Congressional Research Service
Informing the legislative debate since 1914

Artificial Intelligence and National Security

Daniel S. Hoadley
US Air Force Fellow

Nathan J. Lucas
Section Research Manager

April 26, 2018

Congressional Research Service
7-5700
www.crs.gov
R45178

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Artificial Intelligence (AI) is a rapidly growing field of technological development with potentially significant implications for national security. As such, the U.S. Department of Defense (DOD) is developing AI applications for a range of military functions. AI research is underway in the fields of intelligence collection and analysis, logistics, cyberspace operations, command and control, and a variety of military autonomous vehicles. AI applications are already playing a role in operations in Iraq and Syria, with algorithms designed to speed up the target identification process. Congressional action has the potential to shape the technology's trajectory, with fiscal and regulatory decisions potentially influencing growth of national security applications and the standing of military AI development versus international competitors.

AI technology presents unique challenges for military acquisitions, especially since the bulk of AI development is happening in the commercial sector. Although AI is not unique in this regard, the Defense Acquisition Process (DAP) may potentially need to be adapted for acquiring systems like AI. In addition, many commercial AI applications must undergo significant modification prior to being functional for the military. A number of cultural issues challenge AI acquisition, leading to discord with AI companies and potential military aversion to adapting weapons systems and processes to this disruptive technology.

International rivals in the AI market are creating pressure for the United States to compete for innovative military AI applications. China is a leading competitor in this regard, releasing a plan in 2017 to capture the global lead in AI development by 2030. Currently, China is primarily focused on using AI to make faster and more well-informed decisions, as well as developing multiple types of autonomous military vehicles. Russia is also active in military AI development, with a primary focus on robotics.

Although AI has the potential to impart a number of advantages in the military context, it may also introduce distinct challenges. AI technology can facilitate autonomous operations, lead to more informed military decision-making, and will likely increase the speed and scale of military action. However, it is also unpredictable, vulnerable to unique forms of manipulation, and presents challenges to human-machine interaction. Analysts hold a broad range of opinions on how influential AI will be in future combat operations. While a small number of analysts believe that the technology will have minimal impact, a larger number of experts believe that AI will have at least an evolutionary if not revolutionary effect.

Military AI development presents a number of potential issues for Congress

- What is the right balance of commercial and government funding for AI development?
- How might Congress influence Defense Acquisition reform initiatives that ease military AI adaptation?
- What changes, if any, are necessary in Congress and DOD to implement effective oversight of AI development?
- What regulatory changes are necessary for military AI applications?
- What measures can be taken to protect AI from exploitation by international competitors and preserve a U.S. advantage in the field?

Contents

Introduction 1
AI Definitions and Terminology 1
Issues for Congress 4
AI Applications for Defense 8
- Intelligence, Surveillance, and Reconnaissance 9
- Logistics 9
- Cyberspace 10
- Command and Control 10
- Autonomous Vehicles 11
- Lethal Autonomous Weapon Systems (LAWS) 12

AI Acquisitions Challenges 13
International Competition 17
- China 17
- Russia 21
- International Institutions 23

AI Opportunities and Challenges 24
- Autonomy 24
- Speed 26
- Scaling 27
- Information Superiority 28
- Predictability 28
- Explainability 31
- AI Exploitation 33

AI's Impact on Combat 34
- Minimal Impact on Combat 34
- Evolutionary Impact on Combat 35
- Revolutionary Impact on Combat 36

Figures

Figure 1. Categories of AI Applications 3
Figure 2. Relationships of Selected AI Terminology 4
Figure 3. DOD Spending on AI: FY2012-FY2017 5
Figure 4. Chinese Investment in U.S. AI Companies, 2010-2017 20
Figure 5. Value of Autonomy to DOD Missions 25
Figure 6. Human vs. Machine Decision-making 26
Figure 7. AI and Image Classifying Errors 29
Figure 8. AI and Context 30
Figure 9. Adversarial Images 33

Tables

Table 1. Taxonomy of Historical AI Definitions 3

Contacts

Author Contact Information 38

Introduction

Artificial Intelligence (AI) is a rapidly growing field of technological development that is capturing the attention of international rivals, leaders in the commercial sector, defense intellectuals, and policymakers alike. On July 20, 2017, the Chinese government released a strategy detailing its plan to capture the lead in AI by 2030, and less than two months later Vladimir Putin publicly announced Russia's intent to pursue AI technologies, stating, "[W]hoever becomes the leader in this field will rule the world."[1] Elon Musk, the Chief Executive Officer of SpaceX and founder of OpenAI, submitted a letter co-signed by 114 international leaders in the technology sector to the United Nations (UN) warning that autonomous weapons fueled by AI will "permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans comprehend" and appealing for the means to prevent an arms race and protect civilians from potential misuse.[2]

In the meantime, the U.S. military is already integrating AI systems into combat via a spearhead initiative called Project Maven, which is using AI algorithms to identify insurgent targets in Iraq and Syria.[3] These events raise several questions that Congress addressed in hearings during 2017: What types of military AI applications are possible, and what limits, if any, should be imposed? What unique advantages and vulnerabilities come with employing AI for defense? How will AI change warfare, and what influence will it have on the military balance with U.S. competitors? Congress has a number of financial and statutory tools available that it may use to influence the answers to these questions and affect the future trajectory of AI technology.

AI Definitions and Terminology

Almost all academic studies open by acknowledging that there is no commonly accepted definition of AI, in part because of the diverse approaches to research in the field. Likewise, no official government definition of AI exists, but companion bills introduced on December 12, 2017 (H.R. 4625 and S. 2217), would define AI as follows: "Any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance.... They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action." The bills further elaborate on this definition, including many of the descriptions in **Table 1** below, which summarizes various AI definitions in academic literature.

The field of AI research began in 1956, but an explosion of interest in AI began around 2010 due to the convergence of three enabling developments: the availability of "big data" sources,

[1] China State Council, "A Next Generation Artificial Intelligence Development Plan," July 20, 2017, translated by New America, https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf, and Tom Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race," *Wired*, August 8, 2017, https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race.

[2] "An Open Letter to the United Nations Convention on Certain Conventional Weapons," August 20, 2017, https://www.dropbox.com/s/g4ijcaqq6ivq19d/2017%20Open%20Letter%20to%20the%20United%20Nations%20Convention%20on%20Certain%20Conventional%20Weapons.pdf?dl=0.

[3] Marcus Weisgerber, "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS," *Defense One*, May 14, 2017, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/.

improvements to machine learning approaches, and increases in computer processing power.[4] This growth has advanced the state of Narrow AI, which refers to algorithms that address specific problem sets like game playing, image recognition, and self-driving vehicles. All current AI systems fall into the Narrow AI category. The most prevalent approach to Narrow AI is machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets. During the training process, the computer system creates its own statistical model to accomplish the specified task in situations it has not previously encountered.

Experts generally agree that it will be many decades before the field advances to a state of General AI, which refers to systems capable of human level intelligence across a broad range of tasks.[5] Nevertheless, the growing power of Narrow AI algorithms has sparked a wave of commercial interest, with U.S. technology companies investing an estimated $20-$30 billion in 2016. Some studies estimate this will grow to as high as $126 billion by 2025.[6] DOD's unclassified investment in AI for FY2016 totaled just over $600 million.[7]

AI has a number of unique characteristics that may be important to consider as these technologies enter the national security arena. First, AI is an omni-use technology, as it has the potential to be integrated into virtually everything. Kevin Kelley, the founder of *Wired* magazine, states, "It will enliven inert objects, much as electricity did more than a century ago. Everything that we formerly electrified we will now cognitize."[8] Second, many AI applications are dual-use, meaning they have both military and civil applications. For example, image recognition algorithms can be trained to recognize cats in YouTube videos and terrorist activity in full motion video (FMV) captured by remotely piloted aircraft (RPA) over Syria or Afghanistan.[9] Third, AI is relatively transparent, meaning that its integration into a product is not immediately recognizable. By and large, AI procurement will not result in countable things. Rather, the algorithm will be purchased separately and incorporated into an existing system, or it will be part of a tangible system from inception, which may not be considered predominantly AI. An expert in the field points out, "We will not buy AI. It will be used to solve problems, and there will be an expectation that AI will be infused in most things we do."[10] For this reason, it may be useful to think of AI both in terms of the category noted in **Figure 1** below and in terms of the algorithm's functional application as discussed in the "AI Applications for Defense" section of this report.[11]

---

[4] Executive Office of the President, National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, October 12, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, p. 6.

[5] Ibid., pp. 7-9.

[6] McKinsey Global Institute, *Artificial Intelligence, The Next Digital Frontier?*, June 2017, pp. 4-6.

[7] Govini, *Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy*, December 3, 2017, p. 9.

[8] Kevin Kelly, "The Three Breakthroughs That Have Finally Unleashed AI on the World," *Wired*, October 27, 2014, https://www.wired.com/2014/10/future-of-artificial-intelligence.

[9] Greg Allen and Taniel Chan, *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, July 2017, p. 47.

[10] Steve Mills, Presentation at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, 2017.

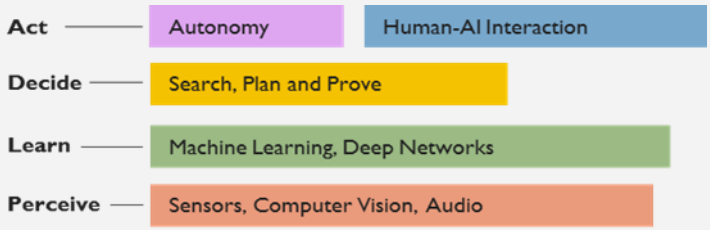
[11] For a broad introduction to the field of AI, see CRS In Focus IF10608, *Overview of Artificial Intelligence*, by Laurie A. Harris

AI Concepts

Table 1. Taxonomy of Historical AI Definitions

Systems That Think Like Humans	Systems That Think Rationally
"The automation of activities that we associate with human thinking, activities such as decision making, problem solving, and learning" —Bellman, 1978	"The study of computations that make possible to perceive, reason, and act" —Winston, 1992
Systems That Act Like Humans	**Systems That Act Rationally**
"The art of creating machines that perform functions that require intelligence when performed by people" —Kurzweil, 1990	"The branch of computer science that is concerned with the automation of intelligent behavior" —Luger and Stubblefield, 1993

Figure 1. Categories of AI Applications



Source: Andrew W. Moore, "AI and National Security in 2017," Presentation at AI and Global Security Summit, Washington, DC, November 1, 2017.

Selected AI Definitions—Where possible, an official U.S. government document is cited.

- **Automation.** "Automated or automatic systems function with no (or limited) human operator involvement, typically in structured and unchanging environments, and the system's performance is limited to the specific set of actions that it has been designed to accomplish ... typically these are well-defined tasks that have predetermined responses according to simple scripted or rule-based prescriptions."[12]
- **Autonomy.** "The condition or quality of being self-governing in order to achieve an assigned task based on the system's own situational awareness (integrated sensing, perceiving, and analyzing), planning, and decision making."[13]
  - Autonomous Weapon System (aka Lethal Autonomous Weapon System, LAWS). "A weapon system that, once activated, can select and engage targets without further intervention by a human operator."[14]
  - Semi-Autonomous Weapon System. "A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator."[15]

[12] Andrew Ilachinski, *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January 2017, p. 6.

[13] Department of Defense, *Joint Concept for Robotic and Autonomous Systems*, October 19, 2016, p. A-3.

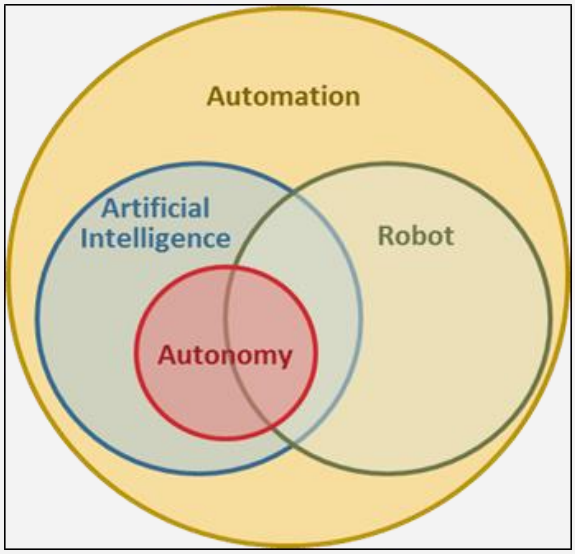
[14] Department of Defense, *Directive 3000.09, Autonomy in Weapon Systems*, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODd/300009p.pdf.

[15] Ibid.

- **Robot.** "A powered machine capable of executing a set of actions by direct human control, computer control, or a combination of both. At a minimum it is comprised of a platform, software, and a power source."[16]

Understanding the relationships between these terms can be challenging, as they may be used interchangeably in the literature and definitions often conflict with one another. Some studies draw a hard line between automation and autonomy, arguing that automated systems are strictly rule-based, lacking an AI component. Other analysts describe AI as a means of automating cognitive tasks, with robotics automating physical tasks. However, experts warn that automation may not be a sufficient term to describe how AI functions, as these systems are not merely replicating human cognitive functions and often come up with surprising solutions. In addition, a robot may be automated or autonomous and may or may not contain an AI algorithm. Virtually all studies agree that AI is a necessary ingredient for fueling a fully autonomous system. **Figure 2** illustrates these relationships, based on the most commonly used descriptions of each term.

Figure 2. Relationships of Selected AI Terminology



Source: CRS.

Issues for Congress

A number of Members of Congress have made calls for action on military AI. During the opening comments to a January 2018 hearing before the House Armed Services Subcommittee on Emerging Threats, the subcommittee chair called for a "national level effort" to preserve a technological edge in the field of AI.[17] Former Deputy Secretary of Defense Robert Work argued in a November 2017 interview that the federal government needs to address AI issues at the highest levels, further stating that "this is not something the Pentagon can fix by itself."[18]

[16] Department of Defense, *Joint Concept for Robotic and Autonomous Systems*, p. A-3.

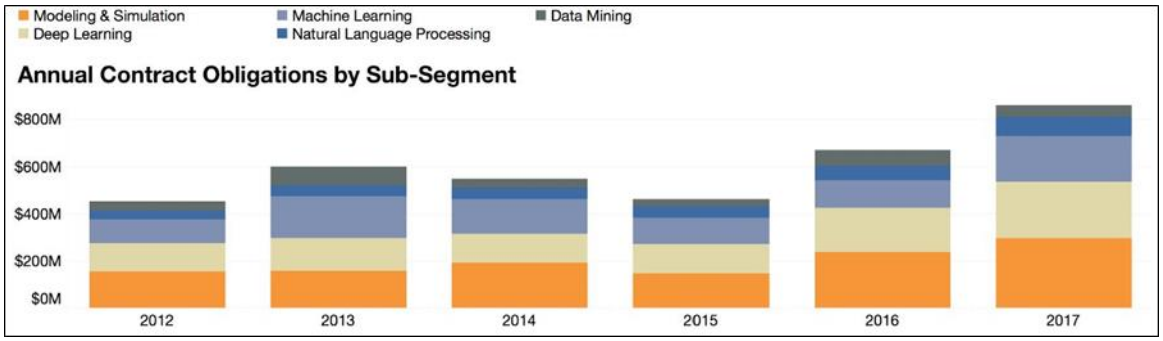
[17] U.S. Congress, House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies*, 115th Cong., 2nd sess., January 9, 2018, transcript available at http://www.cq.com/doc/congressionaltranscripts-5244793?1; remarks by Rep. Joe Wilson.

[18] Colin Clark, "Our Artificial Intelligence 'Sputnik Moment' is Now: Eric Schmidt and Bob Work," *Breaking Defense*, November 1, 2017, https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-now-

(continued...)

Congress may wish to visit the question of funding for AI development. During 2017 testimony before the Senate Committee on Commerce, Science, and Transportation, one expert stated that "federal funding for AI research and development has been relatively flat, even as the importance of the field has dramatically increased."[19] Lieutenant General John Shanahan, lead for the Pentagon's most prominent AI program, identified funding as a barrier to future progress, and a 2017 report by the Army Science Board states that funding is insufficient for the service to pursue disruptive technology like AI.[20] **Figure 3** below illustrates DOD expenditures on AI contracts since 2012.

Figure 3. DOD Spending on AI: FY2012-FY2017



Source: Govini, "Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy," December 3, 2017, p. 9, available at http://www.govini/home/insights/.

Critics of increased federal funding contend that significant increases to appropriations may not be required, as the military should be taking greater advantage of research and development (R&D) conducted in the commercial sector. The 2017 National Security Strategy identifies a need to "establish strategic partnerships to align private sector R&D resources to priority national security applications" and to reward government agencies who "take risks and rapidly field emerging commercial technologies."[21] In addition, guidance to DOD for preparation of its FY2019 budget from the Office of Management and Budget directs the department to "identify existing R&D programs that could progress more efficiently through private sector R&D, and consider their modification or elimination where federal involvement is no longer needed or appropriate."[22] Some experts in the national security community also admit that it would not be a responsible use of taxpayer money to duplicate efforts devoted to AI R&D in the commercial

(...continued)

eric-schmidt-bob-work/.

[19] Testimony of Ed Felten, in U.S. Congress, Senate Committee on Commerce, Subcommittee on Communications, Technology, Innovation, and the Internet, *Hearing on Machine Learning and Artificial Intelligence*, 115th Cong., 2nd sess., December 12, 2017, transcript available at http://www.cq.com/doc/congressionaltranscripts-5235510?1.

[20] Justin Doubleday, "Project Maven Aims to Introduce AI tools into Services' Intel Systems," *Inside Defense*, January 5, 2018, https://insidedefense.com/inside-army/project-maven-aims-introduce-ai-tools-services-intel-systems, and Jason Sherman, "ASB: S&T Funding Inadequate to Support 'Big Bets' on Disruptive Technologies," *Inside Defense*, December 15, 2017, https://insidedefense.com/inside-army/asb-st-funding-inadequate-support-big-bets-disruptive-technologies.

[21] The White House, *National Security Strategy of the United States of America*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf, p. 21.

[22] Executive Office of the President, Director, Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "FY 2019 Administration Research and Development Budget Priorities," August 17, 2017, https://partner-mco-archive.s3.amazonaws.com/client_files/1503000327.pdf.

sector when companies take products 90% of the way to a useable military application.[23] That said, some analysts contend that a number of barriers stand in the way of transitioning AI commercial technology to DOD, and that reforming aspects of the defense acquisition process may be necessary.[24] These issues are discussed in more detail later in this report.[25]

AI also potentially presents oversight challenges for Congress. Analysts assert that AI will create cross-cutting issues in many sectors, and one approach may be to create a federal advisory committee with wide-ranging expertise to inform broad policy concerns. Some initiatives of this type are already in progress. For example, a bill under consideration, the Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2017 (S. 2217), advocates for the creation of a Federal Advisory Committee on the Development and Implementation of AI (a bi-partisan AI caucus formed in the House of Representatives in May 2017).[26]

Likewise, some critics believe that DOD needs to increase its internal oversight of AI development, making the case for an entity inside the department to handle the unique policy questions the technology presents and break through the inertia that stands in the way of quickly moving AI technology from the commercial sector into military applications.[27]

In 2016, the Defense Innovation Board, chaired by Alphabet CEO Eric Schmidt, recommended the creation of an AI and Machine Learning Center of Excellence inside DOD "to spur innovation and transformational change."[28] An organization of this type could also create a single focal point for Congress to consult on defense-related AI issues. So far, DOD has not implemented this recommendation, and AI development continues to be supervised by the Office of the Assistant Secretary of Defense for Research and Engineering.

Within the broad subject of oversight, Congress may consider establishing a separate Program Element (PE) for AI to increase visibility of AI appropriations, as AI appropriation levels in their current format are not readily discernable. There is not a separate PE for AI in the DOD funding tables. The money appropriated for AI R&D is spread throughout generally titled PEs and incorporated into funding for larger systems that have AI components. For example, in the FY2018 National Defense Authorization Act, P.L. 115-91, Army AI funding is spread throughout the PEs for Computer and Software Technology, Advanced Computer Science, and Ground Robotics. The lack of agreed upon definitions in the field further complicates comparisons between federal AI funding and the commercial sector. Each entity draws different boundaries for which programs constitute an investment in AI technology, potentially resulting in disparate AI funding assessments.

---

[23] Dr. Matthijs Broer, Chief Technology Officer, Central Intelligence Agency, Comments at Defense One Summit, November 9, 2017.

[24] Testimony of Paul Scharre, House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies.*

[25] For a discussion of recent defense acquisitions reform initiatives, see CRS Report R45068, *Acquisition Reform in the FY2016-FY2018 National Defense Authorization Acts (NDAAs)*, by Moshe Schwartz and Heidi M. Peters

[26] U.S. Congress, Sen. Maria Cantwell, *Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2017*, and Jordan Novet, "Lawmakers Aim to 'Get Smart' about AI," CNBC, May 24, 2017, https://www.cnbc.com/2017/05/24/congressional-ai-caucus-working-with-amazon-google-ibm.html.

[27] Testimony of Paul Scharre and William Carter, House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies.*

[28] Aaron Mehta, "Defense Innovation Board Lays Out First Concepts," *Defense News*, October 5, 2016, https://www.defensenews.com/pentagon/2016/10/05/defense-innovation-board-lays-out-first-concepts/.

Congress may also consider specific policies on the use of military AI applications. Many experts fear that the pace of AI technology development is moving faster than the speed of implementing policy. House Armed Services Committee Chairman, Representative Mac Thornberry, echoed this sentiment, stating, "It seems to me that we're always a lot better at developing technologies than we are the policies on how to use them."[29] While broad regulation of AI may not be appropriate, Congress may assess the need for new policies or modifications of existing laws to account for AI within sectors. Regulations could be based on risk assessments, considering areas where AI may either increase or decrease risk.[30] Perhaps the most immediate policy concern among AI analysts is the absence of an independent entity inside the DOD or the federal government to develop and enforce AI safety standards.[31]

Lethal Autonomous Weapons Systems (LAWS) are another contentious military AI application for Congress to consider shaping DOD restrictions on development as well as spurring international engagement. Some analysts are concerned that efforts to control LAWS will stifle development of other useful military AI technology due to strict controls on applications that may be put to use in a lethal system, even if they are not fundamentally designed to do so. During recent testimony to the UN, one expert stated, "If we agree to foreswear some technology, we could end up giving up some uses of automation that could make war more humane. On the other hand a headlong rush into a future of increasing autonomy with no discussion of where it is taking us, is not in humanity's interest either." He suggests the leading question for regulating military AI applications ought to be, "What role do we want humans to play in wartime decision making?"[32]

Congress may consider the growth of international competition in the AI market and the danger of foreign exploitation of U.S. AI technology for military purposes. In particular, the Chinese government is aggressively pursuing AI investments in the United States, and in September 2017, President Trump, following the recommendation of the Committee on Foreign Investment in the U.S. (CFIUS), blocked a Chinese firm from acquiring Lattice Semiconductor, a company that manufactures chips that are a critical design element for AI technology.[33] Some experts believe that CFIUS may provide a means of protecting a technology like AI with potentially strategic significance, but changes to the current legislation may be necessary to maintain more thorough oversight of foreign investment.[34]

In addition, many analysts believe that it may be necessary to reform federal data policies. Large data pools are a necessary ingredient for building many AI systems, and government data sources may be particularly important for military AI applications. However, critics point out that much

[29] Morgan Chalfant, "Congress Told to Brace for Robotic Soldiers," *The Hill*, March 1, 2017, http://thehill.com/policy/cybersecurity/321825-congress-told-to-brace-for-robotic-soldiers.

[30] National Science and Technology Council, *Preparing for the Future of Artificial Intelligence*, October 2016, p. 17.

[31] CRS discussion with Mike Garris, National Institute of Standards and Technology, Co-Chairman, Subcommittee on Machine Learning and Artificial Intelligence, Committee on Technology, National Science and Technology Council, October 2, 2017.

[32] Paul Scharre, Remarks to the United Nations, Group of Governmental Experts on Lethal Autonomous Weapons Systems, November 15, 2017, Geneva, Switzerland, https://s3.amazonaws.com/files.cnas.org/documents/Scharre-Remarks-to-UN-on-Autonomous-Weapons-15-Nov-2017.pdf?mtime=20171120095806. For more information on LAWS, see CRS Report R44466, *Lethal Autonomous Weapon Systems: Issues for Congress*, by Nathan J. Lucas.

[33] Ana Swanson, "Trump Blocks China-Backed Bid to Buy U.S. Chip Maker," *The New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/business/trump-lattice-semiconductor-china.html.

[34] Paul Scharre and Dean Cheng, Testimony to Subcommittee on Emerging Threats and Capabilities, *Hearing on China's Pursuit of Emerging Technologies.* For more information on CFIUS, see CRS Report RL33388, *The Committee on Foreign Investment in the United States (CFIUS)*, by James K. Jackson.

of this data is stove-piped by stakeholders in the federal bureaucracy, classified, or protected because of privacy concerns. In addition, storing the requisite data for military AI would pose a problem, with many experts arguing that cloud computing is the most viable solution, although the use of cloud storage may create data security issues. Analysts contend that Congress should implement a new data policy that balances concerns for classification and privacy with the need to fuel AI development.[35]

Closely related, AI development may increase the imperative for strict cybersecurity standards. As discussed later in this report, AI algorithms are exceptionally vulnerable to theft or manipulation, particularly if the training data set is not adequately protected. During a February 2018 conference with defense industry CEOs, Deputy Defense Secretary Patrick Shanahan advocated for higher cybersecurity standards in the commercial sector stating, "[W]e want the bar to be so high that it becomes a condition of doing business."[36]

AI Applications for Defense

DOD is looking into a number of diverse applications for AI. Currently, AI R&D is being left to the discretion of research organizations in the individual services, as well as to the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Agency (IARPA). The Office of the Assistant Secretary of Defense for Research and Engineering (ASD/RE) maintains loose oversight of these initiatives, and it is in the process of producing a DOD AI Strategy, which is forecast to be released in summer 2018. The ASD/RE views the services' disparate approaches to AI research as a strength in the near term, despite some duplication of effort.[37]

The Algorithmic Warfare Cross-Functional Team, also known as Project Maven, is a focal point for DOD AI integration overseen by the Undersecretary of Defense for Intelligence (USDI). Project Maven was launched in April 2017 and charged with rapidly incorporating AI into existing DOD systems to demonstrate the technology's potential.[38] Project Maven's Director states, "Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame for artificial intelligence across the department."[39]Although Project Maven's immediate effort is focused on intelligence processing, the wide variety of AI projects underway elsewhere in the department illustrate the omni-use nature of the technology AI technologies.

---

[35] Paul Scharre, "The US Can Be a World Leader in AI, Here's How," *The National Interest*, November 2, 2017, http://nationalinterest.org/print/feature/the-united-states-can-be-world -leader-ai-heres-how-22921. For more on federal data policy and cloud computing, see CRS Report R42887, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, by Patricia Moloney Figliola and Eric A. Fischer.

[36] Marcus Weisgerber, "Pentagon Warns CEOs: Protect Your Data or Lose Our Contracts," *Defense One*, February 6, 2018, http://www.defenseone.com/business/2018/02/pentagon-warns-ceos-protect-your-data-or-lose-our-contracts/145779/?oref=d-river. For more on cybersecurity legislation, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[37] Based on CRS discussions with Dr. Richard Linderman, Deputy Director for Information System and Cyber Technologies, Office of the Assistant Secretary of Defense for Research and Engineering, October 24, 2017.

[38] Robert Work, Deputy Secretary of Defense, Memorandum, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," April 26, 2017, https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf.

[39] Jack Corrigan, "Three-Star General Wants AI in Every New Weapon System," *Defense One*, November 3, 2017, http://www.defenseone.com/technology/2017/11/three-star-general-wants-artificial-intelligence-every-new-weapon-system/142239/?oref=d-river.

Intelligence, Surveillance, and Reconnaissance

AI is expected to be particularly useful in intelligence due to the large data sets available for analysis.[40] As such, Project Maven's first phase involves automating intelligence processing in support of the counter-ISIL campaign. Specifically, this team is incorporating computer vision and machine learning algorithms into intelligence collection cells that would comb through Remotely Piloted Aircraft (RPA) footage and automatically identify hostile activity for targeting. In this capacity, AI is intended to automate the work of human analysts who currently spend hours sifting through videos for actionable information, and it may free them to make more efficient and timely decisions based on the data.[41] The team initially incorporated these AI tools into 10 sites, with plans to incorporate them into 30 sites by mid-2018.[42]

The intelligence community has a number of publicly-advertised AI research projects in progress. The Central Intelligence Agency (CIA) has 137 projects in development that leverage AI in some capacity to accomplish tasks such as image recognition or labeling (similar to Project Maven's algorithm and data analysis functions) to predict future events like terrorist attacks or civil unrest based on wide-ranging analysis of open source information.[43] IARPA is sponsoring several AI research projects intended to produce tangible tools for the community four to five years from completion. Some examples of its programs include developing algorithms to accomplish multilingual speech recognition and translation in noisy environments; geo-locating images with no associated metadata; fusing 2-D images to create 3-D models; and tools to infer a building's function based on pattern of life analysis.[44]

Logistics

AI may have a promising future in the field of military logistics. For example, the Air Force is working toward using AI to accomplish tailored, predictive aircraft maintenance. Instead of making repairs when an aircraft breaks or in accordance with scripted schedules designed for a whole fleet of airplanes, a tailored approach facilitated by AI would allow technicians to perform maintenance on individual aircraft on an as-needed-basis. This type of AI application would extract real-time sensor data embedded in the aircraft's engines and other onboard systems and feed data into a predictive algorithm to determine when technicians need to accomplish inspections or replace parts.[45]

SparkCognition, an AI company based in Texas, installed an AI system of this type on several of Boeing's commercial aircraft. In one instance the algorithm reported that an engine required replacement within 40 hours of engine operation, far ahead of the normal schedule. Upon inspection, the maintenance team discovered a nicked fan blade, which would have cost the company $50 million to replace if it had broken.[46]

---

[40] CRS discussions with Dr. Richard Linderman, October 24, 2017.

[41] Corrigan, "Three-Star General Wants AI in Every New Weapon System."

[42] Based on CRS discussions with Major Colin Carroll, Project Maven, October 10, 2017.

[43] Patrick Tucker, "What the CIA's Tech Director Wants from AI," Defense One, September 6, 2017, http://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801/.

[44] CRS discussions with Dr. Jason Matheny, IARPA Director, October 10, 2017, and https://www.iarpa.gov/index.php/research-programs.

[45] Marcus Weisgerber, "Defense Firms to Air Force: Want Your Planes' Data? Pay Up," *Defense One*, September 19, 2017, http://www.defenseone.com/technology/2017/09/military-planes-predictive-maintenance-technology/141133/.

[46] Ibid.

In September 2017, the Army Logistics Support Activity (LOGSA) signed a second contract with IBM worth $135 million for an AI proof of concept. During the first project, IBM's Watson (the same AI computer that defeated two Jeopardy champions) employed a tailored maintenance algorithm similar to the one described above to perform individually customized maintenance for the Stryker fleet, based on information pulled from 17 sensors installed on the vehicles. The current project plans to use Watson to analyze shipping flows for repair parts distribution, attempting to determine the most time- and cost-efficient means to deliver supplies. The Army believes this AI system could save up to $100 million a year after analyzing just 10% of shipping requests.[47] These applications further illustrate the potential of AI and the virtually direct correlation between commercial and military AI algorithms.

Cyberspace

AI is likely to be consequential in the cyberspace domain. In his 2016 testimony before the Senate Armed Services Committee, Commander of U.S. Cyber Command Admiral Michael Rogers stated that relying on human intelligence alone in cyberspace is "a losing strategy." At a defense conference he clarified this point, stating, "If you can't get some level of AI or machine learning with the volume of activity you're trying to understand when you're defending networks ... you are always behind the power curve."[48]

Conventional cyber-defense tools look for historical matches to previous malicious code, so hackers only have to modify small portions of that code to circumvent this defense. AI cyber-defense tools are trained to recognize changes to patterns of behavior in a network and detect anomalies, presenting a more comprehensive barrier to previously unobserved attack methods.[49] These tools potentially allow defenders to be more forward thinking, with protection against novel and inventive means of cyber-attack instead of simple observations of past methods.

DARPA's recent Cyber Grand Challenge demonstrated the potential power of AI cyber tools. The competition featured an air-gapped network of seven computers with custom designed software containing vulnerabilities that mimic real world glitches. The contestants developed AI algorithms to autonomously identify and patch vulnerabilities in their own software while simultaneously attacking the other teams' weaknesses. The competing AI algorithms managed to fix these security bugs in a matter of seconds, whereas conventional cybersecurity programs typically take several months to find and patch them.[50] The challenge also demonstrated a singular AI algorithm capable of simultaneously playing offense and defense, which may be a distinct advantage in the future.

Command and Control

The U.S. military is seeking to exploit AI's analytical potential in the area of command and control. The Air Force is developing a system for Multi-Domain Command and Control (MDC2),

[47] Adam Stone, "Army Logistics Integrating New AI, Cloud Capabilities," September 7, 2017, https://www.c4isrnet.com/home/2017/09/07/army-logistics-integrating-new-ai-cloud-capabilities/.

[48] Amaani Lyle, "National Security Experts Examine Intelligence Challenges at Summit," September 9, 2016, https://www.defense.gov/News/Article/Article/938941/national-security-experts-examine-intelligence-challenges-at-summit/.

[49] Scott Rosenberg, "Firewalls Don't Stop Hackers, AI Might," *Wired*, August 27, 2017, https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/.

[50] "Mayhem Declared Preliminary Winner of Historic Cyber Grand Challenge," August 4, 2016, https://www.darpa.mil/news-events/2016-08-04 and http://archive.darpa.mil/cybergrandchallenge/.

which aims to centralize planning and execution of air, space, cyberspace, sea, and land-based effects. In the immediate future, AI may be used to fuse data from sensors in all of these domains to create a single source of information for decisionmakers, also known as a *common operating picture*.[51] The information available to decisionmakers comes in diverse formats from multiple platforms, often with redundancies or unresolved discrepancies. A common operating picture enabled by AI would combine this information into one display, providing an intuitive picture of friendly and enemy forces, and automatically resolving variances from input data.

Later, AI may be used to identify communications links cut by an adversary and find alternative means to distribute information. As the complexity of AI systems mature, AI algorithms may provide commanders with viable courses of action based on real-time analysis of the battle-space, which would enable faster adaptation to unfolding events.

Although MDC2 is still in a concept development phase, the Air Force is working with Lockheed Martin, Harris, and several AI start-ups to develop such a data fusion capability. A series of war-games in 2018 will seek to refine requirements for this project.[52] In the long run, analysts believe this area of AI development will likely be especially consequential, with the potential to improve the quality of wartime decision-making and accelerate the pace of conflict.

Autonomous Vehicles

All the military services are incorporating AI into various types of autonomous vehicles. The services' time frame for fielding these systems is at least a decade in the future. AI applications in this field are similar to commercial self-driving vehicles, which use AI technologies to perceive the environment, recognize obstacles, fuse sensor data, plan navigation, and even communicate with other autonomous vehicles.[53]

The Air Force Research Lab completed phase two of testing on the Loyal Wingman program, which pairs an older-generation, unmanned fighter with a manned F-35 or F-22. During this event, the F-16 test platform (the unmanned "Loyal Wingman") autonomously reacted to events that were not preprogrammed, like unforeseen obstacles and weather.[54] As the program progresses, AI may enable the "loyal wingman" to accomplish tasks for its manned flight lead, such as reacting to electronic threats with jamming or carrying extra weapons.[55]

The Army and the Marine Corps tested prototypes of similar autonomous vehicles that follow soldiers around the battlefield to accomplish independent tasks. The Marine Corps' Multi-Utility

[51] Colin Clark, "Rolling the Marble: BG Saltzman on Air Force's Multi-Domain C2 System," *Breaking Defense*, August 8, 2017, https://breakingdefense.com/2017/08/rolling-the-marble-bg-saltzman-on-air-forces-multi-domain-c2-system/.

[52] Mark Pomerlau, "How Industry's Helping the US Air Force with Multi-Domain Command and Control," *Defense News*, September 25, 2017, https://www.defensenews.com/c2-comms/2017/09/25/industry-pitches-in-to-help-air-force-with-multi-domain-command-and-control/.

[53] CRS Report R44940, *Issues in Autonomous Vehicle Deployment*, by Bill Canis, pp. 2-3.

[54] David Axe, "US Air Force Sends Robotic F-16s into Mock Combat," *The National Interest*, May 16, 2017, http://nationalinterest.org/blog/the-buzz/us-air-force-sends-robotic-f-16s-mock-combat-20684.

[55] Mark Pomerlau, "Loyal Wingman Program Seeks to Realize Benefits of Advancements in Autonomy," October 19, 2016, https://www.c4isrnet.com/unmanned/uas/2016/10/19/loyal-wingman-program-seeks-to-realize-benefits-of-advancements-in-autonomy/.

Tactical Transport (MUTT) is an ATV-sized vehicle capable of carrying extra equipment that follows Marines around the battlefield via a radio link. Although the system is not autonomous in its current configuration, the Marine Corps plans to augment the vehicle with AI in the future to make it completely independent.[56] Likewise, the Army plans to field a number of Remote Combat Vehicles (RCVs) with different types of AI functionality, such as autonomous navigation, surveillance, and IED removal. Experience with these systems aims to inform design of the self-driving Next Generation Ground Vehicle, tentatively scheduled to debut in 2035.[57]

In November 2016, the Navy completed testing on AI-enabled swarm boats. AI-fueled cooperative behavior, or swarming, is a unique subset of autonomous vehicle development, with concepts ranging from large formations of low-cost drones designed to overwhelm defensive systems to small squadrons of RPAs that collaborate to provide electronic attack, fire support, and localized navigation and communication nets for ground-troop formations.[58] This Navy test featured a formation of five unmanned boats that cooperatively patrolled a 4-by-4 mile section of the Chesapeake Bay and intercepted an "intruder" vessel. The results of this experiment may lead to AI technology adapted for defending harbors, hunting submarines, or scouting in front of a formation of larger navy ships.[59]

Swarm Characteristics[60]

- Autonomous (not under centralized control)
- Capable of sensing their local environment and other nearby swarm participants
- Able to communicate locally with others in the swarm
- Able to cooperate to perform a given task

Lethal Autonomous Weapon Systems (LAWS)

LAWS are a special class of AI systems capable of independently identifying a target and employing an onboard weapon system to engage and destroy it with no human interaction. LAWS require a computer vision system and advanced machine learning algorithms to classify an object as hostile, make an engagement decision, and guide a weapon to the target. At the moment, DOD has delayed LAWS development indefinitely on moral grounds, which are codified in regulatory limitations.

The current Department of Defense guidance on LAWS, DOD Directive 3000.09 "Autonomy in Weapon Systems," requires that autonomous systems "allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[61] This guidance does allow

[56] Kristin Houser, "The Marines' Latest Weapon is a Remote-Controlled Robot with a Machine Gun," May 4, 2017, https://futurism.com/the-marines-latest-weapon-is-a-remote-controlled-robot-with-a-machine-gun/.

[57] David Vergun, "The Army Says Remote Combat Vehicles Can Pack as Much Firepower as an Abrams Tank," *Business Insider*, December 13, 2017, http://www.businessinsider.com/army-says-remote-vehicles-can-pack-as-much-firepower-as-an-abrams-tank-2017-12.

[58] Mary-Ann Russon, "Google Robot Army and Military Drone Swarms: UAVs May Replace People in the Theatre of War," *International Business Times*, April 16, 2015, http://www.ibtimes.co.uk/google-robot-army-military-drone-swarms-uavs-may-replace-people-theatre-war-1496615.

[59] Sydney J. Freedberg Jr., "Swarm 2: The Navy's Robotic Hive Mind," *Breaking Defense*, December 14, 2016, https://breakingdefense.com/2016/12/swarm-2-the-navys-robotic-hive-mind/.

[60] Ilachinski, p. 108.

[61] Department of Defense, *Directive 3000.09, Autonomy in Weapon Systems*.

human-supervised systems to select and engage nonhuman targets for defensive purposes, and it authorizes the use of autonomous systems for "non-lethal, non-kinetic force" like electronic attack.[62] Congress and the executive branch, including DOD, continue to debate the military advantages lost by forgoing autonomous systems that lack human operators for offensive engagements. Many contend that the U.S. will sacrifice a strategic advantage if international rivals develop LAWS and the U.S. military does not. However, DOD leadership continues to affirm the prohibition on this type of technology. In 2017 testimony before the Senate Armed Services Committee, Vice Chairman of the Joint Chiefs of Staff General Paul Selva stated, "I am an advocate for keeping the restriction, because we take our values to war.... I do not think it is reasonable for us to put robots in charge of whether or not we take a human life."[63] Regardless, Selva explained that the military will be compelled to address the development of this technology in order to find its vulnerabilities because potential U.S. adversaries are pursuing LAWS.[64]

AI Acquisitions Challenges

From the Cold War era until recently, most major defense-related technologies were first developed by government-directed programs and later spread to the commercial sector.[65] Examples include nuclear technology, the Global Positioning System (GPS), and the internet. In contrast, civilian companies are leading AI development, with DOD adapting their tools after the fact for national security functions. Noting the reversal of the traditional arrangement that has developed over the past decade, one AI expert commented, "It is unusual to have a technology that is so strategically important being developed commercially by a relatively small number of companies."[66]

AI is one of many dual use technologies, with some commercial applications being directly transferable for DOD's purposes. However, there are some exceptions to this generalization, and several unique complications are associated with adjusting to the changing relationship between DOD and commercial companies. A wide variance exists in the adaptability of commercial technology for defense. In some cases, the transition is relatively seamless. For example, the aircraft maintenance algorithms described above will likely require minor adjustments to the training data for the type of aircraft and sensor data available. However, in other circumstances, the combat environments in which military systems operate are often much less structured, with greater potential for unpredictable events. Self-driving vehicles are an illustration. Commercial

[62] Ibid.

[63] U.S. Congress, Senate Committee on Armed Services, *Hearing to Consider the Nomination of General Paul J. Selva, USAF, for Reappointment to the Grade of General and Reappointment to be Vice Chairman of the Joint Chiefs of Staff*, 115th Cong., 1st sess., July 18, 2017 (Washington, DC: GPO, 2017).

[64] Ibid. For a full discussion of LAWS, see CRS Report R44466, *Lethal Autonomous Weapon Systems: Issues for Congress*, by Nathan J. Lucas.

[65] William H. McNeill, *The Pursuit of Power* (Chicago: The University of Chicago Press, 1982), pp. 368-369. In this history of technology, warfare, and international competition, McNeill discusses government mobilization of the science and engineering community. The effort started in WWII with the creation of large research and development organizations dedicated to creating war-winning technology. The government continued to pump large amounts of money into research and development during the Cold War as technological superiority was perceived as a key measure of national strength. McNeill states, "The ultimate test of American society in its competition with the Soviets boiled down to finding out which contestant could develop superior skills in every field of human endeavor.... This would guarantee prosperity at home and security abroad." This effort had lingering effects that have persisted to some extent in the wake of the Cold War.

[66] Dr. Ed Felten, Comments at the Global Security Forum, Center for Strategic and International Studies, Washington, DC, November 7, 2017.

autonomous vehicles are likely to thrive on a data-rich environment with a reliable GPS position, abundant map data of virtually every location it will encounter, and up-to-date information on traffic and weather conditions from other self-driving vehicles.[67]

In contrast, the military variant of the autonomous vehicle will likely operate in locations where map data is comparatively poor, or the vehicle may be driving off-road in rough terrain. Moreover, an adversary may jam the GPS signal and the communications links to other vehicles, further complicating navigation. A commercially developed self-driving vehicle trained to operate on many more inputs will not function well in these circumstances.[68] In such cases, DOD likely needs a specifically-tailored version of the technology, with experts inside the department defining the requirements.

In addition to coping with unstructured environments, military AI must also contend with thinking human adversaries who are actively attempting to thwart the AI system by manipulating or denying information. A team at Carnegie Mellon University created an AI algorithm that beat four humans in 120,000 hands of the card game no-limit Texas hold'em. This feat was significant because it was the first game-playing application designed for an environment in which information is not perfect and the other players have an incentive to deceive. The AI player must develop its own plan for withholding information or bluffing, and it must think strategically, considering how each move will affect the game as a whole.[69] While this type of AI is seen as a promising development for DOD, the department may have to rely on academic institutions or internal laboratories to further this research. One expert argues that commercial companies may not have a strong incentive to create AI of this type, because most of their tools will encounter much less contested situations.[70]

Aligning civilian and military standards of safety and performance present another challenge associated with adapting AI for defense applications. A failure rate deemed acceptable for a civilian AI application may be well outside of tolerances in a combat environment. In addition, a recent study concludes that unpredictable AI failure modes will be exacerbated in the complex environments of the defense sector described previously.[71] One expert asserts that although some civilian AI algorithms will affect decision-making in substantial fields like health care or criminal justice, AI in the defense environment will generally be more consequential, with human lives routinely held at risk.[72] Significantly, no independent entity in the commercial sector or inside government is charged with validating AI system performance and enforcing safety standards.[73] Collectively, these factors may create another barrier for the smooth transfer of commercially developed AI technology to DOD.

In addition to the technological adaptation impediments, the military may need to adjust the DOD acquisitions process to more closely match timelines and processes in commercial companies to smooth the AI transition. Defense acquisition processes might not be agile enough for fast-paced

[67] CRS In Focus IF10658, *Autonomous Vehicles: Emerging Policy Issues*, by Bill Canis.

[68] Based on CRS discussions with Dr. Dai H. Kim, Associate Director for Advanced Computing, Office of the Assistant Secretary of Defense for Research and Engineering, October 4, 2017.

[69] Noam Brown and Tuomas Sandholm, "Superhuman AI for Heads-Up No-limit Poker: Libratus Beats Top Professionals," *Science*, December 17, 2017, http://science.sciencemag.org/content/early/2017/12/15/science.aao1733.full.

[70] CRS discussion with Dr. Dai H. Kim.

[71] Allen and Chan, pp. 4-6.

[72] CRS discussion with Dr. Dai Kim

[73] CRS discussion with Mr. Mike Garris.

software systems like AI.[74] The governing DOD Instruction, 5000.02, stipulates a linear, five-phase process. An internal study of the process with an eye to reform found that it takes an average of 91 months to move from the initial Analysis of Alternatives, defining the requirement for a system, to an Initial Operational Capability.[75] In contrast, commercial companies typically execute an iterative development process for software systems like AI, delivering a product in six to nine months.[76] A Government Accountability Office (GAO) study of this issue surveyed 12 U.S. commercial companies who choose not to do business with DOD, and all 12 cited the complexity of the DAP as a rationale for their decision.[77]

In the long run, it is not clear which, if any, of the existing acquisitions authorities the department will adjust to purchase AI systems. In recognition of the mismatch challenge, the department has created a number of "rapid-acquisitions" organizations with Other Transaction Authorities (OTA), including the Air Force Rapid Capabilities Office, the Army Asymmetric Warfare Group, and the Defense Innovation Unit Experimental (DIUx).

In large part to these efforts, Project Maven made significant improvements to the acquisitions timeline. The team organized in April 2017, and two months later Congress appropriated its funding; by December, the team was fielding a commercially acquired, prototype AI system in combat.[78] However, the March 2018 reduction of the DIUx-brokered cloud contract may be a signal that OTA organizations will not handle larger acquisitions projects in the future.[79] In August 2017, DOD completed a revision to DODI 5000.02, with additional acquisitions milestone models that may be used to smooth purchase of AI systems, including Defense Unique Software Intensive Model, Incrementally Deployed Software Intensive Model, and a Hybrid (Software Dominant) Model.[80]

Alternatively, the department recently released a new acquisitions instruction specifically for Information Technology Systems, DODI 5000.75, which may be adapted to purchase AI systems.[81] Although some analysts argue that these are promising developments, critics point out that the department must replicate the results achieved by Project Maven at scale and settle on a more clear-cut acquisitions process to avoid future frustration.[82]

---

[74] Ilachinski, pp. 190-191.

[75] Department of Defense, *Instruction 5000.02, Operation of the Defense Acquisition System*, at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/500002_DODi_2015.pdf?ver=2017-08-11-170656-430, pp. 6-11; Ilachinski pp. 189; and Defense Science Board, "DOD Policies and Procedures for the Acquisition of Information Technology," March 2009, https://www.acq.osd.mil/dsb/reports/2000s/ADA498375.pdf.

[76] Defense Science Board, "Design and Acquisition of Software for Defense Systems," February 2018, https://www.acq.osd.mil/dsb/reports/2010s/DSB_SWA_Report_FINALdelivered2-21-2018.pdf.

[77] U.S. Government Accountability Office, *Military Acquisitions, DOD is Taking Step to Address Challenges Faced by Certain Companies*, GAO-17-644, July 20, 2017, p. 9. Other rationales cited include unstable budget environment, lengthy contracting timeline, government-specific contract terms and conditions, inexperienced DOD contracting workforce, and intellectual property rights concerns.

[78] Marcus Weisgerber, "The Pentagon's New Artificial Intelligence is Already Hunting Terrorists," *Defense One*, December 21, 2017, http://www.defenseone.com/technology/2017/12/pentagons-new-artificial-intelligence-already-hunting-terrorists/144742/.

[79] Frank Konkel, "Defense Department Drastically Cuts Nearly $1B Cloud Contract," *Defense One*, March 7, 2018, https://www.defenseone.com/technology/2018/03/defense-department-drastically-cuts-nearly-1b-cloud-contract/146448/.

[80] DOD, *Instruction 5000.02*, pp. 12-17.

[81] Department of Defense, *Instruction 5000.75, Business Systems Requirements and Acquisition*, February 2, 2017, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/500075_DODi_2017.pdf.

[82] Ilachinski, p. 190.

An apparent cultural divide between DOD and leading tech companies may also be a roadblock to AI acquisitions. A recent study of the issue concluded that "the relationship is not strained because of a lack of awareness of shared problems, but because productive dialogue is frequently derailed by divergent perspectives and mutual misjudgment."[83] The report was based on a survey of leadership in several top Silicon Valley companies, with 80% of participants rating the relationship with DOD as poor or very poor.[84]

The analysis found a disconnect between the communities on the "incentives for collaboration." Commercial companies are often largely motivated by near-term profits and growth, and government representatives may not adequately explain the long-term mutual security benefits of cooperation.[85] Members of DOD leadership also cited the tech sector's insistence on preserving intellectual property rights as a stumbling block. This is particularly challenging when it comes to AI, because many companies are not selling code to the department along with the AI application, which makes it difficult to gain a deeper understanding of how the system will perform.[86]

In more extreme cases, companies are refusing to work with DOD altogether because of concerns over AI being used for government surveillance and lethal applications. Notably, Google canceled existing government contracts for two robotics companies it acquired, Boston Dynamics and Schaft, and prohibited future government work for DeepMind, another AI software startup Google acquired.[87] None of these developments are widely seen as surprising, but they take on new meaning in a context where the broader relationship between the two groups has changed and DOD is more beholden to the technology sector for developing a critical product.

The culture within the defense sector itself may create an impediment to AI integration. Currently, AI is being integrated into existing systems, which alters standardized procedures and upends well-defined personnel roles. Members of Project Maven have reported a resistance to change because the disruption that comes with AI integration does not provide an intuitive benefit.[88] Deputy Director for CIA technology development, Dawn Meyerriecks, also expressed concern about the willingness of the national leadership and key decisionmakers to accept an AI-generated analysis or recommendation, arguing that the prevalent, risk-averse culture may be more troubling than the pace of adversary AI development.[89]

Finally, some analysts are concerned that DOD will simply use AI to improve existing processes instead of capitalizing on the technology's potential to produce a more significant benefit on the battlefield. The services may use AI to reinforce systems closely tied to their own identities rather than thinking big about what AI can accomplish, or they may reject some AI applications altogether if the technology threatens service-favored hardware.[90] Members of Congress may

[83] Loren DeJonge Schulman, Alexandra Sander, and Madeline Christian, "The Rocky Relationship Between Washington and Silicon Valley, Clearing the Path to Improved Collaboration," Center for a New American Security, July, 19, 2017, https://s3.amazonaws.com/files.cnas.org/documents/COPIA-CNAS-Rocky-Relationship-Between-Washington-And-Silicon-Valley.pdf?mtime=20170719145206, p. 4.

[84] Ibid.

[85] Ibid, pp. 4-5.

[86] CRS discussion with Dr. Richard Linderman.

[87] Allen and Chan, p. 52.

[88] CRS discussion with Major Colin Carroll.

[89] Patrick Tucker, "What the CIA's Tech Director Wants from AI," *Defense One*, September 6, 2017, http://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801/.

[90] CRS discussion with Paul Scharre, Center for a New American Security, September 28, 2017.

explore the complex interaction of these factors as DOD moves beyond the initial stages of AI integration.

International Competition

As AI defense applications grow in scale and complexity, many in Congress and the defense community are becoming increasingly concerned about international competition. In his opening comments at "The Dawn of AI" hearing before the Senate Subcommittee on Space, Science, and Competitiveness, Senator Ted Cruz stated, "Ceding leadership in developing artificial intelligence to China, Russia, and other foreign governments will not only place the United States at a technological disadvantage, but it could have grave implications for national security."[91]

AI has also been discussed for the past two years at the Senate Select Intelligence Committee's annual hearing on the "Worldwide Threat Assessment," consistently making the list of "Emerging and Disruptive Technologies."[92] In his written testimony for the 2017 hearing, Director of National Intelligence Daniel Coates asserted, "The implications of our adversaries' abilities to use AI are potentially profound and broad."[93]

Given the anticipated national security value some ascribe to AI technology, several analysts have cast the increased pace and magnitude of AI development as a "Sputnik Moment" that may spark a global AI arms race.[94] Consequently, it may be important for Congress to understand the state of rival AI development, as well as how international organizations like the United Nations are addressing the technology.

China

China is by far the most ambitious competitor to the United States in the international AI market. China's 2017 "Next Generation AI Development Plan" describes AI as a "strategic technology" that has become a "focus of international competition."[95] According to the document, China will "firmly seize the strategic initiative" and reach "world leading levels" of AI investment by 2030, with over $150 billion in government funding.[96]

Recent Chinese achievements in the field demonstrate China's potential to realize this goal. In 2015, China's leading AI company, Baidu, created AI software capable of surpassing human-levels of language recognition, almost a year in advance of Microsoft, the nearest U.S.

---

[91] U.S. Congress, Senate Subcommittee on Space, Science, and Competitiveness, Committee on Commerce, Science, and Transportation, *Hearing on the Dawn of Artificial Intelligence*, 114th Cong., 2nd sess., November 30, 2016 (Washington, DC: GPO, 2016) p. 2.

[92] U.S. Congress, Senate Committee on Intelligence, *Hearing on Current and Projected National Security Threats to the United States*, 114th Cong., 2nd sess., February 9, 2016 (Washington, DC: GPO, 2016), p. 4, and U.S. Congress, Senate Committee on Intelligence, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, 115th Cong., 1st sess., May 11, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf, p. 3.

[93] Ibid.

[94] Clark, "Our Artificial Intelligence 'Sputnik Moment' is Now," and Tom Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race," *Wired*, August, 8, 2017, https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/.

[95] China State Council, "A Next Generation Artificial Intelligence Development Plan," p. 2.

[96] Ibid., pp. 2-6.

competitor.[97] In 2016 and 2017, Chinese teams won the top prize at the Large Scale Visual Recognition Challenge, an international competition for computer vision systems.[98] Chinese development of military AI applications closely mirrors that of the United States, and while not invulnerable, the AI industry in China may have fewer barriers to commercial and military cooperation.

Chinese development of military AI is influenced in large part by China's observation of U.S. plans for defense innovation and fears of a widening "generational gap" in comparison to the U.S. military.[99] The guiding principle for Chinese AI development is a focus on the use of AI to enhance battlefield decision-making. Similar to U.S. military concepts, the Chinese aim to use AI for exploiting large troves of intelligence information, providing a comprehensive picture of the battlespace and recommending viable actions to military decisionmakers.[100]

China is also researching various types of air, land, sea, and submersible autonomous vehicles. In the spring of 2017, a civilian Chinese university with ties to the military demonstrated an AI-enabled swarm of 1,000 unmanned aerial vehicles (UAVs) at an airshow. A media report released after the fact showed a computer simulation of a similar swarm formation finding and destroying a missile launcher.[101]

Open-source publications also indicate that the Chinese are developing a suite of AI tools for cyber-defense and attack.[102] The close parallels between U.S. and Chinese AI development have some DOD leaders concerned about the prospects for achieving a unique and enduring battlefield advantage as envisioned in current defense innovation guidance.[103]

Analysts point to a number of differences that may influence the comparative rate of military AI adoption in China and the United States. Significantly, unlike the United States, China has not been involved in active combat for several decades. While on the surface this may seem like a weakness, some argue that it may be an advantage, making the Chinese more apt to develop unique concepts for AI in combat. These experts contend that, in contrast, the United States appears to be focused on using AI to solve immediate, tactical-level problems and incremental improvement of existing ideas. Incidentally, the Chinese are using AI-generated war games to overcome gaps in their lack of combat experience.[104]

Nevertheless, the Chinese may have similar reservations about adopting autonomous systems and trusting AI-generated decisions, especially in a military culture dominated by centralized command authority and mistrust of subordinates. However, the Chinese may have fewer moral

[97] Jessi Hempel, "Inside Baidu's Bid to Lead the AI Revolution," *Wired*, December 6, 2017, https://www.wired.com/story/inside-baidu-artificial-intelligence/?mbid=nl_120917_daily_list1_p4.

[98] Aaron Tilley, "China's Rise in the Global AI Race Emerges as it Takes Over the Final ImageNet Competition," *Forbes*, July 31, 2017, https://www.forbes.com/sites/aarontilley/2017/07/31/china-ai-imagenet/#1c1419b9170a.

[99] Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, November 28, 2017, https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235804, pp. 12-14.

[100] Ibid., p. 13.

[101] Ibid., p. 23.

[102] Ibid., p. 27.

[103] CRS discussion with Dr. Richard Linderman.

[104] Kania, 28.

qualms about developing LAWS. While U.S. literature on the subject is dominated by discussions of legal and ethical implications, there have been few publications on this topic in China.[105]

In addition to differences in the military approach to AI, China's management of AI acquisition for the military is distinct.[106] In general, few boundaries exist between Chinese commercial companies, university research laboratories, the military, and the central government. As a result, the Chinese government has a direct means of guiding AI development priorities. To this end, the Chinese government created a Military-Civil Fusion Development Commission in 2017, which is intended to speed the transfer of AI technology from commercial companies and research institutions to the military.[107] The Chinese government is also leveraging lower barriers to data collection to create large databases that will train AI systems.[108] According to one estimate, China is on track to possess 20% of the world's share of data by 2020, with the potential to have over 30% by 2030.[109]

China's centrally-directed effort is also fueling speculation in the U.S. AI market, where China is investing in the same companies that the U.S. military is working with, and often in advance of U.S. investors.[110] **Figure 4** below depicts Chinese venture capital investment in U.S. AI companies between 2010 and 2017, an effort adding up to $1.3 billion. Notably, in March 2017 the U.S. Air Force expressed an interest in AI software being developed by Neurala, a Boston-based start-up. However, before the Air Force returned with an offer, Haiyin Capital, a state-run Chinese company, edged them out, investing a large, undisclosed sum.[111]

[105] Ibid.

[106] Kania, p. 6.

[107] Yujia He, "How China is Preparing for an AI-Powered Future," The Wilson Center, June 20, 2017, https://www.scribd.com/document/352605730/How-China-is-Preparing-for-an-AI-Powered-Future#from_embed., and Kania, p. 19.

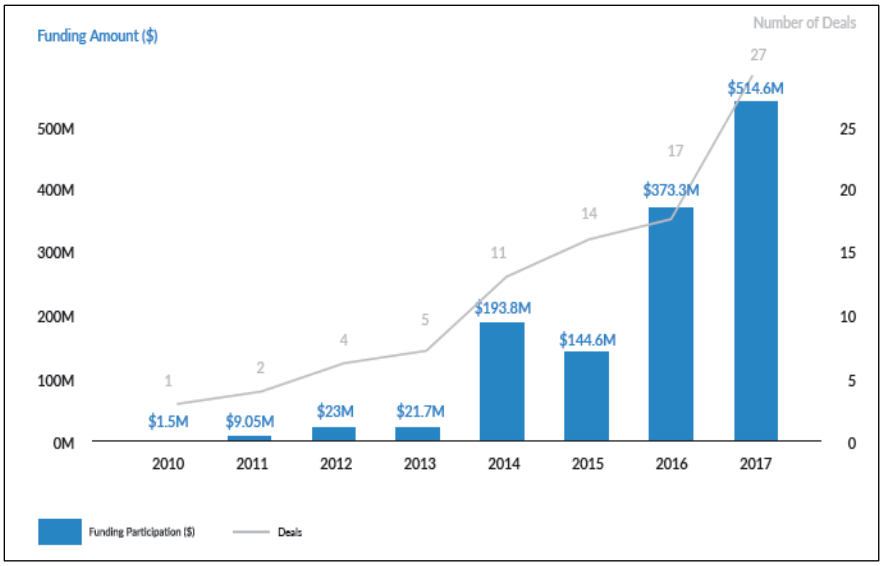
[108] Will Knight, "China's AI Awakening," *MIT Technology Review*, October 10, 2017, https://www.technologyreview.com/s/609038/chinas-ai-awakening.

[109] Kania, p. 12.

[110] Paul Mozur and John Markoff, "Is China Outsmarting America in AI?," *The New York Times*, May 27, 2017, https://www.nytimes.com/2017/05/27/technology/china-us-artificial-intelligence.html.

[111] Paul Mozur and Jane Perlez, "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon," *The New York Times*, March 22, 2017, https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html.

Figure 4. Chinese Investment in U.S. AI Companies, 2010-2017



Source: Michael Brown and Pavneet Singh, China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation, Defense Innovation Unit Experimental, January 2018, https://www.diux.mil/download/datasets/1758/DIUx%20Study%20on%20China's%20Technology%20Transfer%20Strategy%20-%20Jan%202018.pdf, p. 29.

Analysts are particularly concerned about Chinese investment in U.S. graphics processing units, which are a specialized micro-chip critical for running AI software. U.S. companies currently manufacture more capable versions of this hardware component, and China's focus on acquiring these chips may demonstrate an effort to reach parity with the United States.[112] China's history of industrial espionage is also cause for concern of illicit AI technology transfer.[113]

While most analysts view China's unified effort to develop AI as a unique advantage over the United States, many contend that its AI strategy is not perfect. For example, some analysts characterize the Chinese government's funding management as inefficient. They point out that the system is often corrupt, with favored research institutions receiving a disproportionate share of government funding, and that the government has a potential to overinvest in projects that produce surpluses that exceed market demand.[114]

In addition, China is experiencing a deficit of engineers and researchers trained to develop AI algorithms. The top half of data scientists in the United States have been working in the field for over 10 years, while the same proportion of Chinese developers have less than 5 years of experience on average. Furthermore, only 30 Chinese universities produce indigenous experts and research products.[115] Although the Chinese surpassed the United States in the quantity of research papers produced from 2011 to 2015, the quality of their published papers ranked 34th globally.[116]

[112] Patrick Tucker, "China and CIA are Competing to Fund Silicon Valley's AI Startups," *Defense One*, November 13, 2017, http://www.defenseone.com/technology/2017/11/china-and-cia-are-competing-fund-silicon-valleys-ai-startups/142508/?oref=d-mostread.

[113] Kania, p. 40.

[114] He, p. 13.

[115] Dominic Barton and Jonathan Woetzel, "Artificial Intelligence: Implications for China," McKinsey Global Institute, April 2017, https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx, (continued...)

Some experts believe that China's intent to be first may result in comparatively less safe AI applications, with a large amount of systemic risk built into its military AI tools. Such experts assert that a prudent pace of AI development in the United States may result in more capable systems in the long run, further stating that it would be unethical for the military to sacrifice safety standards for the sake of external pressure to move faster.[117] The director of IARPA, Dr. Jason Matheny, commented that China's centralized push for AI may result in a big win, but it may also cause them to fail big with a headlong rush into poorly conceptualized AI applications.[118]

Russia

Judging by nascent AI technology developments and public policy statements, Russia may be another potentially serious rival in the pursuit of military AI applications. Although total Russian investment in AI lags behind the United States and China, Russia is initiating plans to close the gap. As part of a broader defense modernization effort that began in 2008, the Russian Military Industrial Committee set a goal for 30% of military equipment to be robotic by 2025.[119]

In 2016, the Russian government created a defense research organization, roughly equivalent to DARPA, dedicated to autonomy and robotics called the Foundation for Advanced Studies, and initiated an annual conference on "Robotization of the Armed Forces of the Russian Federation."[120] Russia ranks fourth in the world for users of Kaggle, an open-source AI research platform, and Russian venture capitalists are actively seeking opportunities in the AI market abroad, indicating that there may be a united effort in Russia to pursue AI technology.[121]

The Russian military is researching a number of defense applications for AI, with a heavy emphasis on autonomous vehicles and robotics. In an official statement on November 1, 2017, Viktor Bondarev, chairman of the Federation Council's Defense and Security Committee, asserted that "artificial intelligence will be able to replace a soldier on the battlefield and a pilot in an aircraft cockpit," and he later announced that "the day is nearing when vehicles will get artificial intelligence."[122] Bondarev made these remarks in close proximity to the successful test of Nerehta, an unmanned ground system. The modular vehicle, which reportedly "outperformed existing manned combat vehicles" during the test, is capable of carrying a 7.62mm machine gun and may be used in combat, intelligence gathering, or logistics roles. The Russian military plans to use the Nerehta as a research and development platform for AI, potentially incorporating an

(...continued)

p. 8.

[116] Simon Baker, "Which Countries and Universities are Leading on AI Research?" *Times Higher Education, World University Rankings*, May 22, 2017, https://www.timeshighereducation.com/data-bites/which-countries-and-universities-are-leading-ai-research.

[117] Dr. Caitlin Surakitbanharn, Comments at AI and Global Security Summit, Washington, DC, November 1, 2017.

[118] CRS discussion with Dr. Jason Matheny.

[119] Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race."

[120] Samuel Bendett, "Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems," *The Strategy Bridge*, December 12, 2017, https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-the-rapid-development-of-russian-unmanned-military-systems.

[121] Leon Bershidsky, "Take Elon Musk Seriously on the Russian AI Threat," *Bloomberg*, September 5, 2017, https://www.bloomberg.com/view/articles/2017-09-05/take-elon-musk-seriously-on-the-russian-ai-threat.

[122] Samuel Bendett, "Should the US Army Fear Russia's Killer Robots?," *The National Interest*, November 8, 2017, http://nationalinterest.org/blog/the-buzz/should-the-us-army-fear-russias-killer-robots-23098.

autonomous target identification capability.[123] Kalashnikov, a Russian defense company, built a similar unmanned ground vehicle in 2016 called the Soratnik and plans to unveil a suite of autonomous systems infused with machine learning algorithms.[124]

These developments have aroused concerns that Russia may be pursuing Lethal Autonomous Weapon Systems (LAWS). Analysts also note that the Russian military is exploring a diverse set of autonomous vehicle concepts, including "tank-sized devices," while U.S. Army investments to date have focused on smaller vehicles almost exclusively for support functions.[125] Similar to the U.S. military, the Russian military plans to incorporate AI into unmanned aerial vehicles, naval vessels, and unmanned undersea vehicles, to include swarming capability.[126] In addition, some analysts believe that the Russian military is likely researching AI applications for espionage and propaganda. Analysts speculate that Russia may be investigating tools similar to those built by U.S. researchers that are capable of high-fidelity video and audio spoofing based on a small sample size of original source material. These sophisticated products are difficult to detect without a comparable AI tool. [127]

Despite Russia's aspirations, analysts argue that it may be difficult for Russia to put any significant investment into these programs. The Russian defense budget for 2017 dropped by 7%, with subsequent cuts of 3.2% and 4.8% forecast for 2018 and 2019, respectively.[128]

Some analysts point out that the Russian tech industry is not sophisticated enough to produce AI applications on par with the United States or China. Only one Russian made it on to IBM's recent list of global "AI Influencers," and the AI tools produced by Russian startups are generally inferior to developments by comparable companies in the United States and China.[129] Critics of this position counter that Russia was never a leader in internet technology, but that has not stopped it from becoming a substantially disruptive force in cyberspace.[130]

In addition, the Russian position on LAWS seems to be inconsistent. Although the Russian research agenda may indicate an emphasis on autonomous weapons systems, individuals inside the Russian military establishment and leaders of the defense industry have expressed reservations about trusting AI systems for battlefield decision-making.[131] Nevertheless, Russia may be able to overcome its weaknesses and preserve a unique advantage in global military AI technology if it is the first to aggressively pursue LAWS.[132]

---

[123] Patrick Tucker, "Russia Says It Will Field a Robot Tank that Outperforms Humans," *Defense One*, November 8, 2017, http://www.defenseone.com/technology/2017/11/russia-robot-tank-outperforms-humans.

[124] Tristan Greene, "Russia is Developing AI Missiles to Dominate the New Arms Race," *The Next Web*, July 27, 2017, https://thenextweb.com/artificial-intelligence/2017/07/27/russia-is-developing-ai-missiles-to-dominate-the-new-arms-race/.

[125] Sydney J. Feedberg, "Armed Robots: US Lags Rhetoric, Russia," *Breaking Defense*, October 18, 2017, https://breakingdefense.com/2017/10/armed-robots-us-lags-rhetoric-russia/.

[126] Bendett, "Red Robot Rising."

[127] Gregory C. Allen, "Putin and Musk Are Right: Whoever Masters AI Will Run the World," *CNN*, September 5, 2017, http://www.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html.

[128] Michael Kofman, "The Russian Defense Budget and You," *Russia Matters*, March 17, 2017, https://www.russiamatters.org/analysis/russian-defense-budget-and-you.

[129] Bershidsky, "Take Elon Musk Seriously."

[130] Allen, "Putin and Musk Are Right."

[131] Samuel Bendett, "Get Ready, NATO: Russia's New Killer Robots Are Nearly Ready for War," *The National Interest*, November 8, 2017, http://nationinterest.org/blog/the-buzz/russias-new-killer-robots-are-nearly-ready-war-19698.

[132] Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race."

International Institutions

A number of international institutions have examined issues surrounding AI, including the Group of Seven (G7), the Organization for Economic Cooperation and Development, and the Asia-Pacific Economic Cooperation. The United Nations (UN), however, has made the most concerted effort to consider AI in the military context, with most of its attention being devoted to Lethal Autonomous Weapon Systems (LAWS) under the auspices of the Convention on Certain Conventional Weapons (CCW). In general, the CCW is charged with "banning or restricting the use of specific types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilian populations," and it currently adjudicates issues involving weapons such as mines, cluster munitions, and blinding lasers.[133] The CCW began LAWS discussions in 2014 with informal "Meetings of Experts" held annually.[134] In parallel, the International Committee of the Red Cross (ICRC) held similar gatherings of interdisciplinary experts on LAWS, which produced reports for the CCW on technical, legal, moral, and humanitarian issues.[135] During the CCW's April 2016 meeting, the attendees resolved to establish a Group of Governmental Experts (GGE), with an official mandate to "assess questions related to emerging technologies in the area of LAWS."[136]

The first meeting of the GGE convened in November 2017, with the intent to "focus on framing devices such as definitions and other concepts with the potential of narrowing the line of sight to policy pathways."[137] However, the meeting did not result in any official conclusions or policy documents, and one observer described the event as a "chaotic and ultimately inconsequential discussion of AI generally."[138]

Potentially clarifying their position on LAWS, the Russian delegation to the GGE announced that they would not abide by an international ban on the technology. In a paper submitted to the committee, they explained that defining the technology is overly complex and stipulated that "it is hardly acceptable for the work on LAWS to restrict the freedom to enjoy the benefits of autonomous technologies being the future of humankind."[139] Of note, although China sent a delegation to the event, it did not submit a statement for the record and its participation did not generate any substantial press coverage.

---

[133] "The Convention on Certain Conventional Weapons," https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument.

[134] "Background on Lethal Autonomous Weapons Systems in the CCW," https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument.

[135] See "Autonomous Weapons Systems: Technical, Military, Legal, and Humanitarian Aspects," Expert Meeting, International Committee of the Red Cross, March 28, 2014, https://www.icrc.org/en/download/file/1707/4221-002-autonomous-weapons-systems-full-report.pdf, and "Autonomous Weapons Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons," Expert Meeting, International Committee of the Red Cross, March 16, 2016, https://www.icrc.org/en/download/file/21606/ccw-autonomous-weapons-icrc-april-2016.pdf.

[136] "Background on LAWS in the CCW."

[137] Amandeep Singh Gill, "Food for Thought Paper Submitted by the Chairperson," CCW Group of Governmental Experts on LAWS, September 4, 2017, http://undocs.org/ccw/gge.1/2017/WP.1.

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

[139] "Examination of Various Dimensions of Emerging Technologies in the Area of LAWS, in the Context of the Objectives and Purposes of the Convention," Position Paper Submitted by the Russian Federation to the GGE on LAWS, November 10, 2017, https://www.unog.ch/80256EDD006B8954/(httpAssets)/2C67D752B299E6A7C12581D400661C98/$file/2017_GGEonLAWS_WP8_RussianFederation.pdf.

One U.S. participant lamented the fact that the UN could not agree on a definition for LAWS after four years of debate, while also admitting that the CCW is the best international forum to address the issue in the future. He also cautioned that the international community is in danger of "the pace of diplomacy falling behind the speed of technological advancement."[140] Some analysts are concerned that international discussions of military AI applications are occurring primarily in the arms control context, which naturally leads to debate at the extremes of "arms races" and "bans."[141] In the future, Congress may seek to influence CCW engagements, while also encouraging more broad-based international discussions on military AI in other venues.

AI Opportunities and Challenges

Regardless of the country wielding the technology, AI introduces a number of unique opportunities and challenges in the combat environment that are meaningfully different from existing military systems. The AI characteristics discussed in this section are generally the same in other environments, but there are some unique issues in the defense context. Ultimately, the technology's impact in the defense and national security sector will be determined by the extent to which developers, with the assistance of policymakers, are able to maximize strengths while finding work-arounds and policy options to limit vulnerabilities.

Autonomy

AI is the primary driver of autonomous systems, which are often cited as the technology's chief advantage for the military. Autonomy, fueled by AI, was a central focus of the Obama Administration's "Third Offset Strategy," a framework for preserving the U.S. military's technological edge versus global competitors.[142] Depending on the task, autonomous systems are capable of augmenting or replacing humans, freeing them up for more complex and cognitively demanding work. In general, experts assert that the military stands to gain significant benefit from autonomous systems by replacing humans in tasks that are "dull, dangerous, or dirty."[143]

Specific examples include autonomous systems that conduct long-duration intelligence collection and analysis, robotic systems that clean up environments contaminated by chemical weapons, and unmanned systems that sweep a route for improvised explosive devices.[144] In these capacities, autonomous systems may reduce risk to warfighters and reduce costs by taking on labor-intensive tasks.[145] Many analysts argue these advantages create a "tactical and strategic necessity," as well as a "moral obligation" to pursue autonomous systems.[146]

---

[140] Paul Scharre, "We're Losing Our Chance to Regulate Killer Robots," *Defense One*, November 14, 2017, http://www.defenseone.com/ideas/2017/11/were-losing-our-chance-regulate-killer-robots/142517/.

[141] Dr. Rebecca Crootof, Comments at AI and Global Security Summit, Washington, DC, November 1, 2017.

[142] For more information on the Third Offset Strategy, see CRS In Focus IF10790, *What Next for the Third Offset Strategy?*, by Lisa A. Aronsson.

[143] Mick Ryan, "Integrating Humans and Machines," *The Strategy Bridge*, January 2, 2018, https://thestrategybridge.org/the-bridge/2018/1/2/integrating-humans-and-machines.

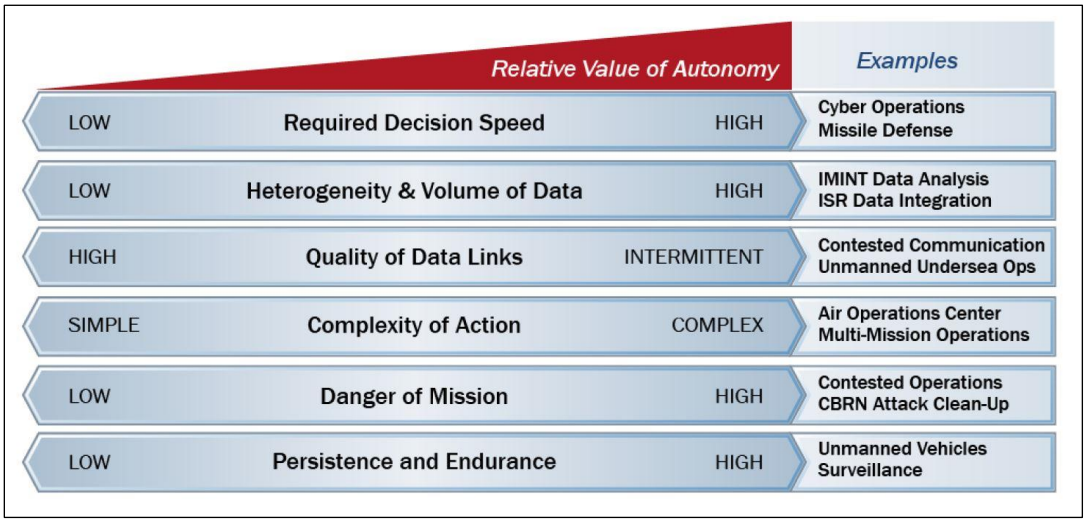
[144] Defense Science Board, "Summer Study on Autonomy," June 9, 2016, https://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf, p. 12.

[145] Office of Technical Intelligence, Office of the Assistant Secretary of Defense for Research and Engineering, "Technical Assessment: Autonomy," February 2015, http://www.defenseinnovationmarketplace.mil/resources/OTI_TechnicalAssessment-AutonomyPublicRelease_vF.pdf, p. 4.

[146] Mick Ryan, "Building a Future: Integrating Human-Machine Military Organization," *The Strategy Bridge*, December 11, 2017, https://thestrategybridge.org/the-bridge/2017/12/11/building-a-future-integrated-human-machine-

(continued...)

Figure 5. Value of Autonomy to DOD Missions



Source: Defense Science Board, "Summer Study on Autonomy," June 9, 2016, https://www.acq.osd.mil/dsb/reports/2010s/DSBSS15.pdf, p. 12.

Autonomy Concepts and Definitions

Much like other terms in the field of AI, there is no general consensus on a definition for autonomy. However, most sources do not view autonomy as an all-or-nothing proposition and specify levels of autonomy based on the amount of human control over the system. These distinctions are significant, because one of the more contentious debates in the field of military AI centers on characterizing "meaningful human control" and determining how much oversight is appropriate for each type of AI application. The following chart is adapted from definitions found in DOD Directive 3000.09, "Autonomy in Weapon Systems."

Semi-Autonomous	Human-Supervised	Autonomous
Human ***in*** the Loop	Human ***on*** the Loop	Human ***out*** of the Loop
The machine stops and waits for human approval before continuing after each task is accomplished.	Once activated, the machine performs a task under human supervision, and will continue performing the task until the operator intervenes.	Once activated, the machine performs its task without any assistance on the part of the human operator, who neither supervises the operation nor has an ability to intervene.

Source: Illachinski, "AI, Robots, and Swarms: Issues, Questions, and Recommended Studies," pp. 146-151.

A common academic autonomy matrix is illustrated below. This is a standard reference point that may be useful in the military context, and variations of this system have been developed for numerous applications, including a Department of Transportation adaptation for vehicle

(...continued)

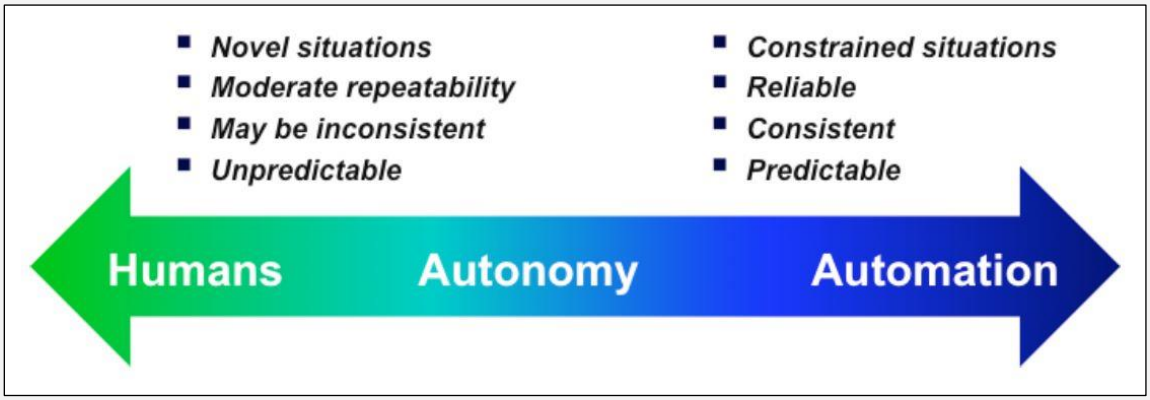
military-organization, and CRS discussion with Paul Scharre.

autonomy. It is more granular than the DOD treatment, organized around a 10-point scale, with higher numbers corresponding to more autonomy.[147]

- **Level 1**—computer offers no assistance, humans make all decisions and take all actions
- **Level 2**—computer offers a complete set of alternatives
- **Level 3**—computer narrows the selection down to a few choices
- **Level 4**—computer suggests one action
- **Level 5**—computer executes that action if the human operator approves
- **Level 6**—computer allows the human a restricted time to veto before automatic execution
- **Level 7**—computer executes automatically then informs the human
- **Level 8**—computer informs human after execution only if asked
- **Level 9**—computer informs human after execution only if it decides to
- **Level 10**—computer decides everything and acts fully autonomously

Discussions of the measure of autonomy feed philosophical debates about the kinds of tasks with which humans and AI systems ought to be trusted, based on characterizing their cognitive advantages. **Figure 6** contrasts the relative strengths of humans versus automated systems, with autonomous systems existing somewhere in between.

Figure 6. Human vs. Machine Decision-making



Source: U.S. Air Force, Office of the Chief Scientist, "Autonomous Horizons, System Autonomy in the Air Force–A Path to the Future, Volume 1," June 1, 2015, p. 5.

Speed

AI introduces a unique means to work at the extremes of the time scale in combat, with an ability to react at gigahertz speed as well as powering systems to accomplish long-duration tasks that exceed human endurance.[148] At the fast end of the spectrum, automated missile defense systems like the Terminal High Altitude Area Defense (THAAD) and the Patriot system have already demonstrated the value and necessity of quick reaction times. AI will infuse systems with a

[147] Ilachinski, p. 152.

[148] Office of Technical Intelligence, "Technical Assessment: Autonomy," p. 6.

similar ability to react at machine speed, potentially boosting the overall pace of combat if deployed simultaneously in numerous military systems.[149]

This technology may enhance response times to other developing technologies that challenge human reaction times (e.g., hypersonic weapons, directed energy systems, and massive, coordinated cyberattacks). AI systems have the potential to provide additional increases to the speed of warfare in command and control applications. AI systems may provide decisionmakers with the ability to quickly assimilate large volumes of data and suggest actions faster than current command and control tools. In this role, AI would facilitate rapid reactions to an adversary, possibly outpacing the opponent's ability to understand the environment and respond in kind if the opponent is relying solely on human judgment.

Although AI may not always suggest better decisions than human beings, experts argue that militaries that use AI at scale to make acceptable decisions may gain a significant advantage over adversaries who choose not to adopt AI. [150] As discussed below, critics contend that a drastic increase to the speed of combat is not an objectively positive development, and it may lead to an environment where machines are operating at a pace that defies a human being's ability to understand or control events. At the other end of the spectrum, AI systems may provide benefits in long-duration tasks. For example, AI systems may enable intelligence systems that stare at large areas, analyze activity over long periods of time, and detect anomalies or broadly characterize behavior.[151]

Scaling

AI has the potential to provide a force-multiplying effect by enhancing the capabilities of human soldiers and infusing less expensive military systems with increased capability. The productivity of individual military members may increase as AI systems take over routine tasks or empower soldiers to control fleets of AI systems programmed to cooperatively accomplish a complex task with minimal human direction.[152]

Although individually a low-cost drone may be powerless against a high-tech tool like an F-35 stealth fighter, a fleet of hundreds of such drones with an AI-enabled swarming algorithm is likely to overwhelm these comparatively expensive military systems. AI applications may even render some current platforms obsolete.[153] Others caution that AI systems may decouple military power from population size and economic strength. As the technology proliferates to smaller countries and nonstate actors, AI may allow them to have a disproportionately large impact on the battlefield if they are able to capitalize on these scaling effects.[154]

[149] Allen and Chan, p. 24.

[150] "Highlighting Artificial Intelligence: An Interview with Paul Scharre," *Strategic Studies Quarterly*, Vol. 11, Issue 4, November 28, 2017, pp. 18-19.

[151] Office of Technical Intelligence, "Technical Assessment: Autonomy," p. 6.

[152] Ronald C. Arklin, "A Roboticist's Perspective on Lethal Autonomous Weapons Systems," *Perspectives on Lethal Autonomous Weapon Systems*, United Nations Office for Disarmament Affairs, Occasional Papers, No. 30, November 2017, p. 36.

[153] Ryan, "Building a Future: Integrated Human-Machine Military Organization."

[154] Allen and Chan, p. 23.

Information Superiority

AI may offer a means to cope with an explosion in the amount of data available for analysis. According to one DOD source, the military operates over 11,000 drones, with each one recording "more than three NFL seasons" of high-definition footage each day.[155] However, the department does not have sufficient people or an adequate system to comb through all of this data to derive useful and timely intelligence analysis. This issue will likely be exacerbated in the future as data continues to accumulate.

According to one study, by 2020 every human on the planet will generate 1.7 megabytes of information every second, growing the global pool of data from 4.4 zettabytes today to almost 44.0 zettabytes.[156] AI-powered intelligence systems may significantly improve intelligence analysis, sorting through these massive troves of data to highlight useful information.[157] AI systems may integrate information from different sources and geographic locations to draw conclusions that may not have otherwise been obvious to human intelligence analysts observing a singular system.[158]

In addition, AI algorithms may generate their own data to feed further analysis, accomplishing tasks like converting unstructured information from polls, financial data, and election results into written reports. AI tools of this type provide potential value because they draw out useful information that would otherwise be elusive, and this potentially superior quality of information may consequently lead to better wartime decision-making.[159]

Predictability

Perhaps an ambiguous trait of the technology, AI algorithms often produce unpredictable results. In March 2016, the AI company DeepMind created a game-playing algorithm called AlphaGo, which defeated a world-champion Go player, Lee Sedol, four games to one. After the match, Sedol commented that AlphaGo made surprising and innovative moves, and other expert Go players subsequently stated that AlphaGo overturned accumulated wisdom on game play. Furthermore, experts did not believe that an AI system would be capable of defeating a human at this complex game for another 10 years.[160] AI's capacity to produce similar unconventional results in military systems may be an advantage in combat, especially if those results surprise an adversary.

However, AI systems also fail in unexpected ways, with some analysts characterizing the technology as "brittle and inflexible."[161] Dr. Arati Prabhakar, the former DARPA Director,

---

[155] Jon Harper, "Artificial Intelligence to Sort Through ISR Data Glut," *National Defense*, January 16, 2018, http://www.nationaldefensemagazine.org/articles/2018/1/16/artificial-intelligence-to—sort-through-isr-data-glut?utm_source=RC+Defense+Morning+Recon&utm_campaign=116224eefb-EMAIL_CAMPAIGN_2018_01_16&utm_medium=email&utm_term=0_694f73a8dc-116224eefb-85612893.

[156] Bernard Marr, "Big Data: 20 Mind-Boggling Facts Everyone Must Read," *Forbes*, September 30, 2015, https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#539121d317b1. For reference 1 zettabyte = 1 trillion gigabytes.

[157] Allen and Chan, p. 27.

[158] Ilachinski, p. 140.

[159] Allen and Chan, p. 32.

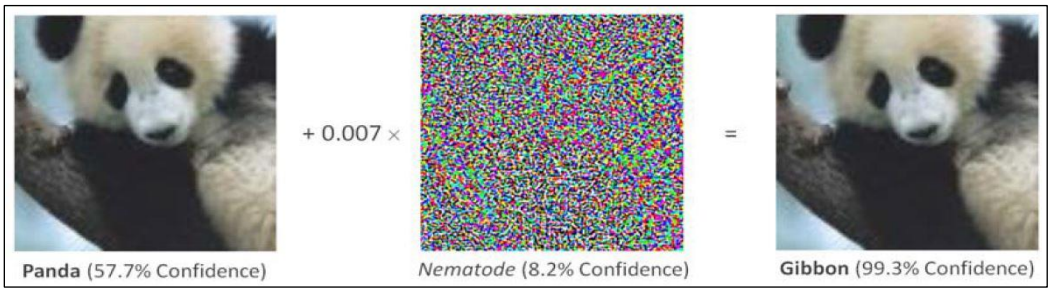
[160] Cade Metz, "In Two Moves, AlphaGo and Lee Sedol Redefined the Future," *Wired*, March 16, 2016, https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/.

[161] Paul Scharre, "A Security Perspective: Security Concerns and Possible Arms Control Approaches," *Perspectives on Lethal Autonomous Weapon Systems*, United Nations Office for Disarmament Affairs, Occasional Papers, No. 30, (continued...)

commented, "When we look at what's happening with AI, we see something that is very powerful, but we also see a technology that is still quite fundamentally limited ... the problem is that when it's wrong, it's wrong in ways that no human would ever be wrong."[162]

AI-based image recognition algorithms surpassed human performance in 2010, most recently achieving an error rate of 2.5% in contrast to the average human error rate of 5%, but some commonly cited experiments with these systems demonstrate their capacity for failure.[163] As illustrated in **Figure 7**, researchers combined a picture that the system correctly identified as a panda with some random distortion that the computer labeled "nematode." The difference in the combined image is imperceptible to human eyes, but the AI system confidently labeled it as a picture of a gibbon.

Figure 7. AI and Image Classifying Errors



Source: Andrew Ilachinski, *AI, Robots, and Swarms, Issues Questions, and Recommended Studies*, Center for Naval Analysis, January 2017, p. 61.

(...continued)

November 2017, p. 24.

[162] Quoted in Mark Pomerlau, "DARPA Director Clear-Eyed and Cautious on AI," *Government Computer News*, May 10, 2016, https://gcn.com/articles/2016/05/10/darpa-ai.aspx.

[163] AI Index, "2017 Annual AI Index Report," November 2017, http://cdn.aiindex.org/2017-report.pdf, p. 26.

In another experiment, an AI system described the picture in **Figure 8** "a young boy is holding a baseball bat," demonstrating the algorithm's inability to understand context. Other experts warn that AI may be operating with different assumptions about the environment than human operators, with little awareness of when the system is outside the boundaries of its original design.[164]

Figure 8. AI and Context

"A Young Boy is Holding a Baseball Bat"

Source: John Launchbury, "A DARPA Perspective on Artificial Intelligence," https://www.darpa.mil/attachments/AIFull.pdf, p. 23.

To further demonstrate the point, developers created an AI system to recognize and understand online text, and they trained it primarily on formal documents like Wikipedia articles. It was later unable to interpret more informal language in Twitter posts.[165] This sensitivity to the training data set is particularly concerning in the military context because it may cause issues with "domain adaptability," which refers to an AI system's capacity to adjust between two settings that are not precisely the same. This is a task humans accomplish routinely, and it would be a necessity for military AI given the unpredictable nature of the combat environment.[166]

Such unpredictable failures of AI systems may create a significant risk if the systems are deployed at scale. One analyst points out that although humans are not immune from errors, their mistakes are typically made on an individual basis and they are different every time. However, AI systems have the potential to fail simultaneously and in the same way.[167] There may be additional surprises in store as U.S. AI systems face adversary AI systems, with the potential for differing cultural biases inherent in the training data sets to produce unpredictable results when they interact with one another.[168]

Analysts warn that if military units rush to field the technology prior to gaining a comprehensive understanding of this phenomena, they may incur a "technical debt," a term that refers to the effect of fielding AI systems that have minimal risk individually but increase the danger of catastrophe as their collective hazard is compounded by each new addition to the inventory.[169] This situation may be further exacerbated if nations engage in an AI arms race.[170]

[164] Defense Science Board, "Summer Study on Autonomy," p. 14.

[165] Aaron M. Bornstein, "Is Artificial Intelligence Permanently Inscrutable?," *Nautilus*, September 1, 2016, http://nautil.us/issue/40/learning/is-artificial-intelligence-permanently-inscrutable.

[166] Paul Scharre, "The Lethal Autonomous Weapons Governmental Meeting, Part 1: Coping with Rapid Technological Change," *Just Security*, November 9, 2017, https://www.justsecurity.org/46889/lethal-autonomous-weapons-governmental-meeting-part-i-coping-rapid-technological-change/.

[167] Paul Scharre, *Autonomous Weapons and Operational Risk*, Center for a New American Security, February 2016, p. 23.

[168] Kania, p. 53.

[169] The Mitre Corporation, "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD," Office of the Assistant Secretary of Defense for Research and Engineering, January 2017, p. 32.

[170] Dr. Dario Amodei, Comments at AI and Global Security Summit, Washington, DC, November 1, 2017.

Explainability

Further complicating issues of predictability, many AI systems produce results with no explanation of the path the system took to derive the solution. Experts in the AI field refer to this trait as *explainability*. For example, Google created an early AI system to identify cats. The algorithm achieved impressive results combing through thousands of YouTube videos to correctly find cats, but none of the developers were able to discern which traits of a cat the system used to make this judgment.[171]

The types of AI algorithms that have the highest performance are also the least explainable at the moment. DARPA is in the midst of a five-year research effort to produce explainable AI tools, and other research organizations are attempting to do a backwards analysis of AI algorithms to gain a better understanding of how they work.[172]

In one such study, researchers analyzed a program designed to identify curtains, and they discovered that the AI algorithm first looked for a bed and not a window, at which point it stopped searching the image. They later discovered that most of the images in the training data set with curtains were also bedrooms.[173] This project demonstrated the significant dissimilarity between AI and human reasoning in addition to uncovering an otherwise transparent vulnerability in the algorithm.

Explainability creates issues in the military context as humans and AI team up to accomplish a mission, because the opacity of AI reasoning may cause an operator to have either too much or too little confidence in system performance. Some analysts are particularly concerned that humans may be averse to making a decision based entirely on AI analysis if they do not understand how the machine derived the solution. Dawn Meyerriecks, Deputy Director for Science and Technology at the CIA, expressed concerns about convincing national decisionmakers to trust AI judgments, arguing, "Until AI can show me its homework, it's not a decision quality product."[174]

At the opposite end of the spectrum, the Tesla Model 3 crash on January 22, 2018, provides an illustration of potential over-trust. The vehicle impacted a parked fire-truck at 65 miles per hour with the auto-pilot engaged, in large part because the driver believed the system was performing within design limitations and did not intervene.[175] Although the Tesla is automated and not necessarily an AI system, this accident may be a harbinger of things to come as humans develop too much trust in systems of this type. Additional human-machine interaction issues that may be challenged by insufficient explainability in the military context include the following:

- **Goal Alignment.** The human and the machine must have a common understanding of the objective. As military systems encounter a dynamic

[171] John Markoff, "How Many Computers to Identify a Cat? 16,000." *The New York Times*, June 25, 2012, http://www.nytimes.com/2012/06/26/technology/in-a-big-network-of-computers-evidence-of-machine-learning.html.

[172] David Gunning, "Explainable AI Program Description," November 4, 2017, https://www.darpa.mil/attachments/XAIIndustryDay_Final.pptx.

[173] Bornstein, "Is Artificial Intelligence Permanently Inscrutable?"

[174] Dawn Meyerriecks, Comments at the Machine Learning and Artificial Intelligence Workshop, National Geospatial Intelligence Agency, November 13, 2017.

[175] Cleve R. Wootson Jr., "Feds Investigating after a Tesla on Autopilot Barreled into a Parked Firetruck," *The Washington Post*, January 24, 2018, https://www.washingtonpost.com/news/innovations/wp/2018/01/23/a-tesla-owners-excuse-for-his-dui-crash-the-car-was-driving/?utm_term=.fccbe73eaebd.

environment, the goals will change, and the human and the machine must adjust simultaneously based on a shared picture of the current environment.[176]

- **Task Alignment.** Humans and machines must understand the boundaries of one another's decision space, especially as goals change. In this process, humans must be consummately aware of the machine's design limitations to guard against inappropriate trust in the system.[177]
- **Human Machine Interface.** Due to the requirement for timely decisions in many military AI applications, traditional machine interfaces like a mouse click may slow down performance, but there must be a way for the human and machine to coordinate in real time in order to build trust. A machine interface will build appropriate human trust as feedback on the machine decision-making process increases.[178]

Increasing explainability will be key to humans calibrating the preceding factors and building appropriate levels of trust in AI systems. In some cases, humans may sacrifice mission effectiveness if they intervene too soon. However, too much trust may cause a loss of the human's situational awareness, which will create a lag in response time and allow damage to accrue as the failure persists.[179] A U.S Army study of this issue concludes, only "prudent trust" will confer a competitive advantage for military organizations.[180]

Explainability and predictability challenge the military's ability to "verify and validate" AI system performance prior to fielding. Conventional methods of verification and validation are based on the assumption that tested performance will indicate future behavior. However, most AI systems exhibit "emergent behavior," adjusting their internal algorithm as they encounter new stimuli.[181] In most military applications this is a positive attribute, as it would allow AI systems to adapt to a complex environment. However, it challenges the current DOD guidance, which stipulates that autonomous and semi-autonomous systems must "go through rigorous hardware and software verification and validation" to ensure the system will "function as anticipated in realistic operational environments against adaptive adversaries."[182] It may be unreasonable to expect the military to anticipate all of the realistic operational environments or adversary reactions that an AI system might encounter.[183]

Finally, due to their current lack of an explainable output, AI systems do not have an audit trail for the military test community to certify that a system is meeting performance standards.[184] DOD is currently developing a framework to test AI system lifecycles and building methods for testing AI systems in diverse environments with complex human-machine interactions.[185]

---

[176] U.S. Air Force, Office of the Chief Scientist, "Autonomous Horizons, System Autonomy in the Air Force," p. 17.

[177] Ibid.

[178] Ilachinski, p. 187.

[179] Sharre, *Autonomous Weapons and Operational Risk*, pp. 10-11.

[180] Eric Van Den Bosch, "Human Machine Decision Making and Trust," in *Closer than You Think: The Implications of the Third Offset Strategy for the US Army* (Carlisle, PA: US Army War College Press, 2017), p.111.

[181] Ilachinski, pp. 202-204.

[182] *DOD Directive 3000.09*, p. 6.

[183] Ilachinski, p. 204.

[184] DSB Study on Autonomy, pp. 14-15.

[185] Ilachinski, p. 204.

AI Exploitation

AI systems present unique pathways for adversary exploitation. First, the proliferation of AI systems will likely grow the inventory of "hackable things," including systems that carry kinetic energy (e.g., moving vehicles), which may allow cyberattacks to have a lethal effect. An adversary may be capable of an outsized impact if an entire class of AI systems all have the same vulnerability.[186]

Figure 9. Adversarial Images

Source: Evan Ackerman, "Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms," IEEE Spectrum, August 4, 2017, https://spectrum.ieee.org/cars-that-think/transportation/sensors/slight-street-sign-modifications-can-fool-machine-learning-algorithms.

In addition, AI systems, much like other cyberspace applications, are more vulnerable to theft by virtue of being almost entirely software-based. As one analyst points out, the Chinese may be able to steal the plans for an F-35, but it will take them years to find the materials and develop the manufacturing processes to build one. However, stealing software code effectively equips the adversary with that tool immediately, and it can then be reproduced at will.[187] This vulnerability is especially concerning because of the dual-use nature of the technology and the fact that the AI research community has been relatively open to collaboration up to this point, with many variants of AI code shared on unclassified internet sites.

Finally, adversaries may be capable of deliberately inducing the kinds of image classification errors discussed in the predictability section above. In one such case, researchers who had access to the training data set and the algorithm for an image classifier on a self-driving vehicle used several pieces of strategically placed tape, as illustrated in **Figure 9**, to cause the system to identify a stop sign as a speed limit sign. In a later research effort, a team at MIT, operating under "black box conditions" with no access to the training data or algorithm, tricked an image classifier into thinking that a picture of machine guns was a helicopter. The researchers point out that the label swap in this case was arbitrary, and they could have just as easily changed the label for an object of military interest, like a tank, into something benign, like an antelope.[188] These vulnerabilities increase the imperative for cybersecurity to be a primary consideration as the military develops AI tools and plans for storing training data sets. Going ahead, DOD may want to train human operators to be on guard for this type of attack, approaching AI solutions with an appropriate level of scrutiny.

[186] Allen and Chan, p. 23.

[187] Ibid., p. 25.

[188] Louise Matsakis, "Researchers Fooled a Google AI into Thinking a Rifle was a Helicopter," *Wired*, December 20, 2017, https://www.wired.com/story/researcher-fooled-a-google-ai-into-thinking-a-rifle-was-a-helicopter/?mbid=nl_122117_daily_list1_p2.

AI's Impact on Combat

Although AI has not yet entered the combat arena in a serious way, experts are predicting the potential impact that AI will have on the future of warfare. This influence will be a function of many factors (as described in the preceding sections of this report), including the rate of commercial investment, the drive to compete with international rivals, the research community's ability to advance the state of AI capability, the military's general attitude toward the technology, and the development of AI-specific warfighting concepts.[189]

Many experts assert that there is a "sense of inevitability" with AI, arguing that it is bound to be substantially influential.[190] Nevertheless, in January 2016, the Vice Chairman of the Joint Chiefs of Staff, General Paul Selva, intimated that it may be too early to tell, pointing out that the DOD was still in the midst of evaluating AI's potential. He stated, "The question we're trying to pose now is, 'Do the technologies that are being developed in the commercial sector principally provide the kind of force multipliers that we got when we combined tactical nuclear weapons or precision and stealth?' If the answer is yes, then we can change the way that we fight.... If not, the military will seek to improve its current capabilities slightly to gain an edge over its adversaries."[191] There are a range of opinions on AI's trajectory, and Congress may consider these future scenarios as it seeks to influence and conduct oversight of military AI applications.

Minimal Impact on Combat

While many analysts admit that military AI technology is in a stage of infancy, it is difficult to find an expert who believes that AI will be inconsequential in the long run.[192] However, AI critics point to a number of trends that may minimize the technology's impact. From a technical standpoint, there is a potential that the current safety problems with AI will be insurmountable and will make AI unsuitable for military applications.[193] In addition, there is a chance the perceived current inflection point in AI development will lead to a plateau. Some experts believe that the present family of algorithms will reach their full potential in another 10 years, and AI development will not be able to proceed without significant leaps in enabling technology, like chips with higher power efficiency or advances in quantum computing.[194] The technology has reached similar roadblocks in the past, resulting in periods called "AI Winters," during which the progress of AI research slowed significantly.

As discussed above, the military's willingness to fully embrace AI technology may be another stifling influence. Many academic studies on technological innovation argue that military organizations are capable of innovation during wartime, but they characterize the services in peace-time as large, inflexible bureaucracies that are prone to stagnation unless there is a crisis

[189] "War at Hyperspeed, Getting to Grips with Military Robotics," *The Economist*, January 25, 2018, https://www.economist.com/news/special-report/21735478-autonomous-robots-and-swarms-will-change-nature-warfare-getting-grips.

[190] Allen and Chan, p. 50.

[191] Andrew Clevenger, "The Terminator Conundrum: Pentagon Weighs Ethics of Paring Deadly Force, AI," *Defense News*, January 23, 2016, https://www.defensenews.com/2016/01/23/the-terminator-conundrum-pentagon-weighs-ethics-of-pairing-deadly-force-ai/.

[192] Brian Bergstein, "The Great AI Paradox," *MIT Technology Review*, December 15, 2017, https://www.technologyreview.com/s/609318/the-great-ai-paradox/.

[193] "Highlighting Artificial Intelligence: An Interview with Paul Scharre," p. 17.

[194] CRS Discussions with Dr. Dai Kim.

that spurs action.[195] Members of the Defense Innovation Board, composed of CEOs from leading U.S. commercial companies, remarked in their most recent report, "DOD does not have an innovation problem, it has an innovation adoption problem" with a "preference for small cosmetic steps over actual change."[196]

Another analysis asserts that AI adoption may be halted by poor expectation management. The report asserts that over-hyped AI capabilities may cause frustration that will "diminish people's trust and reduce their willingness to use the system in the future."[197] The importance of this effect is relevant for DOD and policymakers as they consider what may be profound expectations for AI detailed in the following sections.

Evolutionary Impact on Combat

Most analysts believe that AI will at a minimum have significant impact on the conduct of warfare. One study describes AI as a "potentially disruptive technology that may create sharp discontinuities in the conduct of warfare," further asserting that the technology may "produce dramatic improvements in military effectiveness and combat potential."[198] These analysts point to research projects to make existing weapon systems and processes faster and more efficient, as well as providing a means to cope with the proliferation of data that complicate intelligence assessments and decision-making. However, these analysts caution that in the near future AI is unlikely to advance beyond narrow, task-specific applications that require human oversight.[199]

Some AI proponents contend that although humans will be present, their role will be less significant, and the technology will make combat "less uncertain and more controllable," as machines are not subject to the frailties that cloud human judgment, like being "tired, frightened, bored, or angry."[200] However, critics point to the enduring necessity for human presence on the battlefield alongside AI systems in some capacity as the principle restraining factor that will keep the technology from upending warfare. An academic study of this trend argues,

> At present, even an AI of tremendous power will not be able to determine outcomes in a complex social system, the outcomes are too complex – even without allowing for free will by sentient agents.... Strategy that involves humans, no matter that they are assisted by modular AI and fight using legions of autonomous robots, will retain its inevitable human flavor.[201]

---

[195] Gautam Mukunda, "We Cannot Go On: Disruptive Innovation and the First World War Royal Navy," *Security Studies*, Vol. 19, Issue 1, February, 23, 2010, p. 136. For more on this topic, see Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Cornell: Cornell University Press, 1986), and Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Cornell: Cornell University Press, 1994).

[196] Patrick Tucker, "Here's How to Stop Squelching New Ideas, Eric Schmidt's Advisory Board Tells DOD," *Defense One*, January 17, 2018, http://www.defenseone.com/technology/2018/01/heres-how-stop-squelching-new-ideas-eric-schmidts-advisory-board-tells-DOD/145240/.

[197] "Artificial Intelligence and Life in 2030," One Hundred Year Study on AI, Report of the 2015 Study Panel, Stanford University, September 2016, p. 42.

[198] Robert O. Work and Shawn Brimley, *20YY Preparing for War in the Robotic Age*, Center for a New American Security, January 2014, p. 7.

[199] Ibid., p. 25.

[200] "War at Hyperspeed, Getting to Grips with Military Robotics."

[201] Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *The Journal of Strategic Studies*, Vol. 39. No. 5, November 2015, p. 816.

Pointing to another constraining factor, analysts warn of the psychological impact that autonomous systems will have on an adversary, especially in conflict with cultures that place a premium on courage and physical presence. One study on this topic quotes a security expert from Qatar who stated, "How you conduct war is important. It gives you dignity or not."[202]

In addition, experts highlight that this balance of international AI development will affect the magnitude of AI's influence. As one analyst states, "[T]he most cherished attribute of military technology is asymmetry."[203] In other words, military organizations seek to develop technological applications or warfighting concepts that confer an advantage because they are dissimilar from opponents' who possess no immediate counter-measure. Indeed, that is the U.S. military's intent with the current wave of technological development as it seeks "an enduring competitive edge that lasts a generation or more."[204] However, DOD is concerned that if the United States does not increase the pace of AI development, it will end up with an equivalent capability or fleeting advantage as it cedes the edge associated with being first.[205]

Further complicating the pursuit of an AI advantage, the 2018 National Defense Strategy warns, "The fact that many technological developments will come from the commercial sector means that state competitors and nonstate actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed."[206] In these circumstances, AI could still influence warfighting methods, but the technology's overall impact may be relatively insignificant if adversaries possess a comparable capability.

Revolutionary Impact on Combat

A sizeable contingent of experts believe that AI will have a revolutionary impact on warfare. One analysis asserts that AI will induce a "seismic shift on the field of battle" and "fundamentally transform the way war is waged."[207] The 2018 National Defense Strategy counts AI among a group of emerging technologies that will change the character of war, and Frank Hoffman, a professor at the National Defense University, takes this a step further, arguing that AI may "alter the immutable nature of war."[208]

Statements like this imply that AI's transformative potential is so great that it will challenge long-standing, foundational warfighting principles. In addition, members of the Chinese military establishment assert that AI "will lead to a profound military revolution."[209] Proponents of this

---

[202] Peter W. Singer, *Wired for War, The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009), pp. 305-311.

[203] Mark Grimsley, "Surviving the Military Revolution: The US Civil War," in *The Dynamics of Military Revolution, 1300-2050* (Cambridge: Cambridge University Press, 2001), p.74.

[204] Christian Davenport, "Robots, Swarming Drones, and Iron Man: Welcome to the New Arms Race," *The Washington Post*, June 17, 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/06/17/robots-swarming-drones-and-iron-man-welcome-to-the-new-arms-race/?hpid=hp_rhp-more-top-stories_no-name%3Ahomepage%2Fstory&utm_term=.00284eba0a01.

[205] Department of Defense, *Joint Concept for Robotic and Autonomous Systems*, p. 18, and Elsa Kania, "Strategic Innovation and Great Power Competition," *The Strategy Bridge*, January 31, 2018, https://thestrategybridge.org/the-bridge/2018/1/31/strategic-innovation-and-great-power-competition.

[206] Department of Defense, *Summary of the 2018 National Defense Strategy*, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, p. 3.

[207] John R. Allen and Amir Husain, "On Hyperwar," *Proceedings*, July 2017, p. 30.

[208] *Summary of the 2018 National Defense Strategy*, p. 3, and "War at Hyperspeed, Getting to Grips with Military Robotics."

[209] Kania, "Battlefield Singularity," p. 8.

position point to several common factors when making their case. They argue that the world has passed from the Industrial Era of warfare into the Information Era, in which gathering, exploiting, and disseminating information will be the most consequential aspect of combat operations.

In light of this transition, AI's alleged ability to facilitate information superiority and "purge combat of uncertainty" will be a decisive wartime advantage, enabling faster and higher-quality decisions.[210] As one study of information era warfare states, "[W]inning in the decision space is winning in the battlespace."[211] Members of this camp argue that AI and autonomous systems will gradually distance humans from a direct combat role, and some even forecast a time in which humans make strategic level decisions while AI systems exclusively plan and act at the tactical level.

In addition, analysts contend that AI may contest the current preference for quality over quantity, challenging industrial era militaries built around a few, expensive platforms with exquisite capabilities, instead creating a preference for large numbers of less expensive, adequate systems.[212]

A range of potential consequences flow from the assumptions surrounding AI as a revolutionary influence on warfighting. Some studies point to overwhelmingly positive results, like "near instantaneous responses," "perfectly coordinated action," and "domination at a time and place of our choosing" that will "consistently overmatch the enemy's capacity to respond."[213] However, AI may create an "environment where weapons are too fast, small, numerous, and complex for humans to digest ... taking us to a place we may not want to go but are probably unable to avoid."[214] Further clarifying this point, AI systems reacting at machine speed may push the pace of combat to a point where machine actions surpass the rate of human decision-making. This raises serious concerns among some that AI may surreptitiously lead us to a place where humans lose control of warfare and induce a state of strategic instability.[215]

The speed of AI systems may put the defender at an inherent disadvantage, creating an incentive to strike first against an adversary with like capability. In addition, placing AI systems capable of inherently unpredictable actions in close proximity to an adversary's systems may result in inadvertent escalation or miscalculation, which challenges a human decisionmaker's ability to control the outcome or terminate conflict in a timely manner.[216] Militaries that rely on autonomous systems may be more provocative, since the lives of human soldiers are not at risk.

This raises fundamental questions about the value placed on losing an AI-powered or autonomous system and the definition of an act of war.[217] Although these forecasts project dramatic change,

---

[210] Williamson Murray and MacGregor Knox, "The Future Behind Us," in *The Dynamics of Military Revolution, 1300-2050* (Cambridge: Cambridge University Press, 2001), p. 178.

[211] James W. Mancillas, "Integrating AI into Military Operations: A Boyd Cycle Framework," in *Closer than You Think: The Implications of the Third Offset Strategy for the US Army* (Carlisle, PA: US Army War College Press, 2017), p. 74.

[212] Joint Chiefs of Staff, *Joint Operating Environment 2035, The Joint Force in a Contested and Disordered World*, July 14, 2016, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917, p. 18.

[213] Allen and Husain, pp. 31-33.

[214] Singer, p. 128.

[215] Scharre, "A Security Perspective: Security Concerns and Possible Arms Control Approaches," p. 26.

[216] Jurgen Altmann and Frank Sauer, "Autonomous Weapons and Strategic Stability," *Survival*, Vol. 59, No. 5, October – November 2017, pp. 121-127.

[217] *Joint Concept for Robotic and Autonomous Systems*, p. 18.

analysts point out that concurrent assessments of the impact may be tough to discern. Historians of technology and warfare emphasize that previous technological revolutions are apparent only in hindsight, and the true utility of a new application like AI may not be apparent until it is used in combat.[218]

Nevertheless, given AI's disruptive potential, for better or for worse, it may be incumbent on military leaders and Congress to evaluate the implications of military AI developments and exercise appropriate oversight of emerging trends as the technology progresses. Congress may be alert to the policy issues surrounding AI in the immediate future, as they will likely affect which of the previously discussed scenarios comes to fruition. Congressional action on AI funding, acquisitions legislation, development of AI norms and standards, and issues of international competition has the potential to significantly shape the trajectory of AI technology, and experts agree that continuous evaluation of legislative actions may be necessary to keep this technology pointed in a direction that preserves U.S. national security.

Author Contact Information

Daniel S. Hoadley
US Air Force Fellow
dhoadley@crs.loc.gov, 7-3512

Nathan J. Lucas
Section Research Manager
nlucas@crs.loc.gov, 7-3564

[218] Williamson Murray, p. 154 and p. 185.