discredited objection that machines cannot be held accountable for their actions. See W. Wallach, "Terminating the Terminator: What to Do about Autonomous Weapons," *Science Progress* (29 January 2013): http://scienceprogress.org/2013/01/terminating-the-terminator-what-to-do-about-autonomous-weapons/.

III.2. The Principle of Unnecessary Risk[24]

Within the context of an otherwise lawful and morally justified international armed conflict or domestic security operation, we owe the war-fighter or domestic security agent every possible minimization of risk we can provide them in the course of carrying out their otherwise legally permissible and morally justifiable missions.

III.3. The Principle of the Moral Asymmetry of Adversaries[25]

By contrast, no such obligation is owed to opponents or adversaries during such missions in their pursuit of presumably illegal and morally unjustifiable activities. (E.g., there is no requirement of fairness or technological equality in carrying out justified international armed conflict or lawful domestic security operations. NATO/ISAF forces no more owe combat "parity" or "fairness" to Taliban and al Qaeda operatives than domestic immigration and border security forces owe such parity to armed agents of drug cartels. Both sets of adversaries are engaged in virtually identical behaviour: violation of domestic legal statutes and defiance of duly-elected legal authorities, indiscriminate targeting of civilians and destruction of property, kidnapping, torture, execution, and mutilation of prisoners, etc.)

III.4. The Principle of Greatest Proportional Compliance

Furthermore, in the pursuit of a legally permissible and morally justifiable military (or security) mission, agents are obligated to use the means or methods available that promise the closest compliance with the international laws of armed conflict (LOAC) and applicable rules of engagement (ROEs), such as non-combatant distinction (discrimination) and the economy of force (proportionality).

---

[24] Formulated by B. J. Strawser in "Moral Predators: the Duty to Employ Uninhabited Aerial Vehicles," in G. R. Lucas, Jr., ed., *New Warriors and New Weapons: Ethics & Emerging Military Technologies*, Journal of Military Ethics 2010-9-4: 357-383.

[25] Note that this is not an explicit rejection of the doctrine of the "Moral Equality of Combatants," an essential element in what M. Walzer defines as "the War Convention" (in *Just and Unjust Wars*, 1977). Rather, it is a repudiation of a misplaced notion of "fairness in combat," according to which it would be unfair for one side in a conflict to possess or use weapons or military technologies that afforded them undue advantage. This is sometimes cited in public as an objection to the use of "drones" in warfare. It seems to equate war with a sporting competition, after medieval jousting fashion, and, upon examination, is not only patently ridiculous, but contradicted in most actual armed conflicts of the past, where maneuvering for "technological superiority" was a key element in success. In any case, no such argument is made concerning legitimate domestic security operations, as noted above, and does not obtain either within the realm of wars of "law enforcement" or humanitarian intervention.

III.5. The Modified "Arkin Test"[26]

In keeping with Precept IV, an artefact (such as an autonomous unmanned system) satisfies the requirements of international law and morality pertaining to armed conflict or law enforcement, and may therefore be lawfully used alongside, or substituted for, human agents whenever the artefact can be shown to comply with the relevant laws and ROEs as (or even more) reliably and consistently as human agents under similar circumstances. (Moreover, from application of Precepts II and IV above, the use of such an artefact is not merely legally permissible, but *morally required,* whenever its performance promises both reduced risk to human agents and enhanced compliance with LOAC and ROEs.)

III.6. The Principle of Non-Delegation of Authority and Accountability[27]

The decision to attack an enemy (whether combatants or other targets) with lethal force may not be delegated solely to an unmanned system in the absence of human oversight, nor may eventual accountability for carrying out such an attack be abrogated by human operators in the "kill chain."

III.7. The Principle of Due Care

All research and development, design, and manufacture of artefacts (such as lethally armed and/or autonomous unmanned systems) ultimately intended for use alongside, or in place of human agents, engaged in legally permissible and morally justifiable armed conflict or domestic security operations must rigorously comply with Precepts I-V, above. All R&D, design, and manufacture of unmanned systems undertaken with full knowledge of, and in good faith compliance with, the above Precepts (such good faith at minimum to encompass rigorous testing to ensure safe and reliable operation under the terms of these precepts) shall be understood as legally permissible and morally justifiable.

III.8. The Principle of Product Liability

Mistakes, errors, or malfunctions that nonetheless might reasonably and randomly be expected to occur, despite the full and good faith exercise of due care as defined in Precept VI above, shall be accountable under applicable international and/or domestic product liability law, including full and fair financial and other compensation or restitution for wrongful injury, death, or destruction of property.

III.8. The Principle of Criminal Negligence

[26] As described in Arkin 2010 supra note 5.

[27] This principle is indebted to the work of philosopher Robert Asaro of the New School (NY), co-founder of the International Committee for Robot Arms Control (ICRAC).

By contrast, R&D, design, or manufacture of systems undertaken through culpable ignorance, or in deliberate or wilful disregard of these precepts (to include failure to perform, or attempts to falsify the results of, tests regarding safety, reliability of operation, and compliance with applicable law and ROEs, especially in the aftermath of malfunctions as noted above), shall be subject to designation as "war crimes" under international law, and/or as reckless endangerment or criminally negligent behaviour under the terms of applicable international and/or domestic law. Individual parties to such negligence shall be punished to the full extent of the law, to include trial and conviction in the International Criminal Court for the wilful commission of war crimes, and/or civil and criminal prosecution within the appropriate domestic jurisdiction for reckless endangerment or criminal negligence. (In domestic jurisdictions providing for capital punishment upon conviction for the occurrence of such mishaps within that jurisdiction, such punishment shall be deemed an appropriate form of accountability under the Precepts above.)

III.9. Benchmarking

Testing for safety and reliability of operation under the relevant precepts above shall require advance determination of relevant quantitative benchmarks for human performance under the conditions of anticipated use, and shall require any artefact produced or manufactured to meet or exceed these benchmarks.

III.10. Orientation and Legal Compliance

All individuals and organizations (including military services, industries, and research laboratories) engaged in R&D, design, manufacture, acquisition, or use of unmanned systems for military purposes shall be required to attend an orientation and legal compliance seminar of not less than 8 hours on these precepts, and upon conclusion, to receive, sign, and duly file with appropriate authorities a signed copy of these precepts as a precondition of their continued work. Failure to comply shall render such individuals liable under the principle of criminal liability (Precept IX) above for any phase of their work, including, but not limited to accidents or malfunctions resulting in injury, death, or destruction of property.

Government and military agencies involved in contracting for the design and acquisition of such systems shall likewise require and sponsor this orientation seminar and facilitate the deposit of the required signed precept form by any contractors or contracting organizations receiving federal financial support for their activities. Federal acquisitions and procurement officials shall also receive this training, and shall be obligated to include the relevant safety/reliability benchmarks of human performance along with other technical design specifications established in RFPs or federal contracts.[28]

[28] A similar set of procedures (i.e., Precepts X and XI) is recommended for analogous programs involving cyber weapons and tactics, non-lethal weapons, and human enhancement projects (the

IV. Conclusion

My intent in offering these precepts is to suggest areas of consensus and agreement discerned among contending stakeholders and positions in this debate, and to suggest the norms emerging from this debate that might serve to guide (if not strictly govern) the behaviour of states, militaries, and those involved in the development, testing and manufacture of present and future unmanned systems. I likewise believe that discussion of the meaning, application, and refinement of these precepts as "soft-law" guidelines for proper use of unmanned systems would be substantially more efficacious than further moral "hand-wringing" over their potential risks, let alone a rush to legislation that would have both unenforceable and unintended harmful consequences.

Some of the foregoing precepts are specific to military robotics (e.g., Precepts V & VI, pertaining to the Arkin test, and prohibition on delegation of authority to unmanned systems, respectively). This general approach, based upon mutual consensus regarding emerging norms, and many if not most of the precepts elicited above, however, would prove useful by analogy as well in other areas of technological development, such as non-lethal weapons, cyber warfare, projects for "warrior enhancement" and other military/domestic security technologies.

In the case of cyber conflict, for example, Precept One pertaining to mission legality would likewise suggest that, in any situation in which a use of force was otherwise deemed justifiable, that justification would extend to the use of cyber weapons and tactics as well as to conventional weapons and tactics. Moreover, by the Principle of Greatest Proportional Compliance (Precept IV above), in an instance in which the use of force was otherwise justifiable, and given a choice of cyber versus conventional weaponry, the use of the more discriminate and less destructive weapon (presumably the cyber weapon) would not merely be permitted, but obligatory. This principle also dictates the use of less-lethal ("non-lethal") weaponry, when the effects otherwise achieved are equivalent.

In sum, I believe there is far more consensus than we have been able to discern among adversarial parties arguing about ethics and law in such matters than we have heretofore been able to discern. That emerging consensus, in turn, points toward a more productive regime of governance and regulation to assure against the risk of unintended harm and consequences than do rival attempts at legal regulation or moral condemnation.

---

last already to include compliance with relevant federal requirements regarding human subjects research).