

A.I. JOE:

THE DANGERS OF ARTIFICIAL INTELLIGENCE AND THE MILITARY

Authored by Robert Weissman Savannah Wooten



ACKNOWLEDGMENTS

This report was written by **Robert Weissman**, President of Public Citizen, and **Savannah Wooten**, People Over Pentagon Advocate at Public Citizen.

ABOUT PUBLIC CITIZEN

Public Citizen is a national non-profit organization with more than 500,000 members and supporters. We represent consumer interests through lobbying, litigation, administrative advocacy, research, and public education on a broad range of issues including consumer rights in the marketplace, product safety, financial regulation, worker safety, safe and affordable health care, campaign finance reform and government ethics, fair trade, climate change, and corporate and government accountability.

Contact Public Citizen

Main Office 1600 20th Street NW	Capitol Hill 215 Pennsylvania Avenue SE, #3	Texas Office 309 E 11th Street, Suite 2
Washington, D.C. 20009	Washington, D.C. 20003	Austin, Texas 78701
Phone: 202-588-1000	Phone: 202-546-4996	Phone: 512 477-1155

For more information, please visit www.citizen.org.



Table of Contents

REPORT SUMMARY	4
THE PENTAGON'S AI OUTLOOK AND POLICY	5
AUTONOMOUS WEAPONS AND USE OF FORCE	7
AI CONTROL OVER NUCLEAR LAUNCHES	12
NON-WEAPONRY USE OF AI IN WARFIGHTING	13
AI FIRM COMPETITION AND THE "LITTLE GUY" CONTRACTORS	14
RECOMMENDATIONS	16
1. The Pentagon should pledge not to use autonomous weapons and the U.S. government	

- THE PENTAGON SHOULD PLEDGE NOT TO USE AUTONOMOUS WEAPONS AND THE U.S. GOVERNMEN SHOULD SUPPORT AN INTERNATIONAL TREATY PROHIBITING AND REGULATING THE USE OF SUCH WEAPONS.
- $2. \quad \text{The prohibition on AI launch of nuclear weapons should be codified into law.}$
- 3. The United States should pledge not to use deepfakes in the battlefield or to influence foreign affairs and should negotiate a global instrument banning the use of deepfakes to influence other nations.
- 4. THERE SHOULD BE NO INCREASE IN PENTAGON SPENDING FOR AI.

Report Summary

The U.S. Department of Defense (DOD) and the military-industrial complex are rushing to embrace an artificial intelligence (AI)-driven future.

There's nothing particularly surprising or inherently worrisome about this trend. AI is already in widespread use and evolving generative AI technologies are likely to suffuse society, remaking jobs, organizational arrangements and machinery.

At the same time, AI poses manifold risks to society and military applications present novel problems and concerns, as the Pentagon itself recognizes.

This report outlines some of the primary concerns around military applications of AI use. It begins with a brief overview of the Pentagon's AI policy. Then it reviews:

- The grave dangers of autonomous weapons "killer robots" programmed to make their own decisions about use of lethal force.
- The imperative of ensuring that decisions to use nuclear weapons can be made only by humans, not automated systems.
- How AI intelligence processing can increase not diminish the use of violence.
- The risks of using deepfakes on the battlefield.

The report then reviews how military AI start-ups are crusading for Pentagon contracts, including by following the tried-and-true tactic of relying on revolving door relationships.

The report concludes with a series of recommendations:

- 1. The United States should pledge not to develop or deploy autonomous weapons, and should support a global treaty banning such weapons.
- 2. The United States should codify the commitment that only humans can launch nuclear weapons.
- 3. Deepfakes should be banned from the battlefield.
- 4. Spending for AI technologies should come from the already bloated and wasteful Pentagon budget, not additional appropriations.

The Pentagon's AI Outlook and Policy

In an August 2023 address, Deputy Secretary of Defense Kathleen Hicks asserted that the Pentagon had put in place the foundations to "deliver - <u>now</u> - a data-driven and AI-empowered military."¹

Combining investments in data, computing power and AI, the DOD is building what it calls Combined Joint All-Domain Command and Control (CJADC2). According to Hicks, "This is not a platform or single system that we're buying. It's a whole set of concepts, technologies, policies, and talent that's advancing a core U.S. warfighting function."² And, promises Hicks, CJADC2 is just part of the DOD's commitment to promoting innovation with AI at its core.

In June, the DOD issued its "Data, Analytics, and Artificial Intelligence Adoption Strategy." The subtitle of the document is "Accelerating Decision Advantage," which highlights the core message of the strategy: AI is a powerful tool to enhance DOD warfighting and other capabilities, and the Pentagon must accelerate its development and adoption of AI technologies. "The latest advancements in data, analytics, and artificial intelligence (AI) technologies enable leaders to make better decisions faster, from the boardroom to the battlefield," states the plan's discussion of the strategic environment. "Therefore, accelerating the adoption of these technologies presents an unprecedented opportunity to equip leaders at all levels of the Department with the data they need, and harness the full potential of the decision-making power of our people.³

Meanwhile, traditional Pentagon contractors are incorporating AI into their operations and products – and a new host of AI companies are jockeying for a share of Pentagon dollars. The Pentagon procurement and innovation process is always a push-and-pull between the Pentagon's internally prioritized needs and what contractors are developing and touting, often mediated by Congress. The introduction of the AI companies into this space is poised to complicate this standard process, with competition between the traditional contractors and the new entrants, with new dynamics between the AI companies and the Pentagon, and new channels of corporate influence.

¹ Deputy Secretary of Defense Kathleen Hicks, "Keynote Address: The Urgency to Innovate," U.S. Department of Defense, last modified August 28 2023, accessed December 2023,

https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/

² Deputy Secretary of Defense Kathleen Hicks, "Keynote Address: The Urgency to Innovate," U.S. Department of Defense, last modified August 28 2023, <u>https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/</u>

³ U.S. Department of Defense, "DOD Data Analytics AI Adoption Strategy," November 2, 2023, accessed December 2023, <u>https://media.defense.gov/2023/Nov/02/2003333300/-1/-</u>

^{1/1/}DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

Introducing AI into the Pentagon's everyday business, battlefield decision-making and weapons systems poses manifold risks, as the Pentagon itself recognizes. In 2020, the DOD adopted its AI Ethical Principles.⁴ Those principles are:

- 1. **Responsible.** DoD personnel will exercise judgment and care, and be responsible for, using AI.
- 2. **Equitable.** The Department will take deliberate steps to minimize unintended bias in AI capabilities.
- 3. **Traceable.** AI methodologies should be auditable and have transparent data sources and design.
- 4. Reliable. AI should serve explicit purposes and be subject to constant testing.
- 5. **Governable.** The Pentagon must be able to detect and avoid unintended consequences, and deactivate deployed systems.

In a 2021 memorandum, Deputy Secretary of Defense Hicks reaffirmed the Ethical AI Principles and launched a process to speed the deployment of "Responsible Artificial Intelligence" (RAI).⁵ In the memo, she launched various training initiatives and announced that a RAI Working Council would be charged with developing an implementation strategy for the principles and speeding AI deployment. In June 2022, the Pentagon published its "Responsible Artificial Intelligence Strategy and Implementation Pathway."⁶ This pathway details dozens of "lines of effort" to achieve a variety of AI objectives. These include training DOD personnel and speeding the deployment of AI technologies, and to address identified risks. One stated priority is to "exercise appropriate care in the AI product and acquisition lifecycle to ensure potential AI risks are considered from the outset of an AI project, and efforts are taken to mitigate or ameliorate such risks and reduce unintended consequences, while enabling AI development at the pace the Department needs to meet the National Defense Strategy."⁷

Many of the lines of effort in the RAI pathway are charged to the DOD's Chief Digital and Artificial Intelligence Office (CDAO), which became operational in June 2022 and is dedicated to integrating AI capabilities across the Pentagon. Serving as Chief Digital and Artificial Intelligence Officer is Dr. Craig Martell, who publicly expresses concerns and cautions about the use of AI. Speaking to CNN host Christine Amanpour in August 2023, he warned that large language models (LLMs) don't "generate factual coherent text all the time." But, he said,

⁷ U.S. Department of Defense, Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, D.C.: U.S. Department of Defense, June 22, 2022), accessed December 2023,

 ⁴ U.S. Department of Defense, "DOD Adopts Ethical Principles for Artificial Intelligence," accessed December 2023, <u>https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/</u>.
⁵ U.S. Department of Defense, "Implementing Responsible Artificial Intelligence in the Department of Defense," May 27,

^{2021,} accessed December 2023, <u>https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-</u> RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF.

⁶ U.S. Department of Defense, Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, June 22, 2022, accessed December 2023, <u>https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF</u>.

https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF.

there is a "natural proclivity to believe things that speak authoritatively. And these things speak authoritatively, so we just believe them. That makes me afraid." Martell said that the Pentagon would lay out a list of use cases for LLMs and acceptability criteria. For example, he said, if DOD personnel are going to ask an AI chatbot about how to use a new battlefield technology, it better be right 99.999 percent of the time.⁸

Autonomous Weapons and Use of Force

The single greatest concern involving AI and the Pentagon is the integration of AI into weapons systems such that they can function autonomously, delivering lethal force without intervention or meaningful human control.

The Pentagon recognizes the risks involved with autonomous weapons. DOD Directive 3000.09, issued in January 2023, establishes DOD policy relating to the development and use of autonomous and semi-autonomous functions in weapon systems, with a priority purpose of "minimiz[ing] the probability and consequences of failures in autonomous and semi-autonomous weapon systems that could lead to unintended engagements.⁹ The 2023 directive updates a prior directive from 2012.

The directive establishes that "Autonomous and semi-autonomous weapon systems will be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force." It specifies testing and evaluation standards for autonomous weapons, including to ensure they function as intended in realistic environments in which they must confront countermeasures. It establishes chains of review for approval of autonomous weapons and requires those approving such weapons to ensure they comply with the DOD's responsible AI policies, the law of war, applicable treaties and weapons safety rules.¹⁰

A Human Rights Watch / Harvard Law School International Human Rights Clinic review of the policy concludes that it is "serious" and includes some improvements from the prior directive, but notes numerous shortcomings. One shortcoming is that the required senior review of autonomous weapon development and deployment can be waived "in cases of urgent military need." DOD declines to report if any such waivers have been granted. Another shortcoming is the deletion of the word "control" from elements of the 2012 directive; the earlier directive had specified concerns about how DOD personnel might lose control of autonomous weapons to unauthorized parties. The review notes also that the DOD directive permits international sales and transfers of autonomous weapons; and also, by its nature,

⁸ Craig Martell, interview by Christiane Amanpour, CNN, August 7, 2023, accessed December 2023, <u>https://www.cnn.com/videos/tv/2023/08/07/craig-martell-ai-amanpour-interview.cnn</u>.

⁹ U.S. Department of Defense, "Department of Defense Instruction 3000.09: Autonomy in Weapon Systems," accessed December 2023, <u>https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.PDF</u>.

¹⁰ U.S. Department of Defense, "Department of Defense Instruction 3000.09: Autonomy in Weapon Systems," accessed December 2023, <u>https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.PDF</u>.

applies only to the DOD, but not the Central Intelligence Agency, U.S. Customs and Border Protection, or other U.S. government agencies that might use autonomous weapons.¹¹

The biggest shortcoming of the directive, however, is that it permits the development and deployment of lethal autonomous weapons at all.

For military planners, the upsides of lethal, autonomous weapons are obvious: They can engage in war-fighting without any direct risk to U.S. military personnel. They offer the prospect of acting nearly instantaneously on incoming intelligence. They provide the appeal of highly targeted, computer-controlled force application that may avoid injury to unintended targets. Theoretically, they can be much cheaper than conventional weapons.

But these purported benefits are vastly outweighed by the immorality of delegating decisions over the deployment of lethal force to machines, as well as the massive operational risks of autonomous weapons.

The most serious worry involving autonomous weapons is that they inherently dehumanize the people targeted and make it easier to tolerate widespread killing, including in violation of international human rights law. "The use of autonomous weapon systems entails risks due to the difficulties in anticipating and limiting their effects," contends the International Committee of the Red Cross (ICRC). "This loss of human control and judgment in the use of force and weapons raises serious concerns from humanitarian, legal and ethical perspectives."¹²

Summarizing the key ethical issues, the ICRC notes that "the process by which autonomous weapon systems function: brings risks of harm for those affected by armed conflict, both civilians and combatants, as well as dangers of conflict escalation; raises challenges for compliance with international law, including international humanitarian law, notably, the rules on the conduct of hostilities for the protection of civilians; and raises fundamental ethical concerns for humanity, in effect substituting human decisions about life and death with sensor, software and machine processes.¹³

These problems are inherent in the deployment of lethal autonomous weapons. They will persist and are unavoidable, even with the strongest controls in place. U.S. drone strikes in the so-called war on terror have killed, at minimum, hundreds of civilians – a problem due to bad intelligence and circumstance, not drone misfiring. Because the intelligence shortcomings will continue and people will continue to be people – meaning they congregate and move in unpredictable ways – shifting decision making to autonomous systems will not reduce this death toll going forward. In fact, it is likely to worsen the problem. The patina of

¹¹ Harvard Law School Human Rights Clinic, "Review of the 2023 US Policy on Autonomy in Weapons Systems," accessed December 2023, <u>https://humanrightsclinic.law.harvard.edu/wp-content/uploads/2023/02/Review-of-the-2023-US-Policy-on-Autonomy-in-Weapons-Systems.pdf</u>.

¹² International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," accessed December 2023, <u>https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems</u>.

¹³ International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," accessed December 2023, <u>https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems</u>.

"pure" decision-making will make it easier for humans to launch and empower autonomous weapons, as will the moral distance between humans and the decision to use lethal force against identifiable individuals. The removal of human common sense – the ability to look at a situation and restrain from authorizing lethal force, even in the face of indicators pointing to the use of force – can only worsen the problem still more.

Additional problems are likely to occur because of AI mistakes, including bias. Strong testing regimes will mitigate these problems, but human-created AI has persistently displayed problems with racial bias, including in facial recognition and in varied kinds of decision making, a very significant issue when U.S. targets are so often people of color. To its credit, the Pentagon identifies this risk, and other possible AI weaknesses, including problems relating to adversaries' countermeasures, the risk of tampering and cybersecurity.¹⁴ It would be foolish, however, to expect that Pentagon testing will adequately prevent these problems; too much is uncertain about the functioning of AI and it is impossible to replicate real-world battlefield conditions. Explains the research nonprofit Automated Decision Research: "The digital dehumanization that results from reducing people to data points based on specific characteristics raises serious questions about how the target profiles of autonomous weapons are created, and what pre-existing data these target profiles are based on. It also raises questions about how the user can understand what falls into a weapon's target profile, and why the weapons system applied force."¹⁵

Based on real-world experience with AI, the risk of autonomous weapon failure in the face of unanticipated circumstances (an "unknown unknown") should be rated high. Although the machines are not likely to turn on their makers, Terminator-style, they may well function in dangerous and completely unanticipated ways – an unacceptable risk in the context of the deployment of lethal force. One crucial problem is that AIs are not able to deploy common sense, or reason based on past experience about unforeseen and novel circumstances. The example of self-driving cars is illustrative, notably that of a Cruise self-driving vehicle driving into and getting stuck in wet concrete in San Francisco. The problem, explains AI expert Gary Marcus, is "edge cases," out-of-the-ordinary circumstances that often confound machine learning algorithms. The more complicated a domain is, the more unanticipated outliers there tend to be. And the real world is really complicated and messy; there's no way to list all the crazy and out of ordinary things that can happen."¹⁶ It's hard to imagine a more complicated and unpredictable domain than the battlefield, especially when those battlefields occur in urban environments or are occupied by substantial numbers of civilians.

A final problem is that, as a discrete weapons technology, autonomous weapons deployment is nearly certain to create an AI weapons arms race. That is the logic of international military strategy. In the United States, a geopolitical rivalry-driven autonomous weapons arms race

¹⁵ Automated Research Institute, "Targeting People and Digital Dehumanisation," accessed December 2023, <u>https://automatedresearch.org/news/report/targeting-people-and-digital-dehumanisation/</u>.

¹⁶ Gary, Marcus, "Face It: Self-Driving Cars Still Haven't," Substack, accessed December 2023, <u>https://garymarcus.substack.com/p/face-it-self-driving-cars-still-havent</u>.

¹⁴ U.S. Department of Defense, "Department of Defense Directive 3000.09: Autonomy in Weapon Systems," accessed December 2023, <u>https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.PDF</u>.

will be spurred further by the military-industrial complex and corporate contractors, about which more below.

Autonomous weapons are already in development around the world and racing forward. Automated Decision Research details more than two dozen weapons systems of concern including several built by U.S. corporations.¹⁷ These include:

- A General Dynamics Land Systems Abrams X UGV, an in-development Unmanned Ground Vehicle. The company claims the tank's "AI system can analyze data from sensors and cameras to identify potential threats and targets," and that the autonomous capabilities will "allow the tank to operate without direct human control in certain situations."
- **The Vigor Industrial Seahunter USV**, launched as part of DARPA Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) program. It can reportedly travel thousands of miles underwater with no human crew.
- The Area-I/Anduril ALTIUS-600M and 700M drones. There is some uncertainty about their autonomy, though one of Anduril's founders said in April 2023 that the 600M drone has now been equipped with autonomy. The 700M drone can carry a 35-pound warhead.

Meanwhile, Hicks in August 2023 announced a major new program, the Replicator Initiative, that would rely heavily on drones to combat Chinese missile strength in a theoretical conflict over Taiwan or at China's eastern coast. The purpose, she said, was to counter Chinese "mass," avoid using "our people as cannon fodder like some competitors do," and leverage "attritable, autonomous systems."¹⁸ "Attritable" is a Pentagon term that means a weapon is relatively low cost and that some substantial portion of those used are likely to be destroyed (subject to attrition).¹⁹ "We've set a big goal for Replicator," Hicks stated: "to field attritable autonomous systems at scale of multiple thousands, in multiple domains, within the next 18-to-24 months." In Pentagon lingo, she said, the U.S. "all-domain, attritable autonomous systems will help overcome the challenge of anti-access, area-denial systems. Our ADA2 to thwart their A2AD."²⁰

There is more than a little uncertainty over exactly what Replicator will be. Hicks said it would require no new additional funding, drawing instead on existing funding lines. At the same time, Hicks was quite intentionally selling it as big and transformational, calling it "game-

¹⁷ Automated Research Institute, "Weapons Systems," accessed December 2023, <u>https://automatedresearch.org/weapons-systems/</u>.

¹⁸ Deputy Secretary of Defense Kathleen Hicks, "Keynote Address: The Urgency to Innovate," U.S. Department of Defense, accessed December 2023, <u>https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/</u>.

¹⁹ Magnuson, Stew. "The Meanings of Attritable and Expendable," National Defense Magazine, accessed December 2023, <u>https://www.nationaldefensemagazine.org/articles/2022/2/9/the-meanings-of-attritable-and-expendable</u>.

²⁰ Deputy Secretary of Defense Kathleen Hicks, "Keynote Address: The Urgency to Innovate," U.S. Department of Defense, accessed December 2023, <u>https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/</u>.

changing."²¹ What the plan appears to be is to develop the capacity to launch a "drone swarm" over China, with the number of relatively low-cost drones so great that mathematically some substantial number will evade China's air defenses. While details remain vague, it is likely that this drone swarm model would rely on autonomous weapons. "Experts say advances in data-processing speed and machine-to-machine communications will inevitably relegate people to supervisory roles," reports the Associated Press (AP). AP asked the Pentagon if it is currently formally assessing any fully autonomous lethal weapons system for deployment, but a Pentagon spokesperson refused to answer.²²

The risks of this program, if it is in fact technologically and logistically achievable, are enormous. Drone swarms implicate all the concerns of autonomous weaponry, plus more. The sheer number of agents involved would make human supervision far less practicable or effective. Additionally, AI-driven swarms involve autonomous agents that would interact with and coordinate with each other, likely in ways not foreseen by humans and also likely indecipherable to humans in real time. The risks of dehumanization, loss of human control, attacks on civilians, mistakes and unforeseen action are all worse with swarms.²³

Against the backdrop of the DOD announcements, military policy talk has shifted: The development and deployment of autonomous weapons is, increasingly, being treated as a matter of when, not if. "The argument may be less about whether this is the right thing to do, and increasingly more about how do we actually do it -- and on the rapid timelines required," said Christian Brose, chief strategy officer at the military AI company Anduril, a former Senate Armed Services Committee staff director and author of the 2020 book *The Kill Chain.*²⁴ Summarizes The Hill: "the U.S. is moving fast toward an ambitious goal: propping up a fleet of legacy ships, aircraft and vehicles with the support of weapons powered by artificial intelligence (AI), creating a first-of-its-kind class of war technology. It's also spurring a huge boost across the defense industry, which is tasked with developing and manufacturing the systems."²⁵ Frank Kendall, the Air Force secretary, told the New York Times that it necessary and inevitable that the U.S. move to deploy lethal, autonomous weapons.²⁶

Thomas Hammes, who previously held command positions in the U.S. Marines and is now a research fellow at the U.S. National Defense University, penned an article for the Atlantic

²¹ "The Pentagon's New AI Drone Initiative Seeks 'Game-Changing Shift' to Global Defense," The Hill, accessed December 2023, <u>https://thehill.com/homenews/4189864-pentagons-new-ai-drone-initiative-seeks-game-changing-shift-to-global-defense/</u>.

 ²² Bajak, Frank, "Pentagon's AI initiatives accelerate hard decisions on lethal autonomous weapons," Associated Press, accessed December 2023, <u>https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942</u>.
²³ Increasing Complexity (October 2023), PAX for Peace, accessed December 2023, <u>https://paxforpeace.nl/wp-content/uploads/sites/2/2023/10/PAX_Increasing-Complexity_October-2023.pdf</u>.

 ²⁴ Bajak, Frank, "Pentagon's AI initiatives accelerate hard decisions on lethal autonomous weapons," Associated Press, accessed December 2023, <u>https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942</u>.
²⁵ Dress, Brad, "Inside America's Plans for an Autonomous AI-Powered Military," The Hill, accessed December 2023,

²² Dress, Brad, Inside America's Plans for an Autonomous Al-Powered Military, The Hill, accessed December 2023, <u>https://thehill.com/policy/defense/4224631-inside-americas-plans-for-an-autonomous-ai-powered-military/</u>.

²⁶ Lipton, Eric, "AI Drones Prompt Fears of Autonomous Warfare Without Boundaries," The New York Times, November 21, 2023, accessed December 2023, <u>https://www.nytimes.com/2023/11/21/us/politics/ai-drones-war-law.html</u>.

Council with the headline, "Autonomous Weapons are the Moral Choice."²⁷ Hammes' argument is, on the one hand, killing is killing and it doesn't matter if it's done by a traditional or autonomous weapon. On the other hand, he contends, "No longer will militaries have the luxury of debating the impact on a single target. Instead, the question is how best to protect thousands of people while achieving the objectives that brought the country to war. It is difficult to imagine a more unethical decision than choosing to go to war and sacrifice citizens without providing them with the weapons to win."

Meanwhile, as the technology and U.S. planning is accelerating, so are calls for a global treaty to restrict autonomous weapons. In December, the UN General Assembly voted overwhelmingly for a resolution stressing "the urgent need for the international community to address the challenges and concerns raised by autonomous weapons systems."²⁸ The resolution passed with 152 votes in favor, 4 opposed and 11 abstentions. The United States voted in favor. More than 90 nations – not including the United States – have expressed support for a treaty to ensure meaningful human control over the use of force, and a global civil society coalition, Stop Killer Robots (of which Public Citizen is a member) is demanding rapid action.²⁹

AI Control Over Nuclear Launches

The gravest issue involving autonomous control over the use of lethal force is the case of nuclear weapons. An AI-launched nuclear strike due to error or the failure to exercise human judgment would be catastrophic for humanity.

Current Department of Defense policy states that a human must be involved in all decisions related to launching nuclear weapons. According to the 2022 Nuclear Posture Review, "In all cases, the United States will maintain a human "in the loop" for all actions critical to informing and executing decisions by the President to initiate and terminate nuclear weapon employment."³⁰

But this policy is not codified in law. Sen. Ed Markey, D-Mass. and Reps. Ted Lieu, D-Calif., Don Beyer, D-Va. and Ken Buck, R-Colo, have introduced the bipartisan Block Nuclear Launch by Autonomous AI Act to prohibit by the launch of any nuclear weapon by an automated system without meaningful human control.³¹ Formalizing the policy would not

 ²⁷ Hammes, Thomas X., "Autonomous Weapons Are the Moral Choice," Atlantic Council, accessed December 2023, https://www.atlanticcouncil.org/blogs/new-atlanticist/autonomous-weapons-are-the-moral-choice/.
²⁸ United Nations General Assembly, "Resolution on lethal autonomous weapons systems", A/RES/78/241, accessed

²⁶ United Nations General Assembly, "Resolution on lethal autonomous weapons systems", A/RES/78/241, accessed January 2023, <u>https://www.undocs.org/A/RES/78/241</u>.

²⁹ Campaign to Stop Killer Robots, "Frequently Asked Questions about the Campaign's United Nations General Assembly (UNGA) Meeting," accessed December 2023, <u>https://www.stopkillerrobots.org/wp-content/uploads/2023/10/230907-SKR-UNGA-FAQ-A4.pdf</u>.

³⁰ U.S. Department of Defense, 2022 National Defense Strategy, accessed December 2023,

https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF. ³¹ U.S. Congress, House, "Block Nuclear Launch by Autonomous AI Act of 2023", 118th Congress, 1st session, https://www.markey.senate.gov/imo/media/doc/block_nuclear_launch_by_autonomous_ai_act_-_042623pdf.pdf.

only lock it into place, it may incentivize China, Russia and other nuclear powers to follow suit.

Non-weaponry use of AI in warfighting

The rapid development of AI technologies means it is sure to be used throughout Pentagon operations and other nations' militaries. Many of these uses will be benign, efficiency enhancing or even lifesaving. But the use of AI in warfighting raises disturbing issues beyond those of autonomous weapons.

Al intelligence processing and the use of force

One way AI is already being deployed in warfighting conditions is to process intelligence – with some early disturbing examples. The Palestine-Israeli publication +972, the Israeli Local Call and The Guardian have reported, based on interviews with current and former Israeli intelligence officials, on an Israeli AI intelligence processing system, called The Gospel, which is analyzing data and recommending targets inside Gaza.³² Israeli sources report that the system is providing far more targets than the Israel military was previously able to identify. Rather than focus attacks, according to these reports, the AI system is enabling far broader use of force, providing cover for attacks on residences and civilian buildings. Although the AI system provides information about civilians at risk at target sites, the media accounts describe the dehumanizing effect of reliance on AI: A human eye "will go over the targets before each attack, but it need not spend a lot of time on them," a former intelligence official stated.³³

Battlefield use of deepfakes

In addition to the use of autonomous weaponry and AI systems in warfighting, the rise of sophisticated deep fake technology creates troubling possibilities for use in wartime situations.

In March 2023, the Intercept identified a procurement document from the U.S. Special Operations Command that appears completely out of step with President Biden's commitment on AI. The procurement document says the Pentagon is seeking a contractor to "provide a next generation of 'deep fake' or other similar technology to generate messages and influence operations via non-traditional channels in relevant peer/near peer environments."

The appeal of unilateral use against an adversary is obvious and evidenced in the Special Operations Command document: Tricking an adversaries' troops into following false orders could decisively swing a battle or war. The risks of introducing such a technology, of course,

³² Abraham, Yuval, "Mass Assassination Factory: How Israel Calculated Bombing Gaza," accessed December 2023, <u>https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza</u>; Davies, Harry, Bethan McKernan and Dan Sabbagh, "The Gospel: How Israel Uses AI to Select Bombing Targets," The Guardian, December 1, 2023, accessed December 2023, <u>https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets</u>.

³³ Abraham, Yuval, "Mass Assassination Factory: How Israel Calculated Bombing Gaza," accessed December 2023, <u>https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza</u>.

is that adversaries will do so, as well. Weaponizing deep fake technology carries grave risks – both on the battlefield and in foreign affairs more generally.

AI Firm Competition and the "Little Guy" Contractors

The Pentagon is the biggest single money-moving entity in the world. The major U.S. defense corporations lock in years-long, Pentagon contracts to the tune of tens of billions of dollars, which generate massive annual profits. These companies site and subcontract production facilities throughout the United States to maintain political support. They work for years on new weapons development with the hope of decades-long purchase commitments. They employ hundreds of lobbyists, drawn overwhelmingly from prior government experience, including especially prior service in the Pentagon.

Now, AI companies want a piece of the pie. They can't match the political power and influence of the traditional contractors, but they are proving savvy nonetheless.

Above all, military AI proponents are playing the China card. China is rushing ahead with AI investments, and so the United States must follow suit, they say. "China is working hard to surpass the United States in AI," writes Michele Flournoy, a former DOD undersecretary, the co-founder and managing partner of WestExec Advisors, chair of the Center for a New American Security, and an advisor of the military AI company Shield AI, "particularly when it comes to military applications. If it succeeds, Beijing would then possess a much more powerful military, one potentially able to increase the tempo and effect of its operations beyond what the United States can match." "China is outpacing the United States by innovation measures," Tara Murphy Dougherty, CEO of the defense data firm Govini told Defense One. "We risk falling behind China and doing too little too late," Scale AI CEO Alexander Wang warned the House Armed Services Committee in July 2023. In this messaging, there is broad unanimity across the military-industrial complex.

A second line of political advocacy from the military AI companies – mostly much smaller tech start-ups – is that the Pentagon procurement process discriminates against them in favor of the prime contractors and legacy weapons systems.

These small companies complain that while the Pentagon is touting AI technologies, it is not providing the up-front investment needed for militarized AI. Some are able to raise venture capital, but they burn through that fairly quickly. The AI companies would like long-term procurement contracts, though in many or most cases they don't have technologies ready to go. On the other hand, they point out, the primary contractors regularly are able to obtain massive contracts to support weapons development. The companies talk about "the valley of death" – the period between proving product viability and obtaining large Pentagon contracts. "The United States is at risk of being stuck in an innovator's dilemma because it is comfortable and familiar with investing in traditional sources of military power," says Alexander Wang of Scale AI.

Although the AI start-ups are touting themselves as plucky and agile competitors to the traditional contractors, what they really want is more Pentagon funding. And the easiest way

to get that is not to take money away from traditional Pentagon spending lines but to add more. Shield AI, for example, has created a new DC lobby shop to urge money be added to the Pentagon budget for AI. Flournoy urges more funding to help AI companies get across the "valley of death." Air Force Secretary Kendall says he needs billions more for the projects he would like to fund. And a slew of think tank reports urge more AI funding.

Comparatively smaller firms may begin advocating for separate funding pools or loosened restrictions for AI providers, arguing that they cannot operate on multiple-year funding cycles when they are in the startup phase of a new venture and consequently more strapped for reliable funding streams. At the same time, defense contractor giants may develop an interest in competing in the AI space – either requesting funding to expand AI capacities in-house or looking into the field to buy out smaller competitors.

Notably, the AI firms are emulating the prime contractors in relying on the revolving door as a means to obtain influence. Because most of these companies are small and not publicly traded, they are not required to disclose their key employees, board members and advisors. But several of the larger ones have done so, touting their insider influence:

- **C3.ai**'s board includes former Secretary of State Condoleezza Rice, and it boasts an advisory board that includes retired Air Force General John Hyten, a former vice chair of the Joint Chiefs of Staff, retired Army Lt. Gen. Edward Cardon and Rick Ledgett, former deputy director of the National Security Agency.
- Anduril Industries' advisory board includes retired Air Force General David Goldfein, Katharina McFarland, former Assistant Secretary of Defense for Acquisition and acting Assistant Secretary of the Army, retired Navy Admiral Scott Swift, Kevin McAleenan, former acting secretary of the U.S. Department of Homeland Security, and Constantine Saab, former chief strategy officer at the Central Intelligence Agency.
- **Rebellion Defense** was co-founded by Chris Lynch, who was previously in charge of the Defense Digital Service, and Nicole Camarillo, formerly a senior policy advisor to the Assistant Secretary of the Army, and is currently headed by Ben Fitzgerald, a former high-ranking Defense Department acquisition official.
- **Palantir**'s advisory board includes Christine Fox, the former Acting Deputy Secretary of Defense, retired General Carter F. Ham, formerly commander of the U.S. Africa Command, retired Navy Admiral William H. McRaven, former commander of the U.S. Special Operations Command, and retired General Gustave F. Perna, former commander of the U.S. Army Materiel Command.

The single most important insider pushing military AI applications is Eric Schmidt, former CEO of Google. Schmidt served as a technical adviser to Google when it signed up to work on the Pentagon's Project Maven, an AI tool to process drone imagery and detect targets; Google pulled out after a revolt from its staff.

Schmidt chaired the National Security Commission on Artificial Intelligence, a congressionally chartered body that retired in 2021 upon issuing a massive report that concluded, "we have a duty to convince the leaders in the U.S. Government to make the hard decision and the down payment to win the AI era." The report issued "an uncomfortable message," that "America is not prepared to defend or compete in the AI era." Massive investments are needed, the report declared, "to protect [America's] security, promote its prosperity, and safeguard the future of democracy. Today, the government is not organizing or investing to win the technology competition against a committed competitor, nor is it prepared to defend against AI-enabled threats and rapidly adopt AI applications for national security purposes." AI experts Meredith Whitaker and Lucy Suchman said the report "echoed Cold War rhetoric."

After the National Security Commission on Artificial Intelligence closed shop, Eric Schmidt pledged to fund with his own resources a follow-on effort, the Special Competitive Studies Project. The project declares its mission to be "to make recommendations to strengthen America's long-term competitiveness as artificial intelligence (AI) and other emerging technologies are reshaping our national security, economy, and society."

Schmidt also co-authored a book, with Henry Kissinger and MIT Dean Daniel Huttenlocher, The Age of AI: And Our Human Future, which cautions about AI risks but mostly celebrates its possibilities – and insists on its central importance in national security.

Meanwhile, Schmidt is a significant investor in military AI companies, notably Rebellion Defense, in which he was an early, major investor. According to the conservative populist Bullmoose Project, Schmidt and Innovation Endeavors, a venture capital fund he founded, have made at least 57 investments in AI companies.

As Bloomberg notes, Schmidt is quite open about the symbiosis between his investments in AI policymaking and his investments in AI corporations. "The people who work in the commission and then go into the government, they are your emissaries," Bloomberg reports Schmidt saying at a Capitol Hill event in June 2023. "A rule of business is that if you could put your person in the company, they're likely to buy from you. It's the same principle."

Recommendations

The military is already being significantly altered by the introduction of artificial intelligence technologies into modern-day warfighting and the Pentagon's overall operations. The Pentagon recognizes many of the risks that AI presents and has moved to adopt some precautionary measures. However, at root, the Pentagon's "Responsible AI" policy is very limited – it specifies that someone will have ultimate responsibility for deciding to use AI, but it aims to authorize uses that are fundamentally irresponsible. Much stronger policies and commitments are needed.

1. The Pentagon should pledge not to use autonomous weapons and the U.S. government should support an international treaty prohibiting and regulating the use of such weapons. It is naïve to believe that the foreseeable problems with AI weapons can be solved by predeployment testing. Deploying lethal AI weapons in battlefield conditions necessarily means inserting them into novel conditions for which they have not been programmed, an invitation for disastrous outcomes. Problems with biased training data or bad human intelligence make misidentification and reckless or unintentional attacks on civilians almost inevitable. Even if lethal AI weapons work as intended, they will unavoidably lead to more dehumanization and more killing. And pushing more investments into AI weapons will lead to a militarized AI race that no one can win – and makes even more likely the deployment of unproven, inadequately tested and even more dangerous weaponry.

The United States should pledge not to deploy autonomous weapons and should support international efforts to negotiate a global treaty to that effect. At minimum, the U.S. should support the international negotiation and challenge other great powers to join them.

The outlines of a commitment against autonomous weapons are clear. The key components are:

- A requirement that human have control over the use of force;
- An affirmative ban on weapons that cannot be meaningfully controlled or systems that would target humans; and
- An obligation for human control over AI systems that are permitted.

Notably, human control does not mean what the Pentagon is promising: a human decision to launch a weapon that would then autonomously decide when, where and how to deploy force, or some general human supervisory role over autonomous weapons. The Stop Killer Robots coalition has detailed how these broad principles should be elaborated in an international treaty.

2. The prohibition on AI launch of nuclear weapons should be codified into law.

As artificial intelligence rapidly advances, it is critical to establish a bright-line rule requiring human supervision over any decision pertaining to the use of the most dangerous weapons known to humankind. Regardless of further AI development, nuclear weapons must be ethically stewarded by humans. The idea of automated nuclear launches is a reckless invitation to accidental or mistaken launches and, given the enormous destructive potential of nuclear weapons, wholly unethical.

Congress should immediately pass, and the president should sign, the Block Nuclear Launch by Autonomous AI Act.

3. The United States should pledge not to use deepfakes in the battlefield or to influence foreign affairs and should negotiate a global instrument banning the use of deepfakes to influence other nations.

Deep fake technology poses the possibility of sowing enormous distrust and confusion on the battlefield and in society in general. In the civilian context, deepfake technology is inherently antithetical to democratic functioning.

The United States should publicly commit not to use deepfakes against adversaries or allies in military or civilian contexts, and abandon any and all U.S. government programs to develop a capacity to use deepfakes for any kind of foreign influence.

In parallel, the United States should initiate an immediate effort to reach global agreement among governments not to use deep fake technology and, ideally, to ban altogether its use for deceptive purposes.

4. There should be no increase in Pentagon spending for AI.

Every part of the federal government, and likely every component of society, is going to be increasingly reliant on AI. There's no question that the Pentagon will be making increasing use of artificial intelligence, and it should. There also seems little doubt that AI will be increasingly incorporated into military hardware.

The great promise of AI is that it can unlock new forms of innovation and productivity. It should, at its core, be cost-saving: AI should enable society to get more for less.

The current Pentagon budget is projected to be \$886 billion. It is substantially higher than it was at the peaks of the Korean or Vietnam wars or the height of the Cold War in real, inflationadjusted terms. Even after the withdrawal of the U.S. military from its longest-running overseas conflict in Afghanistan, the military budget has continued to skyrocket. The United States spends more on its military than the next nine countries combined. The Pentagon is replete with waste and fraud. The Defense Department is unable to pass an audit and the Pentagon itself has identified more than \$100 billion in bureaucratic waste.

Combining these two facts – the promise that AI should be productivity enhancing and cost reducing, and the massive bloat in the Pentagon budget – one conclusion follows: there should be no increase in the Pentagon budget to accommodate its greater reliance on AI.

But there's every reason to worry that, instead, AI will be the next excuse for throwing even more at the Pentagon. If the past is any guide, the lobby campaign by the start-up AI companies will result not in reallocation of funding away from legacy and wasteful weapons systems, but billions more poured into new line items. And the prime contractors themselves are reasonably likely to lobby for new AI-related funding.

The Replicator program disturbingly foreshadows how all this may play out. Deputy Defense Secretary Kathleen Hicks indicated the program would not need new funding – the investment was supposed to be primarily in low-cost drones and the plan was to use existing resources to pay the costs. But Rep. Mike Gallagher, R-Wisconsin, chair of the House Armed Services subcommittee on cyber, information technologies and innovation, quickly raised concerns that Replicator might draw money from other projects and programs, a complaint echoed by others. And U.S. drone manufacturers rushed to say that even simple drones for DOD will cost much more than those available commercially. By December 2023, tech executives had organized themselves to complain to Hicks about funding en masse. Replicator "is just very disorganized and confusing," an anonymous tech company executive told Politico. The problem with the initiative is that it's "not actually associated with any dollars to make things happen." Hicks has indicated that the Pentagon may seek additional, designated funding for Replicator in fiscal year 2025.

Decisions made in these early days of AI development will chart the course for decades to come. AI is not going away, but it's up to humans to make decisions about how to deploy it. There's no reason to allow AI to make the world more dangerous and violent, nor to let it become an excuse to throw even more money at the Pentagon.