Artificial Intelligence and National Security

Kelley M. Sayler
Analyst in Advanced Technology and Global Security

Updated January 30, 2019

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Artificial intelligence (AI) is a rapidly growing field of technology with potentially significant implications for national security. As such, the U.S. Department of Defense (DOD) and other nations are developing AI applications for a range of military functions. AI research is underway in the fields of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and in a variety of semiautonomous and autonomous vehicles. Already, AI has been incorporated into military operations in Iraq and Syria. Congressional action has the potential to shape the technology's development further, with budgetary and legislative decisions influencing the growth of military applications as well as the pace of their adoption.

AI technologies present unique challenges for military integration, particularly because the bulk of AI development is happening in the commercial sector. Although AI is not unique in this regard, the defense acquisition process may need to be adapted for acquiring emerging technologies like AI. In addition, many commercial AI applications must undergo significant modification prior to being functional for the military. A number of cultural issues also challenge AI acquisition, as some commercial AI companies are averse to partnering with DOD due to ethical concerns, and even within the department, there can be resistance to incorporating AI technology into existing weapons systems and processes.

Potential 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 on developing a variety 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 could, for example, facilitate autonomous operations, lead to more informed military decisionmaking, and increase the speed and scale of military action. However, it may also be unpredictable or vulnerable to unique forms of manipulation. As a result of these factors, 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, most 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 facilitate military AI development?
- What changes, if any, are necessary in Congress and DOD to implement effective oversight of AI development?
- How should the United States balance research and development related to artificial intelligence and autonomous systems with ethical considerations?
- What legislative or regulatory changes are necessary for the integration of military AI applications?
- What measures can Congress take to help manage the AI competition globally?

Contents

Figures

Tables

Contacts

Introduction[1]

Artificial intelligence (AI) is a rapidly growing field of technology that is capturing the attention of commercial investors, defense intellectuals, policymakers, and international competitors alike, as evidenced by a number of recent initiatives. On July 20, 2017, the Chinese government released a strategy detailing its plan to take the lead in AI by 2030. 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."[2] Similarly, the U.S. National Defense Strategy, released in January 2018, identified artificial intelligence as one of the key technologies that will "ensure [the United States] will be able to fight and win the wars of the future."[3]

The U.S. military is already integrating AI systems into combat via a spearhead initiative called Project Maven, which uses AI algorithms to identify insurgent targets in Iraq and Syria.[4] These dynamics raise several questions that Congress addressed in hearings during 2017 and 2018: 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 oversight, budgetary, and legislative tools available that it may use to influence the answers to these questions and shape the future development of AI technology.

AI Terminology and Background[5]

Almost all academic studies in artificial intelligence acknowledge that no commonly accepted definition of AI exists, in part because of the diverse approaches to research in the field. Likewise, although Section 238 of the FY2019 National Defense Authorization Act (NDAA) directs the Secretary of Defense to produce a definition of artificial intelligence by August 13, 2019, no official U.S. government definition of AI currently exists.[6] The FY2019 NDAA does, however, provide a definition of AI for the purposes of Section 238:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

[1] This report was originally written by Daniel S. Hoadley, U.S. Air Force Fellow. It has been updated by Kelley M. Sayler, Analyst in Advanced Technology and Global Security.

[2] 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.

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

[4] 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/.

[5] For a general overview of AI, see CRS In Focus IF10608, *Overview of Artificial Intelligence*, by Laurie A. Harris.

[6] P.L. 115-232, Section 2, Division A, Title II, §238.

3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.[7]

This definition encompasses 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: (1) the availability of "big data" sources, (2) improvements to machine learning approaches, and (3) increases in computer processing power.[8] This growth has advanced the state of Narrow AI, which refers to algorithms that address specific problem sets like game playing, image recognition, and navigation. 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 develop General AI, which refers to systems capable of human-level intelligence across a broad range of tasks.[9] 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 amount will grow to as high as $126 billion by 2025.[10] DOD's unclassified expenditures in AI contracts for FY2016 totaled just over $600 million, increasing to over $800 million in FY2017.[11]

AI has a number of unique characteristics that may be important to consider as these technologies enter the national security arena. First, AI has the potential to be integrated across a variety of applications, improving the so-called "Internet of Things" in which disparate devices are networked together to optimize performance.[12] As Kevin Kelley, the founder of *Wired* magazine, states, "[AI] will enliven inert objects, much as electricity did more than a century ago. Everything that we formerly electrified we will now cognitize."[13] 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 as well as terrorist

[7] Ibid.

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

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

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

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

[12] See Steve Ranger, "What is the IoT? Everything you need to know about the Internet of Things right now," ZDNet.com, August 21, 2018, https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

[13] 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.

activity in full motion video captured by uninhabited aerial vehicles over Syria or Afghanistan.[14] 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 objects. 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."[15]

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

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

- **Automated systems.** "A physical system that functions 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."[16]
- **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."[17]
  - 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."[18]
  - Human-Supervised Autonomous Weapon System. "An autonomous weapon system that is designed to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur."[19]
  - 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."[20]

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

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

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

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

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

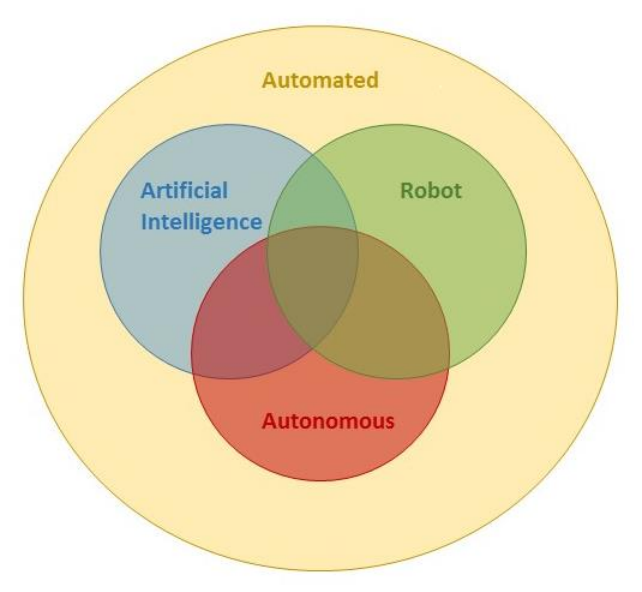
[19] Ibid.

[20] 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."[21]

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. For example, some studies delineate between automated systems and autonomous systems based on the system's complexity, arguing that automated systems are strictly rule-based, while autonomous systems exhibit artificial intelligence. Some, including the Department of Defense, categorize autonomous weapon systems based not on the system's complexity, but rather on the type of function being executed without human intervention (e.g., target selection and engagement).[22] Still others describe AI as a means of automating cognitive tasks, with robotics automating physical tasks. This framework, however, may not be sufficient to describe how AI systems function, as such systems do not merely replicate human cognitive functions and often produce unanticipated outputs. In addition, a robot may be automated or autonomous and may or may not contain an AI algorithm. Figure 1 illustrates these relationships, based on the above selected definitions of each term.

Figure 1. Relationships of Selected AI Definitions



Source: CRS.

Issues for Congress

A number of Members of Congress have called 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.[23] Former Deputy Secretary of Defense Robert Work argued in a November 2017 interview that the federal government needs to address AI issues at the

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

[22] See Paul Scharre and Michael C. Horowitz, *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February 2015, pp. 6-7.

[23] 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.

highest levels, further stating that "this is not something the Pentagon can fix by itself."[24] Other analysts have called for a national AI strategy to articulate AI objectives and drive whole-of-government initiatives and cross-cutting investments.[25]

In the meantime, DOD has published a classified AI strategy and is carrying out multiple tasks directed by DOD guidance and the FY2019 NDAA, including

- establishing a Joint Artificial Intelligence Center (JAIC), which will "coordinate the efforts of the Department to develop, mature, and transition artificial intelligence technologies into operational use";[26]
- publishing a strategic roadmap for AI development and fielding, as well as guidance on "appropriate ethical, legal, and other policies for the Department governing the development and use of artificial intelligence enabled systems and technologies in operational situations";[27]
- establishing a National Security Commission on Artificial Intelligence; and
- conducting a comprehensive assessment of militarily relevant AI technologies and providing recommendations for strengthening U.S. competitiveness.[28]

These initiatives will present a number of oversight opportunities for Congress.

In addition, Congress may consider the adequacy of current DOD funding levels for AI. Lieutenant General John Shanahan, the 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.[29] Although DOD funding for AI has increased in 2018—to include the JAIC's $1.75 billion six-year budget and the Defense Advanced Research Projects Agency's (DARPA's) $2 billion multiyear investment in over 20 AI programs—some experts have argued that additional DOD funding will be required to keep pace with U.S. competitors and avoid an "innovation deficit" in military technology.[30]

---

[24] 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-eric-schmidt-bob-work/.

[25] Jack Corrigan, "U.S. Needs a National Strategy for Artificial Intelligence, Lawmakers and Experts Say," *Defense One*, July 14, 2018, https://www.defenseone.com/technology/2018/07/us-needs-national-strategy-artificial-intelligence-lawmakers-and-experts-say/149644/.

[26] Sydney J. Freedberg, Jr., "Pentagon Rolls Out Major Cyber, AI Strategies This Summer," *Breaking Defense*, July 17, 2018, https://breakingdefense.com/2018/07/pentagon-rolls-out-major-cyber-ai-strategies-this-summer/; and P.L. 115-232, Section 2, Division A, Title X, §1051.

[27] P.L. 115-232, Section 2, Division A, Title II, §238.

[28] Ibid., and P.L. 115-232, Section 2, Division A, Title X, §1051.

[29] 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.

[30] "DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies," DARPA, September 7, 2018, https://www.darpa.mil/news-events/2018-09-07, and Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, November 28, 2017, pp. 40-41, https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235804.

Critics of increased federal funding contend that significant increases to appropriations may not be required, as the military should be leveraging 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 that "take risks and rapidly field emerging commercial technologies."[31] In addition, the Office of Management and Budget directed DOD in preparing its FY2020 budget to "seek to rapidly field innovative technologies from the private sector, where possible, that are easily adaptable to Federal needs, rather than reinventing solutions in parallel."[32] Some experts in the national security community also argue that it would not be a responsible use of taxpayer money to duplicate efforts devoted to AI R&D in the commercial sector when companies take products 90% of the way to a useable military application.[33] Others 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.[34] These issues are discussed in more detail later in this report.[35]

One impediment to accurately evaluating funding levels for AI is the lack of a stand-alone AI Program Element (PE) in DOD funding tables. As a result, AI R&D appropriations are spread throughout generally titled PEs and incorporated into funding for larger systems with AI components. For example, in the FY2019 National Defense Authorization Act, AI funding is spread throughout the PEs for the High Performance Computing Modernization Program and Dominant Information Sciences and Methods, among others.[36] On the other hand, a dedicated PE for AI may lead to a false precision, as it may be challenging to identify exact investments in enabling technologies like AI. The lack of an official U.S. government definition of AI could further complicate such an assessment.

Congress may also consider specific policies for the development and use of military AI applications. Many experts fear that the pace of AI technology development is moving faster than the speed of policy implementation. Former Chairman of the House Armed Services Committee Representative Mac Thornberry has 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."[37] Congress may assess the need for new policies or modifications to existing laws to account for AI developments and ensure that AI applications are free from bias.[38] Perhaps the most immediate policy concern among AI analysts is the absence of an independent entity to develop and enforce

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

[32] Executive Office of the President, Director, Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, "FY 2020 Administration Research and Development Budget Priorities," July 31, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf.

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

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

[35] 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.

[36] P.L. 115-232, Section 2, Division D, Title XLIII, §4301.

[37] 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.

[38] See Parmy Olson, "Racist, Sexist AI Could Be a Bigger Problem than Lost Jobs," *Forbes*, February 26, 2018, https://www.forbes.com/sites/parmyolson/2018/02/26/artificial-intelligence-ai-bias-google/#3326a1951a01.

AI safety standards and to oversee government-wide AI research.[39] Former Secretary of Defense Ashton B. Carter, for example, has suggested the need for an "AI czar" to coordinate such efforts.[40]

Relatedly, Congress may consider debating policy options on the development and fielding of Lethal Autonomous Weapons Systems (LAWS), which may use AI to select and engage targets. Since 2014, the United States has participated in international discussions of LAWS at the United Nations (U.N.) Convention on Certain Conventional Weapons (CCW). Approximately 25 state parties have called for a treaty banning "fully autonomous weapon systems" due to ethical considerations, while others have called for formal regulations or political declarations.[41] Some analysts are concerned that efforts to ban or regulate LAWS could impose strict controls on AI applications that could be adapted for lethal use, thereby stifling development of other useful military—or even commercial—technology. During recent testimony to the U.N., 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 suggested the leading question for considering military AI applications ought to be, "What role do we want humans to play in wartime decision making?"[42]

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 reported to be aggressively pursuing AI investments in the United States. Amid growing scrutiny of transactions involving Chinese firms in the semiconductor industry, in September 2017 President Trump, following the recommendation of the Committee on Foreign Investment in the United States (CFIUS), blocked a Chinese firm from acquiring Lattice Semiconductor, a U.S. company that manufactures chips that are a critical design element for AI technology.[43] In this way, some experts believe that CFIUS may provide a means of protecting strategically significant technologies like AI. [44] Indeed, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) expands CFIUS's ability to review certain foreign investments, including those involving "emerging and foundational technologies." It also authorized CFIUS to consider "whether a covered transaction involves a country of special

[39] 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.

[40] David Ignatius, "China's application of AI should be a Sputnik moment for the U.S. But will it be?," *New York Times*, November 6, 2018, https://www.washingtonpost.com/opinions/chinas-application-of-ai-should-be-a-sputnik-moment-for-the-us-but-will-it-be/2018/11/06/69132de4-e204-11e8-b759-3d88a5ce9e19_story.html?utm_term=.88a808915d9c.

[41] See "Country Views on Killer Robots," Campaign to Stop Killer Robots, April 13, 2018, https://www.stopkillerrobots.org/wp-content/uploads/2018/04/KRC_CountryViews_13Apr2018.pdf; and U.N. CCW Working Papers and Statements at https://www.unog.ch/__80256ee600585943.nsf/(httpPages)/7c335e71dfcb29d1c1258243003e8724?OpenDocument&ExpandSection=3#_Section3.

[42] 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.

[43] 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.

[44] 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.

concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security."[45] Congress may monitor the implementation of FIRRMA and assess whether additional reforms might be necessary to maintain effective congressional oversight of sensitive transactions.

In addition, many analysts believe that it may be necessary to reform federal data policies associated with AI. Large data pools serve as the training sets needed for building many AI systems, and government data may be particularly important in developing military AI applications. However, some analysts have observed that much of this data is either classified, access-controlled, or otherwise protected on privacy grounds. These analysts contend that Congress should implement a new data policy that balances data protection and privacy with the need to fuel AI development.[46]

Closely related, AI development may increase the imperative for strict security standards. As discussed later in this report, AI algorithms are vulnerable to bias, theft, and manipulation, particularly if the training data set is not adequately curated or 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."[47] Some leading commercial technology companies have issued similar calls for increased scrutiny, with Microsoft's president Brad Smith arguing that a lack of regulation in this area could lead to "a commercial race to the bottom, with tech companies forced to choose between social responsibility and market success."[48]

Finally, commercial companies have long cited the potential loss of intellectual property rights as a key impediment to partnering with DOD. In recognition of this issue, Section 813 of the FY2016 NDAA established a "government-industry advisory panel" to provide recommendations on technical data rights and intellectual property reform.[49] The panel's report, released in November 2018, offers a number of recommendations, including increased training in intellectual property rights for acquisitions professionals and a pilot program for intellectual property valuation in the procurement process.[50]

[45] The specific technologies that qualify as "emerging and foundational technologies" are to be identified by an interagency process led by the Department of Commerce. See P.L. 115-232, Title XVII, §1702(c). For more information on FIRRMA, see CRS In Focus IF10952, *CFIUS Reform: Foreign Investment National Security Reviews*, by James K. Jackson and Cathleen D. Cimino-Isaacs.

[46] Alexander Velez-Green and Paul Scharre, "The United States Can Be a World Leader in AI. Here's How.," *The National Interest*, November 2, 2017, https://nationalinterest.org/feature/the-united-states-can-be-world-leader-ai-heres-how-22921.

[47] 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.

[48] Brad Smith, "Facial recognition: It's time for action," *Microsoft*, December 6, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/?mod=article_inline.

[49] P.L. 114-92, Section 2, Division A, Title VIII, §813.

[50] *2018 Report,* Government-Industry Advisory Panel on Technical Data Rights, November 21, 2018, p. 5, https://sbtc.org/wp-content/uploads/2018/11/Final-Report_ExSum_TensionPapers_11132018.pdf.

AI Applications for Defense

DOD is considering 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 DARPA and the Intelligence Advanced Research Projects Agency (IARPA). However, DOD components are currently required to coordinate with the JAIC regarding any planned AI initiatives costing more than $15 million annually.[51] In addition, the JAIC has been tasked with overseeing the National Mission Initiatives, projects that will leverage AI to address pressing operational challenges.[52] The Office of the Under Secretary of Defense for Research and Engineering, which oversaw the development of DOD's AI Strategy, will continue to support AI development and delivery.

The Algorithmic Warfare Cross-Functional Team, also known as Project Maven, has previously been a focal point for DOD AI integration and will transition from the Under Secretary of Defense for Intelligence to the JAIC, where it will become the first of the JAIC's National Mission Initiatives.[53] Project Maven was launched in April 2017 and charged with rapidly incorporating AI into existing DOD systems to demonstrate the technology's potential.[54] Project Maven's inaugural director stated, "Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame for artificial intelligence across the department."[55] AI is also being incorporated into a number of other intelligence, surveillance, and reconnaissance applications, as well as in logistics, cyberspace operations, information operations, command and control, semiautonomous and autonomous vehicles, and lethal autonomous weapon systems.

Intelligence, Surveillance, and Reconnaissance

AI is expected to be particularly useful in intelligence due to the large data sets available for analysis.[56] For example, Project Maven's first phase involves automating intelligence processing in support of the counter-ISIL campaign. Specifically, the Project Maven team is incorporating computer vision and machine learning algorithms into intelligence collection cells that would comb through footage from uninhabited aerial vehicles 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, potentially freeing analysts to make more efficient and timely decisions based on the data.[57]

---

[51] This coordination threshold will be reviewed each year and adjusted upwards, as conditions warrant. Patrick Shanahan, Deputy Secretary of Defense, Memorandum, "Establishment of the Joint Artificial Intelligence Center," June 27, 2018, https://admin.govexec.com/media/establishment_of_the_joint_artificial_intelligence_center_osd008412-18_r.... pdf.

[52] Ibid.

[53] Shanahan, "Establishment of the Joint Artificial Intelligence Center"; and Sydney J. Freedberg, Jr., "Joint Artificial Intelligence Center Created under DoD CIO," *Breaking Defense,* June 29, 2018, https://breakingdefense.com/2018/06/joint-artificial-intelligence-center-created-under-dod-cio/.

[54] 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.

[55] 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.

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

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

The intelligence community also has a number of publicly acknowledged AI research projects in progress. The Central Intelligence Agency alone has around 140 projects in development that leverage AI in some capacity to accomplish tasks such as image recognition and predictive analytics.[58] IARPA is sponsoring several AI research projects intended to produce other analytic tools within the next four to five years. Some examples include developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and building tools to infer a building's function based on pattern-of-life analysis.[59]

Logistics

AI may have a promising future in the field of military logistics. The Air Force, for example, is beginning to use AI for predictive aircraft maintenance. Instead of making repairs when an aircraft breaks or in accordance with monolithic fleet-wide maintenance schedules, the Air Force is testing an AI-enabled approach that tailors maintenance schedules to the needs of individual aircraft. This approach, currently used by the F-35's Automated Logistics Information System, extracts real-time sensor data embedded in the aircraft's engines and other onboard systems and feeds the data into a predictive algorithm to determine when technicians need to inspect the aircraft or replace parts.[60]

Similarly, the Army's Logistics Support Activity (LOGSA) has contracted IBM's Watson (the same AI software that defeated two *Jeopardy* champions) to develop tailored maintenance schedules for the Stryker fleet based on information pulled from the 17 sensors installed on each vehicle. In September 2017, LOGSA began a second project that will use Watson to analyze shipping flows for repair parts distribution, attempting to determine the most time- and cost-efficient means to deliver supplies. This task is currently done by human analysts, who have saved the Army around $100 million a year by analyzing just 10% of shipping requests; with Watson, the Army will have the ability to analyze 100% of shipping requests, potentially generating even greater cost savings in a shorter period of time.[61]

Cyberspace Operations

AI is likely to be a key technology in advancing military cyber operations. 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."[62] He later 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."[63] Conventional cybersecurity tools look for historical

[58] 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/.

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

[60] 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/.

[61] 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/.

[62] Testimony of Michael Rogers, Senate Armed Services Committee, *Hearing to Receive Testimony on Encryption and Cyber Matters*, September 13, 2016, https://www.armed-services.senate.gov/imo/media/doc/16-68_09-13-16.pdf.

[63] 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-

matches to known malicious code, so hackers only have to modify small portions of that code to circumvent the defense. AI-enabled tools, on the other hand, can be trained to detect anomalies in broader patterns of network activity, thus presenting a more comprehensive and dynamic barrier to attack.[64]

DARPA's 2016 Cyber Grand Challenge demonstrated the potential power of AI-enabled cyber tools. The competition challenged participants to develop AI algorithms that could autonomously "detect, evaluate, and patch software vulnerabilities before [competing teams] have a chance to exploit them"—all within a matter of seconds, rather than the usual months.[65] The challenge demonstrated not only the potential speed of AI-enabled cyber tools but also the potential ability of a singular algorithm to play offense and defense simultaneously. These capabilities could provide a distinct advantage in future cyber operations.

Information Operations and "Deep Fakes"[66]

AI is enabling increasingly realistic photo, audio, and video forgeries, or "deep fakes," that adversaries could deploy as part of their information operations. Indeed, deep fake technology could be used against the United States and U.S. allies to generate false news reports, influence public discourse, erode public trust, and attempt to blackmail diplomats.[67] Although most previous deep fakes have been detectable by experts, the sophistication of the technology is progressing to the point that it may soon be capable of fooling forensic analysis tools.[68]

In order to combat deep fake technologies, DARPA has launched the Media Forensics (MediFor) project, which seeks to "automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media."[69] MediFor has developed some initial tools for identifying AI-produced forgeries, but as one analyst has noted, "a key problem … is that machine-learning systems can be trained to outmaneuver forensics tools."[70] For this reason, DARPA plans to host follow-on contests to ensure that forensic tools keep pace with deep fake technologies.[71]

Artificial intelligence could also be used to create full "digital patterns-of-life," in which an individual's digital "footprint" is "merged and matched with purchase histories, credit reports, professional resumes, and subscriptions" to create a comprehensive behavioral profile of

summit/.

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

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

[66] For a more detailed discussion of information operations, see CRS Report R45142, *Information Warfare: Issues for Congress*, by Catherine A. Theohary.

[67] Kyle Rempfer, "Ever heard of 'deep fake' technology? The phony audio and video tech could be used to blackmail US troops," *Military Times*, July 19, 2018, https://www.militarytimes.com/news/your-air-force/2018/07/19/ever-heard-of-deep-fake-technology-the-phony-audio-and-video-tech-could-be-used-to-blackmail-us-troops/.

[68] Allen and Chan, p. 29.

[69] "Media Forensics (MediFor)," DARPA, https://www.darpa.mil/program/media-forensics.

[70] Will Knight, "The Defense Department has produced the first tools for catching deepfakes," *MIT Technology Review*, August 7, 2018, https://www.technologyreview.com/s/611726/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes/.

[71] Ibid.

servicemembers, suspected intelligence officers, government officials, or private citizens.[72] As in the case of deep fakes, this information could, in turn, be used for targeted influence operations or blackmail.

Command and Control

The U.S. military is seeking to exploit AI's analytic potential in the area of command and control. The Air Force is developing a system for Multi-Domain Command and Control (MDC2), which aims to centralize planning and execution of air-, space-, cyberspace-, sea-, and land-based operations. 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, also known as a "common operating picture," for decisionmakers.[73] Currently, information available to decisionmakers comes in diverse formats from multiple platforms, often with redundancies or unresolved discrepancies. An AI-enabled common operating picture would theoretically combine this information into one display, providing a comprehensive picture of friendly and enemy forces, and automatically resolving variances from input data. 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 sought to refine requirements for this project.[74] Similarly, DARPA's Mosaic Warfare program seeks to leverage AI to coordinate autonomous forces and dynamically generate multidomain command and control nodes.[75]

Future AI systems may be used to identify communications links cut by an adversary and find alternative means of distributing information. As the complexity of AI systems matures, AI algorithms may also be capable of providing commanders with a menu of viable courses of action based on real-time analysis of the battle-space, in turn enabling faster adaptation to complex events.[76] In the long run, many analysts believe this area of AI development could be particularly consequential, with the potential to improve the quality of and accelerate wartime decisionmaking.

Semiautonomous and Autonomous Vehicles

All U.S. military services are working to incorporate AI into semiautonomous and autonomous vehicles, including fighter aircraft, drones, ground vehicles, and naval vessels. AI applications in this field are similar to commercial semiautonomous vehicles, which use AI technologies to

[72] Clint Watts, "Artificial intelligence is transforming social media. Can American democracy survive?," *Washington Post*, September 5, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/09/05/artificial-intelligence-is-transforming-social-media-can-american-democracy-survive/?utm_term=.7e7a5ef245db.

[73] 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/.

[74] 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/.

[75] "Strategic Technology Office Outlines Vision for 'Mosaic Warfare,'" DARPA, August 4, 2017, https://www.darpa.mil/news-events/2017-08-04.

[76] See, for example, "Generating Actionable Understanding of Real-World Phenomena with AI," DARPA, January 4, 2019, https://www.darpa.mil/news-events/2019-01-04.

perceive the environment, recognize obstacles, fuse sensor data, plan navigation, and even communicate with other vehicles.[77]

The Air Force Research Lab completed phase-two tests of its Loyal Wingman program, which pairs an older-generation, uninhabited fighter jet (in this case, an F-16) with an inhabited F-35 or F-22. During this event, the uninhabited F-16 test platform autonomously reacted to events that were not preprogrammed, such as weather and unforeseen obstacles.[78] As the program progresses, AI may enable the "loyal wingman" to accomplish tasks for its inhabited flight lead, such as jamming electronic threats or carrying extra weapons.[79]

The Army and the Marine Corps tested prototypes of similar vehicles that follow soldiers or vehicles around the battlefield to accomplish independent tasks.[80] For example, the Marine Corps' Multi-Utility Tactical Transport (MUTT) is a remote-controlled, ATV-sized vehicle capable of carrying hundreds of pounds of extra equipment. Although the system is not autonomous in its current configuration, the Marine Corps intends for follow-on systems to have greater independence.[81] Likewise, the Army plans to field a number of Robotic Combat Vehicles (RCVs) with different types of autonomous functionality, including navigation, surveillance, and IED removal. These systems will be deployed as "wingmen" for the optionally inhabited Next Generation Ground Vehicle, tentatively scheduled for initial soldier evaluations in FY2020.[82]

DARPA completed testing of the Anti-Submarine Warfare Continuous Trail Unmanned Vessel prototype, or "Sea Hunter," in early 2018 before transitioning program development to the Office of Naval Research.[83] If Sea Hunter enters into service, it would provide the Navy with the ability to autonomously navigate the open seas, swap out modular payloads, and coordinate missions with other unmanned vessels—all while providing continuous submarine-hunting coverage for months at a time.[84] Some analysts estimate that Sea Hunter would cost around $20,000 a day to operate, in contrast to around $700,000 for a traditionally inhabited destroyer.[85]

DOD is testing other AI-fueled capabilities to enable cooperative behavior, or *swarming*. Swarming is a unique subset of autonomous vehicle development, with concepts ranging from large formations of low-cost vehicles designed to overwhelm defensive systems to small squadrons of vehicles that collaborate to provide electronic attack, fire support, and localized

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

[78] 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.

[79] 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/.

[80] For an overview of semiautonomous and autonomous ground vehicles, see CRS Report R45392, *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, coordinated by Andrew Feickert.

[81] 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/.

[82] Feickert, p. 24; and Jen Judson, "First Next-Gen Combat Vehicle and robotic wingman prototypes to emerge in 2020," *Defense News*, March 16, 2018, https://www.defensenews.com/land/2018/03/16/first-next-gen-combat-vehicle-and-robotic-wingman-prototypes-to-emerge-in-2020/.

[83] "ACTUV 'Sea Hunter' Prototype Transitions to Office of Naval Research for Further Development," DARPA, January 30, 2018, https://www.darpa.mil/news-events/2018-01-30a.

[84] Ibid.

[85] Julian Turner, "Sea Hunter: inside the US Navy's autonomous submarine tracking vessel," Naval Technology.

navigation and communication nets for ground-troop formations.[86] A number of different swarm capabilities are currently under development. For example, in November 2016, the Navy completed a test of an AI-enabled swarm 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 ships.[87] The Navy also plans to test swarms of underwater drones, and the Strategic Capabilities Office has successfully tested a swarm of 103 air-dropped micro-drones.[88]

Swarm Characteristics[89]

- 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)

Lethal Autonomous Weapon Systems (LAWS) are a special class of weapon 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. This capability enables the system to operate in communications-degraded or -denied environments where traditional systems may not be able to operate. The U.S. military does not currently have LAWS in its inventory, although there are no legal prohibitions on the development of LAWS.

DOD Directive 3000.09, "Autonomy in Weapon Systems," outlines department policies for semiautonomous and autonomous weapon systems. The directive requires that all systems, regardless of classification, be designed to "allow commanders and operators to exercise appropriate levels of human judgment over the use of force" and to successfully complete the department's weapons review process.[90] Any changes to the system's operating state require that the system go through the weapons review process again to ensure that it has retained the ability to operate as intended. Autonomous weapons and a limited type of semiautonomous weapons must additionally be approved before both development and fielding by the Under Secretary of Defense for Policy; the Under Secretary of Defense for Acquisition, Technology, and Logistics;

[86] 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.

[87] 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/.

[88] Gidget Fuentes, "Navy Will Test Swarming Underwater Drones in Summer Exercise," USNI News, June 26, 2018, https://news.usni.org/2018/06/26/navy-will-test-swarming-underwater-drones-summer-exercise; and "Department of Defense Announces Successful Micro-Drone Demonstration," Department of Defense, January 9, 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

[89] Ilachinski, p. 108.

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

and the Chairman of the Joint Chiefs of Staff. Human-supervised autonomous weapons used for point defense of manned installations or platforms—but that do not target humans—and autonomous weapons that "apply non-lethal, non-kinetic force, such as some forms of electronic attack, against materiel targets" are exempted from this senior-level review.[91]

Despite this policy, some senior military and defense leaders have expressed concerns about the prospect of fielding LAWS. For example, in 2017 testimony before the Senate Armed Services Committee, Vice Chairman of the Joint Chiefs of Staff General Paul Selva stated, "I do not think it is reasonable for us to put robots in charge of whether or not we take a human life."[92] Regardless, Selva explained that the military will be compelled to address the development of this class of technology in order to find its vulnerabilities, given the fact that potential U.S. adversaries are pursuing LAWS.[93]

Military AI Integration Challenges

From the Cold War era until recently, most major defense-related technologies, including nuclear technology, the Global Positioning System (GPS), and the internet, were first developed by government-directed programs before later spreading to the commercial sector.[94] Indeed, DARPA's Strategic Computing Initiative invested over $1 billion between 1983 and 1993 to develop the field of artificial intelligence for military applications, but the initiative was ultimately cancelled due to slower-than-anticipated progress.[95] Today, commercial companies—sometimes building on past government-funded research—are leading AI development, with DOD later adapting their tools for military applications.[96] Noting this dynamic, 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."[97] In addition to the shift in funding sources, a number of challenges related to technology, process, personnel, and culture continue to impede the adoption of AI for military purposes.

---

[91] Ibid.

[92] 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).

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

[94] 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.

[95] Alex Roland with Philip Shiman, *Strategic Computing: DARPA and the Quest for Machine Intelligence*, 1983-1993 (Cambridge, Massachusetts: The MIT Press, 2002), p. 1 and p. 285.

[96] For example, the foundational research that eventually led to the creation of Google was funded by a National Science Foundation grant. David Hart, "On the Origins of Google," National Science Foundation, August 17, 2004, https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=100660.

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

Technology

A wide variance exists in the ease of adaptability of commercial AI technology for military purposes. In some cases, the transition is relatively seamless. For example, the aforementioned aircraft maintenance algorithms, many of which were initially developed by the commercial sector, will likely require only minor data adjustments to account for differences between aircraft types. In other circumstances, significant adjustments are required due to the differences between the structured civilian environments for which the technology was initially developed and more complex combat environments. For example, commercial semiautonomous vehicles have largely been developed in and for data-rich environments with reliable GPS positions, comprehensive terrain mapping, and up-to-date information on traffic and weather conditions obtained from other networked vehicles.[98] In contrast, the military variant of such a vehicle would need to be able to operate in locations where map data are comparatively poor and in which GPS positioning may be inoperable due to adversary jamming. Moreover, semiautonomous or autonomous military ground vehicles would likely need the ability to navigate off-road in rough terrain—a capability not inherent in most commercial vehicles.[99]

Process

Standing DOD processes—including those related to standards of safety and performance, acquisitions, and intellectual property and data rights—present another challenge to the integration of military AI. Often, civilian and military standards of safety and performance are either not aligned or are not easily transferable. A failure rate deemed acceptable for a civilian AI application may be well outside of tolerances in a combat environment—or vice versa. In addition, a recent research study concluded that unpredictable AI failure modes will be exacerbated in complex environments, such as those found in combat.[100] Collectively, these factors may create another barrier for the smooth transfer of commercially developed AI technology to DOD.

DOD may need to adjust its acquisitions process to account for rapidly evolving technologies such as AI.[101] A 2017 internal study of the process found that it takes an average of 91 months to move from the initial Analysis of Alternatives, defining the requirements for a system, to an Initial Operational Capability.[102] In contrast, commercial companies typically execute an iterative development process for software systems like AI, delivering a product in six to nine months.[103] 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 defense acquisition process as a rationale for their decision.[104]

---

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

[99] 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.

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

[101] Ilachinski, pp. 190-191.

[102] Ibid, p. 189.

[103] 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.

[104] 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, and inexperienced DOD contracting workforce.

As a first step in addressing this, DOD has created a number of avenues for "rapid-acquisitions," including the Strategic Capabilities Office, the Defense Innovation Unit, and Project Maven, in order to accelerate the acquisitions timeline and streamline cumbersome processes. Project Maven, for example, was established in April 2017; by December, the team was fielding a commercially acquired prototype AI system in combat.[105] 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 implement more comprehensive acquisitions reform.[106]

Commercial technology companies are also often reluctant to partner with DOD due to concerns about intellectual property and data rights.[107] As an official interviewed for a 2017 GAO report on broader challenges in military acquisitions noted, intellectual property is the "life blood" of commercial technology companies, yet "DOD is putting increased pressure on companies to grant unlimited technical data and software rights or government purpose rights rather than limited or restricted rights."[108]

Personnel

Some reports indicate that DOD and the defense industry also face challenges when it comes to recruiting and retaining personnel with expertise in AI due to research funding and salaries that significantly lag behind those of commercial companies.[109] Other reports suggest that such challenges stem from quality-of-life factors, as well as from a belief among many technology workers that "they can achieve large-scale change faster and better outside the government than within it."[110] Regardless, observers note that if DOD and defense industry are unable to recruit and retain the appropriate experts, military AI applications could be delayed, "deficient, or lacking in appropriate safeguards and testing."[111]

To address these challenges, the Obama Administration launched the Defense Digital Service in 2015 as a means of recruiting private sector technology workers to serve in DOD for one to two year assignments—a "tour of duty for nerds," according to director Chris Lynch.[112] Similarly, former Deputy Secretary of Defense Bob Work has proposed an "AI Training Corps," in which DOD "would pay for advanced technical education in exchange for two days a month of training with government systems and two weeks a year for major exercises." Participants in the program

[105] 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/.

[106] Ilachinski, p. 190.

[107] U.S. Government Accountability Office, *Military Acquisitions, DOD is Taking Steps to Address Challenges Faced by Certain Companies*.

[108] Ibid., p. 20.

[109] M.L. Cummings, "Artificial Intelligence and the Future of Warfare," *Chatham House*, January 2017, p. 11, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

[110] Amy Zegart and Kevin Childs, "The Divide between Silicon Valley and Washington Is a National-Security Threat," *The Atlantic*, December 13, 2018, https://www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

[111] Ibid.

[112] Jim Garamone, "Defense Digital Service Emphasizes Results for Service Members," *DOD News*, June 26, 2018, https://dod.defense.gov/News/Article/Article/1560057/defense-digital-service-emphasizes-results-for-service-members/.

could additionally be called to government service in the event of a national emergency.[113] Other analysts have recommended the establishment of new military training and occupational specialties to cultivate AI talent, as well as the creation of government fellowships and accelerated promotion tracks to reward the most talented technology workers.[114]

Culture

An apparent cultural divide between DOD and commercial technology companies may also present challenges for AI adoption. A recent survey of leadership in several top Silicon Valley companies found that nearly 80% of participants rated the commercial technology community's relationship with DOD as poor or very poor.[115] This was due to a number of factors, including process challenges, perceptions of mutual distrust, and differences between DOD and commercial incentive structures.[116]

Moreover, some companies are refusing to work with DOD due to ethical concerns over the government's use of AI in surveillance or weapon systems. Notably, Google canceled existing government contracts for two robotics companies it acquired—Boston Dynamics and Schaft—and prohibited future government work for DeepMind, a Google-acquired AI software startup.[117] In May 2018, Google employees successfully lobbied the company to withdraw from Project Maven and refrain from further collaboration with DOD.[118] Other companies, however, have pledged to continue supporting DOD contracts, with Amazon CEO Jeff Bezos noting that "if big tech companies are going to turn their back on the U.S. Department of Defense, this country is going to be in trouble."[119]

Cultural factors within the defense establishment itself may also impede AI integration. The integration of AI into existing systems alters standardized procedures and upends well-defined personnel roles. Members of Project Maven have reported a resistance to AI integration because integration can be disruptive without always providing an immediately recognizable benefit.[120] Deputy Director for CIA technology development Dawn Meyerriecks has also expressed concern about the willingness of senior leaders to accept AI-generated analysis, arguing that the defense establishment's risk-averse culture may pose greater challenges to future competitiveness than the pace of adversary technology development.[121]

Finally, some analysts are concerned that DOD will not capitalize on AI's potential to produce game-changing warfighting benefits and will instead simply use AI to incrementally improve existing processes or reinforce current operational concepts. Furthermore, the services may reject certain AI applications altogether if the technology threatens service-favored hardware or

[113] Ignatius, "China's Application of AI."

[114] Kania, "Battlefield Singularity," p. 36; and Zegart and Childs, "The Divide between Silicon Valley and Washington."

[115] Ibid.

[116] Ibid., pp. 4-7.

[117] Allen and Chan, p. 52.

[118] Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *New York Times*, June 1, 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

[119] Nitasha Tiku, "Amazon's Jeff Bezos Says Tech Companies Should Work with the Pentagon," *Wired*, October 15, 2018, https://www.wired.com/story/amazons-jeff-bezos-says-tech-companies-should-work-with-the-pentagon/.

[120] CRS discussion with Major Colin Carroll.

[121] 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/.

missions.[122] Members of Congress may explore the complex interaction of these factors as DOD moves beyond the initial stages of AI adoption.

International Competitors

As military applications for AI 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."[123]

Since at least 2016, AI has been consistently identified as an "emerging and disruptive technology" at the Senate Select Intelligence Committee's annual hearing on the "Worldwide Threat Assessment."[124] 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. They include an increased vulnerability to cyberattack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment."[125] Consequently, it may be important for Congress to understand the state of rival AI development—particularly because U.S. competitors may have fewer moral, legal, or ethical qualms about developing military AI applications.[126]

China

China is by far the United States' most ambitious competitor 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."[127] According to the document, China will seek to develop a core AI industry worth over 150 billion RMB[128]—or approximately $21.7 billion—by 2020 and will "firmly seize the strategic initiative" and reach "world leading levels" of AI investment by 2030.

Recent Chinese achievements in the field demonstrate China's potential to realize its goals for AI development. 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

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

[123] 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.

[124] 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, p. 3, https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf.

[125] Ibid.

[126] Kania, p. 28.

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

[128] Ibid., pp. 2-6. It should be noted that this sum refers to the aspirational total value of China's AI industry in 2020. Credible information about Chinese funding levels for military-specific AI applications is not available in the open source.

nearest U.S. competitor.[129] In 2016 and 2017, Chinese teams won the top prize at the Large Scale Visual Recognition Challenge, an international competition for computer vision systems.[130] Many of these systems are now being integrated into China's domestic surveillance network and social credit system, which aims to monitor and, based on social behavior, "grade" every Chinese citizen by 2021.[131]

China is researching various types of air, land, sea, and undersea autonomous vehicles. In the spring of 2017, a civilian Chinese university with ties to the military demonstrated an AI-enabled swarm of 1,000 uninhabited aerial vehicles 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.[132] Open-source publications indicate that the Chinese are developing a suite of AI tools for cyber operations.[133]

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.[134] Similar to U.S. military concepts, the Chinese aim to use AI for exploiting large troves of intelligence, generating a common operating picture, and accelerating battlefield decisionmaking.[135] The close parallels between U.S. and Chinese AI development have some DOD leaders concerned about the prospects for retaining conventional U.S. military superiority as envisioned in current defense innovation guidance.[136]

Analysts do, however, point to a number of differences that may influence the success of military AI adoption in China. 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, enabling the Chinese to develop more innovative concepts of operation. On the other hand, Chinese military culture, which is dominated by centralized command authority and mistrust of subordinates, may prove resistant to the adoption of autonomous systems or the integration of AI-generated decisionmaking tools.[137]

China's management of its AI ecosystem stands in stark contrast to that of the United States.[138] 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 and accessing technology that was ostensibly developed for civilian purposes. To further strengthen these ties, the Chinese government created

[129] 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.

[130] 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.

[131] "Beijing to Judge Every Resident Based on Behavior by End of 2020," *Bloomberg*, November 21, 2018, https://www.bloomberg.com/news/articles/2018-11-21/beijing-to-judge-every-resident-based-on-behavior-by-end-of-2020. It should be noted that Chinese technology companies such as ZTE Corp are working with other authoritarian regimes to develop similar social-control systems. See, for example, Angus Berwick, "How ZTE helps Venezuela create China-style social control," *Reuters*, November 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.

[132] Kania, "Battlefield Singularity," p. 23.

[133] Ibid., p. 27.

[134] Ibid., pp. 12-14.

[135] Ibid., p. 13.

[136] CRS discussion with Dr. Richard Linderman.

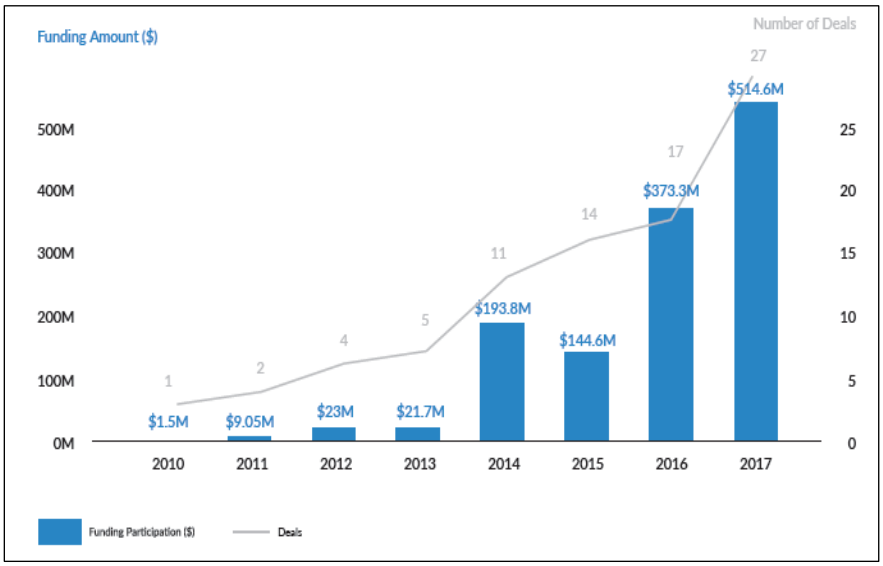
[137] Kania, "Battlefield Singularity," p. 17.

[138] Ibid., p. 6.

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.[139] In addition, the Chinese government is leveraging both lower barriers to data collection and lower costs to data labeling to create the large databases on which AI systems train.[140] 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.[141]

China's centrally directed effort is fueling speculation in the U.S. AI market, where China is investing in companies working on militarily relevant AI applications—potentially granting it lawful access to U.S. technology and intellectual property.[142] **Figure 2** depicts Chinese venture capital investment in U.S. AI companies between 2010 and 2017, totaling an estimated $1.3 billion. The CFIUS reforms introduced in FIRRMA are intended to provide increased oversight of such investments to ensure that they do not threaten national security or grant U.S. competitors undue access to critical technologies.[143]

Figure 2. 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.

[139] 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, "Battlefield Singularity," p. 19.

[140] Will Knight, "China's AI Awakening," *MIT Technology Review*, October 10, 2017, https://www.technologyreview.com/s/609038/chinas-ai-awakening; and Li Yuan, "How Cheap Labor Drives China's A.I. Ambitions," *The New York Times*, November 25, 2018, https://www.nytimes.com/2018/11/25/business/china-artificial-intelligence-labeling.html.

[141] Kania, "Battlefield Singularity," p. 12.

[142] 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-ai-artificial-intelligence.html.

[143] "Reform and Rebuild: The Next Steps, National Defense Authorization Act FY-2019," House Armed Services Committee, July 25, 2018, p. 18, https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/FY19%20NDAA%20Conference%20Summary%20.pdf.

Even with these reforms, however, China may likely gain access to U.S. commercial developments in AI given its extensive history of industrial espionage and cyber theft.[144] Indeed, China has reportedly stolen design plans in the past for a number of advanced military technologies and continues to do so despite the 2015 U.S.-China Cyber Agreement, in which both sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property."[145]

While most analysts view China's unified, whole-of-government effort to develop AI as having a distinct advantage over the United States' AI efforts, many contend that it does have shortcomings. 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.[146]

In addition, China faces challenges in recruiting and retaining AI engineers and researchers. Over half of the data scientists in the United States have been working in the field for over 10 years, while roughly the same proportion of data scientists in China have less than 5 years of experience. Furthermore, fewer than 30 Chinese universities produce AI-focused experts and research products.[147] Although China surpassed the United States in the quantity of research papers produced from 2011 to 2015, the quality of its published papers, as judged by peer citations, ranked 34th globally.[148] China is, however, making efforts to address these deficiencies, with a particular focus on the development of military AI applications. Indeed, the Beijing Institute of Technology—one of China's premier institutes for weapons research—recently established the first educational program in military AI in the world.[149]

Some experts believe that China's intent to be the first to develop military AI applications may result in comparatively less safe applications, as China will likely be more risk-acceptant throughout the development process. These experts stated that it would be unethical for the U.S. military to sacrifice safety standards for the sake of external time pressures, but that the United States' more conservative approach to AI development may result in more capable systems in the long run.[150]

---

[144] Kania, "Battlefield Singularity," p. 40.

[145] "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[146] He, p. 13.

[147] Dominic Barton and Jonathan Woetzel, "Artificial Intelligence: Implications for China," McKinsey Global Institute, April 2017, p. 8, https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx.

[148] 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.

[149] Stephen Chen, "China's brightest children are being recruited to develop AI 'killer bots,'" *South China Morning Post*, November 8, 2018, https://www.scmp.com/news/china/science/article/2172141/chinas-brightest-children-are-being-recruited-develop-ai-killer.

[150] Dr. Caitlin Surakitbanharn, Comments at AI and Global Security Summit, Washington, DC, November 1, 2017; and CRS discussion with Dr. Jason Matheny.

Russia

Like China, Russia is actively pursuing military AI applications. At present, Russian AI development lags significantly behind that of the United States and China. In 2017, the Russian AI market had an estimated value of $12 million[151] and, in 2018, the country ranked 20th in the world by number of AI startups.[152] However, Russia is initiating plans to close the gap. As part of this effort, Russia will continue to pursue its 2008 defense modernization agenda, with the aim of robotizing 30% of its military equipment by 2025.[153]

Russia is establishing a number of organizations devoted to the development of military AI. In March 2018, the Russian government released a 10-point AI agenda, which calls for the establishment of an AI and Big Data consortium, a Fund for Analytical Algorithms and Programs, a state-backed AI training and education program, a dedicated AI lab, and a National Center for Artificial Intelligence, among other initiatives.[154] In addition, Russia recently 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."[155] Some analysts have noted that this recent proliferation of research institutions devoted to AI may, however, result in overlapping responsibilities and bureaucratic inertia, hindering AI development rather than accelerating it.[156]

The Russian military has been researching a number of AI applications, with a heavy emphasis on semiautonomous and autonomous vehicles. In an official statement on November 1, 2017, Viktor Bondarev, chairman of the Federation Council's Defense and Security Committee, stated that "artificial intelligence will be able to replace a soldier on the battlefield and a pilot in an aircraft cockpit" and later noted that "the day is nearing when vehicles will get artificial intelligence."[157] Bondarev made these remarks in close proximity to the successful test of Nerehta, an uninhabited Russian ground vehicle that reportedly "outperformed existing [inhabited] combat vehicles." Russia plans to use Nerehta as a research and development platform for AI and may one day deploy the system in combat, intelligence gathering, or logistics roles.[158] Russia has also reportedly built a combat module for uninhabited ground vehicles that is capable of autonomous

[151] This sum refers to the estimated total value of Russia's AI industry in 2017. Credible information about Russian funding levels for military-specific AI applications is not available in the open source. For comparison, DOD alone spent an estimated $2.4 billion on AI in 2017. See Govini, *Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy*, p. 7.

[152] Jill Dougherty and Molly Jay, "Russia Tries to Get Smart about Artificial Intelligence," *The Wilson Quarterly*, Spring 2018, https://wilsonquarterly.com/quarterly/living-with-artificial-intelligence/russia-tries-to-get-smart-about-artificial-intelligence/; and Asgard and Roland Berger, "The Global Artificial Intelligence Landscape," Asgard, May 14, 2018, https://asgard.vc/global-ai/.

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

[154] Samuel Bendett, "Here's How the Russian Military Is Organizing to Develop AI," *Defense One*, July 20, 2018, https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/.

[155] 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.

[156] Ibid.

[157] 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.

[158] Patrick Tucker, "Russia Says It Will Field a Robot Tank that Outperforms Humans," *Defense One*, November 8, 2017, https://www.defenseone.com/technology/2017/11/russia-robot-tank-outperforms-humans/142376/; and Bendett, "Red Robots Rising."

target identification—and, potentially, target engagement—and plans to develop a suite of AI-enabled autonomous systems.[159]

In addition, the Russian military plans to incorporate AI into uninhabited aerial, naval, and undersea vehicles and is currently developing swarming capabilities.[160] It is also exploring innovative uses of AI for electronic warfare, including adaptive frequency hopping, waveforms, and countermeasures.[161] Finally, Russia has made extensive use of AI technologies for domestic propaganda and surveillance, as well as for information operations directed against the United States and U.S. allies, and can be expected to continue to do so in the future.[162]

Despite Russia's aspirations, analysts argue that it may be difficult for Russia to make significant progress in AI development. In 2017, Russian military spending dropped by 20% in constant dollars, with subsequent cuts forecast in both 2018 and 2019.[163] In addition, many analysts note that Russian academics have produced few research papers on AI and that the Russian technology industry has yet to produce AI applications that are on par with those produced by the United States and China.[164] Others analysts counter that such factors may be irrelevant, arguing that while Russia has never been a leader in internet technology, it has still managed to become a notably disruptive force in cyberspace.[165]

International Institutions

A number of international institutions have examined issues surrounding AI, including the Group of Seven (G7), the Organisation for Economic Co-operation and Development (OECD), and the Asia-Pacific Economic Cooperation (APEC). The U.N. CCW, however, has made the most concerted effort to consider certain military applications of AI, with a particular focus on LAWS. 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 has previously debated weapons such as mines, cluster munitions, and blinding lasers.[166] The CCW began discussions on LAWS in 2014 with informal annual

[159] 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/; and Kyle Mizokami, "Kalashnikov Will Make an A.I.-Powered Killer Robot," Popular Mechanics, July 19, 2017, https://www.popularmechanics.com/military/weapons/news/a27393/kalashnikov-to-make-ai-directed-machine-guns/.

[160] Bendett, "Red Robot Rising."

[161] Dougherty and Jay, "Russia Tries to Get Smart."

[162] Alina Polyakova, "Weapons of the Weak: Russia and AI-driven Asymmetric Warfare," Brookings Institution, November 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/; and Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018, https://foreignpolicy.com/2018/05/25/disinformation-wars/.

[163] "Military expenditure by country, in constant (2016) US$ m., 1988-1997," Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/1_Data%20for%20all%20countries%20from%201988%E2%80%932017%20in%20constant%20%282016%29%20USD.pdf.

[164] 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; and Polyakova, "Weapons of the Weak."

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

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

"Meetings of Experts."[167] In parallel, the International Committee of the Red Cross (ICRC) held similar gatherings of interdisciplinary experts on LAWS that produced reports for the CCW on technical, legal, moral, and humanitarian issues.[168] During the CCW's April 2016 meeting, state parties agreed to establish a formal Group of Governmental Experts (GGE), with an official mandate to "assess questions related to emerging technologies in the area of LAWS."[169] Although the GGE has now convened three times, it has not produced an official definition of LAWS or issued official guidance for their development or use. As a result, one U.S. participant cautioned that the international community is in danger of "the pace of diplomacy falling behind the speed of technological advancement."[170]

AI Opportunities and Challenges

AI poses a number of unique opportunities and challenges within a national security context. However, its ultimate impact will likely be determined by the extent to which developers, with the assistance of policymakers, are able to maximize its strengths while identifying options to limit its vulnerabilities.

Autonomy

Many autonomous systems incorporate AI in some form. Such systems were a central focus of the Obama Administration's "Third Offset Strategy," a framework for preserving the U.S. military's technological edge against global competitors.[171] 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 benefits from autonomous systems by replacing humans in tasks that are "dull, dangerous, or dirty."[172] Specific examples of autonomy in military systems include systems that conduct long-duration intelligence collection and analysis, clean up environments contaminated by chemical weapons, or sweep routes for improvised explosive devices.[173] In these roles, autonomous systems may reduce risk to warfighters and cut costs, providing a range of value to DOD missions, as

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

[168] 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.

[169] "Background on Lethal Autonomous Weapons in the CCW."

[170] 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/.

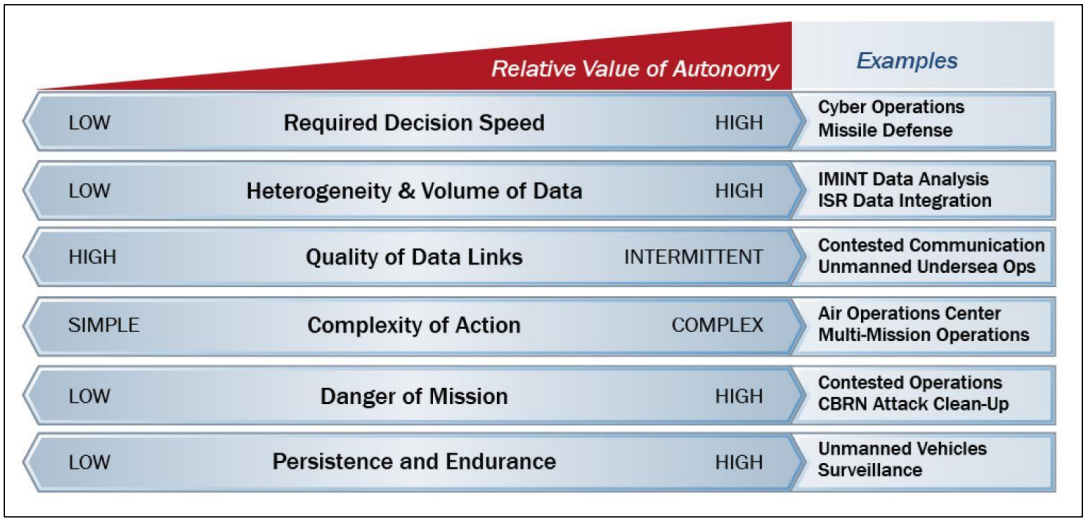
[171] For more information on the Third Offset Strategy, see CRS In Focus IF10790, *What Next for the Third Offset Strategy?*, by Lisa A. Aronsson.

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

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

illustrated in **Figure 3**.[174] Some analysts argue these advantages create a "tactical and strategic necessity" as well as a "moral obligation" to develop autonomous systems.[175]

Figure 3. Value of Autonomy to DOD Missions



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

Speed and Endurance

AI introduces a unique means of operating in combat at the extremes of the time scale. It provides systems with an ability to react at gigahertz speed, which in turn holds the potential to dramatically accelerate the overall pace of combat.[176] As discussed below, some analysts contend that a drastic increase in the pace of combat could be destabilizing—particularly if it exceeds human ability to understand and control events—and could increase a system's destructive potential in the event of a loss of system control.[177] Despite this risk, some argue that speed will confer a definitive warfighting advantage, in turn creating pressures for widespread adoption of military AI applications.[178] In addition, AI systems may provide benefits in long-duration tasks that exceed human endurance. For example, AI systems may enable intelligence gathering across large areas over long periods of time, as well as the ability to autonomously detect anomalies and categorize behavior.[179]

[174] Office of Technical Intelligence, Office of the Assistant Secretary of Defense for Research and Engineering, "Technical Assessment: Autonomy," February 2015, p. 4, https://apps.dtic.mil/dtic/tr/fulltext/u2/a616999.pdf.

[175] 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-military-organization, and CRS discussion with Paul Scharre.

[176] Allen and Chan, p. 24.

[177] Paul Scharre, *Autonomous Weapons and Operational Risk*, Center for a New American Security, February 2016, p. 35.

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

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

Scaling

AI has the potential to provide a force-multiplying effect by enhancing human capabilities and infusing less expensive military systems with increased capability. For example, although an individual low-cost drone may be powerless against a high-tech system like the F-35 stealth fighter, a swarm of such drones could potentially overwhelm high-tech systems, generating significant cost-savings and potentially rendering some current platforms obsolete.[180] AI systems could also increase the productivity of individual servicemembers as the systems take over routine tasks or enable tactics like swarming that require minimal human involvement.[181]

Finally, some analysts caution that the proliferation of AI systems may decouple military power from population size and economic strength. This decoupling may enable smaller countries and nonstate actors to have a disproportionately large impact on the battlefield if they are able to capitalize on the scaling effects of AI.[182]

Information Superiority

AI may offer a means to cope with an exponential increase 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 worth" of high-definition footage each day.[183] However, the department does not have sufficient people or an adequate system to comb through the data in order to derive actionable intelligence analysis.

This issue will likely be exacerbated in the future as data continue 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.[184] AI-powered intelligence systems may provide the ability to integrate and sort through large troves of data from different sources and geographic locations to identify patterns and highlight useful information, significantly improving intelligence analysis.[185] 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 thus hold the potential to bestow a warfighting advantage by improving the quality of information available to decisionmakers.[186]

Predictability

AI algorithms often produce unpredictable and unconventional results. In March 2016, the AI company DeepMind created a game-playing algorithm called AlphaGo, which defeated a world-

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

[181] 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.

[182] Allen and Chan, p. 23.

[183] 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.

[184] 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.

[185] Allen and Chan, p. 27, and Ilachinski, p. 140.

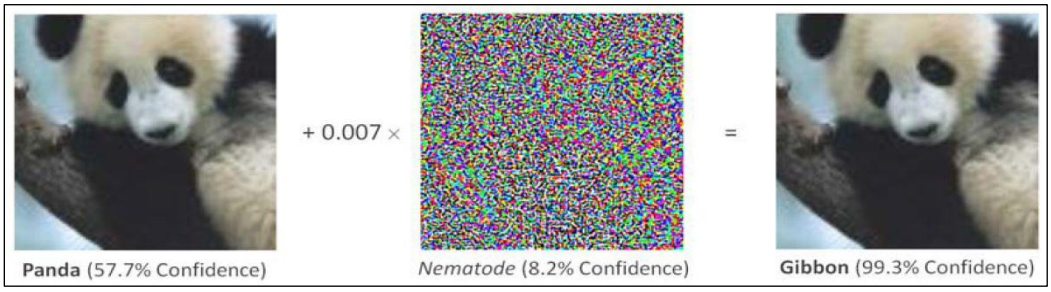
[186] Allen and Chan, p. 32.

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.[187] AI's capacity to produce similarly unconventional results in a military context may provide an advantage in combat, particularly if those results surprise an adversary.

However, AI systems can fail in unexpected ways, with some analysts characterizing their behavior as "brittle and inflexible."[188] Dr. Arati Prabhakar, the former DARPA Director, 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."[189]

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%; however, some commonly cited experiments with these systems demonstrate their capacity for failure.[190] As illustrated in **Figure 4**, researchers combined a picture that an AI system correctly identified as a panda with random distortion that the computer labeled "nematode." The difference in the combined image is imperceptible to human eyes, but the AI system labeled the image as a gibbon with 99.3% confidence.

Figure 4. AI and Image Classifying Errors



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

[187] 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/.

[188] 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, November 2017, p. 24.

[189] 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.

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

In another experiment, an AI system described the picture in **Figure 5** as "a young boy is holding a baseball bat," demonstrating the algorithm's inability to understand context. Some experts warn that AI may be operating with different assumptions about the environment than human operators, who would have little awareness of when the system is outside the boundaries of its original design.[191]

Figure 5. 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.

Similarly, AI systems may be subject to algorithmic bias as a result of their training data. For example, researchers have repeatedly discovered instances of racial bias in AI facial recognition programs due to the lack of diversity in the images on which the systems were trained, while some natural language processing programs have developed gender bias.[192] This could hold significant implications for AI applications in a military context, particularly if such biases remain undetected and are incorporated into systems with lethal effects.

"Domain adaptability," or the ability of AI systems to adjust between two disparate environments, may also present challenges for militaries. For example, one AI system developed to recognize and understand online text was trained primarily on formal language documents like Wikipedia articles. The system was later unable to interpret more informal language in Twitter posts.[193] Domain adaptability failures could occur when systems developed in a civilian environment are transferred to a combat environment.[194]

AI system failures may create a significant risk if the systems are deployed at scale. One analyst noted that although humans are not immune from errors, their mistakes are typically made on an individual basis, and they tend to be different every time. However, AI systems have the potential to fail simultaneously and in the same way, potentially producing large-scale or destructive effects.[195] Other unanticipated results may arise when U.S. AI systems interact with adversary AI systems trained on different data sets with different design parameters and cultural biases.[196]

---

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

[192] Brian Barrett, "Lawmakers Can't Ignore Facial Recognition's Bias Anymore," *Wired*, July 26, 2018, https://www.wired.com/story/amazon-facial-recognition-congress-bias-law-enforcement/; and Will Knight, "How to Fix Silicon Valley's Sexist Algorithms," *MIT Technology Review*, November 23, 2016, https://www.technologyreview.com/s/602950/how-to-fix-silicon-valleys-sexist-algorithms/.

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

[194] 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/.

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

[196] Kania, p. 44.

Analysts warn that if militaries rush to field the technology prior to gaining a comprehensive understanding of potential hazards, they may incur a "technical debt," a term that refers to the effect of fielding AI systems that have minimal risk individually but compounding collective risk due to interactions between systems.[197] This risk could be further exacerbated in the event of an AI arms race.[198]

Explainability

Further complicating issues of predictability, the types of AI algorithms that have the highest performance are currently unable to explain their processes. For example, Google created a cat-identification system, which achieved impressive results in identifying cats on YouTube; however, none of the system's developers were able to determine which traits of a cat the system was using in its identification process.[199] This lack of so-called "explainability" is common across all such AI algorithms. To address this issue, DARPA is conducting a five-year research effort to produce explainable AI tools.[200]

Other research organizations are also attempting to do a backwards analysis of these types of algorithms to gain a better understanding of their internal processes. In one such study, researchers analyzed a program designed to identify curtains and discovered that the AI algorithm first looked for a bed rather than a window, at which point it stopped searching the image. Researchers later learned that this was because most of the images in the training data set that featured curtains were bedrooms.[201] The project demonstrated the possibility that training sets could inadvertently introduce errors into a system that might not be immediately recognized or understood by users.

Explainability can create additional issues in a military context, because the opacity of AI reasoning may cause operators to have either too much or too little confidence in the system. 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 this concern, arguing, "Until AI can show me its homework, it's not a decision quality product."[202] Increasing explainability will thus be key to humans building appropriate levels of trust in AI systems. As a U.S Army study of this issue concludes, only "prudent trust" will confer a competitive advantage for military organizations.[203]

Additional human-machine interaction issues that may be challenged by insufficient explainability in a military context include the following:

---

[197] 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.

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

[199] 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.

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

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

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

[203] 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.

- **Goal Alignment.** The human and the machine must have a common understanding of the objective. As military systems encounter a dynamic environment, the goals will change, and the human and the machine must adjust simultaneously based on a shared picture of the current environment.[204]
- **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.[205]
- **Human Machine Interface.** Due to the requirement for timely decisions in many military AI applications, traditional machine interfaces 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.[206]

Finally, explainability could challenge the military's ability to "verify and validate" AI system performance prior to fielding. 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.[207] 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.[208]

Exploitation

AI systems present unique pathways for adversary exploitation. First, the proliferation of AI systems will increase the number of "hackable things," including systems that carry kinetic energy (e.g., moving vehicles), which may in turn allow exploitive actions to induce lethal effects. These effects could be particularly harmful if an entire class of AI systems all have the same exploitable vulnerability.[209]

In addit ion, AI systems are particularly 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. In contrast, stolen software code can be used immediately and

Figure 6. 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.

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

[205] Ibid.

[206] Ilachinski, p. 187.

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

[208] Ilachinski, p. 204.

[209] Allen and Chan, p. 23.

reproduced at will.[210] This risk is amplified by 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. Indeed, numerous AI tools developed for civilian use—but that could be adapted for use in weapon systems—have been shared widely on unclassified internet sites, making them accessible to major military powers and nonstate actors alike.[211]

Finally, adversaries may be capable of deliberately introducing the kinds of image classification and other errors discussed in the "Predictability" section above. In one such case, researchers who had access to the training data set and algorithm for an image classifier on a semiautonomous vehicle used several pieces of strategically placed tape (as illustrated in **Figure 6**) to cause the system to identify a stop sign as a speed limit sign. In a later research effort, a team at MIT successfully tricked an image classifier into thinking that a picture of machine guns was a helicopter—without access to the system's training data or algorithm.[212] These vulnerabilities highlight the need for robust data security, cybersecurity, and testing and evaluation processes as military AI applications are developed.

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, 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 AI applications, and the development of AI-specific warfighting concepts.[213]

Many experts assert that there is a "sense of inevitability" with AI, arguing that it is bound to be substantially influential.[214] 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 DOD is still 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."[215] 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.

---

[210] Ibid., p. 25.

[211] Amy Nordrum, "Darpa Invites Techies to Turn Off-the-Shelf Products into Weapons in New 'Improv' Challenge," *IEEE Spectrum*, March 11, 2016, https://spectrum.ieee.org/tech-talk/aerospace/military/darpa-invites-techies-to-turn-offtheshelf-products-into-weapons-in-new-improv-challenge.

[212] 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.

[213] "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.

[214] Allen and Chan, p. 50.

[215] 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/.

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.[216] 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.[217] In addition, there is a chance the perceived current inflection point in AI development will instead lead to a plateau. Some experts believe that the present family of algorithms will reach its full potential in another 10 years, and AI development will not be able to proceed without significant leaps in enabling technologies, such as chips with higher power efficiency or advances in quantum computing.[218] The technology has encountered similar roadblocks in the past, resulting in periods called "AI Winters," during which the progress of AI research slowed significantly.

As discussed earlier, the military's willingness to fully embrace AI technology may pose another constraint. Many academic studies on technological innovation argue that military organizations are capable of innovation during wartime, but they characterize the services in peacetime as large, inflexible bureaucracies that are prone to stagnation unless there is a crisis that spurs action.[219] 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."[220]

Another analysis asserts that AI adoption may be halted by poor expectation management. The report asserts that overhyped AI capabilities may cause frustration that will "diminish people's trust and reduce their willingness to use the system in the future."[221] This effect could have a significant chilling effect on AI adoption.

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."[222] These analysts point to

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

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

[218] CRS Discussions with Dr. Dai Kim.

[219] 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).

[220] 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/.

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

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

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 decisionmaking. However, these analysts caution that in the near future AI is unlikely to advance beyond narrow, task-specific applications that require human oversight.[223]

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 emotions that cloud human judgment.[224] However, critics point to the enduring necessity for human presence on the battlefield 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.[225]

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."[226]

In addition, experts highlight that the 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."[227] In other words, military organizations seek to develop technological applications or warfighting concepts that confer an advantage for which their opponent possesses no immediate countermeasure. 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."[228] For this reason, DOD is concerned that if the United States does not increase the pace of AI development and adoption, it will end up with either a symmetrical capability or a capability that bestows only a fleeting advantage, as U.S. competitors like China and Russia accelerate their own respective military AI programs.[229]

The democratization of AI technology will further complicate the U.S. military's pursuit of an AI advantage. As the 2018 National Defense Strategy warns, "The fact that many technological developments will come from the commercial sector means that state competitors and nonstate

---

[223] Ibid., p. 25.

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

[225] 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.

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

[227] 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.

[228] 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.

[229] 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.

actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed."[230] In these circumstances, AI could still influence warfighting methods, but the technology's overall impact may be limited if adversaries possess comparable capabilities.

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."[231] 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."[232]

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."[233] Proponents of this 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 potential ability to facilitate information superiority and "purge combat of uncertainty" will be a decisive wartime advantage, enabling faster and higher-quality decisions.[234] As one study of information era warfare states, "[W]inning in the decision space is winning in the battlespace."[235] 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 will 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 limited number of expensive platforms with exquisite capabilities, instead creating a preference for large numbers of adequate, less expensive systems.[236]

A range of potential consequences flow from the assumptions surrounding AI's impact on warfighting. Some studies point to overwhelmingly positive results, like "near instantaneous responses" to adversary operations, "perfectly coordinated action," and "domination at a time and place of our choosing" that will "consistently overmatch the enemy's capacity to respond."[237]

---

[230] *Summary of the 2018 National Defense Strategy*, p. 3.

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

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

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

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

[235] 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.

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

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

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."[238] In other words, AI systems could accelerate the pace of combat to a point in which machine actions surpass the rate of human decisionmaking, potentially resulting in a loss of human control in warfare.[239]

There is also a possibility that AI systems could induce a state of strategic instability. 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.[240]

Although these forecasts project dramatic change, analysts point out that correctly assessing future impacts may be challenging. 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 has been used in combat.[241]

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 oversight of emerging AI trends. Congressional actions that affect AI funding, acquisitions, norms and standards, and international competition have the potential to significantly shape the trajectory of AI development and may be critical to ensuring that advanced technologies are in place to support U.S. national security objectives and the continued efficacy of the U.S. military.

Author Contact Information

Kelley M. Sayler
Analyst in Advanced Technology and Global Security
[redacted]@crs.loc.gov, 7-....

Acknowledgments

This report was originally written by Daniel S. Hoadley while he was a U.S. Air Force Fellow at the Congressional Research Service. It has been updated by Kelley M. Sayler.

[238] Singer, p. 128.

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

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

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