LETTING GO OF THE LOOP: COMING TO GRIPS WITH AUTONOMOUS DECISION-MAKING IN MILITARY OPERATIONS

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
14-06-2018	FINAL	

4. TITLE AND SUBTITLE

Letting Go of the Loop: Coming to Grips with Autonomous Decision-Making in Military Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

JOHN C. HEINS, Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES

A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy

14. ABSTRACT

Lethal autonomous weapon systems (LAWS) seem inevitable. Despite warnings from the scientific community not to pursue this "third revolution in warfare," the U.S. and its principal adversaries are exploring LAWS. U.S. commanders must be willing to relinquish some control to autonomous weapons in order to preserve the U.S. military advantage. This paper reviews current and upcoming technology, as well as U.S. and adversary efforts to implement it. It also discusses how the U.S. might increase its integration of AI-powered weaponry without compromising its values. A defensive focus, at least at first, will be more politically palatable, and will help to develop the necessary technology for offensive weapons if needed. Commanders should adapt human command and control models such as mission command to autonomous systems. Having established a trustworthy command and control model, the U.S. must accept that true autonomy will require removing the human from the loop in order to realize the weapons' capabilities. If the U.S. fails to do so, it will likely find itself on the receiving end of more effective weaponry in war.

15. SUBJECT TERMS

Lethal autonomous weapon systems, LAWS, autonomy, artificial intelligence, AI, drone swarms, OODA loop, air mines, AI mission command

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chariman, JMO Dept
UNCLASS	UNCLASS	UNCLASS		20	19b. TELEPHONE NUMBER *(Include area code)* 401-841-3556

Contents

Abstract

Lethal autonomous weapon systems (LAWS) seem inevitable. Despite warnings from the scientific community not to pursue this "third revolution in warfare," the U.S. and its principal adversaries are exploring LAWS. U.S. commanders must be willing to relinquish some control to autonomous weapons in order to preserve the U.S. military advantage. This paper reviews current and upcoming technology, as well as U.S. and adversary efforts to implement it. It also discusses how the U.S. might increase its integration of AI-powered weaponry without compromising its values. A defensive focus, at least at first, will be more politically palatable, and will help to develop the necessary technology for offensive weapons if needed. Commanders should adapt human command and control models such as mission command to autonomous systems. Having established a trustworthy command and control model, the U.S. must accept that true autonomy will require removing the human from the loop in order to realize the weapons' capabilities. If the U.S. fails to do so, it will likely find itself on the receiving end of more effective weaponry in war.

INTRODUCTION

In 1893, a detachment of 300 British South African Police were attacked by thousands of Matabele tribesmen in Rhodesia, known today as Zimbabwe. With only five machine guns, the British repelled the attack.[1] The *New York Times* reported at the time: "The Matabeles fought with desperate fury, but they found it impossible to stand up against machine guns, which laid the dead in swaths upon the field. It was not until 2,000 of the Matabeles were killed that the remainder retreated… The British loss was only five men killed."[2]

Through centuries of warfare, commanders have been duty-bound to adapt to changing technologies, both defending against them and incorporating them into their operations. Occasionally, an innovation on one side of a war catches the other side flat-footed, as happened in Zimbabwe in 1893. Adapting to new technology is a particularly important feature of the operational level of war: it is this level which directs tactical forces' employment, and where accomplishment of objectives can spell success or failure for national strategies. Successfully integrating new technology into operations—or failing to do so—can be decisive. Nonetheless, military leaders are not always eager to adopt new capabilities. Even after the machine gun proved its terrible effectiveness in Africa many times, military leaders in Europe were loath to abandon their pre-industrial sensibilities about what war should be like. The proliferation of machine guns in the First World War served as a jarring proclamation that while the nature of war endured, technology had changed its character forever.

Now, more than a century after the bloodshed of World War I, the world seems poised to learn a similar lesson again. This time, instead of machine guns, the emerging technology is

[1] John Ellis, *The Social History of the Machine Gun* (New York: Pantheon Books, 1975), 90.

[2] "Flee Before Machine Guns: The Matabeles Forced to Abandon Buluwayo," *New York Times*, November 10, 1893, 3, https://search.proquest.com/docview/95138505?pq-origsite=summon.

autonomous weaponry. In 2015, a consortium of researchers, scientists, and technologists known as "The Future of Life Institute" penned an open letter exhorting world governments to ban what they called "killer robots," otherwise known as Lethal Autonomous Weapon Systems (LAWS)—weapons capable of selecting and engaging targets without human intervention. The institute called killer robots "the third revolution in warfare, after gunpowder and nuclear arms."[3] Signatories included such luminaries as Elon Musk, Noam Chomsky, and Stephen Hawking. The letter has not slowed the pace of research, and although the United Nations (UN) has convened to discuss the matter several times, it has not come close to promulgating any agreements.[4]

LAWS represent the culmination of many technologies which are poised to enter the battlefield. Small, multirotor unmanned aircraft systems (UASs), commonly called "drones," can be programmed to attack in coordinated swarms, overwhelming defenses designed to repel attacks from fewer or larger targets. Artificial intelligence (AI)[5] is a burgeoning field with numerous possible applications in warfare—supplementing or perhaps even supplanting human warfighters entirely, despite the admonitions of the Future of Life Institute. So significant are the changes portended by AI that U.S. Secretary of Defense James Mattis speculated that it might

[3] Stuart Russell et al., "Autonomous Weapons: An Open Letter from AI & Robotics Researchers," Future of Life Institute, accessed April 13, 2018, https://futureoflife.org/open-letter-autonomous-weapons/.

[4] "UN: 'Killer Robots' Talks Fall Short," Human Rights Watch, November 28, 2017, https://www.hrw.org/news/2017/11/28/un-killer-robots-talks-fall-short.

[5] A note about AI: The notion of "artificial intelligence" often conjures images of a robot revolution led by self-aware machines. This is not the type of AI currently in use, nor the type expected to appear on battlefields any time soon. For existing and near-future technologies, "AI" refers to complex, learning systems and algorithms which can process and manipulate enormous quantities of data for specific tasks. This is known as "narrow" or "weak" AI, as opposed to "general AI," the self-aware systems currently relegated to the realm of science fiction. When using the term "AI," this paper is referring to narrow AI.

alter what has never changed before: the fundamental nature of war.[6]

In order to preserve the U.S. military edge, operational commanders must be willing to relinquish some control to artificially intelligent decision-making. The great combat potential of such technologies will make this abdication a necessity, and a diligent combination of policy and technology can make it palatable. This paper first explores the attributes which make AI-powered weapons so potent, including their independence, their decision-making speed, and their potential to mass combat power at minimal cost. It then considers some adversary efforts in the field of autonomous weapons which should be cause for concern, in addition to the current U.S. stance on the matter. Third, it will discuss how the U.S. could implement such technologies in an effective, trustable, and morally acceptable way. The paper will close with recommendations for specific actions the U.S. can take to maintain its military superiority in the changing technological landscape without compromising its values.

Automation is often discussed in terms of a decision loop. Systems in which the human operator must approve actions are known as "in-the-loop" systems. That is to say, the human operator is in the decision loop. In other systems, the human operator has the ability to intervene, but if he or she does not, the system will take action. These are known as "on-the-loop" systems, where the operator can affect the decision cycle, but is not necessarily part of it. This paper discusses a move toward "off-the-loop" systems, where human control is neither necessary nor even possible beyond initial mission parameters, at least for portions of a system's mission.

Commanders are right to be wary of such a loss of control, particularly when it could mean a loss of agency in the prosecution of violence. After all, a commander is ultimately

[6] James Mattis, "Press Gaggle by Secretary Mattis En Route to Washington, D.C.," U.S. Department of Defense, February 17, 2018, https://www.defense.gov/News/Transcripts/Transcript-View/Article/1444921/press-gaggle-by-secretary-mattis-en-route-to-washington-dc/.

responsible for every action taken under his or her command. Commanders should bear in mind that if properly implemented, being "off the loop" does not mean a loss of control in the military sense, but rather an evolution in the way they exercise control. In enemy hands, these technologies have the potential to severely disrupt another decision loop: commanders' "OODA loop" (observe, orient, decide, and act)[7]—and therefore endanger the commanders' chances of prevailing. For that reason alone, it is important to fully understand the implications of these technologies, and make an informed decision about their role in military operations. As European commanders learned in the crucible of World War I, survival of the force, and the ability to achieve objectives, hinges on the ability to adapt to and overcome change.

ADVANTAGES OF AI WEAPONRY

Imagine a vehicle on tank-like treads with a turret-mounted laser cannon. Its unblinking eye continuously surveys its sector. It detects a swarm of objects in the distance. Their flight is erratic, but the swarm is closing distance. The vehicle instantaneously compares the objects' profile to its target portfolio, finds a match, and without consulting any human, energizes its laser and destroys 40 targets in one second. The entire battle is over in the blink of an eye.

Astonishingly, the preceding paragraph is not fiction. But the flying objects were not a drone swarm; they were a swarm of mosquitoes. The vehicle was not a military weapon, but a pest control product from LeiShen Intelligent, a Chinese LiDAR[8] company, called "Laser

[7] The OODA loop model was coined by U.S. Air Force fighter pilot Colonel John Boyd as a way of thinking about tactical awareness, information processing, and decision-making in the cockpit. A faster, or smaller, OODA loop, as might be achieved with the help of AI weapons, confers a tactical, operational, and strategic advantage (corresponding to the level of the decision cycle). *Business: The Ultimate Resource*, *s.v.* "OODA loop," accessed May 4, 2018, https://search.credoreference.com/content/entry/ultimatebusiness/ooda_loop/0.

[8] LiDAR is a system comparable to radar which uses laser pulses to illuminate objects.

Movable Mosquito Killer Robot," which they are attempting to market to hospitals, schools, and other facilities plagued by mosquitoes or mosquito-borne diseases.[9] If LeiShen Intelligent's claims about the device are to be believed (and some skepticism is warranted[10]), then comparable battlefield technologies are only a matter of scale, not feasibility. Such a weapon, with sufficient power, could provide an extraordinarily effective counter-air capability to protect a naval fleet, as one example. In the hands of an enemy, it could neutralize U.S. cruise missiles, air strikes, or even intercontinental ballistic missiles.

AI-powered weaponry has multiple unique attributes which distinguish it from other types of weapons. Chief among these are its ability to scale nearly effortlessly, its ability to make instantaneous decisions without supervision, and its low cost. These attributes are interrelated and complementary, and cannot be considered in isolation: their potency lies in their combination. One example of a system which effectively combines these attributes is the drone swarm.

Until defensive systems such as the mosquito-killer described above become reality on a larger scale, drone swarms will present a significant problem. In February 2018, China claimed the world record for the largest drone swarm, with a formation of 1,108 small drones lighting up the sky in a variety of configurations for the 2017 Global Fortune Forum.[11] The drones demonstrated self-organizing abilities such as collision avoidance, deconfliction, and configuration changes; compensation for meteorological factors without losing swarm cohesion;

---

[9] Tony Skinner, "Presenting, the Mosquito-Killer Robot," *Quill or Capture,* September 14, 2016, https://quillorcapture.com/2016/09/14/presenting-the-mosquito-killer-robot/.

[10] Outside of promotional materials and a series of articles based on such materials, there appears to be no proof of the device's functionality. However, comparable systems have been developed in the U.S., but they are currently very large: https://www.youtube.com/watch?v=fH_x3kpG8Z4.

[11] Scott N. Romaniuk and Tobias Burgers, "China's Swarms of Smart Drones Have Enormous Military Potential," *The Diplomat* (Tokyo), Feb 2, 2018, https://search-proquest-com.usnwc.idm.oclc.org/docview/1993637936;

and the ability to operate through component failure (malfunctioning drones could self-identify and safely land). In such a swarm, when a component fails, that portion of the "mission" does not fail; the remaining drones coordinate to dynamically re-assign themselves and repair the swarm.[12] The Chinese record was soon broken by American technology company Intel in a display at the 2018 Olympics featuring 1,218 drones, but China, perhaps to reassert its leadership in the field, reclaimed the record three months later with a swarm of 1,374 drones.[13]

While the record-setting drone swarms served as entertainment, the capabilities they demonstrated could be extraordinarily useful in a military operation. A thousand drones, simply by their presence, could overwhelm, distract, or deplete anti-aircraft defenses, torment a land force during an invasion, or render aircraft carrier flight operations unsafe or impossible—all for around $1.5 million.[14] If each drone were fitted with a small explosive, the swarm could damage every plane on a carrier, wreak havoc on a military base, or destroy a convoy. To reiterate, these are not speculative capabilities; existing technology could perform these tasks today.

While no nation-states have employed drone swarm technology on the battlefield yet—perhaps in an effort to avoid setting a precedent, or perhaps simply because the opportunity has not yet presented itself—the technology's low cost means that its use is not limited to nation-states. In January of 2018, a swarm of thirteen explosives-laden drones attacked two Russian bases in Syria. Russia was able to stop the kamikaze-style attack with a combination of kinetic and unspecified non-kinetic defenses, and was able to trace their origin to a rebel encampment.

---

[12] *Ibid*.

[13] "Flight of Imagination: Chinese Firm Breaks Record with 1,374 Dancing Drones," *Reuters,* May 2, 2018, https://www.reuters.com/article/us-china-drones/flight-of-imagination-chinese-firm-breaks-record-with-1374-dancing-drones-idUSKBN1I3189.

[14] Jeffrey Lin and P.W. Singer, "China is making 1,000-UAV Drone Swarms Now," *Popular Science,* January 8, 2018, https://www.popsci.com/china-drone-swarms.

Three of the thirteen drones still exploded when they struck the ground.[15] In this case, the difference between thirteen drones and 1,300 is a matter of resources, not technical feasibility. Had the rebels attacked with 1,300 drones, Russian defenses would almost certainly have proved inadequate to stop the whole swarm, and even with the same demonstrated success rate, 300 of them would have exploded—a highly successful attack by almost any measure.

This cost-effective approach to achieving mass in a military operation poses a distinct problem for human defenders and existing weaponry. But mass is not the only principle through which existing defenses might be attacked. Another is speed—not of the weapon, but of the decisions it makes. The "OODA loop" decision cycle mentioned above could also be described as a model for collecting, processing, and acting upon information. But information collection and processing is not limited to humans. The three essential functions of a computer system are input, processing, and output. With sufficient sophistication (which, in the realm of computers, is only a matter of time), there is no reason computers could not absorb the same information humans do (observe and orient), process it according to pre-established or learned parameters (decide), and behave in accordance with the outcome of that processing (act).

Two differences between such future systems and humans are that the computers will process more information, and they will process it more quickly and accurately. This does not bode well for advocates of human decision-making in military operations. AI has already been applied to comparable problems, such as weather prediction, where the explosion of available data has overwhelmed human forecasters, but not their artificially intelligent counterpart systems.[16] Data proliferation plagues the military decision-maker as well. Modern cockpits and

[15] Mauro Lubrano, "Swarm Drone Attack in Syria Points to New Kind of Warfare," *Global Risk Insights,* January 18, 2018, https://globalriskinsights.com/2018/01/swarm-drone-attack-syria-uav/.
[16] Amy McGovern et al., "Using Artificial Intelligence to Improve Real-Time Decision-Making for High-Impact Weather," *Bulletin of the American Meteorological Society* 98 no. 10 (2017): 2073.

even pilots' helmets are crowded with instruments and data readouts seeking to maximize pilots' situational awareness.[17] Remotely piloted aircraft (RPA) ground control stations, where the size of the cockpit is no constraint, have been fitted with as many as nine computer screens, far more than the operators can effectively monitor and, according to a NASA human factors engineer, more likely to cause an error than prevent one.[18] These examples of information overload at the tactical level pale in comparison to the task of the operational commander, who has access to the same volume of information from each of hundreds or thousands of endpoints. AI could be applied to decision support systems, distilling multitudinous video feeds, signals intelligence products, and tactical data links into the key elements a commander needs to make decisions—and perhaps make the straightforward decisions automatically. Failure to allow such automation could place the commander one step behind an adversary willing to do so.

While commanders may become comfortable with automating some decisions, many would balk at automating the decision to kill a human. Unfortunately, the clear speed advantages automation confers will likely prove too tempting for an otherwise disadvantaged party in a conflict. In other words, a U.S. adversary may automate killing in order to shrink their OODA loop beyond the U.S.'s ability to react. In response to such provocation, the U.S. would have no choice but to similarly implement automation, or risk losing the engagement.[19]

In aggregate, the picture seems bleak: Systems less error-prone than their human

[17] "F-35 Helmet Mounted Display," Lockheed Martin, accessed May 6, 2018, https://www.f35.com/about/capabilities/helmet.

[18] Alan Hobbs, "Human Factors of Remotely Piloted Aircraft Systems: Lessons from Incident Reports," National Aeronautics and Space Administration, February 10, 2017, https://www.nasa.gov/mediacast/human-factors-of-remotely-piloted-aircraft-systems-lessons-from-incident-reports.

[19] *The Economist,* "Autonomous weapons are a game-changer," January 25, 2018, https://www.economist.com/news/special-report/21735472-ai-empowered-robots-pose-entirely-new-dangers-possibly-existential-kind-autonomous.

counterparts; systems with smaller OODA loops than the fastest human; weapons too numerous to defend against, able to "think" among themselves and dynamically "heal." Admittedly, with much of LAWS' operative technology still in development, little assurance of its battlefield capability may be obtained beyond speculation. Based on its expected usefulness, however, some U.S. adversaries are already integrating it into their militaries.

ADVERSARY AND U.S. STANCES

In spite of the aforementioned cautions from the global scientific community, U.S. adversaries are already experimenting with new technologies of war which they hope will give them a competitive advantage against the world's military behemoth—the United States. In fact, Russia has openly declared its intention to disregard any UN ban on autonomous weapons. During UN discussions on the matter, Russia alleged that there is not sufficient information to ban devices which do not yet exist, and objected to a lack of proper definitions for terms such as "meaningful human control."[20] Meanwhile, the Russian weapons manufacturer Kalashnikov (famous for the ubiquitous AK-47 assault rifle) has already begun work on such an autonomous weapon. Russian state news network *RT* (formerly *Russia Today*) reported that the weapon already exists, and quoted the Kalashnikov communications director saying, "In the nearest

[20] Patrick Tucker, "Russia to the United Nations: Don't Try to Stop Us From Building Killer Robots," *Defense One,* November 21, 2017, https://www.defenseone.com/technology/2017/11/russia-united-nations-dont-try-stop-us-building-killer-robots/142734/?oref=d-topstory;

Russian Federation, "Examination of Various Dimensions of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, in the Context of the Objectives and Purposes of the Convention," Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW), November 10, 2017, https://admin.govexec.com/media/russia.pdf.

future we plan to unveil a whole line of neural network[21] based products. A fully automated combat module based on that technology is to be unveiled during the ARMY-2017 forum."[22] At the same time, Russia has fielded and tested autonomous tanks which, it says, have "outperformed" tanks operated by human drivers for certain tasks—although the specific tasks were not revealed. A Russian colonel told a Russian journalist, "In the Armed Forces new robots come, they perform the tasks of reconnaissance, de-mining, firefighting. In the future, in addition to these, the tasks of shock, assault will also be decided."[23]

China, perhaps surprisingly, was in 2016 among the first nations to call for a ban on LAWS, and the first UN Security Council member to do so. Its justification for the proposal was a concern that such weapons might violate human rights through an inability to adhere to the principles of Just War—particularly Distinction between combatants and noncombatants, and Proportionality of harm done when compared to the achieved military advantage. Since that original call, China has shifted its position from an outright ban to advocacy for "responsible use of LAWS," likely due to a desire not to be caught at a disadvantage should its peer adversaries continue to develop the weapons.[24]

During the same time that its stance on LAWS was evolving, China declared its intention to be the world leader in AI by the year 2030. Nominally, the effort seeks economic benefits, but

---

[21] A neural network is a common feature of AI systems which seeks to mimic the information-processing patterns of an organic brain.

[22] "Kalashnikov develops fully automated neural network-based combat module," *RT,* July 5, 2017, https://www.rt.com/news/395375-kalashnikov-automated-neural-network-gun/.

NOTE: No further information about any such unveilings could be located for this paper.

[23] *News.com.au*, "Russia Moving Towards an Increasingly Automated Arsenal, With New Robots Being Tested," November 20, 2017, http://www.news.com.au/technology/innovation/inventions/russia-moving-towards-an-increasingly-automated-arsenal-with-new-robots-being-tested/news-story/9ff893493df2fb6dd654c1ddeeb0575b.

[24] Bedavyasa Mohanty, "Lethal Autonomous Dragon: China's Approach to Artificial Intelligence Weapons," *Observer Research Foundation,* November 15, 2017, https://www.orfonline.org/expert-speak/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence/.

China acknowledged its ancillary military value. Such declarations have prompted concern among U.S. leaders that ongoing Chinese investment in U.S. AI firms could amount to the U.S. providing its own adversary with a technological edge.[25] China has already begun incorporating AI into its weapon systems, according to one analyst's testimony before the U.S.-China Economic and Security Review Commission.[26] An additional source of concern is that China is not domestically constrained from developing artificially intelligent systems by legal, political, or privacy issues. Such systems could be trained and tested on citizens' data, to which the government has unfettered access.[27] These concerns highlight an imbalance between the U.S. and Chinese governments' ability to rapidly incorporate new technology into their militaries.

The U.S., meanwhile, has issued policy *preventing* the pursuit of broad categories of autonomous weapons. Department of Defense Directive 3000.09, published in 2012 but still in force, states, "*Human-supervised* autonomous weapon systems may be used to select and engage targets, *with the exception of selecting humans as targets.*" [Emphasis added.][28] The directive does provide a provision for exceptions, which must be approved by two Undersecretaries of Defense and the Chairman of the Joint Chiefs of Staff.[29] No information is publicly available about any systems which have received such approval. The directive does provide significant

[25] Arjun Kharpal, "China Wants to be a $150 Billion World Leader in AI in Less than 15 Years," *CNBC,* July 21, 2017, https://www.cnbc.com/2017/07/21/china-ai-world-leader-by-2030.html.

[26] Elsa B. Kania, "Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence—the PLA's Trajectory towards Unmanned, 'Intelligentized' Warfare," Testimony before the U.S.-China Economic and Security Review Commission, February 23, 2017, https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf.

[27] Aleksandra Urman, "Smart Killer Robots: China's Military Future Could Rest on Artificial Intelligence," *The Defense Post,* January 2, 2018, https://thedefensepost.com/2018/01/02/china-artificial-intelligence-drones/.

[28] U.S. Department of Defense, "Autonomy in Weapon Systems," DoD Directive 3000.09, November 21, 2012, incorporating change 1, May 8, 2017, 3, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.

[29] *Ibid,* 3.

latitude for systems to engage non-human targets, but requires "commanders and operators to exercise appropriate levels of *human judgment* over the use of force." [Emphasis added.][30] It does not define what "appropriate levels of human judgment" entail, but the very requirement precludes ceding human judgment to machine judgment. The directive also requires human supervision "in order for operators to make informed and appropriate decisions in engaging targets," and specifies that there should be an interface which provides system status to the operator.[31] The requirement for human supervision, and human involvement in engagement decisions, undermines and perhaps even invalidates the concept of "autonomy." Additionally, a system status interface and the ability for a human operator to intervene would necessitate a control channel comparable to today's RPAs. A control channel creates the possibility of tracking the craft, jamming or hacking the channel, and otherwise increases the weapon's vulnerability to enemy cyber or kinetic defenses.

The apparently divergent approaches between the U.S. and its principal adversaries, Russia and China, in the realm of autonomous weaponry could result in a combat disadvantage for the U.S., jeopardizing the success of military operations and undermining the longstanding deterrent effect which U.S. military superiority has exerted against adversary actions. An interest in preserving that superiority, and the concomitant deterrent effect, necessitates a closer look at how the U.S. could counter these forthcoming adversary capabilities and incorporate evolving technology into its own arsenal.

BUILDING TRUST WITH AI

[30] *Ibid,* 2.

[31] *Ibid,* 2.

Artificial intelligence is often poorly understood and inaccurately depicted in popular culture as a malevolent adversary. As a result, skepticism and distrust of the implications of its use are common. No implementation of any weapon can be successful unless those who wield the weapon have confidence that the weapon will be effective and controllable. Furthermore, the citizenry on whose behalf the military does violence should have confidence that the military can use its weapons in a manner which comports with their values. As human decision-makers ponder for the first time weapons which might make decisions on their behalf, it is important to understand how those weapons could earn and keep that confidence. This can be achieved, in part, by better understanding how the military might use such weapons, including a consideration of systems which the military already uses and trusts. Additionally, it is useful to consider how command and control might be extended over nominally autonomous systems.

Because U.S. adversaries are actively pursuing autonomous weaponry, a logical first step would be to approach the matter from a defensive perspective. Protection is a vital function of all military operations, and commanders would be unwise to discard capabilities which fulfill a previously unmet defensive requirement. Adversary AI-powered weapons present just such an unmet requirement. The U.S. might seek to supplement defensive counter-air, anti-submarine warfare, and mine countermeasures with “counter-AI” systems and doctrine which themselves rely heavily on AI. Air weapons, once in flight, must be countered in the air; similarly, AI weapons, once unleashed, must perhaps be countered with AI-based defenses.

Acknowledgement that autonomous weapons already exist outside the realm of experimentation, and have already been integrated into successful operations, is another endorsement for the technology. South Korea has weapons guarding the Demilitarized Zone which are reportedly capable of automatically killing human targets—although South Korea

appears not to operate them in that mode regularly.[32] The U.S. Navy's Phalanx Close-in Weapons System, which is designed to be the last line of defense against airborne threats to the fleet, is an "on-the-loop" system consisting of a shipboard rotary cannon which can identify, select, and destroy threats such as aircraft or anti-ship missiles with no human involvement.[33] Additionally, four subsystems of the U.S. Ballistic Missile Defense System are identified in the 2014 assessment report as "autonomous combat systems," designed to defend against incoming threats more quickly than human operators could respond.[34] Autonomous weapons seem to be palatable to both leaders and voters when they are employed in a defensive manner.

While limiting autonomous weapons to a defensive posture may seem restrictive, it still permits and encourages the development of many of the same capabilities which would be critical for offense; both offense and defense require all elements of the OODA loop. "Observe" is arguably more vital for defense, where an incomplete observation can be catastrophic. If, after fielding robust and varied autonomous defensive capabilities, the U.S. decides to employ autonomy offensively (perhaps against an enemy's autonomous defenses), the relevant functions will already have been combat-tested. For example, a defensive drone swarm designed to protect the approaches to an aircraft carrier's flight deck, with minimal reprogramming, could be dispatched to interfere with flight deck operations on an enemy carrier instead.

Protecting or attacking carrier operations in this way can be seen as an airborne analog to sea mines. Air Force Lieutenant Colonel Leslie Hauck and Colonel (retired) John Geis authored a paper in 2017 entitled "Air Mines," which paints a picture of near-future drone swarm

---

[32] Rebecca Crootof, "War Torts: Accountability for Autonomous Weapons," *University of Pennsylvania Law Review* 164 no. 6 (2016): 1367.

[33] U.S. Navy, "MK 15 - Phalanx Close-in Weapons System (CIWS)," last modified January 27, 2017.

[34] U.S. Department of Defense Director of Operational Test & Evaluation, *2014 Assessment of the Ballistic Missile Defense System (BMDS)* (Washington, DC: 2015), http://www.dtic.mil/dtic/tr/fulltext/u2/a617330.pdf.

technology in which, thanks to projected developments in battery technology, drones can loiter in the airspace of a military base for long periods of time—unlimited periods of time, with sufficient replenishment. They compare such swarms to efforts in World War II to deny airspace to low-flying bombers by flying large hydrogen balloons trailing wires. Drones, however, would be nearly impossible to detect, and could autonomously maneuver to intercept aircraft. This sort of technology could be used both defensively—to protect a fleet or base from incoming airborne threats—or offensively, to suppress air operations at an enemy base, or to follow and attack ground forces.[35] A marginal (and fully expected) increase in today's technological capability would create the possibility of extending a previously two-dimensional effect—area denial by means of mines—into the third dimension. The use of air mines in this way might be termed "sky denial." Sky denial could be much more flexible than mine-based area or sea denial: airborne minefields composed of drones could be deployed and retracted on command, could maneuver around friendly aircraft, or could deploy in response to an imminent or ongoing threat. An aircraft carrier outfitted with such defensive systems could become a "hornet's nest"—for more reasons than housing F/A-18 Hornets. Attacking it could provoke a swarming response, instantly launching hundreds or thousands of drones to defend their assailed ship.

The value of such defensive measures might extend beyond the immediate engagement: it could confer a deterrent effect. While "deterrence by punishment" was a fixture of the Cold War in the form of mutually assured destruction, another type of deterrence is by denial. Deterrence by denial exists when the defender emplaces defenses of such effectiveness that the attacker recognizes the attack is unlikely to achieve the desired effect, and declines to pursue it.[36] While

[35] Leslie F. Hauck III and John P. Geis II, "Air Mines: Countering the Drone Threat to Aircraft," *Air & Space Power Journal* 31 no. 1 (2017): 26-28.

[36] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41 no. 3 (2017): 56.

mutually assured destruction is an element of strategic deterrence, deterrence by denial is an important element at all levels of war.

In order to fully reap the benefits of these imminent technologies, U.S. decision makers will need to adjust to some new ideas. The 2012 requirement that "autonomous" systems have synchronous human control is incompatible with a contested electromagnetic spectrum, a highly likely feature of any conflict with a near-peer adversary. In such a contested environment, jamming or control signal hijacking would be major concerns for systems reliant on a control link. If the U.S. does proactively reduce or eliminate its reliance on that link, one of the consequences would be the loss of the human failsafe. While losing the human failsafe introduces risk, that risk may be mitigated by adapting the concept of mission command to AI.

Mission command refers to a commander's ability to provide a mission and his or her intent to subordinate leaders, who in unanticipated circumstances will act according to the senior commander's wishes without his or her direct approval or intervention.[37] This is precisely how autonomous weapons must function. Aside from their computerized nature, they must be trusted to act appropriately in much the same way military members are when they are unable to seek approval for every action. For military members, this trust is built through a time-honored process of training, education, indoctrination, and mentoring. Whenever the U.S. sends its military members into action, it takes a risk that one of them will behave unexpectedly—which does sometimes happen, necessitating corrective action. Sophisticated machines can be managed in a similar manner. Like humans, they can be trained; the CEO of Uber, in response to an autonomous vehicle accident, said that their fleet of self-driving cars should be considered

[37] Martin E. Dempsey, "Mission Command White Paper," Office of the Chairman, U.S. Joint Chiefs of Staff, April 3, 2012, http://www.jcs.mil/Portals/36/Documents/Publications/missioncommandwhitepaper2012.pdf.

"student drivers," but that eventually they would be superior to their human counterparts.[38] One advantage computerized systems will have is that once trained, they will all execute tasks at the same level of proficiency, unlike humans. Additionally, it will be possible to adjust ("mentor") them all simultaneously. Due to the sheer complexity of the systems, they may sometimes act unexpectedly; the same is true of human beings, who are themselves extraordinarily complex. As with human soldiers, we must manage machines to reduce risk as much as possible, and accept what risk cannot be mitigated.

Because some autonomous systems are already in use defensively and are trusted, increasing reliance on such systems will be a matter of evolution, not revolution—at first. When the U.S. needs more *revolutionary* capability, such as offensive autonomy, a foundation of trust with similarly sophisticated defensive systems will be vital to the successful and timely integration of capabilities which might mean the difference between victory and defeat.

CONCLUSIONS

AI-powered weapons bring unprecedented capabilities, and with them unprecedented questions—some of which cannot be answered until the technology matures. The warnings of the scientific community should not be ignored, and the U.S. should support good-faith efforts of the United Nations and other countries to restrict certain types of weapons, including autonomous offensive weapons, when consensus permits. But the march of technology imparts an air of inevitability; it would be irresponsible not to be prepared and willing to employ these technologies in an operational scenario should the need arise.

Commanders must educate themselves about AI in order to understand its place in

[38] Cara Lombardo, "Uber CEO Says Self-Driving Cars Are 'Student Drivers'," *Wall Street Journal*, April 12, 2018, https://www.wsj.com/articles/uber-ceo-says-self-driving-cars-are-student-drivers-1523538431.

warfare, and to accept that they must release some control to technology in order to preserve their combat edge. In order to foster this understanding, the U.S. must conduct a thorough exploration of the military possibilities created by the technologies, after which it can make informed policy decisions about their employment. The actions of U.S. adversaries will necessarily have great influence over those decisions. No matter to what degree the U.S. integrates autonomous weapons into its arsenal, it will be vital for operational commanders to trust the weapons, and to be comfortable that such weapons are capable of prosecuting a mission within the bounds of the commander's intent.

Above all, it is critical to remember the errors of previous generations, whose lessons were measured in millions of deaths as the infantry charged across the open field into a hail of machine gun fire. Adherence to familiar paradigms and technologies is comforting until those paradigms are challenged by superior ones on the battlefield. As social historian John Ellis said: "When faced with the machine gun…, [traditional] soldiers either did not understand the significance of the new weapon at all, or tried to ignore it, dimly aware that [it] spelled the end of their own conception of war."[39] If U.S. decision-makers and military leaders hesitate to release some control from human hands, they risk being a new generation of "traditional soldiers"—standing stubbornly in the loop and staring down the swarm.

RECOMMENDATIONS

Educate Commanders

Commanders—and rising officers who will soon command—must become familiar with the technologies they may be facing, or may be asked to wield. An idea of AI drawn from science

[39] Ellis, 16.

fiction will cause needless apprehension and delay in adopting important technologies. In the absence of service-sponsored education, commanders should seek to educate themselves to eliminate misconceptions.

Broaden the U.S.-sanctioned definition of "autonomy"

The 2012 U.S. governing document for autonomous weapon systems establishes guidelines which are incompatible with true autonomy and which create EW and cyber vulnerabilities. Future systems may have an emergency abort capability (such as a passive antenna listening for an abort code), but there must be no requirement for synchronous oversight or human decision-making in routine operations if the U.S. hopes to realize the full advantages of AI.

Develop mission command and trust models for AI

While the technology is nascent, the U.S. must adapt the concept of mission command to AI in order to establish proper training, test, and evaluation standards. These standards should be used to establish sufficient trust to allow systems to operate unsupervised. This will require not just examining code and engineering, but also observing deep-learning systems' behavior, which will manifest in ways not deducible through component analysis. The U.S. must exercise the same care when implementing training for self-learning systems as it does for the training of humans. The systems will be best prepared for scenarios to which they are exposed in training. Such training could be done on a small scale, and the lessons promulgated to the force.

Support a ban on *offensive* autonomous weapons

An international agreement not to employ autonomous weapons offensively would not eliminate the possibility of their use, but may reduce the death and destruction they cause. By continuing

research into dual-use technologies, the U.S. will preserve a deterrent “broken glass” capability to use against nations which employ autonomy offensively and which can only be stopped by similarly autonomous systems.

Selected Bibliography

Crootof, Rebecca. “War Torts: Accountability for Autonomous Weapons.” *University of Pennsylvania Law Review* 164 no. 6 (2016): 1347-1402.

Dempsey, Martin E. “Mission Command White Paper.” Office of the Chairman of the Joint Chiefs of Staff, April 3, 2012. http://www.jcs.mil/Portals/36/Documents/Publications/missioncommandwhitepaper2012.pdf.

The Economist. “Autonomous weapons are a game-changer.” January 25, 2018. https://www.economist.com/news/special-report/21735472-ai-empowered-robots-pose-entirely-new-dangers-possibly-existential-kind-autonomous.

Ellis, John. *The Social History of the Machine Gun.* New York: Pantheon Books, 1975.

Gilboa, Eytan. "The CNN Effect: The Search for a Communication Theory of International Relations." *Political Communication* 22 no. 1 (February 2005): 27.

Hauck III, Leslie F. and John P. Geis II. “Air Mines: Countering the Drone Threat to Aircraft.” *Air & Space Power Journal* 31 no. 1 (2017): 26-40.

Hobbs, Alan. “Human Factors of Remotely Piloted Aircraft Systems: Lessons from Incident Reports.” National Aeronautics and Space Administration. February 10, 2017. https://www.nasa.gov/mediacast/human-factors-of-remotely-piloted-aircraft-systems-lessons-from-incident-reports.

Human Rights Watch. “UN: ‘Killer Robots’ Talks Fall Short.” November 28, 2017. https://www.hrw.org/news/2017/11/28/un-killer-robots-talks-fall-short.

Kania, Elsa B. “Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence—the PLA’s Trajectory towards Unmanned, ‘Intelligentized’ Warfare.” Testimony before the U.S.-China Economic and Security Review Commission, February 23, 2017. https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf.

Kharpal, Arjun. “China Wants to be a $150 Billion World Leader in AI in Less than 15 Years.” *CNBC*, July 21, 2017. https://www.cnbc.com/2017/07/21/china-ai-world-leader-by-2030.html.

Lin, Jeffrey and P.W. Singer. “China is making 1,000-UAV Drone Swarms Now.” *Popular Science*, January 8, 2018. https://www.popsci.com/china-drone-swarms.

Lockheed Martin. “F-35 Helmet Mounted Display.” Accessed May 6, 2018. https://www.f35.com/about/capabilities/helmet.

Lubrano, Mauro. “Swarm Drone Attack in Syria Points to New Kind of Warfare.” *Global Risk Insights*, January 18, 2018. https://globalriskinsights.com/2018/01/swarm-drone-attack-syria-uav/.

Mattis, James. “Press Gaggle by Secretary Mattis En Route to Washington, D.C.” U.S. Department of Defense, February 17, 2018. https://www.defense.gov/News/Transcripts/Transcript-View/Article/1444921/press-gaggle-by-secretary-mattis-en-route-to-washington-dc/.

McGovern, Amy et al. “Using Artificial Intelligence to Improve Real-Time Decision-Making for High-Impact Weather.” *Bulletin of the American Meteorological Society* 98 no. 10 (2017): 2073-2090.

Mohanty, Bedavyasa. “Lethal Autonomous Dragon: China’s Approach to Artificial Intelligence Weapons.” Observer Research Foundation, November 15, 2017. https://www.orfonline.org/expert-speak/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence/.

New York Times. "Flee Before Machine Guns: The Matabeles Forced to Abandon Buluwayo." November 10, 1893. https://search.proquest.com/docview/95138505?pq-origsite=summon.

News.com.au. “Russia Moving Towards an Increasingly Automated Arsenal, With New Robots Being Tested.” November 20, 2017. http://www.news.com.au/technology/innovation/inventions/russia-moving-towards-an-increasingly-automated-arsenal-with-new-robots-being-tested/news-story/9ff893493df2fb6dd654c1ddeeb0575b.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41 no. 3 (2017): 44-71.

Reuters. “Flight of Imagination: Chinese Firm Breaks Record with 1,374 Dancing Drones.” May 2, 2018. https://www.reuters.com/article/us-china-drones/flight-of-imagination-chinese-firm-breaks-record-with-1374-dancing-drones-idUSKBN1I3189.

Romaniuk, Scott N. and Tobias Burgers. “China’s Swarms of Smart Drones Have Enormous Military Potential.” *The Diplomat* (Tokyo), Feb 2, 2018. https://search-proquest-com.usnwc.idm.oclc.org/docview/1993637936.

RT. “Kalashnikov develops fully automated neural network-based combat module.” July 5, 2017. https://www.rt.com/news/395375-kalashnikov-automated-neural-network-gun/.

Russell, Stuart et al. "Autonomous Weapons: An Open Letter from AI & Robotics Researchers." Future of Life Institute. Accessed April 13, 2018. https://futureoflife.org/open-letter-autonomous-weapons/.

Russian Federation. “Examination of Various Dimensions of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, in the Context of the Objectives and Purposes of the Convention.” Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW), November 10, 2017. https://admin.govexec.com/media/russia.pdf.

Skinner, Tony. “Presenting, the Mosquito-Killer Robot.” *Quill or Capture*, September 14, 2016. https://quillorcapture.com/2016/09/14/presenting-the-mosquito-killer-robot/.

Tucker, Patrick. “A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid.” *Defense One*. May 3, 2018. https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/.

Tucker, Patrick. “Russia to the United Nations: Don’t Try to Stop Us From Building Killer Robots.” *Defense One*, November 21, 2017. https://www.defenseone.com/technology/2017/11/russia-united-nations-dont-try-stop-us-building-killer-robots/142734/?oref=d-topstory.

U.S. Department of Defense Director of Operational Test & Evaluation. *2014 Assessment of the Ballistic Missile Defense System (BMDS).* Washington, DC: 2015. http://www.dtic.mil/dtic/tr/fulltext/u2/a617330.pdf.

U.S. Department of Defense. “Autonomy in Weapon Systems.” DoD Directive 3000.09, November 21, 2012, incorporating Change 1, May 8, 2017. http://www.esd.whs.mil/Directives/issuances/dodd/.

U.S. Navy. “MK 15 - Phalanx Close-in Weapons System (CIWS).” Last modified January 27, 2017.

Urman, Aleksandra. “Smart Killer Robots: China’s Military Future Could Rest on Artificial Intelligence.” *The Defense Post*, January 2, 2018. https://thedefensepost.com/2018/01/02/china-artificial-intelligence-drones/.