Utah Law Review

Volume 2013 | Number 5 Article 4

2013

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

George R. Lucas
Navy Postgraduate School

Recommended Citation
George R. Lucas, Legal and Ethical Precepts Governing Emerging Military Technologies: Research and Use, 2013 ULR 1271 (2013). https://doi.org/10.26054/0d-2qzk-fkxd

LEGAL AND ETHICAL PRECEPTS GOVERNING EMERGING MILITARY TECHNOLOGIES: RESEARCH AND USE

George R. Lucas, Jr.*

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 us, 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 harbor distinctive and incompatible—and sometimes conceptually confused and unclear—notions of what "ethics" entail. From individual and culturally determined intuitions regarding morally right conduct, through the achievement of beneficial outcomes, all the way to equating ethics to mere legal compliance, this discord 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 proponents of ethics as little more than 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 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

 Professor of Philosophy & Public Policy, Global Public Policy Academic Group, Naval Postgraduate School; Distinguished Chair in Ethics, Stockdale Center, U.S. Naval Academy. A similar version of this Article is being published by the *Amsterdam Law Forum*.

[1] *See, e.g.*, ARMIN KRISHNAN, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS 117–44 (2009); P.W. SINGER, WIRED FOR WAR 382–412 (2009); George R. Lucas, Jr., *Postmodern War*, 9 J. MIL. ETHICS 289, 289–98 (2010); George R. Lucas, Jr., *"This Is Not Your Father's War"—Confronting the Moral Challenges of "Unconventional" War*, 3 J. NAT'L SEC. L. & POL'Y 329 (2009).

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 by this development is merely the application of appropriate analogical reasoning to determine how the known constraints extrapolate to these novel conditions?[4]

In this Essay, I propose the 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. Finally, I offer a set of precepts for the development and operation of autonomous systems and invite discussion on their accuracy and degree of comprehensiveness. I suggest how this methodology, and many of these precepts, applies to 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 the 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] and third, the identification of areas of emerging consensus or agreement among the contending stakeholders regarding the role of ethics in cyber warfare. This third debate centers on the development of cyber weapons and tactics, both those aimed indiscriminately at civilian personnel and "objects" such as vital civil infrastructure, and highly discriminate cyber weapons like Stuxnet

---

[2] *See* George R. Lucas, Jr., *Engineering, Ethics, & Industry: The Moral Challenges of Lethal Autonomy*, *in* KILLING BY REMOTE CONTROL: THE ETHICS OF AN UNMANNED MILITARY 211, 217–21 (Bradley Jay Strawser ed., 2013).

[3] *See* Randall Dipert, *The Ethics of Cyber Warfare*, 9 J. MIL. ETHICS 384, 394–95 (2010).

[4] *See* George R. Lucas, Jr., Jus in Silico*: Moral Restrictions on the Use of Cyberwarfare*, *in* THE ROUTLEDGE HANDBOOK OF ETHICS AND WAR: JUST WAR THEORY IN THE TWENTY-FIRST CENTURY 367, 368–71 (Fritz Allhoff et al. eds., 2013).

[5] *See* Ronald C. Arkin, *The Case for Ethical Autonomy in Unmanned Systems*, 9 J. MIL. ETHICS 332, 332–34 (2010); Noel Sharkey, *Saying 'No!' to Lethal Autonomous Targeting*, 9 J. MIL. ETHICS 369, 376–81 (2010).

[6] *See Who We Are*, INT'L COMMITTEE FOR ROBOT ARMS CONTROL, http://icrac.net/who/ (last visited Oct. 13, 2013).

and Flame that may be used in a preemptive or preventive fashion against perceived threats that have resulted in no actual harm, as yet, inflicted by the recipient of the cyber attack.[7]

These three examples do not exhaust all of the features of the wider debate over emerging military technologies, by any means. The increasing array of so-called nonlethal weapons, for example, involves questions about the use of such weapons on noncombatants and 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 specters 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. Such questions range from topics like informed consent for the use of these techniques, to the likely long-term health prospects for enhanced individuals following their military service, to the potentially undesirable social conflicts and transformations (i.e., "civilian blowback") that such techniques might inadvertently bring about.[10] For the present, however, I will stick to the three illustrations above because they collectively 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

---

[7] *See* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 188–209 (2012) (providing a retrospective account of the "Olympic Games" project to deploy the Stuxnet worm against Iranian nuclear facilities); George R. Lucas, Jr., *Permissible Preventive Cyber Warfare*, *in* THE ETHICS OF INFORMATION WARFARE (Luciano Floridi & Mariarosaria Taddeo eds., forthcoming 2013) (giving a preliminary summary of the discovery and strategic implications of the Stuxnet worm against the backdrop of three prior conflicts in Estonia, Syria, and Georgia in 2007 and 2008).

[8] *See, e.g.*, Paula Kaurin, *With Fear and Trembling: An Ethical Framework for Nonlethal Weapons*, 9 J. MIL. ETHICS 100, 100–02 (2010).

[9] *See, e.g.*, James J. Hughes, *Global Technology Regulation and Potentially Apocalyptic Technological Threats*, *in* NANOETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF NANOTECHNOLOGY 201, 201–04 (Fritz Allhoff et al. eds., 2007) (discussing the environmental threat of "grey goo" or unrestrained self-replicating nanotechnologies); Ray Kurzweil, *On the National Agenda: U.S. Congressional Testimony on the Societal Implications of Nanotechnology*, *in* NANOETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF NANOTECHNOLOGY, *supra*, at 40, 44–47 (providing examples of true nanotechnology such as the military's development of "smart dust," which consists of millions of nanodevices dropped on enemy territory to provide detailed surveillance).

[10] See PATRICK LIN ET AL., ENHANCED WARFIGHTERS: RISK, ETHICS AND POLICY 11–27, 66–76 (2013), *available at* http://ethics.calpoly.edu/Greenwall_report.pdf (providing an account of enhancement technologies and their prospective military uses and potential abuses).

developing working computational models of reasoning, including moral reasoning, is hardly impossible, 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 fulfill their programmable purposes without error or accident, and to have that programming designed to conform to relevant international law (such as the 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 behavioral benchmarks set by human agents performing similar tasks under similar circumstances.[12]

Second, proposals at this juncture to outlaw research, development, design, and manufacturing of autonomous weapons systems seem at once premature, ill timed, and 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 overregulate relevant behaviors.[13] Ultimately,

---

[11] The degree of futuristic speculation involved in such efforts is indicated in the Arkin-Sharkey debate. *See* Arkin, *supra* note 5; Sharkey, *supra* note 5; *see also* RONALD ARKIN, GOVERNING LETHAL BEHAVIOR IN AUTONOMOUS ROBOTS 93–113 (2009) (giving a proponent's account of the formidable challenges entailed in such efforts); Ronald Craig Arkin et al., *Moral Decision Making in Autonomous Systems: Enforcement, Moral Emotions, Dignity, Trust, and Deception*, 100 PROC. IEEE 571, 572–86 (2012) (providing an account of the progress on such efforts to date).

[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* George. R. Lucas, Jr., *Industrial Challenges of Military Robotics*, 10 J. MIL. ETHICS 274, 281 (2011); *see also* Robert Sparrow, *Building a Better Warbot: Ethical Issues in the Design of Unmanned Systems for Military Applications*, 15 SCI. & ENGINEERING ETHICS 169, 177–78 (2009) (explaining the need to design systems capable of complying with LOAC).

[13] In addition to proposals to outlaw armed or autonomous military robotic systems by ICRAC itself, a recent report from Human Rights Watch makes similar recommendations. *See* HUMAN RIGHTS WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 5 (2012), *available at* 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

such regulatory statutes would prove unacceptable to, and unenforceable against, many of the relevant 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 that might engage in reckless or criminally negligent behavior in the design, manufacture, and ultimate 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 a grave "cyber Armageddon"—of the sort predicted by Clarke and Brenner[17]—somewhat exaggerated. These commentators have even denied that the genuine equivalent of armed conflict has or could likely occur within this domain: no one has yet been killed, nor have objects been 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 and results in cumulative harm greater or more concrete than damage

---

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.

[14] Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 300–05 (2011).

[15] *See* MICHAEL SCHMIDT ET AL., THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 15–41 (2012), *available at* https://www.ccdcoe.org/249.html; *see also* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 98–100 (2010) (summarizing the applicability of the existing laws of war to cyber warfare); Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARVARD INT'L L.J. ONLINE 13, 15–18 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (discussing the applicability of international law to cyberspace). Cyber conflict and international law is also a topic of a special issue of the U.S. Naval War College's journal, *International Law Studies*. *See* Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger, *Preface* to 87 INT'L L. STUD. xxiii, xxiv–xxvi (2011).

[16] Randall Dipert authored the first article by an ethicist to address cyber warfare. Dipert, *supra* note 3, at 394–95. Computer scientist Neil C. Rowe had earlier raised moral concerns about cyber weapons and strategy. *See id.* at 394.

[17] JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 137–47 (2011); RICHARD A. CLARK & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 64–68 (2010).

[18] Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 10–15 (2011).

caused by conventional war.[19] However, several recent conflicts, at least one of which (Stuxnet) did cross the boundary defining an act of war, [20] have suggested the emergence of increasingly shared norms by which such conflict can be assessed, and perhaps constrained.

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 boundaries 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—have already been largely established. What is urgently needed at this juncture is a clear summary of the results of the discussions and debates (such as those surveyed above) 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 summarize the past several years of contentious debate in the following precepts, which define good or best practices and address the limits of acceptable versus unacceptable practices. I have already undertaken this task in the realm of cyber conflict[22] due to the reactions to several internationally acknowledged examples of

---

[19] John Arquilla, *Cyber War is Already Upon Us*, FOREIGN POL'Y, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us (last visited Mar. 5, 2013); Thomas Rid, *Think Again: Cyberwar*, FOREIGN POL'Y, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (last visited Mar. 5, 2013).

[20] *See* SANGER, *supra* note 7, at 188–209; Lucas, *supra* note 7.

[21] Marchant et al., *supra* note 14, at 306–14.

[22] *See* Lucas, *supra* note 4 at 367–75. There I summarize from extant literature that the use of a cyber weapon against an adversary is justified whenever there is a compelling reason for doing so, when every reasonable effort toward resolution has been expended with little likelihood of success, and when further delay will only make matters even worse. *See id.* at 372–73. Resort to cyber conflict is only justified, moreover, when the weapon is directed purely at military targets, the attack would inflict no more damage or loss of life than is reasonably proportionate to the threat posed, and finally, every effort is made to avoid or minimize harm to noncombatant lives or property. *Id.* In other respects, as noted below, these precepts of cyber conflict are similar to, or can be straightforwardly derived

cyber conflict that have recently occurred, from Estonia in 2007 to Stuxnet/Operation Olympic Flame in 2010.[23] The point of these exercises is not to presume or preempt proper legislative authority, but 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 ambiguities of moral discourse.

III. PRECEPTS FOR USE OF AUTONOMOUS SYSTEMS

Law and moral discourse, famously, always lag behind technological innovations—especially, if not exclusively, in warfare—and the innovations' transformative impact on the cultures in which they arise. That does not mean that law and morality are irrelevant and must be cast aside; neither 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 organize 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.

Precept #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). However, this does not hold true if the technology in question represents or employs weapons or methods that are already specifically proscribed under existing international weapons conventions, is in violation of the prohibitions in international humanitarian law against means or methods that inflict superfluous injury or unnecessary suffering, or is otherwise judged to constitute means *mala in se* (i.e., evil in themselves).[24]

---

from, several of the precepts regarding the development and use of unmanned systems discussed in this Article.

[23] *See supra* note 7.

[24] Wendell Wallach of Yale University, a well-respected ethicist, has recently proposed that lethal autonomous systems, at least, should—like rape and biological weapons—be classified among the means and methods of warfare that are *mala in se*. *See* Wendall Wallach, *Terminating the Terminator: What to Do About Autonomous Weapons*, SCI. PROGRESS (Jan. 29, 2013), http://scienceprogress.org/2013/01/terminating-the-termina tor-what-to-do-about-autonomous-weapons. This position would render the argument

Precept #2: The Principle of Unnecessary Risk[25]

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

Precept #3: The Principle of the Moral Asymmetry of Adversaries[26]

By contrast, no such obligation is owed to opponents or adversaries during such missions in their pursuit of presumably illegal and morally unjustifiable activities. That is, 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 longer 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 behavior: violation of domestic legal statutes and defiance of duly elected legal authorities, indiscriminate targeting of civilians and destruction of property, kidnapping, torture, execution, mutilation of prisoners, and so on.

Precept #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

---

regarding mission legality with respect to the use of such technology moot. It is not at all clear, however, that the reasons adduced for this classification are compelling in the case of unmanned systems generally. Not only does the analogy between autonomous systems and the examples of means *mala in se* given above not appear obvious, but Wallach's argument also rests on the largely discredited objection that machines cannot be held accountable for their actions.

[25] Bradley Jay Strawser, *Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles*, 9 J. MIL. ETHICS 342, 343–49 (2010).

[26] Note that this is not an explicit rejection of the doctrine of the "Moral Equality of Combatants," an essential element in what Michael Walzer defines as "the War Convention." *See* MICHAL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 34–37, 44–46 (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 the fashion of medieval jousting, 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.

available that promise the closest compliance with the international LOAC and applicable ROEs, such as noncombatant distinction (i.e., discrimination) and the economy of force (i.e., proportionality).

Precept #5: The Modified "Arkin Test"[27]

In keeping with Precept 4, an artifact (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 artifact 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 2 and 4 above, the use of such an artifact 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.

Precept #6: The Principle of Nondelegation of Authority and Accountability[28]

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."

Precept #7: The Principle of Due Care

All research and development, design, and manufacturing of artifacts such as lethally armed or autonomous unmanned systems that are 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 1–5 above. All R&D, design, and manufacturing of unmanned systems undertaken with full knowledge of, and in good faith compliance with, the above precepts (with 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.

Precept #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 6 above, shall be accountable under applicable international or domestic product liability law. Such accountability shall include full and fair

[27] *See* Arkin, *supra* note 5, at 332–34.

[28] This principle is indebted to the work of philosopher Robert Asaro of the New School in New York City, cofounder of ICRAC.

financial and other compensation or restitution for wrongful injury, death, or destruction of property.

Precept #9: The Principle of Criminal Negligence

By contrast, R&D, design, or manufacturing of systems undertaken through culpable ignorance or in deliberate or willful disregard of these precepts (including failure to perform or attempts to falsify the results, tests regarding safety, reliability of operation, or 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, or as reckless endangerment or criminally negligent behavior under the terms of applicable international 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 willful commission of war crimes 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.

Precept #10: 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 artifact produced or manufactured to meet or exceed these benchmarks.

Precept #11: Orientation and Legal Compliance

All individuals and organizations (including military services, industries, and research laboratories) engaged in R&D, design, manufacturing, acquisition, or use of unmanned systems for military purposes shall be required to attend an orientation and legal compliance seminar of not less than eight hours on these precepts, and upon its conclusion, to receive, sign, and duly file with appropriate authorities a 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 9) 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.[29]

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 behavior 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 rushing to legislation that would have both unenforceable and unintended harmful consequences.

Some of the foregoing precepts are specific to military robotics (e.g., Precepts 5 & 6, 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 nonlethal weapons, cyber warfare, projects for "warrior enhancement," and other military or domestic security technologies.

In the case of cyber conflict, for example, Precept 1 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 4 above), in an instance in which the use of force was otherwise justifiable, 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 (or nonlethal) weaponry, when the effects otherwise achieved are equivalent.

In sum, I believe there is far more consensus 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 ensure against the risk of unintended harm and consequences than do rival attempts at legal regulation or moral condemnation.

[29] A similar set of procedures (i.e., Precepts 10 and 11) is recommended for analogous programs involving cyber weapons and tactics, nonlethal weapons, and human enhancement projects (the last already to include compliance with relevant federal requirements regarding research on human subjects).