EYE TO EYE IN AI

Developing Artificial Intelligence for National Security and Defense

Margarita Konaev and Tate Nurkin

EYE TO EYE IN AI

Developing Artificial Intelligence for National Security and Defense

EXECUTIVE SUMMARY

Over the past several years, militaries around the world have increased interest and investment in the development of artificial intelligence (AI) to support a diverse set of defense and national security goals. However, general comprehension of what AI is, how it factors into the strategic competition between the United States and China, and how to optimize the defense-industrial base for this new era of deployed military AI is still lacking. It is now well past time to see *eye to eye* in AI, to establish a shared understanding of modern AI between the policy community and the technical community, and to align perspectives and priorities between the Department of Defense (DoD) and its industry partners. Accordingly, this paper addresses the following core questions.

What is AI and Why Should National Security Policymakers Care?

AI-enabled capabilities hold the potential to deliver game-changing advantages for US national security and defense, including

- greatly accelerated and improved decision-making;
- enhanced military readiness and operational competence;
- heightened human cognitive and physical performance;
- new methods of design, manufacture, and sustainment of military systems;
- novel capabilities that can upset delicate military balances; and
- the ability to create and detect strategic cyberattacks, disinformation campaigns, and influence operations.

Recognition of the indispensable nature of AI as a horizontal enabler of the critical capabilities necessary to deter and win the future fight has gained traction within the DoD, which has made notable investments in AI over the past five years.

But, policymakers beyond the Pentagon—as well as the general public and the firms that are developing AI technologies—require a better understanding of the capabilities and limitations of today's AI, and a clear sense of both the positive and the potentially destabilizing implications of AI for national security.

Why Is AI Essential to Strategic Competition?

The Pentagon's interest in AI must also be seen through the lens of intensifying strategic competition with China—and, to a lesser extent, Russia—with a growing comprehension that falling behind on AI and related emerging technologies could compromise the strategic, technological, and operational advantages retained by the US military since the end of the Cold War. Some defense leaders even argue that the United States has already lost the military-technological competition to China.[1]

While this paper does not subscribe to such a fatalist perspective, it argues that the stakes of the military AI competition are high—and that time is short.

What Are the Obstacles to DoD AI Adoption?

The infamous Pentagon bureaucracy, an antiquated acquisition and contracting system, and a risk-averse organizational culture continue to inhibit the DoD's ability to bring in external innovation and move more rapidly toward widespread AI integration and adoption. Solving systemic problems of this caliber is a tall order. But, important changes are already under way to facilitate DoD engagement with the commercial technology sector and innovative startups, and there seems to be a shared sense of urgency to solidify these public-private partnerships in order to ensure sustained US technological and military advantage. Still, much remains to be done in aligning the DoD's and its industry partners' perspectives about the

---

1   Katrina Manson, "US Has Already Lost AI Fight to China, Says Ex-Pentagon Software Chief," *Financial Times,* October 10, 2021, https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.

most impactful areas for AI development, as well as articulating and implementing common technical standards and testing mechanisms for trustworthy and responsible AI.

Key Takeaways and Recommendations

The DoD must move quickly to transition from a broad recognition of AI's importance to the creation of pathways, processes, practices, and principles that will accelerate adoption of the capabilities enabled by AI technologies. Without intentional, coordinated, and immediate action, the United States risks falling behind competitors in the ability to harness game-winning technologies that will dominate the kinetic and non-kinetic battlefield of the future. This report identifies three courses of action for the DoD that can help ensure the US military retains its global leadership in AI by catalyzing the internal changes necessary for more rapid AI adoption and capitalizing on the vibrant and diverse US innovation ecosystem, including

- prioritizing safe, secure, trusted, and responsible AI development and deployment;

- aligning key priorities for AI development and strengthening coordination between the DoD and industry partners to help close AI capability gaps; and

- promoting coordination between leading defense-technology companies and nontraditional vendors to accelerate DoD AI adoption.

This report is published at a time that is both opportune and uncertain in terms of the future trajectory of the DoD's AI adoption efforts *and* global geopolitics. The ongoing conflict in Ukraine has placed in stark relief the importance of constraining authoritarian impulses to control territory, populations, standards, and narratives, and the role that alliances committed to maintaining long-standing norms of international behavior can play in this effort. As a result, the authors urge the DoD to engage and integrate the United States' allies and trusted partners at governmental and, where possible, industry levels to better implement the three main recommendations of this paper.

INTRODUCTION

AI embodies a significant opportunity for defense policymakers. The ability of AI to process and fuse information, and to distill data into insights that augment decision-making, can lift the "fog of war" in a chaotic, contested environment in which speed is king. AI can also unlock the possibility of new types of attritable and single-use uncrewed systems that can enhance deterrence.[2] It can help safeguard the lives of US service members, for example, by powering the navigation software that guides autonomous resupply trucks in conflict zones.[3] While humans remain in charge of making the final decision on targeting, AI algorithms are increasingly playing a role in helping intelligence professionals identify and track malicious actors, with the aim of "shortening the kill chain and accelerating the speed of decision-making."[4]

AI development and integration are also imperative due to the broader geostrategic context in which the United States operates—particularly the strategic competition with China.[5] The People's Liberation Army (PLA) budget for AI seems to match that of the US military, and the PLA is developing AI technology for a similarly broad set of applications and capabilities, including training and simulation, swarming autonomous systems, and information operations—among many others—all of which could abrogate the US military-technological advantage.[6]

As US Secretary of Defense Lloyd Austin noted in July 2021, "China's leaders have made clear they intend to be globally dominant in AI by the year 2030. Beijing already talks about using AI for a range of missions, from surveillance to cyberattacks to autonomous weapons."[7] The United States cannot afford to fall behind China or other competitors.

To accelerate AI adoption, the Pentagon must confront its demons: a siloed bureaucracy that frustrates efficient data-management efforts and thwarts the technical infrastructure needed to leverage DoD data at scale; antiquated acquisition and contracting processes that inhibit the DoD's ability to bring in external innovation and transition successful AI technology prototypes to production and deployment; and a risk-averse culture at odds with the type of openness, experimentation, and tolerance for failure known to fuel innovation.[8]

Several efforts are under way to tackle some of these problems. Reporting directly to the under secretary of defense, the chief data and artificial intelligence officer (CDAO) role was recently announced to consolidate the office of the chief data officer, the Joint Artificial Intelligence Center (JAIC), and the Defense Digital Service (DDS). This reorganization brings the DoD's data and AI efforts under one roof to deconflict overlapping authorities that have made it difficult to plan and execute AI

2   Yuna Huh Wong, et al., *Deterrence in the Age of Thinking Machines*, *RAND*, 2020. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf.

3   Maureen Thompson, "Utilizing Semi-Autonomous Resupply to Mitigate Risks to Soldiers on the Battlefield," Army Futures Command, October 26, 2021, https://www.army.mil/article/251476/utilizing_semi_autonomous_resupply_to_mitigate_risks_to_soldiers_on_the_battlefield.

4   Amy Hudson, "AI Efforts Gain Momentum as US, Allies and Partners Look to Counter China," *Air Force Magazine*, July 13, 2021, https://www.airforcemag.com/dods-artificial-intelligence-efforts-gain-momentum-as-us-allies-and-partners-look-to-counter-china.

5   On AI and the strategic competition, see: Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, 3 (May 2018), https://repositories.lib.utexas.edu/bitstream/handle/2152/65638/TNSR-Vol-1-Iss-3_Horowitz.pdf; Michael C. Horowitz, et al., "Strategic Competition in an Era of Artificial Intelligence," Center for National Security, July 2018, http://files.cnas.org.s3.amazonaws.com/documents/CNAS-Strategic-Competition-in-an-Era-of-AI-July-2018_v2.pdf.

6   Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, "Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence," Center for Security and Emerging Technology, Georgetown University, October 2021, https://cset.georgetown.edu/publication/harnessed-lightning.

7   C. Todd Lopez, "Ethics Key to AI Development, Austin Says," *DOD News*, July 14, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2692297/ethics-key-to-ai-development-austin-says/.

8   Danielle C. Tarraf, et al., *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*, *RAND*, 2019, https://www.rand.org/pubs/research_reports/RR4229.html.

projects.[9] Expanding use of alternative acquisition methods, organizations like the Defense Innovation Unit (DIU) and the Air Force's AFWERX are bridging the gap with the commercial technology sector, particularly startups and nontraditional vendors. Still, some tech leaders believe these efforts are falling short, warning that "time is running out."[10]

As the DoD shifts toward adoption of AI at scale, this report seeks to provide insights into outstanding questions regarding the nature of modern AI, summarize key advances in China's race toward military AI development, and highlight some of the most compelling AI use cases across the DoD. It also offers a brief assessment of the incongruencies between the DoD and its industry partners, which continue to stymie the Pentagon's access to the game-changing technologies the US military will need to deter adversary aggression and dominate future battlefields.

The urgency of competition, however, must not overshadow the commitment to the moral code that guides the US military as it enters the age of deployed AI. As such, the report reiterates the need to effectively translate the DoD's ethical AI guidelines into common technical standards and evaluation metrics for assessing trustworthiness, and to enhance cooperation and coordination with the DoD's industry partners—especially startups and nontraditional vendors across these critical issues.

We conclude this report with a number of considerations for policymakers and other AI stakeholders across the national security ecosystem. Specifically, we urge the DoD to prioritize safe, secure, trusted, and responsible AI development and deployment, align key priorities for AI development between the DoD and industry to help close the DoD's AI capability gaps, and promote coordination between leading defense technology companies and nontraditional vendors to accelerate the DoD's AI adoption efforts.

---

9   Brian Drake, "A To-Do List for the Pentagon's New AI Chief," *Defense One*, December 14, 2021, https://www.defenseone.com/ideas/2021/12/list-pentagons-new-ai-chief/359757.

10   Valerie Insinna, "Silicon Valley Warns the Pentagon: 'Time Is Running Out,'" Breaking Defense, December 21, 2021, https://breakingdefense.com/2021/12/silicon-valley-warns-the-pentagon-time-is-running-out.

DEFINING AI

Artificial Intelligence, Machine Learning, and Big-Data Analytics

The term "artificial intelligence" encompasses an array of research approaches, techniques, and technologies spread across a wide range of fields, from computer science and engineering to medicine and philosophy.

The 2018 DoD AI Strategy defined AI as "the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action."[11] This ability to execute tasks traditionally thought to be only possible by humans is central to many definitions of AI, although others are less proscriptive. The National Artificial Intelligence Act of 2020 merely describes AI as machine-based systems that can "make predictions, recommendations or decisions" for a given set of human-defined objectives.[12] Others have emphasized rationality, rather than fidelity to human performance, in their definitions of artificial intelligence.[13]

As the list of tasks that computers can perform at human or near-human levels continues to grow, the bar for what is considered "intelligent" rises, and the definition of AI evolves accordingly.[14] The task of optical character recognition (OCR), for instance,

once stood at the leading edge of AI research, but implementations of this technology, such as automated check processing, have long since become routine, and most experts would no longer consider such a system an example of artificial intelligence. This constant evolution of the definition is, in part, responsible for the confusion surrounding modern AI.[15]

This report adopts the Defense Innovation Board's (DIB) definition by considering AI as "a variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason in the pursuit of that task."[16] These techniques, as the DIB explains, can include, but are not limited to, symbolic logic, expert systems, machine learning (ML), and hybrid systems. We use the term "AI" when referring to the broad range of relevant techniques and technologies, and "ML" when dealing with this subset of systems more specifically. For alternative conceptualizations, the 2019 RAND study on the DoD's posture for AI offers a useful sample of relevant definitions put forth by federal, academic, and technical sources.[17]

Much of the progress made in AI over the past decade has come from ML, a modern AI paradigm that differs fundamentally from the human-driven expert systems that dominated in the past. Rather than following a traditional software-development process, in which programs are designed and then coded by human engineers, "machine

11   "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," US Department of Defense, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

12   "Artificial Intelligence," US Department of State, accessed May 4, 2022, https://www.state.gov/artificial-intelligence.

13   Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, Fourth Edition (Hoboken, NJ: Pearson, 2021), 1. For further definitions of AI, see, for example: Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge: Cambridge University Press, 2010); Shane Legg and Marcus Hutter, "A Collection of Definitions of Intelligence," Dalle Molle Institute for Artificial Intelligence, June 15, 2007, https://arxiv.org/pdf/0706.3639.pdf.

14   Robert W. Button, *Artificial Intelligence and the Military*, *RAND*, September 7, 2017, https://www.rand.org/blog/2017/09/artificial-intelligence-and-the-military.html.

15   Ibid.

16   "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense," Defense Innovation Board, October 2019, https://admin.govexec.com/media/dib_ai_principles_-_supporting_document_-_embargoed_copy_(oct_2019).pdf.

17   Danielle C. Tarraf, William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, et al., *The Department of Defense Posture for Artificial Intelligence*.

Figure 1. The progression from, and variance among, big-data analytics, predictive big-data analytics, and machine learning, three terms that are occasionally conflated in discussions of AI.
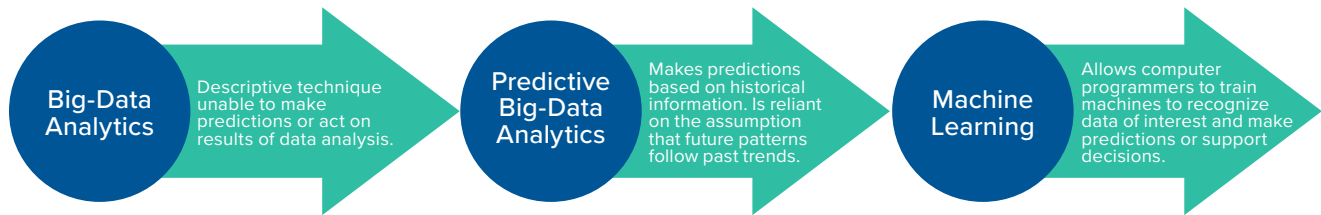
Source: Authors.

learning systems use computing power to execute algorithms that learn from data."[18]

Three elements—algorithms, data, and computing power—are foundational to modern AI technologies, although their relative importance changes depending on particular methods used and, inherently, the trajectory of technological development.

Given that the availability of very large data sets has been critical to the development of ML and AI, it is worth noting that, while the fields of big-data analytics and AI are closely related, there are important differences between the two. Big-data analytics look for patterns, define and structure large sets of data, and attempt to gain insights, but are an essentially descriptive technique unable to make predictions or act on results. Predictive data analytics go a step further, and use collected data to make predictions based on historical information. Such predictive insights have been extremely useful in commercial settings such as marketing or business analytics, but the practice is nonetheless reliant on the assumption that future patterns will follow past trends, and depends on human data analysts to create and test assumptions, query the data, and validate patterns. Machine-learning systems, on the other hand, are able to autonomously generate assumptions, test those assumptions, and learn from them.[19]

ML is, therefore, a subset of AI techniques that have allowed researchers to tackle many problems previously considered impossible, with numerous promising applications across national security and defense, as discussed later in the report.

Limitations of AI

There are, however, important limitations and drawbacks to AI systems—particularly in operational environments—in large part, because of their brittleness. These systems perform well in stable simulation and training settings, but they can struggle to function reliably or correctly if the data inputs change, or if they encounter uncertain or novel situations.

ML systems are also particularly vulnerable to adversarial attacks aimed at the algorithms or data upon which the system relies. Even small changes to data sets or algorithms can cause the system to malfunction, reach wrong conclusions, or fail in other unpredictable ways.[20]

Another challenge is that AI/ML systems do not typically have the capacity to explain their own reasoning, or the processes by which they reach certain conclusions, provide recommendations, and take action, in a way that is evident or understandable to humans. Explainability—or what some have referred to as interpretability—is critical for building trust in human-AI teams, and is especially important as advances in AI enable

18   Ben Buchanan, *"The AI Triad and What It Means for National Security Strategy,"* Center for Security and Emerging Technology, Georgetown University, August 2020, iii, https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy.

19   Ibid.

20   Alexey Kurakin, Ian Goodfellow, and Samy Bengio, "Adversarial Machine Learning at Scale," Arxiv, Cornell University, February 2017, https://arxiv.org/abs/1611.01236.

greater autonomy in weapons, which raises serious ethical and legal concerns about human control, responsibility, and accountability for decisions related to the use of lethal force.

A related set of challenges includes transparency, traceability, and integrity of the data sources, as well as the prevention or detection of adversary attacks on the algorithms of AI-based systems. Having visibility into who trains these systems, what data are used in training, and what goes into an algorithm's recommendations can mitigate unwanted bias and ensure these systems are used appropriately, responsibly, and ethically. All these challenges are inherently linked to the question of trust explored later in the report.

Figure 2. Understanding AI limitations.
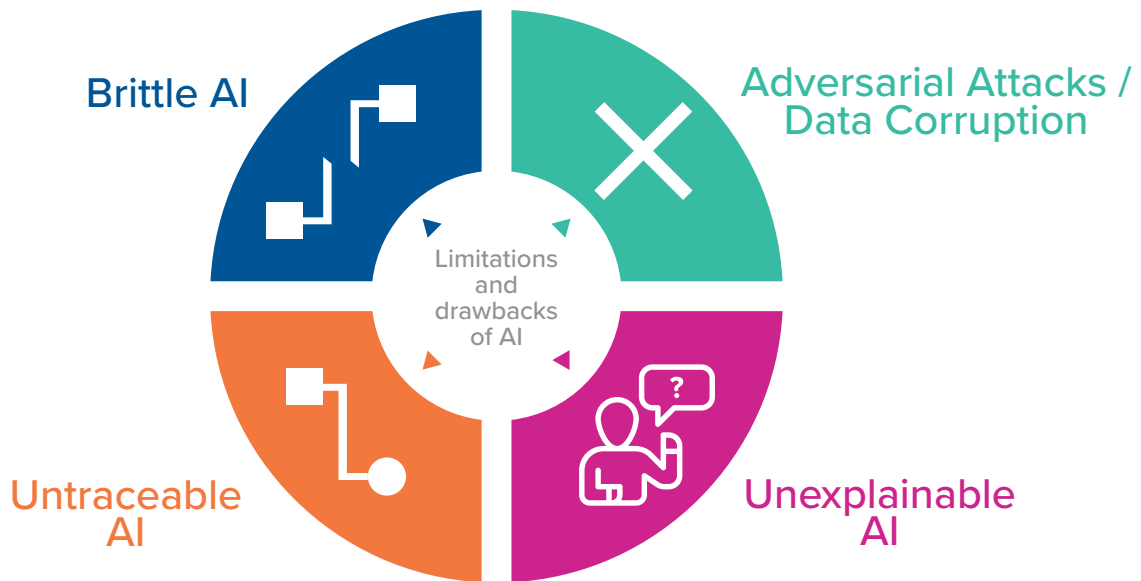
Source: Authors. Lower right icon created by Ranah Pixel Studio.

MILITARY COMPETITION IN AI INNOVATION AND ADOPTION

Much of the urgency driving the DoD's AI development and adoption efforts stems from the need to ensure the United States and its allies outpace China in the military-technological competition that has come to dominate the relationship between the two nations. Russia's technological capabilities are far less developed, but its aggression undermines global security and threatens US and NATO interests.

China

China has prioritized investment in AI for both defense and national security as part of its efforts to become a "world class military" and to gain advantage in future "intelligentized" warfare—in which AI (alongside other emerging technologies) is more completely integrated into military systems and operations through "networked, intelligent, and autonomous systems and equipment."[21]

While the full scope of China's AI-related activities is not widely known, an October 2021 review of three hundred and forty-three AI-related Chinese military contracts by the Center for Security and Emerging Technology (CSET) estimates that PLA "spends more than $1.6 billion each year on AI-related systems and equipment."[22] The National Security Commission on Artificial Intelligence's (NSCAI) final report assessed that "China's plans, resources, and progress should concern all Americans. It is an AI peer in many areas and an AI leader in some applications."[23]

CSET's review and other open-source assessments reveal that China's focus areas for AI development, like those of the United States, are broad, and include[24]

- intelligent and autonomous vehicles, with a particular focus on swarming technologies;

- intelligence, surveillance, and reconnaissance (ISR);
- predictive maintenance and logistics;
- information, cyber, and electronic warfare;
- simulation and training (to include wargaming);
- command and control (C2); and
- automated target recognition.

Progress in each of these areas constitutes a challenge to the United States' capacity to keep pace in a military-technological competition with China. However, it is worth examining China's advancing capabilities in two areas that could have a particularly potent effect on the military balance.

Integration

First, AI can help the PLA bridge gaps in operational readiness by artificially enhancing military integration and cross-domain operations. Many observers have pointed to the PLA's lack of operational experience in conflict as a critical vulnerability. As impressive as China's advancing military modernization has been from a technological perspective, none of the PLA's personnel have been tested under fire in a high-end conflict in the same ways as the US military over the last twenty years. The PLA's continuing efforts to increase its "jointness" from an organizational and doctrinal standpoint is also nascent and untested.

The use of AI to improve the quality, fidelity, and complexity of simulations and wargames is one way the PLA is redressing this area of concern. A 2019 report by the Center for a New American Security observed that "[for] Chinese military strategists, among the lessons learned from AlphaGo's victory was the fact that an AI could create tactics and stratagems superior to those of a human player in a game that can be compared to a wargame"

---

21 Fedasiuk, Melot, and Murphy, "Harnessed Lightning," 4.

22 Ibid., iv.

23 "Final Report," National Security Commission on AI, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

24 Fedasiuk, Melot, and Murphy, "Harnessed Lightning," 13.
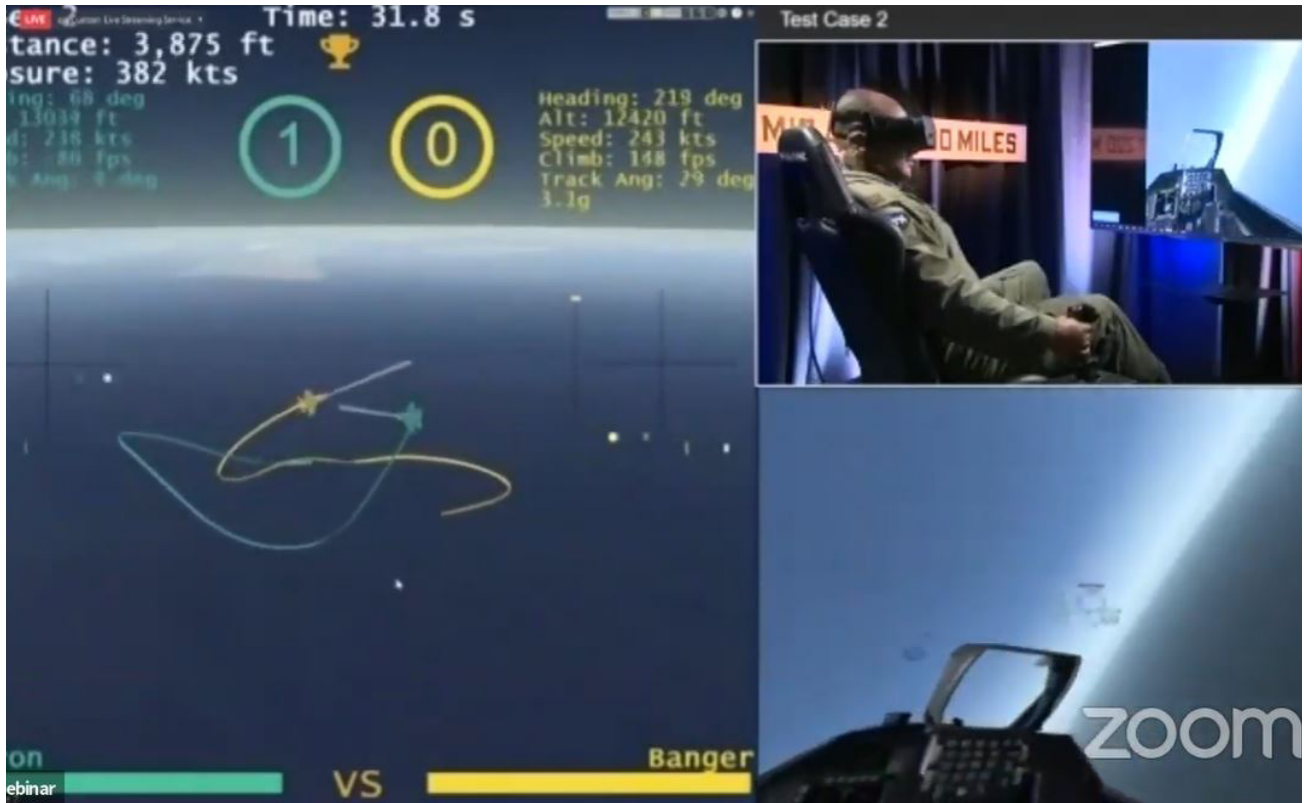
During the Defense Advanced Research Projects Agency's (DAPRA)'s AlphaDogfight Trials, an operational F-16 pilot flies in a virtual reality simulator against the champion F-16 AI agent developed by Heron Systems. The Heron AI agent defeated the human pilot in five straight dogfights to conclude the trials. *Source*: DARPA, https://www.darpa.mil/news-events/2020-08-26.

that can more arduously test PLA decision-makers and improve upon command decision-making.[25] In fact, the CSET report found that six percent of the three hundred and forty-three contracts surveyed were for the use of AI in simulation and training, including use of AI systems to wargame a Taiwan contingency.[26]

The focus on AI integration to reduce perceived vulnerabilities in experience also applies to operational and tactical training. In July 2021, the Chinese Communist Party mouthpiece publication *Global Times* reported that the PLA Air Force (PLAAF) has started to deploy AI as simulated opponents in pilots' aerial combat training to "hone their decision-making and combat skills against fast-calculating computers."[27]

Alongside virtual simulations, China is also aiming to use AI to support pilot training in real-world aircraft. In a China Central Television (CCTV) program that aired in November 2020, Zhang Hong, the chief designer of China's L-15 trainer, noted that AI onboard training aircraft can "identify different habits each pilot has in flying. By managing them, we will let the pilots grow more safely and gain more combat capabilities in the future."[28]

Notably, the PLAAF's July 2021 AI–human dogfight was similar to the Defense Advanced Research Projects Agency's (DARPA) September 2020

---

25 Elsa Kania, "Learning Without Fighting: New Developments in PLA Artificial Intelligence War-Gaming," Jamestown Foundation, China Brief, 19, 7 (2019), https://jamestown.org/program/learning-without-fighting-new-developments-in-pla-artificial-intelligence-war-gaming.

26 Fedasiuk, Melot, and Murphy, "Harnessed Lightning," 22–23.

27 Liu Xuanzun, "PLA Deploys AI in Mock Warplane Battles, 'Trains Both Pilots and Ais,'" *Global Times,* June 14, 2021, https://www.globaltimes.cn/page/202106/1226131.shtml.

28 Liu Xuanzun, "China's Future Fighter Trainer Could Feature AI to Boost Pilot's Combat Capability: Top Designer," *Global Times,* November 16, 2020, http://en.people.cn/n3/2020/1116/c90000-9780437.html.

AlphaDogFight Challenge in which an AI agent defeated a human pilot in a series of five simulated dogfights.[29] Similarly, the United States announced in September 2021 the award of a contract to training-and-simulation company Red 6 to integrate the company's Airborne Tactical Augmented Reality System (ATARS)—which allows a pilot flying a real-world plane to train against AI-generated virtual aircraft using an augmented-reality headset—into the T-38 Talon trainer with plans to eventually install the system in fourth-generation aircraft.[30] AI-enabled training and simulation are, therefore, key areas in which the US military is in a direct competition with the PLA. As the Chinese military is leveraging AI to enhance readiness, the DoD cannot afford to fall behind.

Autonomy

A second area of focus for Chinese AI development is in autonomous systems, especially swarming technologies, in which several systems will operate independently or in conjunction with one another to confuse and overwhelm opponent defensive systems. China's interests in, and capacity for, developing swarm technologies has been well demonstrated, including the then record-setting launch of one hundred and eighteen small drones in a connected swarm in June 2017.[31]

In September 2020, China Academy of Electronics and Information Technology (CAEIT) reportedly launched a swarm of two hundred fixed-wing CH-901 loitering munitions from a modified Dongfeng Mengshi light tactical vehicle.[32] A survey of the Unmanned Exhibition 2022 show in Abu Dhabi in February 2022 revealed not only a strong Chinese presence—both China National Aero-Technology Import and Export Corporation (CATIC) and China North Industries Corporation (NORINCO) had large pavilions—but also a focus on "collaborative" operations and intelligent swarming.[33]

An example of collaborative swarming drones on display at the UMEX 2022 exhibition in Abu Dhabi in February. *Source*: Tate Nurkin.

This interest in swarming is not limited to uncrewed aerial vehicles (UAVs). China is also developing the ability to deploy swarms of autonomous uncrewed surface vehicles (USVs) to "intercept, besiege and expel invasive targets," according to the *Global Times*.[34] In November 2021, Chinese company Yunzhou Tech—which in 2018 carried out a demonstration of a swarm of fifty-six USVs—released a video showing six USVs engaging in a "cooperative confrontation" as part of an effort to remove a crewed vessel from Chinese waters.[35] It is not difficult to imagine how such cooperative confrontation could be deployed against US or allied naval vessels, or even commercial ships, to develop or maintain sea control. This capability is especially powerful in a gray-zone contingency in which escalation concerns may limit response options.

Russia

Russia lags behind the United States and China in terms of investments and capabilities in AI. The sanctions imposed over the war in Ukraine are also likely to take a massive toll on Russia's science and

29   Joseph Trevithick, "Chinese Pilots Are Also Dueling With AI Opponents in Simulated Dogfights and Losing: Report," *Drive,* June 18, 2021, https://www.thedrive.com/the-war-zone/41152/chinese-pilots-are-also-dueling-with-ai-opponents-in-simulated-dogfights-and-losing-report.

30   "Red 6 to Continue Support ATARS Integration into USAF T-38 Talon," Air Force Technology, February 3, 2022, https://www.airforce-technology.com/news/red-6-atars-integration.

31   Xiang Bo, "China Launches Record Breaking Drone Swarm," XinhuaNet, June 11, 2017, http://www.xinhuanet.com/english/2017-06/11/c_136356850.htm.

32   David Hambling, "China Releases Video Of New Barrage Swarm Drone Launcher," *Forbes,* October 14, 2020, https://www.forbes.com/sites/davidhambling/2020/10/14/china-releases-video-of-new-barrage-swarm-drone-launcher/?sh=29b76fa12ad7.

33   An author of this paper attended the exhibition.

34   Cao Siqi, "Unmanned High-Speed Vessel Achieves Breakthrough in Dynamic Cooperative Confrontation Technology: Developer," *Global Times,* November 28, 2021, https://www.globaltimes.cn/page/202111/1240135.shtml.

35   Ibid.

technology sector. That said, US national decision-makers should not discount Russia's potential to use AI-enabled technologies in asymmetric ways to undermine US and NATO interests. The Russian Ministry of Defense has numerous autonomy and AI-related programs at different stages of development and experimentation related to military robotics, unmanned systems, swarming technology, early-warning and air-defense systems, ISR, C2, logistics, electronic warfare, and information operations.[36]

Russian military strategists see immense potential in greater autonomy and AI on future battlefields to speed up information processing, augment decision-making, enhance situational awareness, and safeguard the lives of Russian military personnel. The development and use of autonomous and AI-enabled systems are also discussed within the broader context of Russia's military doctrine. Its doctrinal focus is on employing these technologies to disrupt and destroy the adversary's command-and-control systems and communication capabilities, and use non-military means to establish information superiority during the initial period of war, which, from Russia's perspective, encompasses periods of non-kinetic conflict with adversaries like the United States and NATO.[37]

The trajectory of Russia's AI development is uncertain. But, with continued sanctions, it is likely Russia will become increasingly dependent on China for microelectronics and fall further behind in the technological competition with the United States.

36   Jeffrey Edmonds, et al., "Artificial Intelligence and Autonomy in Russa," CNA, May 2021, https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf.

37   "Advanced Military Technology in Russia," Chatham House, September 2021, https://www.chathamhouse.org/2021/09/advanced-military-technology-russia/06-military-applications-artificial-intelligence.

OVERVIEW OF US MILITARY PROGRESS IN AI

The Pentagon's interest and urgency related to AI is due both to the accelerating pace of development of technology and, increasingly, the transformative capabilities it can enable. Indeed, AI is poised to fundamentally alter how militaries think about, prepare for, carry out, and sustain operations. Drawing on a previous Atlantic Council report outline, the "Five Revolutions" framework for classifying the potential impact of AI across five broad capability areas, Figure 3 below illustrates the different ways in which AI could augment human cognitive and physical capabilities, fuse networks and systems for optimal efficiency and performance, and usher in a new era of cyber conflict and chaos in the information space, among other effects.[38]

The DoD currently has more than six hundred AI-related efforts in progress, with a vision to integrate AI into every element of the DoD's mission—from warfighting operations to support and sustainment functions to the business operations and processes that undergird the vast DoD enterprise.[39] A February 2022 report by the US Government Accountability Office (GAO) has found that the DoD is pursuing AI capabilities for warfighting that predominantly focus on "(1) recognizing targets through intelligence and surveillance analysis, (2) providing recommendations to operators on the battlefield (such as where to move troops or which weapon is best positioned to respond to a threat), and (3) increasing the autonomy of uncrewed systems."[40] Most of the DoD's AI capabilities, especially the efforts related to warfighting, are still in development, and not yet aligned with or integrated into specific systems. And, despite notable progress in experimentation and some experience

with deploying AI-enabled capabilities in combat operations, there are still significant challenges ahead for wide-scale adoption.

In September 2021, the Air Force's first chief software officer, Nicolas Chaillan, resigned in protest of the bureaucratic and cultural challenges that have slowed technology adoption and hindered the DoD from moving fast enough to effectively compete with China. In Chaillan's view, in twenty years, the United States and its allies "will have no chance competing in a world where China has the drastic advantage in population."[41] Later, he added that China has essentially already won, saying, "Right now, it's already a done deal."[42]

Chaillan's assessment of the United States engaged in a futile competition with China is certainly not shared across the DoD, but it reflects what many see as a lack of urgency within the risk-averse and ponderous culture of the department.

Lt. General Michael Groen, the head of the JAIC, agreed that "inside the department, there is a cultural change that has to occur."[43] However, he also touted the innovative capacity of the United States and highlighted the establishment of an AI accelerator and the finalization of a Joint Common Foundation (JCF) for AI development, testing, and sharing of AI tools across DoD entities.[44] The cloud-enabled JCF is an important step forward that will allow for AI development based on common standards and architectures. This should help encourage sharing between the military services and DoD components and, according to the JAIC, ensure that "progress by one DoD AI initiative

38   Tate Nurkin, *The Five Revolutions: Examining Defense Innovation in the Indo-Pacific, Atlantic Council*, November 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-five-revolutions-examining-defense-innovation-in-the-indo-pacific-region.

39   Hudson, "AI Efforts Gain Momentum as US, Allies and Partners Look to Counter China."

40   "Artificial Intelligence: Status of Developing and Acquiring," US Government Accountability Office, February 2022, 17.https://www.gao.gov/assets/gao-22-104765.pdf.

41   Nicolas Chaillan, "Its Time to Say Goodbye," LinkedIn, September 2, 2021, https://www.linkedin.com/pulse/time-say-goodbye-nicolas-m-chaillan.

42   Manson, "US Has Already Lost AI Fight to China, Says Ex-Pentagon Software Chief."

43   Patrick Tucker, "Pentagon AI Chief Responds to USAF Software Leader Who Quit in Frustration," *Defense One*, October 26, 2021, https://www.defenseone.com/technology/2021/10/pentagon-ai-chief-responds-usaf-software-leader-who-quit-frustration/186368.

44   Ibid.

Figure 3: High-level overview of priority AI development programs across five broad objectives for the development of future military capabilities.

Toward Perfect Situational Awareness: Perception, Processing, and Cognition

- Speeding up processing, integration, and visualization of large and complex datasets to improve situational awareness and decision-making
- Predictive analysis to anticipate likely contingencies or crises or pandemic outbreaks

The Impending Design Age: Manufacturing, Supply Chain, and Logistics

- Enabling digital engineering, advanced manufacturing, and new supply chain management tools to speed up and reduce costs associated with defense production
- Predictive maintenance to enhance platform and system readiness and increase efficiency of sustainment

Hyper-Enabled Platforms and People: Human and Machine Performance Enhancement

- Improving and making training more accessible and less costly and also improving the complexity and fidelity of simulations and wargaming
- Enhancing cognitive and physical capacities of humans
- Human-machine teaming and symbiosis, including brain-computer interfaces and AI agents performing mundane tasks to allow humans to focus on mission management

Connectivity, Lethality, and Flexibility: Communication, Navigation, Targeting, and Strike

- Cognitive sensing, spectrum management, threat detection and categorization, cognitive electronic warfare
- Autonomous systems
- AI enabled or supported targeting
- Swarms

Monitoring, Manipulation, and Weaponization: Cyber and Information Operations

- Detecting and defending against cyber attacks and disinformation campaigns
- Offensive cyber and information operations
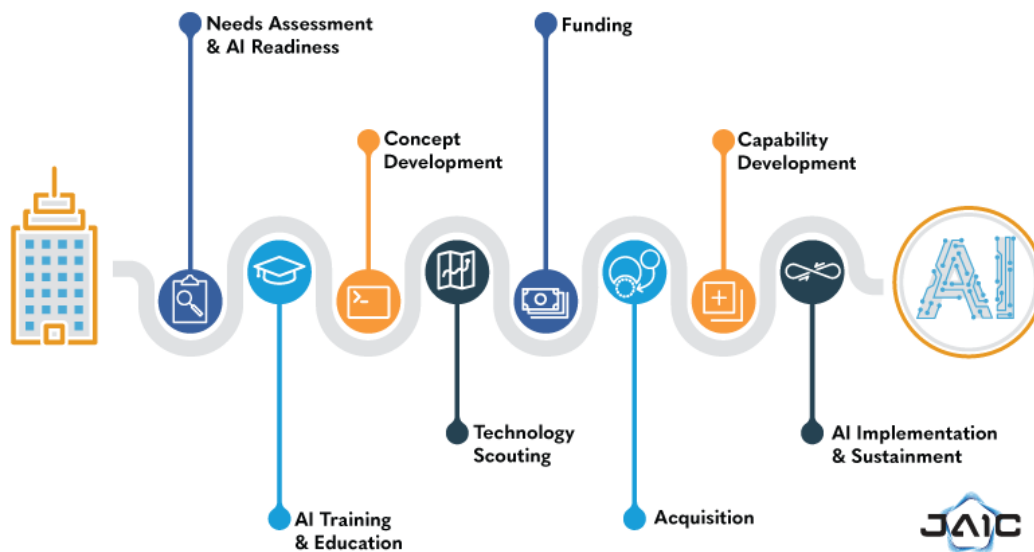
Source: Authors.

will build momentum across the entire DoD enterprise."[45]

While progress should be commended, obstacles remain that are slowing the adoption of AI capabilities critical to deterring threats in the near future, and to meeting China's competitive challenges in this decade and beyond.

The three case studies below provide examples of the technological, bureaucratic, and adoption advancements that have occurred in DoD AI efforts. These cases also highlight the enduring issues hindering the United States' ability to bring its national innovation ecosystem fully to bear in the intensifying military-technological competition with China and, to a lesser extent, Russia.

---

45 "AI Adoption Journey," Joint Artificial Intelligence Center, https://www.ai.mil/#:~:text=The%20JAIC's%20Joint%20Common%20Foundation%20%28JCF%29%20is%20a,will%20build%20momentum%20across%20the%20entire%20DoD%20enterprise.

Figure 4: The stages of the Joint Artificial Intelligence Center's (JAIC's) AI adoption journey.

Source: JAIC, https://www.ai.mil/.

Use Case 1: The Irreversible Momentum, Grand Ambition, and Integration Challenges of JADC2

Among the Pentagon's most important modernization priorities is the Joint All-Domain Command and Control (JADC2) program, described as a "concept to connect sensors from all the military services…into a single network."[46] According to the Congressional Research Service, "JADC2 intends to enable commanders to make better decisions by collecting data from numerous sensors, processing the data using AI algorithms to identify targets, then recommending the optimal weapon—both kinetic and non-kinetic—to engage the target."[47] If successful, JADC2 holds the potential to eliminate silos between service C2 networks that previously slowed the transfer of relevant information across the force and, as a result, generate more comprehensive situational awareness upon which commanders can make better and faster decisions.

AI is essential to this effort, and the DoD is exploring how best to safely integrate it into the JADC2 program.[48] In December 2021, reports emerged that the JADC2 cross-functional team (CTF) would start up an "AI for C2" working group, which will examine how to leverage responsible AI to enhance and accelerate command and control, reinforcing the centrality of responsible AI to the project.[49]

In March 2022, the DoD released an unclassified version of its JADC2 Implementation Plan, a move that represented, in the words of General Mark Milley, chairman of the Joint Chiefs of Staff, "irreversible momentum toward implementing" JADC2.[50]

However, observers have highlighted several persistent challenges to implementing JADC2 along the urgent timelines required to maintain (or regain)

---

46 Jackson Bennett, "2021 in Review: JADC2 Has Irreversible Momentum, but What Does That Mean?" FedScoop, December 29, 2021, https://www.fedscoop.com/2021-in-review-jadc2-has-irreversible-momentum.
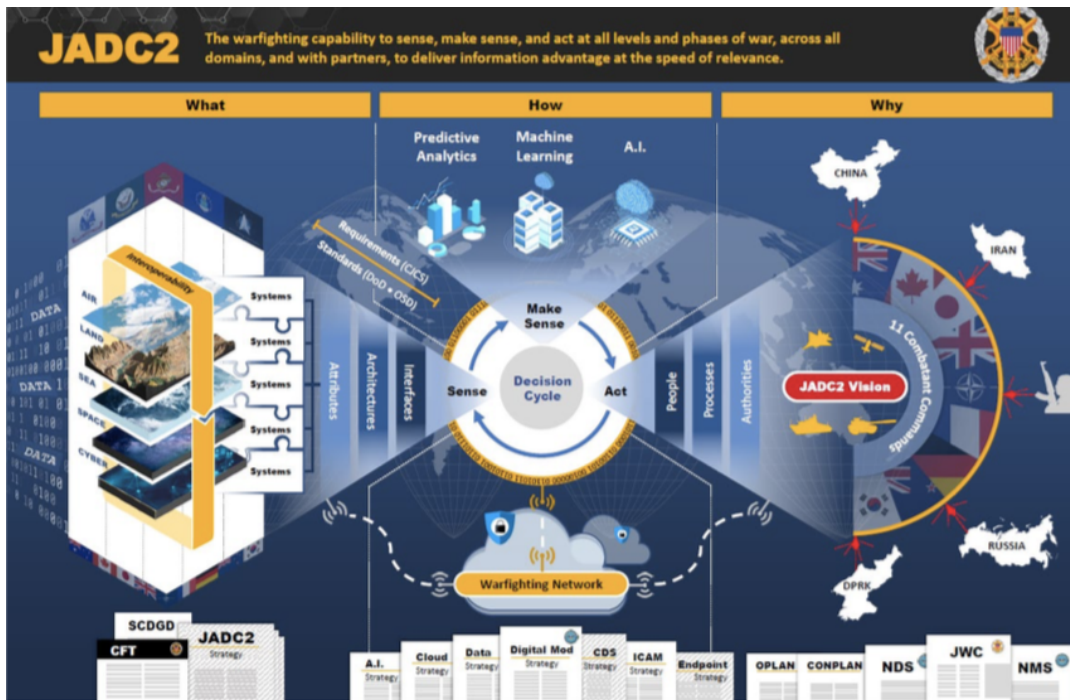
47 "Joint All-Domain Command and Control (JADC2) In Focus Briefing," Congressional Research Service, January 21, 2022.

48 Ibid.

49 Jackson Bennett, "JADC2 Cross Functional Team to Stand Up AI-Focused Working Group," FedScoop, December 16, 2021, https://www.fedscoop.com/jadc2-cft-stands-up-ai-working-group.

50 "DoD Announces Release of JADC2 Implementation Plan," US Department of Defense, press release, March 17, 2022, https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan.

Figure 5. The JADC2 Placemat reflects the complexity and ambition associated with the Department of Defense's JADC2 Implementation Plan. Source:

Source: US Department of Defense. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

advantage in perception, processing, and cognition, especially vis-à-vis China.

Data security and cybersecurity, data-governance and sharing issues, interoperability with allies, and issues associated with integrating the service's networks have all been cited as challenges with recognizing the ambitious promise of JADC2's approach. Some have also highlighted that all-encompassing ambition as a challenge as well. The Hudson Institute's Bryan Clark and Dan Patt argue that "the urgency of today's threats and the opportunities emerging from new technologies demand that Pentagon leaders flip JADC2's focus from what the US military services want to what warfighters need."[51]

To be sure, grand ambition is not necessarily something to be avoided in AI development and integration programs. However, pathways to

adoption will need to balance difficult-to-achieve, bureaucratically entrenched, time-consuming, and expensive objectives with developing systems that can deliver capability and advantage along the more immediate threat timelines facing US forces.

Use Case 2: Brittle AI and the Ethics and Safety Challenges of Integrating AI into Targeting

Demonstrating that the age of deployed AI is indeed here, in September 2021 Secretary of the Air Force Frank Kendall announced that the Air Force had "deployed AI algorithms for the first time to a live operational kill chain."[52] According to Kendall, the objective of incorporating AI into the targeting process is to "significantly reduce the manpower-intensive tasks of manually identifying targets—shortening the kill chain and accelerating the speed

---

51 Bryan Clark and Dan Patt, "The Pentagon Should Focus JADC2 on Warfighters, Not Service Equities," Breaking Defense, March 30, 2022, https://breakingdefense.com/2022/03/the-pentagon-should-focus-jadc2-on-warfighters-not-service-equities.

52 Amanda Miller, "AI Algorithms Deployed in Kill Chain Target Recognition," *Air Force Magazine,* September 21, 2021, https://www.airforcemag.com/ai-algorithms-deployed-in-kill-chain-target-recognition.

of decision-making."[53] The successful use of AI to support targeting constitutes a milestone for AI development, though there remain ethical, safety, and technical challenges to more complete adoption of AI in this role.

For example, a 2021 DoD test highlighted the problem of brittle AI. According to reporting from *Defense One,* the AI-enabled targeting used in the test was accurate only about 25 percent of the time in environments in which the AI had to decipher data from different angles—though it believed it was accurate 90 percent of the time—revealing a lack of ability "to adapt to conditions outside of a narrow set of assumptions."[54] These results illustrate the limitations of today's AI technology in security-critical settings, and reinforce the need for aggressive and extensive real-world and digital-world testing and evaluation of AI under a range of conditions.

The ethics and safety of AI targeting could also constitute a challenge to further adoption, especially as confidence in AI algorithms grows. The Air Force operation involved automated target recognition in a supporting role, assisting "intelligence professionals"—i.e., human decision-makers.[55] Of course, DoD has a rigorous targeting procedure in place, of which AI-enabled targeting algorithms would be a part, and that, thinking further ahead, autonomous systems would have to go through. Still, even as they are part of this process and designed to support human decisions, a high error rate combined with a high level of confidence in AI outputs could potentially lead to undesirable or grave outcomes.

Use Case 3: The Limits of AI Adoption in the Information Domain

Intensifying competition with China and Russia is increasingly playing out in the information and cyber domains with real, enduring, and disruptive implications for US security, as well as the US economy, society, and polity.

For cyber and information operations, AI technologies and techniques are central to the future of both offensive and defensive operations, highlighting both the peril and promise of AI in the information domain.

Concern is growing about the threat of smart bots, synthetic media such as deepfakes—realistic video or audio productions that depict events or statements that did not take place—and large-language models that can create convincing prose and text.[56] And, these are just the emerging AI-enabled disinformation weapons that can be conceived of today. While disinformation is a challenge that requires a societal and whole-of-government response, DoD will undoubtably play a key role in managing and responding to this threat—due to its prominence in US politics and society, the nature of its functional role, and the impact of its ongoing activities.

AI is at the forefront of Pentagon and other US government efforts to detect bots and synthetic media. DARPA's MediaForensics (MediFor) program is using AI algorithms to "automatically quantify the integrity of an image or video," for example.[57]

Still, there is concern about the pace at which this detection happens, given the speed of diffusion of synthetic media via social media. As Lt. General Dennis Crall, the Joint Staff's chief information officer, observed, "the speed at which machines and AI won some of these information campaigns changes the game for us…digital transformation, predictive analytics, ML, AI, they are changing the game…and if we don't match that speed, we will make it to the right answer and that the right answer will be completely irrelevant."[58]

---

53   Ibid.

54   Patrick Tucker, "Air Force Targeting AI Thought It Had a 90% Success Rate. It Was More Like 25%," *Defense One,* December 9, 2021, https://www.defenseone.com/technology/2021/12/air-force-targeting-ai-thought-it-had-90-success-rate-it-was-more-25/187437.

55   Miller, "AI Algorithms Deployed in Kill Chain Target Recognition."

56   Alex Tamkin and Deep Ganguli, "How Large Language Models Will Transform Science, Society, and AI", Stanford University Human-Centered Artificial Intelligence, February 21, 2021, https://hai.stanford.edu/news/how-large-language-models-will-transform-science-society-and-ai.

57   Matt Turek, "Media Forensics (MediFor)," Defense Advanced Research Projects Agency, accessed May 4, 2022, https://www.darpa.mil/program/media-forensics.

58   Patrick Tucker, "Joint Chiefs' Information Officer: US is Behind on Information Warfare. AI Can Help," *Defense One,* November 5, 2021, https://www.defenseone.com/technology/2021/11/joint-chiefs-information-officer-us-behind-information-warfare-ai-can-help/186670.

ACCELERATING DOD AI ADOPTION

As the discussion above illustrates, the DoD has a broad set of AI-related initiatives across different stages of development and experimentation, building on the successful deployment of AI-enabled information-management and decision-support tools. As the focus shifts toward integration and scaling, accelerating these adoption efforts is critical for maintaining US advantage in the strategic competition against China, as well as effectively containing Russia.

In this section, the paper highlights some of the incongruencies in the relationship between the DoD and its industry partners that may cause lost opportunities for innovative and impactful AI projects, the positive impact of expanding the use of alternative acquisition methods, and the growing urgency to align processes and timelines to ensure that the US military has access to high-caliber technological capabilities for future warfare. Additionally, this section discusses the DoD's approach to implementing ethical AI principles, and issues related to standards and testing of trusted and responsible systems.

DoD and Industry Partnerships: Aligning Perspectives, Processes, and Timelines

Although the DoD has issued a number of high-level documents outlining priority areas for AI development and deployment, the market's ability to meet, or even understand, these needs is far from perfect. A recent IBM survey of two hundred and fifty technology leaders from global defense organizations reveals some important differences in how defense-technology leaders and the DoD view the value of AI for the organization and the

mission.[59] For instance, only about one-third of the technology leaders surveyed said they see significant potential value in AI for military logistics, medical and health services, and information operations and deepfakes. When asked about the potential value of AI-enabled solutions to business and other noncombat applications, less than one-third mentioned maintenance, procurement, and human resources.[60]

These views are somewhat incongruent with the DoD's goals in AI. For example, military logistics and sustainment functions that encompass equipment maintenance and procurement are among the top DoD priorities for implementing AI. Leidos' work with the Department of Veterans Affairs also illustrates the potential of AI in medical and health services.[61] Finally, with the use of AI in disinformation campaigns already under way, and as the discussion in the previous section highlights, there is an urgent need to develop technical measures and AI-enabled tools for detecting and countering AI-powered information operations.[62]

The DoD and its industry partners have different priorities and incentives based on their respective problem sets and missions. But, divergent perspectives on valuable and critical areas for AI development could result in lost opportunities for impactful AI projects. That said, even when the Pentagon and its industry partners see eye to eye on AI, effective collaboration is often thwarted by a clumsy bureaucracy that is too often tethered to legacy processes, structures, and cultures.

The DoD's budget planning, procurement, acquisition, and contracting processes are, by and large, not designed for buying software. These

---

59   "Deploying AI in Defense Organizations: The Value, Trends, and Opportunities," IBM, May 2021, https://www.ibm.com/downloads/cas/EJBREOMX.

60   Ibid.

61   Authors' interview with a defense technology industry executive.

62   Katerina Sedova, et al., "AI and the Future of Disinformation Campaigns, Part 1: The RICHDATA Framework," Center for Security and Emerging Technology, Georgetown University, December 2021, https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/; Katerina Sedova et.al, "AI and the Future of Disinformation Campaigns, Part 2: A Threat Model, Center for Security and Emerging Technology," Center for Security and Emerging Technology, Georgetown University, December 2021, 1. https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Disinformation-Campaigns-Part-2.pdf; Ben Buchanan, et al., "Truth, Lies, and Automation: How Language Models Could Change Disinformation," Center for Security and Emerging Technology, Georgetown University, May 2021. https://cset.georgetown.edu/publication/truth-lies-and-automation.

institutional barriers, coupled with the complex and protracted software-development and compliance regulations, are particularly hard on small startups and nontraditional vendors that lack the resources, personnel, and prior knowledge required to navigate the system in the same way that defense primes do.[63]

The DoD is well aware of these challenges. Since 2015, the Office of the Secretary of Defense and the military services have set up several entities—such as DIU, AFWERX, NavalX, and Army Applications Laboratory—to interface with the commercial technology sector, especially startups and nontraditional vendors, with the aim of accelerating the delivery of best-in-class technology solutions. Concurrently, the DoD has taken other notable steps to promote the use of alternative authorities for acquisition and contracting, which provide greater flexibility to structure and execute agreements than traditional procurement.[64] These include "other transaction authorities, middle-tier acquisitions, rapid prototyping and rapid fielding, and specialized pathways for software acquisition."[65]

The DIU has been at the forefront of using some of these alternative acquisition pathways to source AI solutions from the commercial technology sector. The Air Force's AFWERX has also partnered with the Air Force Research Lab and the National Security Innovation Network to make innovative use of the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) funding to "increase the efficiency, effectiveness, and transition rate" of programs.[66] In June 2021, for instance, the USAF SBIR/STTR AI Pitch Day awarded more than $18 million to proposals on the topic of "trusted artificial intelligence, which indicates systems are safe, secure, robust, capable, and effective."[67]

These are steps in the right direction, and it has indeed become easier to receive DoD funding for research, development, and prototyping. Securing timely funding for production, however, remains a major challenge. This "valley of death" problem—the gap between the research-and-development phase and an established, funded program of record—is particularly severe for nontraditional defense firms, because of the disparity between venture-capital funding cycles for startups and how long it takes to get a program into the DoD budget.[68]

The Pentagon understands that bridging the "valley of death" is crucial for advancing and scaling innovation, and has recently launched the Rapid Defense Experimentation Reserve to deal with these issues.[69] Still, the systematic changes necessary to align budget planning, acquisition, and contracting processes with the pace of private capital require congressional action and could take years to implement. Delays in implementing such reforms are undermining the DoD's ability to access cutting-edge technology that could prove essential on future battlefields.

Building Trusted and Responsible AI Systems

Ensuring that the US military can field safe and reliable AI-enabled and autonomous systems and use them in accordance with international humanitarian law will help the United States maintain its competitive advantage against authoritarian countries, such as China and Russia, that are less committed to ethical use of AI. An emphasis on trustworthy AI is also crucial because the majority of the DoD's AI programs entails elements of human-machine teaming and collaboration, and their successful implementation depends, in large part, on operators trusting the system enough to use it. Finally, closer coordination between DoD and industry partners on shared standards and testing requirements for trustworthy and responsible AI is critical for moving forward with DoD AI adoption.

63 Daniel K. Lim, "Startups and the Defense Department's Compliance Labyrinth," *War on the Rocks*, January 3, 2022, https://warontherocks.com/2022/01/startups-and-the-defense-departments-compliance-labyrinth.

64 Moshe Schwarz and Heidi M. Peters, "Department of Defense Use of Other Transaction Authority: Background, Analysis, and Issues for Congress," Congressional Research Service, February 22, 2019, https://sgp.fas.org/crs/natsec/R45521.pdf.

65 "Final Report."

66 "SBIR Open Topic," US Department of the Air Force, Air Force Research Laboratory, https://afwerx.com/sbirsttr.

67 "Trusted AI at Scale," Griffiss Institute, July 26, 2021, https://www.griffissinstitute.org/about-us/events/ev-detail/trusted-ai-at-scale-1.

68 Insinna, "Silicon Valley Warns the Pentagon: 'Time is Running Out.'"

69 Jory Heckman, "DoD Seeks to Develop New Career Paths to Stay Ahead of AI Competition," *Federal News Network*, July 13, 2021, https://federalnewsnetwork.com/artificial-intelligence/2021/07/dod-seeks-to-develop-new-career-paths-to-stay-ahead-of-ai-competition.

Alongside the DoD's existing weapons-review and targeting procedures, including protocols for autonomous weapons systems, the department is also looking to address the ethical, legal, and policy ambiguities and risks raised more specifically by AI.[70] In February 2020, the Pentagon adopted five ethical principles to guide the development and use of AI, calling for AI that is responsible, equitable, traceable, reliable, and governable. Looking to put these principles into practice, Deputy Secretary of Defense Kathleen Hicks issued a memorandum directing a "holistic, integrated, and disciplined approach" for integrating responsible AI (RAI) across six tenets: governance, warfighter trust, product-and-acquisition lifecycle, requirements validation, responsible AI ecosystem, and AI workforce.[71] While JAIC was tasked with the implementation of the RAI strategy, it is unclear how this effort will unfold now that it has been integrated into the new CDAO office.

Meanwhile, in November 2021, the DIU released its responsible-AI guidelines, responding to the memo's call for "tools, policies, processes, systems, and guidance" that integrate the ethical AI principles into the department's acquisition policies.[72] These guidelines are a tangible step toward operationalizing and implementing ethics in DoD AI programs, building on DIU's experience working on AI solutions in areas such as predictive health, underwater autonomy, predictive maintenance, and supply-chain analysis. They are meant to be actionable, adaptive, and useful while ensuring that AI vendors, DoD stakeholders, and DIU program managers take fairness, accountability, and transparency into account during the planning,

development, and deployment phases of the AI system lifecycle.[73]

The success of the DoD's AI programs will depend, in large part, on ensuring that humans develop and maintain the appropriate level of trust in their intelligent-machine teammates. The DoD's emphasis on trusted AI is, therefore, increasingly echoed throughout some of its flagship AI projects. In August 2020, for instance, DARPA's Air Combat Evolution (ACE) program attracted a great deal of attention when an AI system beat one of the Air Force's top F-16 fighter pilots in a simulated aerial dogfight contest.[74] Rather than pitting humans against machines, a key question for ACE is "how to get the pilots to trust the AI enough to use it."[75] ACE selected the dogfight scenario, in large part, because this type of air-to-air combat encompasses many of the basic flight maneuvers necessary for becoming a trusted wing-mate within the fighter-pilot community. Getting the AI to master the basic flight maneuvers that serve as the foundation to more complex tasks, such as suppression of enemy air defenses or escorting friendly aircraft, is only one part of the equation.[76] The AlphaDogfight Trials, according to the ACE program manager, are "all about increasing trust in AI."[77]

AI development is moving fast, making it difficult to design and implement a regulatory structure that is sufficiently flexible to remain relevant without being so restrictive that it stifles innovation. Companies working with the DoD are seeking guidelines for the development, deployment, use, and maintenance of AI systems compliant with the department's ethical principles for AI. Many of these industry partners have adopted their own frameworks for trusted

---

70   "DOD Adopts Ethical Principles for Artificial Intelligence," US Department of Defense, February 24, 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

71   "Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, Defense Agency, and DOD Field Activity Directors on Implementing Responsible Artificial Intelligence in the Department of Defense," Deputy Secretary of Defense, May 26, 2021, https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF.

72   Ibid.

73   Jared Dunnmon, et al., "Responsible AI Guidelines in Practice," Defense Innovation Unit, https://assets.ctfassets.net/3nanhbfkr0pc/acoo1Fj5uungnGNPJ3QWy/3a1dafd64f22efcf8f27380aafae9789/2021_RAI_Report-v3.pdf.

74   Margarita Konaev and Husanjot Chahal, "Building Trust in Human-Machine Teams," Brookings, February 18, 2021, https://www.brookings.edu/techstream/building-trust-in-human-machine-teams/ ; Theresa Hitchens, "AI Slays Top F-16 Pilot in DARPA Dogfight Simulation," Breaking Defense, August 20, 2020. https://breakingdefense.com/2020/08/ai-slays-top-f-16-pilot-in-darpa-dogfight-simulation.

75   Sue Halpern, "The Rise of A.I. Fighter Pilots," New Yorker, January 17, 2022, https://www.newyorker.com/magazine/2022/01/24/the-rise-of-ai-fighter-pilots.

76   Adrian P. Pope, et al., "Hierarchical Reinforcement Learning for Air-to-Air Combat," Lockheed Martin, June 11, 2021. https://arxiv.org/pdf/2105.00990.pdf.

77   "AlphaDogfight Trials Go Virtual for Final Event," Defense Advanced Research Projects Agency, July 2020, https://www.darpa.mil/news-events/2020-08-07.

A US Army soldier uses the tactical robotic controller to control the expeditionary modular autonomous vehicle as a practice exercise in preparation for Project Convergence at Yuma Proving Ground, Arizona, on October 19, 2021. During Project Convergence 21, soldiers experimented with using this vehicle for semi-autonomous reconnaissance and re-supply. Both on and beyond the battlefield, trust in AI-enabled capabilities like autonomous and semi-autonomous vehicles is crucial to success. *Source*: US Army photo by Sgt. Marita Schwab, US Army flickr. https://www.flickr.com/photos/35703177@N00/51690959553/

and responsible AI solutions, highlighting attributes such as safety, security, robustness, resilience, accountability, transparency, traceability, auditability, explainability, fairness, and other related qualities.[78] That said, there are important divergences in risk-management approaches, organizational policies, bureaucratic processes, performance benchmarks, and standards for integrating trustworthiness considerations across the AI system lifecycle.

Currently, there are no shared technical standards for what constitutes ethical or trustworthy AI systems, which can make it difficult for nontraditional AI vendors to set expectations and

navigate the bureaucracy. The DoD is not directly responsible for setting standards. Rather, the 2021 National Defense Authorization Act (NDAA) expanded the National Institute of Standards and Technology (NIST) mission "to include advancing collaborative frameworks, standards, guidelines for AI, supporting the development of a risk mitigation framework for AI systems, and supporting the development of technical standards and guidelines to promote trustworthy AI systems."[79] In July 2021, the NIST issued a request for information from stakeholders as it develops its AI Risk Management Framework, meant to help organizations "incorporate trustworthiness considerations into

78   A recent IBM survey of two hundred and fifty technology leaders from global defense organizations revealed that about 42 percent have a framework for deploying AI ethically and safely; notably, formalized plans for the ethical application of AI are more common in organizations whose mission functions include combat and fighting arms than organizations with non-combat missions. These leaders surveyed represent organizations from a broad range of mission functions, including combat and fighting arms (18 percent), combat support (44 percent), and combat service-support (37 percent) organizations. "Deploying AI in Defense Organizations," 4. https://www.ibm.com/downloads/cas/EJBREOMX; "Autonomy and Artificial Intelligence: Ensuring Data-Driven Decisions," C4ISR, January 2021, https://hub.c4isrnet.com/ebooks/ai-autonomy-2020; "How Effective and Ethical Artificial Intelligence Will Enable JADC2," Breaking Defense, December 2, 2021, https://breakingdefense.com/2021/12/how-effective-and-ethical-artificial-intelligence-will-enable-jadc2.

79   Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021), https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.

the design, development, use, and evaluation of AI products, services, and systems."[80]

There are no easy solutions to this challenge. But, a collaborative process that engages stakeholders across government, industry, academia, and civil society could help prevent AI development from going down the path of social media, where public policy failed to anticipate and was slow to respond to the risks and damages caused by disinformation and other malicious activity on these platforms.

Related to standards are the challenges linked to testing, evaluation, verification, and validation (TEVV). Testing and verification processes are meant to "help decision-makers and operators understand and manage the risks of developing, producing, operating, and sustaining AI-enabling systems," and are essential for building trust in AI.[81] The DoD's current TEVV protocols and infrastructure are meant primarily for major defense acquisition programs like ships, airplanes, or tanks; it is linear, sequential, and, ultimately, finite once the program transitions to production and deployment. With AI systems, however, "development is never really finished, so neither is testing."[82] Adaptive, continuously learning emerging technologies like AI, therefore, require a more agile and iterative development-and-testing approach—one that, as the NSCAI recommended, "integrates testing as a continuous part of requirements specification, development, deployment, training, and maintenance and includes run-time monitoring of operational behavior."[83]

An integrated and automated approach to development and testing, which builds upon the commercial best practice of development, security, and operations (DevSecOps), is much better suited for AI/ML systems. While the JAIC's JCF has the potential to enable a true AI DevSecOps approach, scaling such efforts across the DoD is a major challenge because it requires significant changes to the current testing infrastructure, as well as more resources such as bandwidth, computing support, and technical personnel. That said, failing to develop new testing methods better suited to AI, and not adapting the current testing infrastructure to support iterative testing, will stymie efforts to integrate and adopt trusted and responsible AI at scale.

The above discussion of standards and TEVV encapsulates the unique challenges modern AI systems pose to existing DoD frameworks and processes, as well as the divergent approaches commercial technology companies and the DoD take to AI development, deployment, use, and maintenance. To accelerate AI adoption, the DoD and its industry partners need to better align on concrete, realistic, operationally relevant standards and performance requirements, testing processes, and evaluation metrics that incorporate ethical AI principles. A defense-technology ecosystem oriented around trusted and responsible AI could promote the cross-pollination of best practices and lower the bureaucratic and procedural barriers faced by nontraditional vendors and startups.

---

80   "Summary Analysis of Responses to the NIST Artificial Intelligence Risk Management Framework (AI RMF)—Request for Information (RFI)," National Institute of Standards and Technology, October 15, 2021, https://www.nist.gov/system/files/documents/2021/10/15/AI%20RMF_RFI%20 Summary%20Report.pdf.

81   Michele A. Flournoy, Avril Haines, and Gabrielle Chefitz, "Building Trust through Testing: Adapting DOD's Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems," WestExec, October 2020, 3–4, https://cset. georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf.

82   Flournoy, Haines, and Chefitz, "Building Trust through Testing," 3.

83   "Final Report," 384.

KEY TAKEAWAYS AND RECOMMENDATIONS

Fully exploiting AI's capacity to drive efficiencies in cost and time, support human decision-makers, and enable autonomy will require more than technological advancement or development of novel operational concepts. Below, we outline three key areas of prioritized effort necessary to more successfully integrate AI across the DoD enterprise and ensure the United States is able to deter threats and maintain a strategic, operational, and tactical advantage over its competitors and potential adversaries.

Prioritize Safe, Secure, Trusted, and Responsible AI Development and Deployment

The intensifying strategic competition with China, the promise of exquisite technological and operational capabilities, and repeated comparisons to the rapid pace of technology development and integration in the private sector are all putting pressure on the DoD to move faster toward fielding AI systems. There is much to gain from encouraging greater risk tolerance in AI development to enable progress toward adopting AI at scale. But, rushing to field AI-enabled systems that are vulnerable to a range of adversary attacks, and likely to fail in an operational environment, simply to "one-up" China will prove counterproductive.

The ethical code that guides the US military reflects a fundamental commitment to abiding with the laws of war at a time when authoritarian countries like China and Russia show little regard for human rights and humanitarian principles. Concurrently, the DoD's rigorous approach to testing and assurance of new capabilities is designed to ensure that new weapons are used responsibly and appropriately, and to minimize the risk from accidents, misuse, and abuse of systems and capabilities that can have dangerous, or even catastrophic, effects. These values and principles that the United States shares with many of its allies and partners are a strategic asset in the competition against authoritarian

countries as they field AI-enabled military systems. To cement the DoD's advantage in this arena, we recommend the following steps.

- The DoD should integrate DIU's Responsible AI Guidelines into relevant requests for proposals, solicitations, and other materials that require contractors to demonstrate how their AI products and solutions implement the DoD's AI ethical principles. This will set a common and clear set of expectations, helping nontraditional AI vendors and startups navigate the Pentagon's proposal process.

  There is recent precedent of the DoD developing acquisition categories for programs that required industry to pivot its development process to meet evolving DoD standards. In September 2020, for example, the US Air Force developed the e-series acquisition designation for all procurement efforts that required vendors to use digital engineering practices—rather than building prototypes—as part of their bid to incentivize industry to embrace digital engineering.[84]

- DoD industry partners, especially nontraditional AI vendors, should actively engage with NIST as the institute continues its efforts to develop standards and guidelines to promote trustworthy AI systems, to ensure their perspectives inform subsequent frameworks.

- Among the challenges to effective AI adoption referenced in this paper were brittle AI and the potential for adversary cyberattacks designed to corrupt the data on which AI algorithms are based. Overcoming these challenges will require a continued commitment within the DoD to increase the speed, variety, and capability of test and evaluation of DoD AI systems to ensure that these systems function as intended under a broader range of different environments. Some of this testing will need to take place in real-world environments, but advances in model-based simulations can allow for an increasing amount of validation of AI system performance in

---

84 "Air Force Acquisition Executive Unveils Next E-Plane, Publishes Digital Engineering Guidebook," US Department of the Air Force, January 19, 2021, https://www.af.mil/News/Article-Display/Article/2476500/air-force-acquisition-executive-unveils-next-e-plane-publishes-digital-engineer.

Artificial intelligence can drastically reshape the battlefield of the future. In order to realize this vision, the Department of Defense must undertake critical steps to effectively leverage AI. Source: US Army.

the digital/virtual world, reducing the costs and timelines associated with this testing.

- Moreover, the DoD should also leverage the under secretary of defense for research and engineering's (USDR&E) testing practices and priorities to ensure planned and deployed AI systems are hardened against adversary attacks, including data pollution and algorithm corruption.

- The DoD should leverage allies and foreign partners to develop, deploy, and adopt trusted AI. Engagement of this nature is vital for coordination on common norms for AI development and use that contain and counter China and Russia's authoritarian technology models. Pathways for expanding existing cooperation modes and building new partnerships can include the following.

i. Enhancing an emphasis on ethical, safe, and responsible AI as part of the JAIC's Partnership for Defense, through an assessment of commonalities and differences in the members' approaches to identify concrete opportunities for future joint projects and cooperation.

ii. Cross-sharing and implementing joint ethics programs with Five Eyes, NATO, and AUKUS partners.[85] In addition to supporting interoperability, this will add a diversity of perspectives and experiences, as well as help to ensure that AI development efforts limit various forms of bias. As one former general officer interviewed for this project noted, "diversity is how we ensure reliability. It is essential."[86]

iii. Broadening outreach to allies and partners of varying capabilities and geographies,

---

85   Zoe Stanley-Lockman, "Responsible and Ethical Military AI: Allies and Allied Perspectives," Center for Security and Emerging Technology, Georgetown University, August 2021, https://cset.georgetown.edu/wp-content/uploads/CSET-Responsible-and-Ethical-Military-AI.pdf.

86   Authors' interview with a former US military general.

including India, South Africa, Vietnam, and Taiwan, to explore opportunities for bilateral and multilateral research-and-development efforts and technology-sharing programs that address the technical attributes of trusted and responsible AI.[87]

Align Key Priorities for AI Development and Strengthen Coordination between the DoD and Industry Partners to Help Close DoD AI Capability Gaps.

The DoD will not be able to fulfill its ambitions in AI and compete effectively with the Chinese model of sourcing technology innovation through military-civil fusion without close partnerships with a broad range of technology companies. This includes defense-industry leaders with long-standing ties to the Pentagon, technology giants at the forefront of global innovation, commercial technology players seeking to expand their government portfolio, and startups at the cutting edge of AI development. But, the DoD's budget-planning, procurement, acquisition, contracting, and compliance processes will likely need to be fundamentally restructured to effectively engage with the entirety of this vibrant and diverse technology ecosystem.

Systemic change is a slow, arduous process. But, delaying this transition risks the US military falling behind on exploiting the advantages AI promises to deliver, from operational speed to decision dominance. In the meantime, the following actions could help improve coordination with industry partners to accelerate the DoD's AI adoption efforts.

- The DoD should assess its communications and outreach strategy to clarify and streamline messaging around the department's priorities in AI.
- The DoD should partner with technology companies to reexamine their assessments regarding the potential value of AI solutions in certain categories, including, but not limited to, logistics, medical and health services, and information operations.
- The DoD should implement the NSCAI's recommendation to accelerate efforts to train

acquisition professionals on the full range of available options for acquisition and contracting, and incentivize their use for AI and digital technologies."[88] Moreover, such acquisition-workforce training initiatives should ensure that acquisition professionals have a sufficient understanding of the DoD's ethical principles for AI and the technical dimensions of trusted and responsible AI. The DIU's ethical guidelines can serve as the foundation for this training.

Promote Coordination between Leading Defense Technology Companies and Nontraditional Vendors to Accelerate DoD AI Adoption.

Rather than building entirely new AI-enabled systems, in the short to medium term, the DoD will be integrating AI into a range of existing software and hardware systems—from cyberdefense architectures to fighter jets to C2. Progress toward implementing AI will, therefore, also depend upon streamlining collaboration between the startups and nontraditional AI vendors that the DoD has been courting for their innovative and cutting-edge technologies and the defense primes responsible for integrating new capabilities into legacy systems.

The NSCAI recommends identifying "new opportunities for defense primes to team with non-traditional firms to adopt AI capabilities more quickly across existing platforms."[89] We echo this recommendation: improved coordination between defense primes and nontraditional firms can help ensure AI solutions are robust, resilient, and operationally relevant, as well as usher promising prototypes through the "valley of death."

Without a doubt, moving from concept to practice can be tricky. This paper's research revealed a significant disconnect in perspectives on where the main challenges to moving innovative new technologies from the lab to adoption in programs of record reside. Startups tend to view system integrators as resistant to engaging, while startups may be viewed as lacking understanding of the acquisition process and of developing technologies that are difficult to integrate into, or scale for, programs of record.[90]

87   Zoe Stanley-Lockman, "Military AI Cooperation Toolbox: Modernizing Defense Science and Technology Partnerships for the Digital Age," Center for Security and Emerging Technology, Georgetown University, August 2021, https://cset.georgetown.edu/publication/military-ai-cooperation-toolbox/.

88   "Final Report," 65.

89   Ibid., 305.

90   Authors' interview with a defense technology executive.

Bridging this gap will require new government approaches to resolving concerns of nontraditional suppliers around intellectual property. Most are reticent to give ownership of sensitive technologies that are sold largely to customers outside the defense market. It will also involve the DoD helping small businesses navigate the federal acquisition process through steps such as speeding up cyber certification and the Authority To Operate (ATO) process, as well as helping interesting companies develop use cases for different components of the DoD. Such proactive facilitation will help nontraditional suppliers that have worked with DoD through research-and-development grants come to a partnership with systems integrators more prepared.

Most importantly, optimizing the benefits of both large systems integrators and smaller innovators will require the DoD to play a more active interlocutor role in connecting small companies with those that are running programs of record. There is currently some understandable hesitancy for the DoD to demand that companies work together, largely for fear of running afoul of Federal Acquisition Regulations (FAR). But, as one industry expert interviewed for this project argued, the DoD could be more aggressive in understanding what is permissible under the FAR and helping companies connect, especially to meet a specific acquisition priority or program.

CONCLUSION

Over the last several years, interest and investment in AI have gained momentum. This is especially true in the national security and defense community, as strategists, policymakers, and executives seek decisive advantages amid rising geostrategic competition and prepare for future operating environments characterized by complexity, uncertainty, and, most importantly, speed. AI is now at the center of military-technological competition between the United States and China, and both countries, as well as other militaries throughout the world, are already deploying AI-enabled systems with the goal of dominating the battlefield of the future.

The United States cannot risk falling behind China—not in AI innovation, not in AI adoption, and not in the full-scale integration of AI across the national defense enterprise. Urgency is required in addressing the range of technical and bureaucratic processes, and cultural issues that have, to date, dampened the pace of AI adoption within the DoD. Specifically, the DoD should prioritize the following.

- *Building trust in AI:* Rather than replacing humans, DoD AI efforts are primarily centered on technologies that augment human understanding, decision-making, and performance. Building trust and confidence between humans and their intelligent-machine teammates is, therefore, a critical aspect of the successful development and deployment of military AI.

- *Developing and implementing standards for trusted and responsible AI:* Currently, there are no commonly held standards or system-performance requirements for what constitutes trusted and responsible AI. The Pentagon and its industry partners must, therefore, work collaboratively with bodies like NIST to develop and implement operationally relevant standards, testing processes, and evaluation metrics that incorporate ethical, trustworthy, and responsible AI principles. This will help advance successful AI research prototypes into production-ready solutions.

- *Facilitating the optimization of the US innovation ecosystem and defense industrial base:* Bringing cutting-edge AI technologies into the DoD also requires the Pentagon to reduce the bureaucratic challenges frequently associated with the DoD acquisition process, especially for innovative companies that are outside the traditional defense-industrial base. Developing new means of supporting and incentivizing engagement of these companies and promoting intra-industry partnerships between leading defense-technology companies and startups and nontraditional suppliers will be crucial.

- *Engaging allies and partners:* As noted at the outset of this paper, the war in Ukraine has reinforced the importance of allies and partners in enforcing geopolitical norms and standards. The same is likely to be true of the future of AI development and adoption. The DoD will benefit not only from collaboration across industry and the national security community, but also with allies and foreign partners to ensure establishment and promulgation of norms and standards that will enable trusted, responsible, and interoperable AI development and deployment.

● ●

ACKNOWLEDGMENTS

To produce this report, the authors conducted a number of interviews and consultations. They list alphabetically below, with gratitude, some of the individuals consulted and whose insights informed this report. The analysis and recommendations presented in this report are those of the authors alone, and do not necessarily represent the views of the individuals consulted. Moreover, the named individuals participated in a personal, not institutional, capacity.

● **Mr. Prashant Bhuyan**, *Founder and CEO*, Accrete AI

● **Gen James Cartwright, USMC (Ret.),** *Board Director*, Atlantic Council; *Former Vice Chairman*, US Joint Chiefs of Staff; *Former Commander*, US Strategic Command

● **Mr. Jonathan Doyle**, *Partner*, Axion Partners

● **Mr. Brian Drake**, *Federal Chief Technology Officer,* Accrete AI

● **Ms. Evanna Hu**, *Nonresident Senior Fellow, Forward Defense, Scowcroft Center for Strategy and Security*, Atlantic Council

● **Mr. Ron Keesing**, *Senior Vice President for Technology Integration*, Leidos

● **Mr. Stephen Rodriguez,** *Senior Advisor, Scowcroft Center for Strategy and Security*, Atlantic Council

The authors would also like to thank the following individuals for their peer review of various drafts of this report, listed below in alphabetical order. The analysis and recommendations presented in this report are those of the authors alone, and do not necessarily represent the views of the peer reviewers. Moreover, the named individuals participated in a personal, not institutional, capacity.

● **Gen James Cartwright, USMC (Ret.),** *Board Director*, Atlantic Council; *Former Vice Chairman*, US Joint Chiefs of Staff; *Former Commander*, US Strategic Command

● **Mr. Jonathan Doyle**, *Partner*, Axion Partners

● **Mr. Brian Drake**, *Federal Chief Technology Officer,* Accrete AI

● **Ms. Evanna Hu**, *Nonresident Senior Fellow, Forward Defense, Scowcroft Center for Strategy and Security*, Atlantic Council

● **Mr. Justin Lynch,** *Director, Research and Analysis*, Special Competitive Studies Project

● **Ms. Kelley Sayler,** *Analyst, Advanced Technology and Global Security*, Congressional Research Service

ABOUT THE AUTHORS

Margarita Konaev is a nonresident senior fellow in the *Forward* Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security. Additionally, she serves as associate director of analysis and a research fellow at Georgetown's Center for Security and Emerging Technology (CSET) with interests in military applications of artificial intelligence and in Russian military innovation. She is also an adjunct senior fellow with the Center for a New American Security. Previously, she was a non-resident fellow with the Modern War Institute at West Point, a post-doctoral fellow at the Fletcher School of Law and Diplomacy, and a post-doctoral fellow at the University of Pennsylvania's Perry World House. Before joining CSET, she worked as a senior principal in the Marketing and Communications practice at Gartner.

Dr. Konaev's research on international security, armed conflict, non-state actors and urban warfare in the Middle East, Russia, and Eurasia has been published by the Journal of Strategic Studies, the Journal of Global Security Studies, Conflict Management and Peace Science, the French Institute of International Relations, the Bulletin of the Atomic Scientists, Lawfare, War on the Rocks, Modern War Institute, Foreign Policy Research Institute, and a range of other outlets and organizations. She holds a PhD in political science from the University of Notre Dame, an MA in conflict resolution from Georgetown University, and a BA from Brandeis University.

Tate Nurkin is the founder of OTH Intelligence Group and a nonresident senior fellow with *Forward* Defense at the Atlantic Council's Scowcroft Center for Strategy and Security.

Before establishing OTH Intelligence Group in March 2018, Mr. Nurkin spent twelve years at Jane's by IHS Markit where he served in a variety of roles, including managing Jane's Defense, Risk, and Security Consulting practice. From 2013 until his departure, he served as the founding Executive Director of the Strategic Assessments and Futures Studies (SAFS) Center, which provided thought leadership and customized analysis on global competition in geopolitics, future military capabilities, and the global defence industry.

Substantively, Mr. Nurkin's research and analysis has a particularly strong focus on US-China competition, defense technology, the future of military capabilities, and the global defense industry and its market issues. He also specializes in the design and delivery of alternative futures analysis exercises such as scenario planning, red teaming, and wargaming.

He previously worked for Joint Management Services, the Strategic Assessment Center of SAIC, and the Modeling, Simulation, Wargaming, and Analysis team of Booz Allen Hamilton. From 2014 – 2018 he served consecutive two-year terms on the World Economic Forum's Nuclear Security Global Agenda Council and its Future Council on International Security, which was established to diagnose and assess the security and defense implications of the Fourth Industrial Revolution.

Mr. Nurkin holds a master of science degree in international affairs from the Sam Nunn School of International Affairs at Georgia Tech and a bachelor of arts in history and political science from Duke University.

Atlantic Council