Chapter 3: AI and Warfare

AI Ready by 2025

Top-Down Leadership

Innovative Concepts

Advanced Technologies and R&D

AI-Readiness Performance Goals

AI-Enabled Allies and Partners

Even with the right artificial intelligence (AI)-ready technology foundations in place, the U.S. military will still be at a battlefield disadvantage if it fails to adopt the right concepts and operations to integrate AI technologies. Throughout history, the best adopters and integrators, rather than the best technologists, have reaped the military rewards of new technology.[1] The Department of Defense (DoD) should not be a witness to the AI revolution in military affairs, but should deliver it with leadership from the top, new operating concepts, relentless experimentation, and a system that rewards agility and risk.

A new warfighting paradigm is emerging because of AI. Our competitors are making substantial investments to take advantage of it. This idea has been called "algorithmic" or "mosaic" warfare[2]; China's theorists have called it "intelligentized" war.[3] All of these terms capture, in various ways, how a new era of conflict will be dominated by AI and pit algorithms against algorithms. Advantage will be determined by the amount and quality of a military's data, the algorithms it develops, the AI-enabled networks it connects, the AI-enabled weapons it fields, and the AI-enabled operating concepts it embraces to create new ways of war.
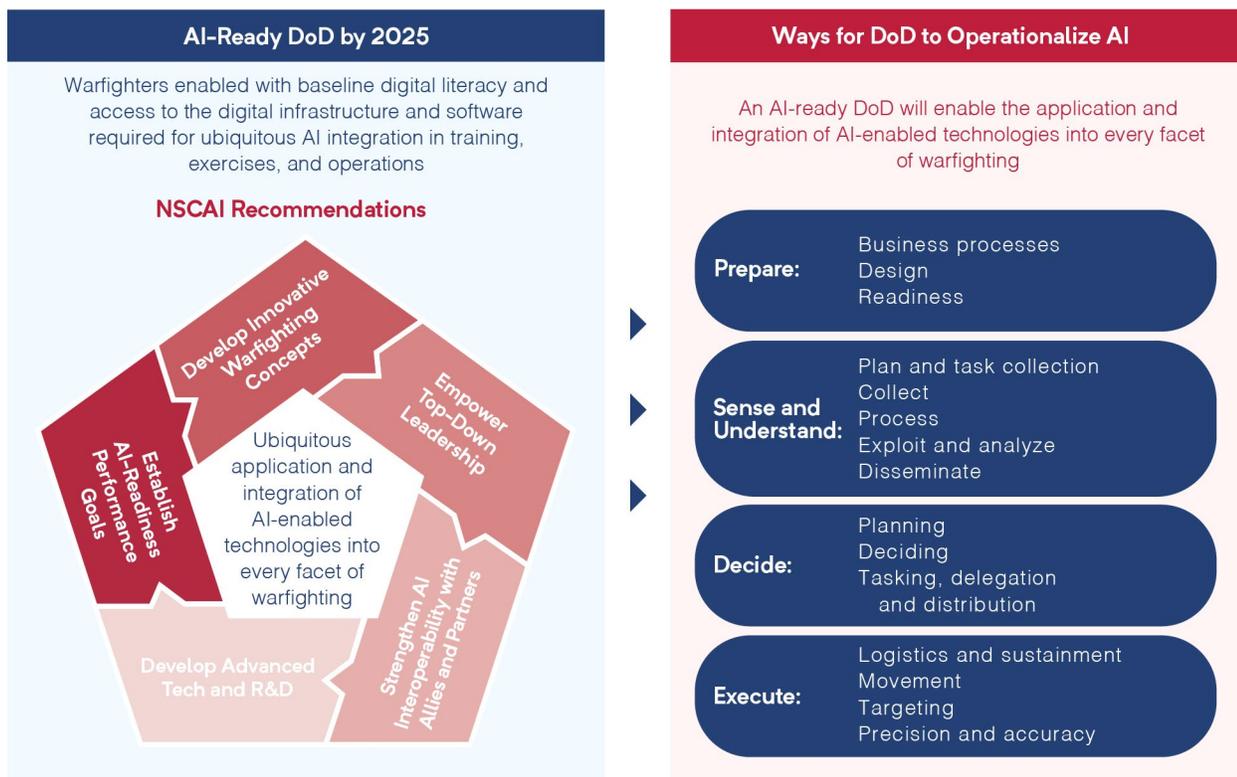
Today's DoD is trying to execute an AI pivot, but without urgency. Despite pockets of imaginative reform and a few farsighted leaders, DoD remains locked in an Industrial Age mentality in which great-power conflict is seen as a contest of massed forces and monolithic platforms and systems. The emerging ubiquity of AI in the commercial realm and the speed of digital transformation punctuate the risk of not pivoting fast enough. The Department must act now to integrate AI into critical functions, existing systems, exercises, and wargames to become an AI-ready force by 2025. Simultaneously, DoD must develop more creative warfighting concepts that are paired with investments in future AI-enabled technologies to continuously out-innovate potential adversaries. If our forces are not equipped with AI-enabled systems guided by new concepts that exceed those of their adversaries, they will be outmatched and paralyzed by the complexity of battle.

An AI-Ready DoD by 2025:

Warfighters enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in training, exercises, and operations.

"The Department must act now to integrate AI into critical functions, existing systems, exercises and wargames to become an AI-ready force by 2025."

AI and Warfare

AI-Ready DoD by 2025

Warfighters enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in training, exercises, and operations

NSCAI Recommendations

- Develop Innovative Warfighting Concepts
- Empower Top-Down Leadership
- Establish AI-Readiness Performance Goals
- Ubiquitous application and integration of AI-enabled technologies into every facet of warfighting
- Strengthen AI Interoperability with Allies and Partners
- Develop Advanced Tech and R&D

Ways for DoD to Operationalize AI

An AI-ready DoD will enable the application and integration of AI-enabled technologies into every facet of warfighting

Prepare:
Business processes
Design
Readiness

Sense and Understand:
Plan and task collection
Collect
Process
Exploit and analyze
Disseminate

Decide:
Planning
Deciding
Tasking, delegation and distribution

Execute:
Logistics and sustainment
Movement
Targeting
Precision and accuracy

To compete, deter, and, if necessary, fight and win in future conflicts requires wholesale adjustments to operational concepts, technologies, organizational structures, and how we integrate allies and partners into operations. It will also require risk-based assessments of both the benefits and drawbacks of widespread integration of AI-enabled capabilities, to include future autonomous weapon systems. Lastly, it will require a willingness to engage in bilateral and multilateral dialogues with our allies and partners to urge them to make similar AI pivots to ensure future interoperability.

How AI Will Change Warfare.

AI-enabled warfare will not hinge on a single new weapon, technology, or operational concept; rather, it will center on the application and integration of AI-enabled technologies into every facet of warfighting. AI will transform the way war is conducted in every domain from undersea to outer space, as well as in cyberspace and along the electromagnetic spectrum. It will impact strategic decision-making, operational concepts and planning, tactical maneuvers in the field, and back-office support. In this new kind of warfare, traditional confines of the battlefield will be expanded through AI-enabled micro-targeting, disinformation, and cyber operations, as described in Chapter 1 of this report. AI will reshape many attributes of war, such as its speed, tempo, and scale; the relationships service members have with machines; the persistence with which the battlefield can be monitored; and the discrimination and precision with which targets can be attacked. There will be a premium on speed and accuracy in developing knowledge, acting, and reacting as the conflict unfolds.

"**AI-enabled warfare will not hinge on a single new weapon, technology, or operational concept; rather, it will center on the application and integration of AI-enabled technologies into every facet of warfighting.**"

DoD AI RDT&E Investments by Warfighting Domains, FY 2015–2025
Source: Govini

■ Research   □ Multi-domain   ■ Land   ■ Naval   □ Air   ■ Cyber, EMS, Info   ■ Space
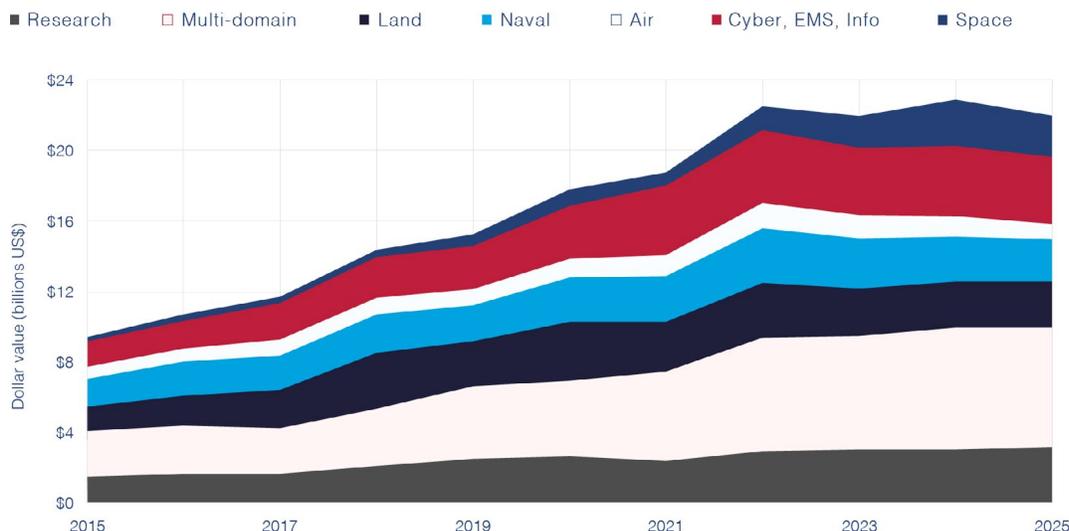
DoD AI RDT&E Investments.

DoD's AI investments are well distributed across the various warfighting domains (land, naval, air, space, cyber, electromagnetic spectrum, information), with over 25% of investments in multi-domain applications of AI, signaling AI's potential for integrating multi-domain operations. Investments in AI applications for Space operations more than quadrupled from FY2019 to FY2025, from $500M to $2.2B, increasing from 3% to almost 9% of AI-enabled investment.

Note the spending levels presented in figure represent estimates based on an analysis of DoD RDT&E budget documents for FY2021-FY2025. See Analysis of DoD RDT&E Investments in AI, NSCAI (on final with the Commission). Due to inherent quality issues in the source data, estimates presented contain significant, difficult to estimate margins of error.

AI will make the process of finding and hitting targets of military value faster and more efficient. It will also increase accuracy of target identification and minimize collateral damage. Currently, this process generally involves passing data in a serial fashion from a sensor, through a series of humans, to a platform that can shoot at the target. AI will help automate some of the intermediate stages of the decision process. AI will also create opportunities for more advanced processes that would operate more akin to a web, fusing multiple sensors and platforms to manage complex data flows and transmitting actionable information to human operators and machines across all domains.[4]

In war, many of the military uses of AI will complement, rather than supplant, the role of humans. AI tools will improve the way service members perceive, understand, decide, adapt, and act in the course of their missions. However, new concepts for military operations will also need to account for the changing ways in which humans will be able to delegate increasingly complex tasks to AI-enabled systems. In the near term, this will be managed through the military's principle of "mission command," which stresses decentralized execution and disciplined initiative by subordinates who follow a commander's intent. This human-centric approach to fighting should remain the standard for the foreseeable future. But as AI continues to advance into the cognitive and neuromorphic domain, and human-machine teaming becomes more sophisticated, the military will need to develop more imaginative concepts and organizational constructs that take full advantage of AI technologies without relinquishing the principles that undergird mission command.

Prepare

Business processes. Robotic Process Automation and AI-enabled analysis can generate significant savings, speed administrative actions, and provide decision-makers with superior insights into core business processes such as finance, budget, contracting, travel, and human resources.

Design. AI will support a holistic system-of-systems approach to developmental force design via digital engineering, digital twins, and modeling and simulation to enable a more comprehensive understanding of system vulnerabilities and adjacent capabilities, concepts, and technologies.

Readiness. AI will enhance training by relieving the cognitive burden of doing repetitive tasks that can be performed better by machines. AI will be prevalent in all exercises and wargames and will enhance the military's ability to train in live, virtual, and constructive environments.

Plan and task collection. Through automation, AI-enabled systems will optimize tasking and collection for platforms, sensors, and assets in near-real time in response to dynamic intelligence requirements or changes in the environment.

Sense and Understand

Collect. At the tactical edge, "smart" sensors will be capable of pre-processing raw intelligence and prioritizing what data to transmit and store, which will be especially helpful in degraded or low-bandwidth environments.

Process. AI-enabled natural language processing, computer vision, and audiovisual analysis can vastly reduce manual data processing. AI can also be used to automate data conversion such as translations and decryptions, accelerating the ability to derive actionable insights.

Exploit and analyze. AI-enabled tools have the potential to augment filtering, flagging, and triage across multiple data sets. Such tools can identify connections and correlations more efficiently and at a greater scale than human analysts and can flag those findings and the most important content for human analysis. AI will improve indications and warnings for military leaders.

- AI can fuse data from multiple sources, types of intelligence, and classification levels to produce accurate predictive analysis in a way that is not currently possible.
- Advances in speech-to-text transcription and language analytics now enable reading comprehension, question answering, and automated summarization of large quantities of text.

Disseminate. AI will be able to automatically generate machine-readable versions of intelligence products and disseminate them at machine speed so that computer systems across the IC and the military can ingest and use them in real time without manual intervention.

Decide

Planning. AI decision-support applications will utilize modeling and simulation algorithms and real-time data sets to optimize planning options.

Deciding. AI will integrate command-and-control networks and compress the speed of finding and attacking targets of military value.

Tasking, delegation, and distribution. Edge processing enhanced by delegated authorities will allow frontline units to operate in a coordinated manner with minimal to no communications. AI techniques like machine learning, and rule-based models will support network resiliency.

Execute

Logistics and sustainment. AI-enabled predictive analytics, optimization, and tracking will improve efficiency and effectiveness across all facets of logistics. Intelligent systems will aid in the development of courses of action for routine and contingency logistics and sustainment operations. Robotic process automation will streamline human-centric maintenance and supply chain workflows.

Movement. AI will enhance the ability of commanders to maneuver, position, and protect units and forces. AI will help network and coordinate movements of autonomous swarms via human-machine and machine-machine teaming.

Targeting. AI-enabled systems will expand a single targeting chain into a complex targeting web that considers numerous variables across units and domains.

Precision and accuracy. Through AI-enabled smart weapons and autonomous platforms, AI will enable the military to be more precise and discern friendly forces, non-combatants, and adversary targets with greater accuracy.

This list of how AI might transform warfighting principles and capabilities—as well as others like it—is by no means exhaustive. Innovation will lead to future capabilities that are unknowable at present and will only become clearer in time.

> "Innovation will lead to future capabilities that are unknowable at present and will only become clearer in time."

Stronger Together.

If the United States wants to fight with AI, it will need allies and partners with AI-enabled militaries and intelligence agencies. Uneven adoption of AI will threaten interoperability and the political cohesion and resiliency of U.S. alliances.[5] As it deepens and expands conventional defense arrangements across the globe––especially in Europe and the Indo-Pacific––the United States should incorporate AI and emerging technology into coordinated defense and intelligence activities. Given the dual-use nature of many software-based capabilities, DoD will need more flexibility to work with civilian agencies, companies, and research institutions in partner nations.

Promote AI interoperability and the adoption of critical emerging technologies among allies and partners, including the Five Eyes, the North Atlantic Treaty Organization (NATO), and across the Indo-Pacific. This should include:

Recommendation

- Enhancing existing Five Eyes AI–related defense and intelligence efforts.

- Supporting NATO efforts to accelerate agreements on architectures and standards, develop allied technical expertise, and pursue coalition AI use cases for exercises and wargames.

- Fostering the Joint Artificial Intelligence Center (JAIC)'s International AI Partnership for Defense as a critical vehicle to further AI defense and security cooperation.[6]

- Creating an Atlantic–Pacific Security Technology Partnership to improve military and intelligence capabilities and interoperability across European and Indo–Pacific allies and partners.

> # "Uneven adoption of AI will threaten military interoperability, and the political cohesion and resiliency of U.S. alliances."

AI-enabled Alliances and Partnerships.
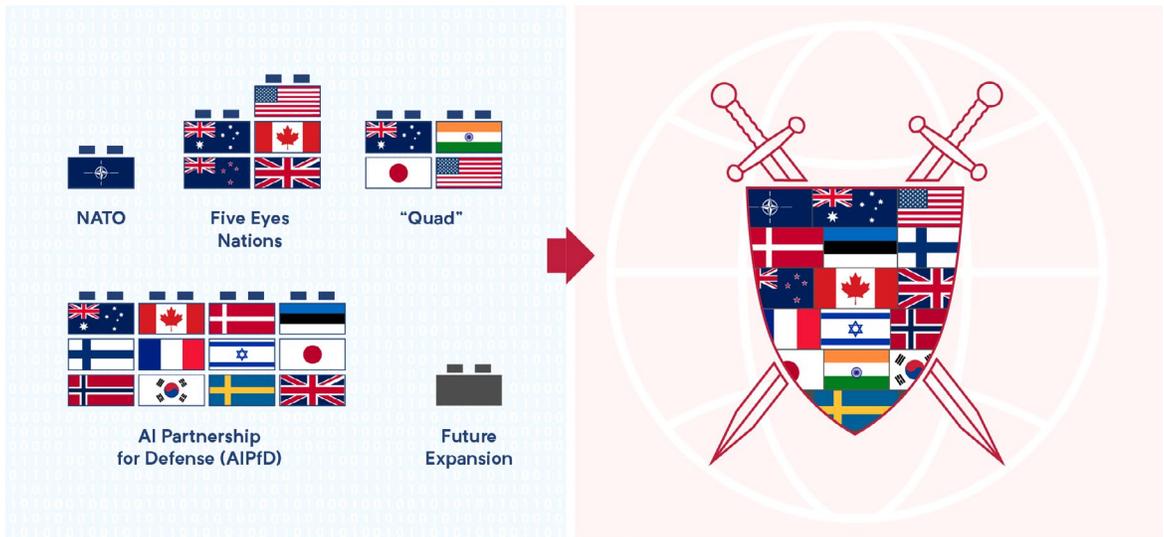
Achieve a State of Military AI Readiness by 2025.

To reach this goal, the DoD should:

Drive organizational reform through top-down leadership. Senior civilian and military officials should set clear priorities and direction, empower subordinates, and accept higher uncertainty and risk in pursuing new technologies. Specifically, DoD should:

- Establish a high-level Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence[7];

- Ensure that the JAIC Director remains a three-star general or flag officer with significant operational experience who reports directly to the Secretary of Defense or Deputy Secretary of Defense;

- Appoint the Under Secretary of Defense for Research and Engineering as the co-chair and chief science advisor to the Joint Requirements Oversight Council; and

- Assign an AI Operational Advocate on the staff of every Combatant Command. This officer would perform a similar role to that played by the Staff Judge Advocate. He or she would be an expert in AI systems, advise the commander and staff on the capabilities and limitations of AI systems, and identify when AI-enabled systems are being used inappropriately.

Develop innovative operational concepts that integrate new warfighting capabilities with emerging technologies.[8] These concepts should strive for seamless interoperability across the military services and across operational domains. The concept developers should work closely with technologists to articulate how the military could fight most effectively in future scenarios, and they should assume that AI-enabled capabilities will be ubiquitous on future battlefields. These concepts can also drive future investments.

By the end of 2021, establish AI and digital readiness performance goals.[9] To achieve more substantial integration of AI across DoD, the Deputy Secretary of Defense should:

- Direct DoD components to assess military AI and digital readiness through existing readiness management forums and processes. The Tri-Chaired Steering Committee on Emerging Technology should work closely with the Under Secretary of Defense for Personnel and Readiness and the Joint Staff to ensure the identified AI readiness criteria are incorporated into the military services' readiness reporting and resourcing strategies.

- Direct the military services to accelerate review of specific skill gaps in AI to inform recruitment and talent-management strategies.[10]

- Direct the military services—in coordination with the Under Secretary of Defense for Acquisition and Sustainment, the Joint Staff, the Defense Logistics Agency, and the JAIC—to prioritize integration of AI into logistics and sustainment systems wherever possible.

- Integrate AI into major wargames and exercises to promote field-to-learn approaches to technology adoption. Operators need persistent interaction with AI-enabled capabilities early in the development cycle to generate critical feedback on how they function and how they impact the mission. Widespread experimentation will advance both concept development and the performance of the technology.[11]

- Incentivize experimentation with AI-enabled applications through the Warfighting Lab Incentive Fund, which could be overseen by the proposed Tri-Chaired Steering Committee.[12]

Define a joint warfighting network architecture by the end of 2021. The key objective of this joint warfighting network should be a secure, open-standards systems network that supports the integration of AI applications at operational levels and across domains.[13] It should be accessible by all of the military services and encompass several elements, including command and control networks; data transport, storage, and secure processing; and weapon system integration. The technical infrastructure for the network should be supported by best practices in digital engineering.[14] It should also be interoperable with the digital ecosystem described in Chapter 2 of this report.[15]

Invest in priority AI R&D areas that could support future military capabilities, including the following:

Research Area	Time Horizon		Key Challenges	Category
Future of Teaming	**Near:** Understanding and designing support for human-machine interdependence. Proper management of interdependence to achieve smooth and efficient coordination of activity.	**Long:** Reasoning over changing context to flexibly adapt teaming strategy for the best available team performance. Achieving team resilience through flexible adaptation.	Understanding interdependencies and the impact of dynamic adaptation on team performance.	**Work with Humans**
Advanced Scene Understanding	**Near:** Ability to sense fundamental changes in the operating environment and alert the human operator while switching to a better-suited, environmentally-tuned perceptual model, if one exists	**Long:** Maintaining a perceptual model that supports actionable awareness and insight across a range of complex, dynamic environments and scenarios	Incorporating multi-source and multi-modal information from complex and changing environments	**Sense & Perceive**
Intelligent Edge Devices, Computing & Networking	**Near:** Narrow AI applications within edge sensors, such as remote cameras positioned to monitor a highly contested space	**Long:** Autonomous edge devices that dynamically learn, share, and team with other devices, while exercising intelligent data collection, exploitation, and retention; mastery of domain-specific physical manipulation	Network limitation; size, weight, and power (SWaP)	**Hardware, Devices, and Robotics**
Robust and Resilient AI	**Near:** Standard practice for exchanging trained AI models with tamper resistance and non-repudiation	**Long:** AI systems that are resilient on attack surfaces and able to learn securely via privacy-centric machine learning, including use of encryption	Many attack surfaces; addressing rise of adversarial machine-learning methods with robust learning; applying security techniques while maintaining high accuracy	**Integrate & Assure**
Test & Evaluation, Verification & Validation (TEVV)	**Near:** Common framework for AI TEVV	**Long:** TEVV for fully autonomous AI systems that employ dynamic learning along with self-awareness and monitoring, and autonomous AI test ranges involving cohorts of humans and machines	Knowing how much and what types of testing are sufficient to determine an acceptable level of risk for a given use case	
Integrated AI, Modeling & Simulation for Decision Support	**Near:** Decision support for highly constrained scenarios and environments	**Long:** Real-time decision support and course of action development for open-world environments with longer time horizons	Multi-modal data integration; assessing the predictive fidelity of simulation models	
Autonomous AI Systems	**Near:** Operate for relatively short periods of delegated autonomy from human operators in relatively unchanging and predictable environments while carrying out simple, independent tasks	**Long:** Longer periods of independent mission engagement with awareness and understanding of a dynamically changing operational environment, requiring continual assurance and self-monitoring, while carrying out complex mission sets involving multi-agent collaboration	Independent accomplishment of goals in environments that are complex, changing, and unpredictable; understanding how and when to engage with human operators	**Learn & Reason**
Toward More General Artificial Intelligence	**Near:** Growth in interpretability and explainability for narrow AI; methods for performing transfer learning; fine-tuning of models	**Long:** AI systems able to learn by engaging with the operational environment, make decisions based on contextual knowledge, and amass experiential knowledge	Unlocking multiple mysteries of human learning and reasoning; more general situational awareness and problem-solving	

Chapter 3 - Endnotes

[1] On military adoption, see, e.g., Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, Princeton University Press (2010).

[2] The Defense Advanced Research Projects Agency (DARPA) Mosaic warfare central concept is built around the "adaptability for U.S. forces and complexity or uncertainty for the enemy through the rapid composition and recomposition of a more disaggregated U.S. military force using human command and machine control." Bryan Clark, et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*, CSBA at vi (Feb. 11, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations/publication/1.

[3] The People's Liberation Army has developed a warfighting concept for what it calls "intelligentized operations" with AI at its core. Within this construct, China theorizes that in future conflict, the central contest will be between adversarial battle networks rather than traditional weapons platforms, and that information advantage and algorithmic superiority will be a determinant of victory. See Elsa Kania, *Chinese Military Innovation in Artificial Intelligence*, CNAS at 1 (June 7, 2019), https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence (testimony before the U.S.-China Economic and Security Review Commission).

[4] See *Creating Cross-Domain Kill Webs in Real Time*, DARPA (Sept. 18, 2020), https://www.darpa.mil/news-events/2020-09-18a. See also *AI Fusion: Enabling Distributed Artificial Intelligence to Enhance Multi-Domain Operations & Real-Time Situational Awareness*, Carnegie Mellon University (2020), http://www.cs.cmu.edu/~ai-fusion/overview.

[5] On military interoperability challenges related to AI, see Erik Lin-Greenberg, *Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making*, Texas National Security Review (Spring 2020), https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/.

[6] The AI Partnership for Defense, launched in September 2020, includes the United States and 12 partner nations: Australia, Canada, Denmark, Estonia, Finland, France, Israel, Japan, Norway, South Korea, Sweden, and the United Kingdom. It seeks to "provide values-based global leadership" on adoption of AI in the defense and security context and align "like-minded nations to promote the responsible use of AI, advance shared interests and best practices on AI ethics implementation, establish frameworks to facilitate cooperation, and coordinate strategic messaging on AI policy." *Joint Statement*, AI Partnership for Defense (Sept. 15-16, 2020), https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf. The Partnership held its second formal dialogue in January 2021. *DoD Joint AI Center Facilitates Second International AI Dialogue for Defense*, JAIC (Jan. 27, 2021), https://www.ai.mil/news_01_27_21-dod_joint_ai_center_facilitates_second_international_ai_dialogue_for_defense.html.

[7] The Commission acknowledges Section 236 of the Fiscal Year 2021 National Defense Authorization Act, which permits the Secretary of Defense to establish a steering committee on emerging technology and national security threats composed of the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, the Under Secretary of Defense for Intelligence and Security, the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Acquisition and Sustainment, the Chief Information Officer, and such other officials of the Department of Defense as the Secretary determines appropriate. However, the structure described in Sec. 236 does not include leadership from the Intelligence Community and will thus not drive the intended action. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

[8] Notably, the National Defense Strategy emphasizes the need to "evolve innovative operational concepts" and "foster a culture of experimentation and calculated risk-taking." Tighter coordination between concept writers and technologists would create a more dynamic cycle of technology development and integration. *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 7 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Chapter 3 - Endnotes

[9] "Readiness" is a key measure of military effectiveness and remains at the heart of budget, policy, and oversight debates on defense preparedness. In this context, DoD should establish key AI and digital readiness performance objectives to measure and drive Department and service accountability. See G. James Herrera, *The Fundamentals of Military Readiness*, Congressional Research Service at 2 (Oct. 2, 2020), https://fas.org/sgp/crs/natsec/R46559.pdf.

[10] As noted in Chapter 6 of this report, there is already an identified need for the creation of digital corps, civilian and military AI and AI-related career fields, an expansion of recruiting pathways, and the creation of recruiting offices. The military services need to assess the number of personnel in those fields and structures, not the need to establish them.

[11] Although AI will be ubiquitous across all domains, the high-data volumes associated with the space, cyber, and information operations domains make use cases in those domains particularly well-suited for prioritized integration of AI-enabled applications in wargames, exercises, and experimentation.

[12] The Warfighting Lab Incentive Fund is intended to spur field experiments and demonstrations to "evaluate, analyze and provide insight into more effective ways of using current capabilities, and to identify new ways to incorporate technologies into future operations and organizations." See Memorandum from the Deputy Secretary of Defense, *Warfighting Lab Incentive Fund and Governance Structure*, U.S. Department of Defense (May 6, 2016), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/DSD_memo.pdf.

[13] The network envisioned is well-aligned with ongoing DoD efforts to embrace standards-driven interoperability, system adaptability, and data-sharing. See Memorandum from the Secretary of the Navy, Secretary of the Army, and Secretary of the Air Force for Service Acquisition Executives and Program Executive Officers, U.S. Department of Defense (Jan. 7, 2019), https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf.

[14] Such as the goals and focus areas outlined in the DoD Digital Engineering Strategy; terms, any knowledge, and guidelines shared as part of the Digital Engineering Body of Knowledge; and incorporating Section 231 of the National Defense Authorization Act for Fiscal Year 2020, which requires the creation of a digital engineering capability to automate testing and evaluation. See *Department of Defense Digital Engineering Strategy*, Office of the Deputy Assistant Secretary of Defense for Systems Engineering (June 2018); see also Pub. L. 116-92, The National Defense Authorization Act for Fiscal Year 2020, 133 Stat. 1198 (2019). For a description of the Digital Engineering Body of Knowledge, see Andrew Monje, *Future Direction of Model-Based Engineering Across the Department of Defense*, U.S. Department of Defense (Jan. 27, 2020), https://ac.cto.mil/wp-content/uploads/2020/05/RAMS-Monje-27Jan2020-Future.pdf.

[15] See the Chapter 2 Blueprint for Action for details on how this architecture should interact with the digital ecosystem.