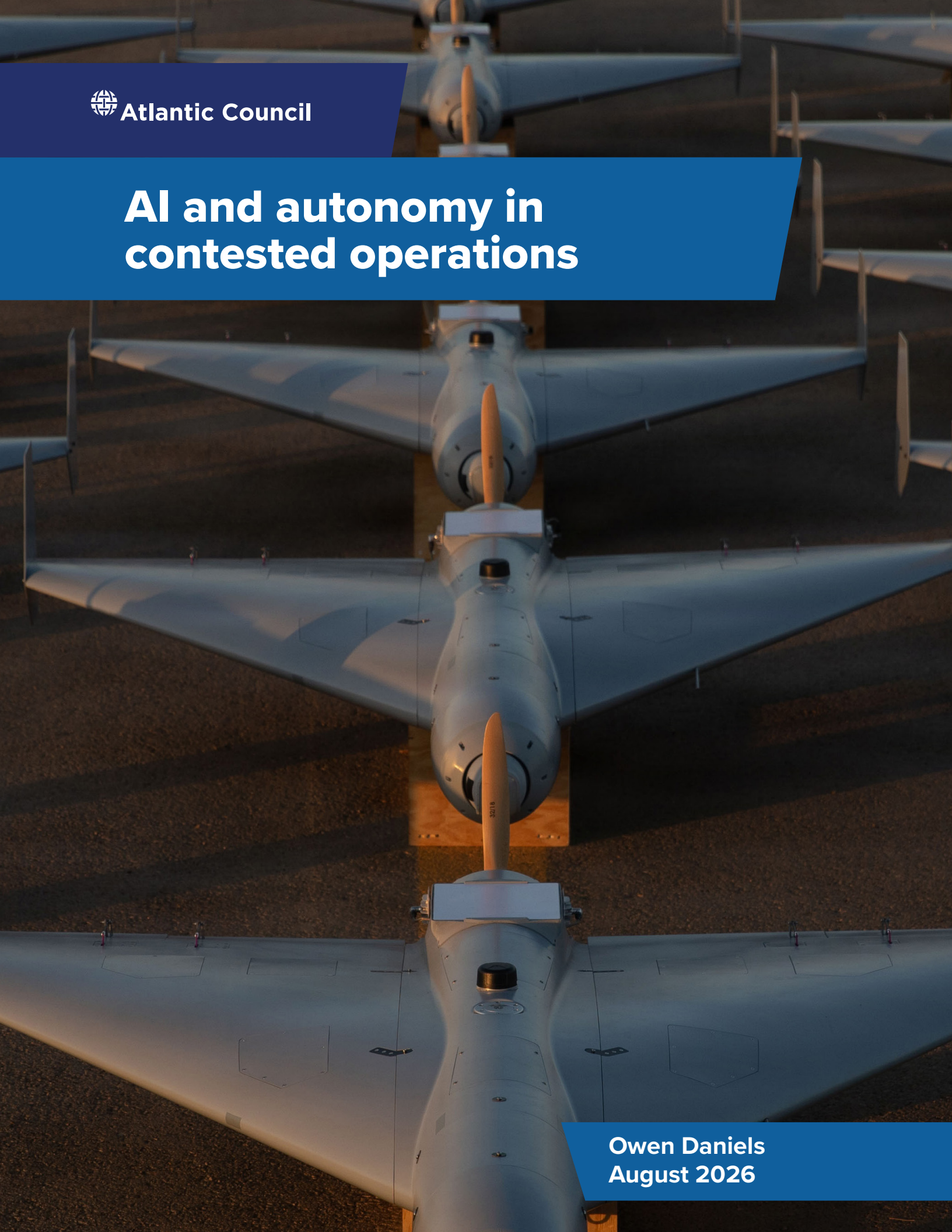

Atlantic Council

AI and autonomy in contested operations

Owen Daniels
August 2026

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Within the Scowcroft Center for Strategy and Security, Forward Defense (FD) leads the Atlantic Council's US and global defense programming, developing actionable recommendations for the United States and its allies and partners to compete, innovate, and navigate the rapidly evolving character of warfare. Through its work on US defense policy and force design, military applications of advanced technology, space security, strategic deterrence, artificial intelligence, and defense industrial revitalization, it informs the strategies, policies, and capabilities that the United States will need to deter, and, if necessary, prevail in major-power conflict.

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2026

Authors

Owen Daniels

Cover: Several Low-cost Unmanned Combat Attack System (LUCAS) drones sit idle on tarmac at US Central Command (CENTCOM) base. Picture taken November 23, 2025.

Atlantic Council
SCOWCROFT CENTER

Table of contents

Bottom lines up front

- The US military should presume that, from now on, most future operations will occur in contested environments where connectivity is poor or nonexistent.
- Acquiring military AI capabilities for such environments is one challenge; building servicemembers' trust in and ability to use them responsibly is a related but distinct challenge.
- The private sector's experience managing the rollout of autonomous capabilities and incorporating user feedback into subsequent updates offers valuable lessons.

Introduction

The Department of Defense (DOD) is intensely focused on rapidly integrating artificial intelligence (AI) across a range of application areas and capabilities to gain and sustain advantage. The US National Security Strategy has focused on addressing threats from peer competitors—the People's Republic of China (PRC) and Russia—for nearly a decade, and AI is likely to provide valuable capability to the US joint force in rising to the challenge. However, compared to experiences in Iraq and Afghanistan, the environments in which the US military may conduct operations will be highly contested in areas where American operators have traditionally enjoyed superiority. To effectively use AI to compete with the PRC or Russia, operators will need to rely on AI-enabled systems that perform well and remain resilient in denied, degraded, intermittent, and limited (DDIL) environments—environments where technological capabilities will be contested to varying degrees. The US military should presume that, from now on, most future operations will occur in DDIL environments.

At a general level, the acquisition of AI capabilities for and adoption in DDIL environments are two interrelated challenges. Acquiring systems that are useful and reliable to operators at the edge is essential. Adoption at the edge involves putting AI-enabled systems in the hands of warfighters and building their familiarity with, understanding of, and confidence in these systems to facilitate their diffusion and use. It also involves acquiring systems that are interoperable and can easily rely on shared resources, such as data (when available), and the ability to incorporate AI solutions into existing systems and processes. Ensuring that adoption accounts for culture and user needs will be paramount for augmenting warfighter performance with AI. These challenges are magnified when acquiring commercial technology solutions and adapting them for military use. While many AI-related concerns for DDIL environments are tactical, they also involve understanding policy implementation challenges, roles, and authorities at the operational and strategic levels.

This report provides insights related to the development and adoption of AI in DDIL environments and highlights priority issues for DOD to address. It highlights the most important differences for developers to take into account between highly contested battlespaces and more permissive environments. The issues addressed here are swiftly evolving amid technological progress and policy changes, but they represent persistent challenges. The report outlines the DDIL challenge; examines near-term AI applications for contested operations; and details potential adoption hurdles that must be overcome to harness the technology's potential. It offers a road map of policy recommendations that can guide understanding of the landscape of AI for contested operations and facilitate AI adoption.

- Delineating authorities related to AI-enabled systems in DDIL contexts.
- Encouraging DDIL-related iterative development between industry and end users.
- Implementing and sustaining relevant testing, "red-teaming," and experimentation practices for edge AI.
- Adapting professional military education to expand the AI-ready force.

Understanding the problem

US competitors and adversaries are expressly developing capabilities to target traditional American advantages in the era of network-centric warfare, including satellites, the electromagnetic spectrum, cyberspace, and other information systems. Strategies to create DDIL environments for US operations aim to physically and digitally hinder the achievement of American objectives across the continuum of conflict. In the Indo-Pacific region, the People's Liberation Army (PLA) has developed a multidomain denial strategy geared toward impeding US approaches to the Western Pacific, particularly in the event of a contingency scenario involving Taiwan. The PLA development of multilayered maritime area denial in its extended littoral, combining attacks on information systems with long-range antiship cruise missiles and ballistic missiles, couple physical and digital denial to try to undercut qualitatively superior US military capabilities.[1] Russia has previously referred to US reliance on global positioning systems as "the Achilles' heel of Washington's military power," and its operations since the full-scale invasion of Ukraine in 2022 have made jamming and electromagnetic spectrum denial key components of its warfighting approach.[2] In sum, DDIL environments pose direct and immediate challenges for conducting operations.

The acronym DDIL conveys the spectrum of obstacles that warfighters may face in contested operations. Warfighters in *denied* environments may have no access to physical maneuver or certain technological capabilities, while *degraded* capabilities may fail over the course of an operation. *Intermittent* capabilities may come in and out of functionality. *Limited* environments, typically referring to internet bandwidth, may mean capabilities reliant on internet access will have low functionality. The acronym also helps capture the complexity of contested operations: Environments will not simply be denied or fully available, but will comprise mixes of functional, degraded, or offline capabilities at different points in missions.

Physically denied environments represent areas where access to territory is contested and difficult to achieve for conventional forces. Forces may have limited freedom to maneuver due to physical threats from adversaries, terrain, or political limitations and sensitivities. Operational environments may also be digitally denied. In these cases, physically accessing an area may be possible, but establishing connections and communications across modalities and domains—including the electromagnetic spectrum, satellites in space, or cyberspace—will be challenged. This can result in restricted access to information networks, even when maneuver is possible. Digitally denied environments contribute to so-called low bandwidth, high-latency scenarios, limiting access to necessary electromagnetic channels and increasing wait times for effective use of systems that rely on the spectrum. Digital denial may be caused by electronic warfare (EW) systems, cyber warfare, anti-space operations, and other threat vectors. It can necessitate decentralized warfighting, resupply, logistics, and other operations at the tactical edge. It can also result in limited internet connectivity and reduce access to data resources in the operating area. In worst case scenarios, inconsistent access to critical services may require falling back to manual systems. Physical and digital DDIL environments are certainly not binary and, as potential adversaries explicitly target traditional US advantages in the information domain during operations, both types of denial will converge and threaten US objectives and operators.

Artificial intelligence and the DDIL challenge

Enter artificial intelligence. AI is redefining a range of military systems, capabilities, and tasks, from autonomous weapons systems to command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance, and targeting (C5ISRT) capabilities to cyber operations and electronic warfare. AI offers the potential for the US military to overcome some DDIL challenges. Many of these capabilities have been identified as priorities for research and development, and some have already been fielded, while others are nascent.

Currently, many of the AI applications that will be immediately useful at the tactical edge involve AI capabilities like computer

1. Ben Noon and Chris Bassler, "Schrodinger's Military? Challenges for China's Military Modernization Ambitions," War on the Rocks, 2021, https://warontherocks.com/2021/10/schrodingers-military-challenges-for-the-chinas-military-modernization-ambitions/; Elsa B. Kania, Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power (Washington, DC: Center for a New American Security, November 2017), https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power; Ben Noon and Chris Bassler, "How Chinese Strategists Think AI Will Power a Military Leap Ahead," Defense One, September 17, 2021, https://www.defenseone.com/ideas/2021/09/how-chinese-strategists-think-ai-will-powermilitary-leap-ahead/185409/; and Gregory C. Allen, Understanding China's AI Strategy, Center for a New American Security, February 6, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.
2. Staff, "This is the Achilles' Heel of Washington's Military Power," Sputnik News (Russian state agency), January 30, 2016, article cited in Spencer S. Waters, "Training in the DDIL Environment," Marine Corps Gazette, WE26, September 2022, https://www.mca-marines.org/wp-content/uploads/Training-in-the-DDIL-Environment.pdf.

vision, sensor fusion, and autonomous navigation. AI systems with benefits in DDIL environments include:

- AI-enabled target recognition.
- AI-enabled autonomous systems with terminal guidance (lock-on) capabilities for hitting a target, even when connection with an operator is lost.
- Various decision-support systems at the tactical level that can draw on wide ranges of sensors and data, helping humans pick signals from noise and maintain robust operating pictures.
- AI-enabled cyber defenders and EW systems, among others.

AI applications that perform robustly under DDIL conditions can help maintain technological capability and mission effectiveness in the face of adversary disruption efforts. The AI models that will be critical enablers of such systems differ in their size and sophistication. AI-enabled autonomous systems for targeting and intelligence, surveillance, and reconnaissance (ISR) rely on computer vision, sensor fusion, reinforcement learning, and autonomous navigation to classify vehicles, personnel, equipment, and other targets without cloud connectivity. This allows them to operate in EW-heavy environments where GPS signals may be denied or degraded, executing missions and holding positions based on point-to-point navigation while contributing to faster targeting and ISR decision-making cycles.

AI-enabled autonomous weapons systems and loitering munitions have received notoriety for their ability to lock onto targets using computer vision in denied environments, ensuring that they can prosecute a target even if they lose contact with a human controller under heavy jamming. These systems are contributing to what some experts have referred to as the era of precise mass.[3] Swarm AI capabilities for autonomous systems, which consist of self-organizing teams without single points of failure, are a priority focus area under DOD's 2026 AI strategy (referred to as the AI Acceleration Strategy) for their potential to overwhelm limited forces or saturate defenses in attacking targets or completing ISR missions.[4] Recent efforts to field attritable (i.e., expendable) autonomous systems at scale for contested operations illustrate this priority. The Biden administration's Replicator Initiative was one early effort; after it stalled, the department dissolved it in late 2025 and absorbed it into the Defense Autonomous Warfare Group (DAWG), which, alongside the Drone Dominance Program, now leads this push under the Trump administration.[5]

Defensively, AI may be incorporated into counter-UAS (unmanned aircraft systems), fusing signals from radar, radio frequency, acoustic, and other signals to identify and intercept rapid, low-signature threats quickly.[6] The DOD's Joint Interagency Task Force 401 (JIATF-401) leads joint and interagency efforts to test and field counter-UAS capabilities. JIATF-401 is actively fielding AI-enabled systems that integrate computer vision, radio frequency sensing, and autonomous targeting against small UAS threats, reflecting the DOD's broader shift toward autonomous solutions against small drones at scale. [7]

Generative models have become popularly identified with the concept of AI in recent years. These models can produce multimodal outputs, including text, images, videos, and computer code. They allow users to communicate with digital systems in plain language. Large generative models have a role to play at the operational level, for instance through their integration into decision-support systems like the Maven Smart System (MSS). However, the most sophisticated generative models require access to more computing power for inference (generating real-world outputs) than currently available to onboard systems at the edge based on size, weight, and power constraints.

These capabilities are advancing at various levels of maturity and sophistication. As evidenced in Ukraine, loitering munitions and autonomous ISR platforms have made significant strides, even incorporating computer vision for visual-assisted navigation. Other areas, like contested logistics and resupply or casualty recovery, are less advanced and will require more progress in autonomous ground capabilities. Nonetheless, the potential benefits of using AI to complete the tactical mission sets described above are clear.

DDIL environments are likely to complicate existing challenges for AI-enabled systems in several ways. Persistent challenges for AI-enabled systems—such as model drift, or degraded ac-

3. Michael C. Horowitz, "Battles of Precise Mass: Technology Is Remaking War—and America Must Adapt," Foreign Affairs, November/December 2024, https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz.
4. "Artificial Intelligence Strategy for the Department of War," Department of Defense, January 12, 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF.
5. Michael O'Connor, "Replicator: A Bold New Path for DoD," Center for Security and Emerging Technology, Georgetown University, https://cset.georgetown.edu/article/replicator-a-bold-new-path-for-dod/; "DOD Replicator Initiative: Background and Issues for Congress," Congressional Research Service, IF12611, updated January 21, 2026, https://www.congress.gov/crs-product/IF12611; and "Drone Dominance," DOD, n.d., https://www.war.gov/Spotlights/Drone-Dominance/.
6. "Pentagon Task Force to Deploy AI-Powered UAS Systems to Capture Drones," Defense News, Sightline Media Group, January 13, 2026, https://www.defensenews.com/unmanned/2026/01/13/pentagon-task-force-to-deploy-ai-powered-uas-systems-to-capture-drones/.
7. Army Lt. Col. Adam Scher, "Joint Interagency Task Force 401 Awards $500 Million Counter-UAS Contract," Joint Interagency Task Force 401, DOD, May 18, 2026, https://www.war.gov/News/News-Stories/Article/Article/4495165/joint-interagency-task-force-401-awards-500-million-counter-uas-contract/.

curacy for novel targets, or false-positive risks for computer vision systems—will remain in contested environments. However, models will be unable to be safely and securely updated based on new data, changes to rules of engagement, or other mission parameters until systems can be removed from the contested environment. Swarm coordination abilities may break under aggressive jamming or electronic warfare pressure, and human oversight of autonomous platforms may occasionally be lost. Edge deployments necessarily run lighter (i.e., compressed versions of larger models that perform well in the cloud), which heightens the importance of understanding performance thresholds when a system is operating near the limit of its competence.

In addition, AI-enabled platforms offer attack surfaces for adversaries in DDIL scenarios. These include (but are not limited to) models themselves and the data used for model training and inference. Where AI systems rely on sensor data, for instance, from networked autonomous platforms in an area of operations, destruction of assets could contribute to incomplete operating pictures above the tactical level. Cyberattacks on models could take capabilities offline or badly degrade their performance. For predictive and generative systems, the US National Institute of Standards and Technology categorizes attacks on AI in terms of model integrity, availability, privacy, and abuse. These attack surfaces span the full development-to-deployment pipeline. Recent joint guidance from the Cybersecurity and Infrastructure Security Agency, National Security Agency, and DOD partner agencies emphasizes that training data curation, model compilation, supply-chain dependencies, and over-the-air update channels represent points of potential compromise that must be defended end to end.[8]

Attacks on data sources may pose likely near-term challenges for military AI applications, taking place as models are trained or after they are deployed in DDIL environments. Deception of models, from low-tech to high-tech methods, could degrade algorithmic performance and make AI tools less reliable. Data poisoning, or the introduction of data into a training set that compromises a model's performance, is an upstream threat.[9] Data poisoning would typically entail cyber actors or malicious insiders introducing irrelevant or inaccurate data into datasets to decrease the model's performance after it is deployed. The goal of such attacks may be to elicit particular behaviors from models under specific circumstances by planting triggers, possibly even without alerting users to degraded performance. Sophisticated actors may be able to execute data-poisoning attacks cheaply and easily.[10]

Post-deployment adversarial attacks may seek to alter real-world data to generate harmful AI outputs during inference. Adversarial attacks aim to tweak inputs into an enemy's AI systems to negatively affect system inference. Sophisticated examples in AI research have included manipulating image pixels to greatly degrade the performance of image-recognition models, but on the battlefield, adversarial attacks may be decidedly lower tech. For instance, decoys—some of which include heat signatures or other signature-confusing capabilities—have been used by both sides in the Russia-Ukraine war to fool human drone operators and AI recognition systems alike.[11] Camouflage that changes the profile of the targets that models have trained on can also disrupt inference. Model performance can be improved with new real-world data, continuous iteration and updates, and effective human-machine teaming, but these challenges highlight the importance of appropriately calibrating operators' expectations for AI-enabled military systems.

Some of the DDIL challenges described above will be broadly similar across the joint force, while others will manifest differently across domains. In the maritime domain, for instance, distributed maritime operations will require knitting together information from dispersed sensors on, below, and above the waves to contribute to a commander's battlefield picture. Distributed operations will present decision-making challenges for adversaries in determining the most salient threats and create trade-offs between sensing and time pressure; US multimodal data collection in adversary-controlled environments during peacetime can both improve system performance and suggest where the United States can impose reciprocal data-denial costs on adversary AI systems.[12] However, distributed operations may also heighten the challenges of intermittent access to force-spanning resources and degraded communications for distributed units.

8. Apostol Vassilev et al., Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, US National Institute of Standards and Technology, NIST 100-2e2023, 2024, https://doi.org/10.6028/NIST.AI.100-2e2023NIST 100-2e2023 (National Institute of Standards and Technology (U.S.; and Cybersecurity and Infrastructure Security Agency (CISA) et al., "AI Data Security," May 2025, defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF.

9. "What Is AI Data Poisoning?," Cloudfare, accessed November 21, 2025, https://www.cloudflare.com/learning/ai/data-poisoning/.

10. Daniel Alexander Alber et al., "Medical Large Language Models Are Vulnerable to Data-Poisoning Attacks," Nature Medicine 31, no. 2 (2025): 618–26, https://doi.org/10.1038/s41591-024-03445-1.

11. Jorge L. Rivero, "Decoy Warfare: Lessons and Implications of the War in Ukraine," US Naval Institute Proceedings, April 2024, https://www.usni.org/magazines/proceedings/2024/april/decoy-warfare-lessons-and-implication-war-ukraine.

12. Robert Richbourg, "'It's Either a Panda or a Gibbon': AI Winters and the Limits of Deep Learning," War on the Rocks, May 10, 2018, https://warontherocks.com/2018/05/its-either-a-panda-or-a-gibbon-ai-winters-and-the-limits-of-deep-learning/; and Dmitry Filipof, Distributed Maritime Operations: Solving What Problems and Seizing Which Opportunities?, Atlantic Council, June 2024, https://www.atlanticcouncil.org/wp-content/uploads/2024/06/Distributed-Maritime-Operations-Solving-what-problems-and-seizing-which-opportunities.pdf.

From a US perspective, military applications of AI against a sophisticated adversary like China would likely face many of these AI-specific DDIL challenges. The Chinese idea of "intelligentized" warfare, for instance, specifically aims to gain competitive advantages for the PLA using AI and other capabilities to weaken the enemy's understanding of the battlefield and disrupt warfighters' cognitive processes. Algorithmic competition is a major component of this "intelligentization" vision.[13] Against a determined peer—both in terms of hardware and AI capabilities—effectively developing and adopting AI capabilities for contested operations will be critical.

Twin goals: Development and adoption

Developing AI capabilities that are effective and resilient in DDIL environments will require continued technical innovation and integration with human processes to facilitate broader, responsible adoption. As with other military systems, AI-enabled capabilities will not always perform perfectly; indeed, human operators should not expect perfection from AI systems, but they should be equipped to understand risks from choosing to deploy or not deploy AI-enabled capabilities—to "shoot or not to shoot"—in DDIL environments. Creating AI-enabled capabilities that are well-suited to denial challenges must proceed in lockstep with efforts at the strategic, operational, and tactical levels to cultivate effective human-machine teams at the tactical edge.

Calibrating operators' trust and expectations is a necessary complement to technology development for spurring AI adoption throughout the services, both for AI capabilities broadly and DDIL applications specifically. Warfighters do not need deep expertise in AI to use AI-enabled capabilities; however, the technology development process for DDIL-relevant capabilities should be geared toward incorporating operator feedback at multiple stages to ensure AI capabilities are militarily effective and can be adopted reliably in compliance with mission objectives, rules of engagement, the laws of war, and ethical principles.[14] If operators do not have "justified confidence" in an AI-enabled system, this may hamper adoption, with hesitancy due to uncertainty about an AI-enabled system's reliability, particularly in contested operations; difficulty or inertia incorporating new tools into existing processes and authorities; interoperability challenges with legacy capabilities; unclear differentiation between human and machine roles; and other hurdles. The relationship between AI and user trust is complex, multifaceted, and evolving. [15] While a deep dive on trust is beyond this report's scope, it is clear that poorly calibrated trust in AI capabilities could impede DOD's adoption goals.

To effectively tackle DDIL challenges for AI and facilitate confident, responsible adoption, the joint force will need to develop and integrate AI applications into human-centric processes. The rest of this report focuses on understanding how the DOD can address DDIL challenges at the strategic, operational, and tactical levels to achieve development and adoption goals. Across each of these areas, DOD has launched promising initiatives. The recommendations in this report focus on completing them and adapting them specifically for the demands of DDIL environments, where the gap between policy and operational practice is most consequential. Priority areas include:

- Delineating authorities for different aspects of developing, securing, and fielding AI systems intended for use in DDIL environments.
- Encouraging and facilitating iterative development with end users.
- Implementing effective testing, evaluation, verification, and validation practices for and experimentation with AI-enabled systems in DDIL conditions.
- Incorporating robust red-teaming, coordinated with test and evaluation (T&E).
- Running a series of increasingly complex exercises, from single-service through joint and combined events.
- Incorporating lessons learned for edge AI into professional military education.

DOD has initiated notable efforts in each of these areas. The challenge is not merely identifying priorities but execution: Across programs, policies have occasionally outpaced authority structures and integration work to help field capabilities at scale. For instance, the Replicator Initiative aimed to field thousands of autonomous systems by 2025 but reportedly delivered well below that level, which some observers attributed to integration burdens transitioning fielded systems across doctrine, organization, training, and policy.[16] The DOD's successor efforts, the DAWG and the Drone Dominance Program, ostensibly seek to address these gaps by shifting from traditional

13. On the PLA concept of intelligentized warfare and algorithmic competition, see Kania, Battlefield Singularity; and Allen, Understanding China's AI Strategy.
14. This is in accordance with Department policies like Directive 3000.09 on Autonomy in Weapons Systems, established in 2012 and updated in 2023; see Office of the Under Secretary of Defense for Policy, "Directive 3000.09 on Autonomy in Weapons Systems," January 25, 2023, https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF.
15. Michael C. Horowitz et al., "Adopting AI: How Familiarity Breeds Both Trust and Contempt," AI & Society 39 (2024): 1721–1735, https://doi.org/10.1007/s00146-023-01666-5.
16. "DoD Replicator Initiative," Congressional Research Service; and Richard Haley, Michael Harteveldt, and Ethan Kessler, "Is Replicator Replicable?," Belfer Center for Science and International Affairs, Harvard Kennedy School, September 25, 2025, https://www.belfercenter.org/research-analysis/replicator-replicable.

acquisition toward operator-driven competition, embedding engineers and acquisition professionals at the tactical edge, and prioritizing software that can be rapidly deployed across low-cost drone platforms.[17] Nevertheless, DDIL environments could amplify implementation gaps, highlighting the importance of accounting for them before fielding.

Tackling the multilevel DDIL challenge

Delineating authorities

Delineating authorities over the full life cycle of AI capabilities in DDIL environments—from data governance and model updates to deployment and repatriation, i.e., secure data transmission and ingestion from the edge into centralized repositories—can help clarify where steps to solve key security challenges for different AI vulnerabilities can be addressed up and down the chain of command. It can also help the DOD and services calibrate the balance between centralizing AI support functions and pushing capability decisions out to the operational edge. Clear authorities can help minimize friction in integrating edge AI capabilities into existing authorities and processes, contributing to the DOD's diffusion and adoption goals.

For instance, one area where authorities could be more clearly delineated surrounds computing power and data for edge systems. AI models operating in DDIL environments, such as drones, autonomous vehicles, or systems carried by operators, are reliant on edge computing due to the possibility that connection to central computing networks can be cut off. These systems collect and store data locally, which can then be used for model updates through secure links or at safer positions away from the tactical edge. To incorporate new data from mission environments and update models, data transfers must occur between edge systems and centralized data and computing resources.

Data used for training and tuning models resides at the operational level, with the services controlling baseline model data and combatant commands retaining contextual data within an area of operations but often relying on commercial computing resources managed by private actors. Transferring data in both directions between edge and operational systems not only complicates processes but also expands distinct attack surfaces. At the operational level, combatant commands rely heavily on centralized computing infrastructure, such as the Defense Information Systems Agency's Hybrid Compute Centers, which present attractive concentrated targets for cyberattacks. Conversely, at the tactical edge, dispersed computing nodes face vulnerabilities ranging from electronic signal interception during data synchronization to actual hardware destruction. Protecting the development, training, distribution, and deployment pipeline is paramount for ensuring model and data security and performance, both at garrisons and at the edge.

The security-accreditation machinery that governs fielded systems compounds this challenge. The Authority to Operate process and the Risk Management Framework (RMF) were designed for traditional software and accommodate AI imperfectly. Model drift and continuous retraining require ongoing monitoring and reauthorization that these frameworks do not currently account for.[18] Clarifying who holds reauthorization authority for an updated model and under what conditions in a DDIL environment is therefore both a command-authority question and a security-accreditation one.

One way to resolve this would be to shift from passive, compliance-based frameworks toward a more active Admiral Rickover-style model of absolute engineering accountability, named for the father of the "nuclear Navy."[19] Under this model, security accreditation would shift away from static, administrative RMF checklists toward a singular, technically competent command authority. This authority would be responsible for the continuous operational safety and algorithmic integrity of the system and would work in concert with other authority holders in the chain of command to manage technology design, interactions with private developers, and procurement. Clear authorities would enable service stakeholders to move with speed; integrate testing, evaluation, and security considerations; and implement real-time, engineering-driven reautho-

17. "Drone Dominance Hearing Sharpens Pentagon's Small UAS Industrial Strategy," Inside Unmanned Systems, June/July 2025, https://insideunmannedsystems.com/drone-dominance-hearing-sharpens-pentagons-small-uas-industrial-strategy/; and "A New DAWG in the Fight: The Pentagon's $54 Billion Bet on Autonomous Warfare," Defense Security Monitor, May 21, 2026, https://dsm.forecastinternational.com/2026/05/21/a-new-dawg-in-the-fight-the-pentagons-54-billion-bet-on-autonomous-warfare/.

18. "Developmental Test and Evaluation of Artificial Intelligence-Enabled Systems Guidebook," Office of the Under Secretary of Defense for Research and Engineering, DTE&A, February 26, 2025, https://www.cto.mil/wp-content/uploads/2025/02/TE_of_AIES_Guidebook_Final_26Feb25.pdf. On the adaptation of the Risk Management Framework and Authority to Operate processes for AI characteristics such as model drift and continuous retraining, see industry commentary in "The State of AI in DoD: Trends and Opportunities for 2026," Zapata Technology, April 19, 2026.

19. Connor S. McLemore and Eric Jimenez, "Who is the Admiral Rickover of Naval Artificial Intelligence?," War on the Rocks, September 18, 2018, https://warontherocks.com/who-is-the-admiral-rickover-of-naval-artificial-intelligence/.

rizations for edge AI systems.[20] Through this model or other clearer authorities, decisions for how and when to make decisions to safely update or retrain models could be integrated into doctrine, concepts of operations, training, and tactics, techniques, and procedures (TTPs). Operational authorities could set clear timelines for model updates in peace and wartime, for example, updating and troubleshooting within two to four weeks in peacetime and twenty-four to forty-eight hours in a conflict.[21] Services and commands must also put in place policies delineating the authorities under which personnel in tactical units are allowed to update fielded AI models and capabilities and what training and certifications they need. Such authorities could play a role in helping operational research teams navigate testing and evaluation and model update issues when deployed forward, as discussed in greater detail in a subsequent section.

Authority ambiguity extends beyond the military operational chain. For instance, the services lead testing and evaluation processes for acquired AI capabilities in accordance with strategic-level standards and guidance; yet even at the standards-setting level, authority has not always been clear. In 2024, the DOD's inspector general found that delays in implementing the department's AI adoption strategy through the Chief Digital and Artificial Intelligence Office (CDAO) created ambiguity over AI-related roles and responsibilities relative to the DOD's chief information officer. Amid this matter and related concerns, CDAO was realigned under the Office of the Under Secretary of Defense for Research and Engineering in August 2025.[22]

Some of the costs of these unclear authorities have already manifested. The Maven Smart System operated for years on short-term contracts and ad hoc appropriations before being designated a formal program of record in 2026, years after its launch, leaving funding, oversight, and accountability arrangements unsettled even as it was used to support real-world operations.[23] Preestablishing the authority map for AI capabilities, rather than resolving it retroactively, would help avoid similar ambiguity for systems fielded in DDIL environments.

Key issues at the strategic, operational, and tactical levels

Iterative development and innovation with industry

Both iterative technology development and innovation with industry can contribute to effective capability creation and build warfighter familiarity with AI intended for DDIL environments. As the DOD and services focus on developing newer, more efficient acquisition pathways for software and other digital technologies—like those captured under the Adaptive Acquisition Framework (AAF) in DOD Instruction 5000.02—they should also explore industry engagement models for AI applications intended for use under DDIL conditions that incorporate warfighter perspectives earlier and more frequently in technology development.[24] Where warfighters will face decisions with trade-offs about what capabilities to bring into contested missions, getting as broad a range of user feedback as possible and understanding the timelines involved in consistent user adoption at the edge can help the department understand how to overcome cultural barriers to adoption, ensure AI solutions cater to specific needs for contested operations, and aid effective, reliable uptake. It may also help program managers identify urgency of need and risk considerations that inform acquisition strategies under the AAF.

More sprint demos and other hands-on opportunities to shorten the feedback loop between operators and technology developers about the usefulness of different AI-enabled capabilities for high-pressure, contested mission sets would be especially valuable. Earlier and more frequent demonstrations can help warfighters develop familiarity with AI capabilities through hands-on experience and begin to calibrate expectations for how DDIL conditions are likely to affect system performance or

20. Jerry T. Kim, "Would Admiral Rickover's Method Still Work in Today's Complex Acquisition and S&T Landscape?," in Proceedings of the Twenty-Second Annual Acquisition Research Symposium and Innovation Summit 1 (2025), https://dair.nps.edu/bitstream/123456789/5394/1/SYM-AM-25-331.pdf.
21. Cybersecurity and Infrastructure Security Agency and Australian Signals Directorate's Australian Cyber Security Centre, "Principles for the Secure Integration of Artificial Intelligence in Operational Technology," CISA, December 3, 2025, https://www.cisa.gov/resources-tools/resources/principles-secure-integration-artificial-intelligence-operational-technology.
22. DOD Office of Inspector General report on the effectiveness of CDAO's AI services and governance, November 2024 (finding delays in the CDAO's AI implementation plan and ambiguity over roles relative to the DOD CIO); and Kelley M. Sayler, "Realignment of DOD's Chief Digital and Artificial Intelligence Officer (CDAO)," Congressional Research Service, IN12615, December 2025, https://www.congress.gov/crs-product/IN12615.
23. Brandi Vincent, "Feinberg's New Maven Directive Sets AI-enabled Decision-making as 'The Cornerstone' for CJADC2," DefenseScoop, April 3, 2026, https://defensescoop.com/2026/04/03/palantir-maven-feinberg-directive/; and Brandi Vincent, "DOD Components Face 'Aggressive' Timeline for Maven Smart System Transition," DefenseScoop, April 15, 2026, https://defensescoop.com/2026/04/15/palantir-maven-smart-system-pentagon-program-transition-feinberg/. The designation derives from a March 9, 2026, memorandum issued by Deputy Secretary of Defense Steve Feinberg.
24. DOD, Instruction 5000.02: Operation of the Adaptive Acquisition Framework, Office of the Under Secretary of War for Acquisition and Sustainment, January 23, 2020, incorporating Change 2, April 8, 2026, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.PDF.

reliability. From the industry side, technology developers can design system components that users identify as important for edge systems. Warfighters at the edge are well-positioned to understand the impact of distributional shifts in tactical conditions, where a model's deployed performance differs from its performance in training, and their experience can help uncover edge cases in conjunction with engineers. Design choices that will likely deserve special attention in DDIL contexts include notifications of degraded system performance, user interface designs, and considerations for what graceful degradation looks like. Other methods for iteratively incorporating warfighter feedback could also include embedding contractors within deployed units to make in-theater adjustments to models and systems; nonprime vendors with higher levels of risk tolerance may have flexibility to execute upon such agreements. This would prove more difficult, particularly in wartime, and would hinge on special contracting mechanisms and agreements with companies.

Some related contracting mechanisms for iterative development and other engagements already exist. The Swarm Forge Prototype Project, including the Crucible demonstrations involving warfighter participation as part of the AI acceleration strategy, is one example of efforts to adopt iterative prototyping for DDIL-relevant capabilities.[25] The Commercial Solutions Opening and Other Transaction Authority are two mechanisms that have accelerated prototyping, and the DOD's Software Acquisition Pathway for procuring software programs is explicitly built around active user engagement and rapid, iterative delivery.[26] Yet transitioning prototypes to capabilities can be difficult. A February 2025 GAO report found that scaling Defense Innovation Unit efforts proved difficult because the unit was not positioned to help overcome systemic integration challenges after developing successful prototypes.[27] The Defense Innovation Unit (DIU) itself is now pursuing a more embedded model along these lines: Through its "Thunderforge" initiative, launched in 2025 with Scale AI and industry partners, it has placed personnel at Pacific Command and European Command to develop AI-assisted planning and wargaming tools alongside the operational users who will rely on them.[28] For DDIL-relevant capabilities specifically, iterative development should be tied both to capability refinement and the doctrine, training, and updates to TTPs required to field it. The services should explore developing explicit requirements in demonstrations and sprints related to AI applications intended to be used in DDIL conditions.

The iterative design-feedback loop can ultimately benefit both warfighters and industry. For operators, frequent sprint engagements that incorporate DDIL conditions can surface challenges around confronting cognitive overload, calibrating expectations for degraded performance, and developing judgment about the validity of AI-generated operating pictures. For industry, the same interactions yield behavioral data that goes beyond standard testing metrics and can sharpen understanding of human-machine interactions in DDIL environments as tangible design problems to be addressed. They may help identify technical solutions that make operators more likely to take AI-enabled capabilities into contested missions and point toward longer-term research priorities.

Testing, red-teaming, and experimentation

Operational testing, evaluation, verification, and validation (TEVV) practices for AI present unique challenges. Unlike hardware systems, AI models can perform differently in complex deployed environments than in controlled training and testing conditions, and they require frequent updates to maintain consistent performance. As both DOD guidance and TEVV practitioners have previously noted, the linearly oriented test and evaluation processes developed for traditional systems are poorly suited to these characteristics. Pushing AI capabilities to the tactical edge often necessitates using lighter, more fragile versions of models, meaning that continued observation of model performance is critical to identifying and addressing limitations.

Adapting TEVV practices for edge AI capabilities should not be viewed as an impediment to rapid adoption, but rather a valuable way to ensure continued military effectiveness and calibrated trust. Updating test processes throughout the life cycle of AI-enabled capabilities will help ensure systems keep pace with existing and emerging threats. A useful organizing

25. Miles Jamison, "DOW CDAO Selects 25 Companies for Crucible 2 Swarm Forge Initiative," ExecutiveGov, June 3, 2026, https://www.executivegov.com/articles/cdao-crucible-2-swarm-forge-initiative-pentagon.

26. Department of Defense Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF; and Jon Harper, "Hegseth Issues Edict on DOD Software acquisition," DefenseScoop, March 7, 2025, https://defensescoop.com/2025/03/07/hegseth-memo-dod-software-acquisition-pathway-cso-ota/.

27. "Defense Innovation Unit: Actions Needed to Assess Progress and Further Enhance Collaboration," US Government Accountability Office, GAO-25-106856, February 2025, https://files.gao.gov/reports/GAO-25-106856/index.html.

28. Brandi Vincent, "Combatant Commands to Get New Generative AI Tech for Operational Planning, Wargaming," DefenseScoop, March 5, 2025, https://defensescoop.com/2025/03/05/diu-thunderforge-scale-ai-combatant-commands-indopacom-eucom/; and Sydney J. Freedberg Jr., "AI for War Plans: Pentagon Innovation Shop Taps Scale AI to Build 'Thunderforge' Prototype," Breaking Defense, March 5, 2025, https://breakingdefense.com/2025/03/ai-for-war-plans-pentagon-innovation-shop-taps-scale-ai-to-build-thunderforge-prototype/.

frame from the DOD's AI Assurance Framework identifies four interlocking layers of TEVV:[29]

1. **Testing the model in isolation**. Ensuring that an AI model can perform as expected in controlled environments with few adversarial challenges.
2. **Testing integration with legacy platforms.** Identifying where integration failures may arise in interactions among AI and legacy components within complex systems-of-systems. This is especially relevant for near-term operational readiness at the edge as AI components are integrated into existing systems and hardware.
3. **Human-factors testing.** Incorporating human feedback to uncover gaps in human-machine integration, including warfighters' mental models for AI-enabled systems and the "co-situation" of human and machine roles fitting practically into operations. Such testing can highlight boundary awareness issues, i.e., understanding the conditions under which the model is likely to perform at or near capacity and whether this is obvious to a human operator. Task allocation can delineate between functions an operator reasonably expects the system to perform and where human intervention is necessary or desirable. It is also important for highlighting where critical skills should not inadvertently be permitted to atrophy by assuming that AI capabilities can fulfill current human roles, particularly if AI capabilities will have imperfect performance in DDIL contexts. Identifying model drift and out-of-domain identification can illustrate where model performance may degrade or exceed boundaries. This process can help generate metrics for explicit bounds of acceptable use to aid warfighters with mission planning and deployment choices for DDIL environments.
4. **Operational testing under realistic conditions.** Testing an AI-enabled capability in an exercise or controlled, real-world environment to uncover previously unforeseen challenges.[30]

These four pillars highlight threat and vulnerability vectors from both technical and human-factors considerations critical for AI-enabled capabilities. They reflect current guidance, but implementation likely remains in early stages as DOD's developmental test and evaluation guidebook for AI was published in 2025. Supporting modernized TEVV processes should be a cross-cutting priority at the service level.

The human-factors layer is particularly crucial given DDIL challenges. Research suggests large-sample testing approaches suited to algorithmic performance face severe limitations in contexts where only handfuls of operators may be able to test human-machine teaming dynamics.[31] Limited data on DDIL conditions, combined with the structural challenge that AI systems do not reliably signal their own uncertainty to operators, makes dedicated human-factors testing capacity nearer to the edge an essential requirement. Such testing can build trust and understanding, while also helping generate metrics across programs to measure what effectiveness in complex human-machine teams looks like.[32]

Furthermore, TEVV practices need to be reinforced with rigorous red-teaming for DDIL conditions. Red teams represent a critical component of AI test design and, for DDIL environments specifically, red teams must be capable of emulating current and future peer competitor capabilities and performance. Red-teaming should be integrated into the entire AI life cycle and should focus on operational performance and mission resilience in the face of adversarial attacks. Such red-teaming would include pitting AI-enabled systems against challenges like sensor spoofing, electronic warfare, and degraded functionality. The Defense Advanced Research Projects Agency's Securing Artificial Intelligence for Battlefield Effective Robustness provides an exemplar for red-teaming efforts focused on contested conditions that could be extended to service-level capabilities.[33]

29. The four-layer framing draws on the test and evaluation approach developed by the department's Joint AI Center (now CDAO). See Jackson Barnett, "How the DOD Is Developing Its AI Ethics Guidance," FedScoop, September 2, 2020, https://fedscoop.com/jaic-alka-patel-ai-ethics/; the article describes the JAIC testing strategy's focus on evaluating models against requirements, integration with existing systems, the human-machine relationship, and operational testing.
30. See National Academies of Sciences, Engineering, and Medicine, T&E Challenges for Artificial Intelligence-Enabled Systems for the Department of the Air Force, Consensus Study Report, 2023, doi.org/10.17226/27092.
31. "Developmental Test and Evaluation of Artificial Intelligence Enabled Systems," Office of the Under Secretary of Defense for Research and Engineering, n.d., https://www.cto.mil/dtea/te_aies/; and for information on the incompatibility of large-sample testing approaches with human-machine teaming evaluation, see David Helmer et al., "Human-centered Test and Evaluation of Military AI," Panel Session Summary, Responsible AI in the Military Domain 2024, Seoul Korea, September 9–10 2024, arXiv:2412.01978; and National Academies, T&E Challenges.
32. Jay Wilkins et al., "A Team-Centric Metric Framework for Testing and Evaluation of Human-Machine Teams," Systems Engineering 27, no. 3 (2024): 466–84, https://doi.org/10.1002/sys.21730.
33. Defense Advanced Research Projects Agency, "SABER: Securing Artificial Intelligence for Battlefield Effective Robustness," n.d., https://www.darpa.mil/research/programs/saber-securing-artificial-intelligence.

The continuous battlefield adaptation with emerging technologies evidenced in Ukraine suggests that services and combatant commands should consider adding specific billets for certified AI testers within tactical units, specifically for evaluating the performance of deployed AI models when intended for use in new contexts and to rapidly retrain, test, and field new and updated capabilities.[34] The services should more deeply explore embedding operational research teams forward with units using AI at the edge. These teams would consist of small groups of data scientists, engineers, and operational analysts who can diagnose system performance issues on site, validate fixes on operational hardware, and push updates (where possible) within the short (or even the same) operational windows. Such teams could help decrease the lag time between issue discovery and fixes in DDIL conditions by responding to performance problems in near real-time, relying on edge compute nodes and taking tactical conditions into account. This could confer the advantage of enabling rapid fixes and increased responsiveness to adversarial conditions rapidly, with sensitivities to local, mission-specific data and targeted updates that facilitate more predictable system performance across mission sets. With established, clearly delineated authorities in place for combat, operational research teams with certified-tester billets could theoretically implement safe fixes without needing to transfer data rearward or waiting for analysis and updates to be pushed from the front. Sustaining TEVV capacity beyond initial deployment in this way would require dedicated resources for both pre-deployment testing budgets and post-deployment sustainment costs, a reality for which the services likely have not currently planned.

To complement progress in incorporating AI-specific TEVV practices into capability development and deployment, the Joint Force should continue to experiment at scale with AI-enabled capabilities in exercises and simulations of operations in denied conditions. Such experimentation will be essential to understanding how model performance holds up as DDIL conditions intensify. For example, simulations in virtual environments may allow users to understand how AI-enabled capabilities' ability to comply with changing rules of engagement holds or declines with corresponding increases in the contested nature of the environment. Such exercises also can present operators with realistic mission planning scenarios for DDIL conditions. Working through decisions about which AI-enabled capabilities to bring on a given mission based on power, thermal, bandwidth, and connectivity constraints, and when analog alternatives may be preferable, offers practical experience difficult to attain elsewhere. High-fidelity exercises, informed by education and training, can help operators "tinker" with edge systems and innovate at the unit level within safe parameters. Simulations may also allow for AI capabilities to be integrated into live, virtual, constructive training (LVCT) and serve as another venue for iterative feedback on DDIL-relevant capability development. Given the difficulty of accessing training data for DDIL contexts, such simulations may also generate useful synthetic and behavioral data.

Concrete venues for this already exist. The Marine Corps' Project Tripoli is building a networked LVCT environment incorporating AI- and machine-learning-assisted scenarios across the Marine Expeditionary Forces, which can host iterative testing of edge AI under realistic operational conditions.[35] A/B testing methods associated with commercial software can be adapted to surface what cognitive overload looks like in practice without adding burden to warfighters.[36] Together, these approaches can support the unit-level initiative and experimentation that have traditionally been considered enduring advantages for the US military.

Adapting professional military education for AI

The services are beginning to implement training and professional military education (PME) programs geared toward helping end users incorporate AI into military planning processes and course of action development. Some of these programs, such as the Marine Corps' Basic AI Course, aim to provide warfighters with a "foundational understanding" of AI systems' strengths and limitations, including in relation to generative AI capabilities, in line with department-wide guidance and AI education strategy.[37] Other services are producing comparable efforts: The Army's Command and General Staff College

34. Margarita Konaev and Owen J. Daniels, "The Russians Are Getting Better: What Moscow Has Learned in Ukraine," Foreign Affairs, 2023, https://www.foreignaffairs.com/ukraine/russians-are-getting-better-learning.
35. Heather Mongilio, "Marine Corps Rolling out LVC Training Under Project Tripoli," US Naval Institute, June 27, 2023, https://news.usni.org/2023/06/27/marine-corps-rolling-out-lvc-training-under-project-tripoli; for more on AI- and machine-learning-assisted training scenarios, see Jamie Bennet, "US Marine Corps Seeks Industry Input on Live, Virtual & Constructive Training Program," ExecutiveGov, June 17, 2024, https://executivegov.com/2023/03/us-marine-corps-seeks-industry-input-on-live-virtual-and-constructive-training/.
36. Whitney M. McNamara, Peter Modigliani, and Tate Nurkin, Commission on Software-Defined Warfare: Final Report, Atlantic Council, March 2025, https://www.atlanticcouncil.org/wp-content/uploads/2025/03/Commission-on-Software-Defined-Warfare-Final-Report.pdf.
37. "Marine Corps Mandates Basic AI Training Course for All Troops," DefenseScoop, May 13, 2026; and John Harper, "Pathway to AI Readiness: Workforce Training," DefenseScoop, May 13, 2026, https://defensescoop.com/2026/05/13/marine-corps-mandates-basic-ai-training-course-for-all-troops/; DOD Chief Digital and AI Office, "Expanding Access to the Data, Analytics & AI Workforce for DoW", https://www.ai.mil/Initiatives/DoD-Digital-Workforce/

has begun integrating AI into wargaming; the Air Force Special Operations Command has launched AI bootcamps; and the Naval Postgraduate School has stood up an accelerated AI master's program.[38] These initiatives represent important steps toward building and upskilling an AI-literate force, but they largely emphasize general AI literacy and generative AI use, and understanding the challenges likely to confront users of AI systems in DDIL environments will be critical.

PME curricula should address examples of specific decision-making challenges presented by edge systems in contested environments, including automation bias (the tendency for humans to default to machine judgment), calibrated trust, and skill preservation. As a complement to unit-level training, education can help calibrate expectations for AI-enabled decision systems as tools that can usefully increase operational speed and lethality yet, nonetheless, have shortcomings to be managed. Overconfidence in edge AI systems carries risk, as excessive trust in AI outputs without knowledge of limitations may result in operators failing to exercise human judgment when system performance is degraded near the point of failure. Beyond behavioral risks from human use, AI systems also present structural risks. AI systems operating outside their training distribution will not reliably signal their own uncertainty, meaning operators must supply judgment the system itself cannot.[39] Simultaneously, reflexive skepticism could lead operators to forgo valuable capabilities in mission planning.

Furthermore, PME and training should complement growing AI literacy in the force with measures to help avoid skills decline or the elimination of key roles, should AI capabilities become degraded during contested operations. Avoiding skills decline must be a priority. Determining the propriety of AI solutions to certain operational challenges versus analog ones will be key, and gaps in determining this balance appear to be persistent. A 2023 National Academies review found that human-systems integration has not been prioritized in AI T&E frameworks, and that human-AI interaction models do not yet account for the dynamic and stressful situations warfighters face.[40]

Private sector case studies: John Deere and Tesla

When it comes to incorporating AI into real-world systems and building user confidence, the private sector offers examples for determining user intentions and responding to consumers' needs and wishes. John Deere and Tesla provide two examples for integrating user feedback and salient opportunities and risks for the DOD and services to consider.

John Deere has integrated AI into a range of so-called precision farming capabilities ("precision ag") at scale.[41] In the past decade, the company acquired smaller technology firms to incorporate AI and autonomy into farming products and help mitigate pressing labor shortages.[42] The company developed its StarFire guidance system and the AutoTrac Vision system to power autonomous tractors like the 9RX for crop yielding and the See and Spray Select™ for weed killing using computer vision.[43] Company publications suggested that such precision ag systems could boost productivity by 15 percent and improve the efficient use of fuel, herbicide, and fertilizer inputs.[44] However, adoption of autonomous farm equipment was not a given, since system misperformance could harm crop yields and subsequent profits.

38. Sarah Hauck, "U.S. Army Command and General Staff College leads AI Integration in Professional Military Education," US Army, January 16, 2026, https://www.army.mil/article/290053/; "AI Bootcamp Readies Air Commandos," Air Force Special Operations Command, April 3, 2026; and Brandi Vincent, "Naval Postgraduate School Offering New Accelerated Master's Degree Program in AI," DefenseScoop, December 22, 2025, https://defensescoop.com/2025/12/22/nps-ai-masters-degree-program-naval-postgraduate-school/.
39. National Academies, T&E Challenges; for more on out-of-distribution data and the limits of model robustness, see chapter 3 of T&E Challenges, "Test and Evaluation of DAF AI-Enabled Systems," https://nap.nationalacademies.org/read/27092/chapter/5.
40. National Academies, T&E Challenges; for more on human-systems integration and human-AI interaction under operational conditions, see chapter 6 of that report and the report summary, https://nap.nationalacademies.org/read/27092/chapter/8 and https://nap.nationalacademies.org/read/27092/chapter/2, respectively.
41. Michael Wolf, "John Deere's Robotic Tractor Is the Result of Years of Investment in AI-Powered Farming," Spoon, April 10, 2023, https://thespoon.tech/john-deeres-robotic-tractor-is-the-result-of-years-of-investment-in-ai-powered-farming/#:~:text=Still%20in%20the%20trial%20phase%2C%20early%20versions,describes%20as%20its%20%E2%80%9Cpaying%20test%20cooperators.%E2%80%9D%20But.
42. Katherine Lacey, "The Number of U.S. Farms Continues Slow Decline," Chart, Economic Research Service, US Department of Agriculture, March 12, 2025, https://www.ers.usda.gov/data-products/chart-gallery/chart-detail?chartId=58268.
43. John Deere, 2024 Business Impact Report, 2024, 5, https://www.deere.com/assets/pdfs/common/our-company/sustainability/business-impact-report-2024.pdf; and "AutoTrac Vision 2.0.," John Deere (website), n.d., https://www.deere.com/en/technology-products/precision-ag-technology/guidance/auto-trac-vision-2-0.
44. Ashwing Telang, "Artificial Intelligence at John Deere," Emerj Artificial Intelligence Research, October 13, 2025, https://emerj.com/artificial-intelligence-at-john-deere/.

John Deere's approach to calibrating user trust has relied on a supervised cooperator model. The company used combinations of demos and paid test cooperators to validate its autonomous tractors' performance through a real-time app, allowing farmers to view live video feeds, monitor system metrics, and adjust or pause operations with the goal of incorporating consumer feedback before releasing autonomous farming products broadly. It facilitated word-of-mouth adoption and diffusion across geographic locations as early adopters touted benefits to peers.[45] User feedback enabled the company to understand areas for necessary improvement to complement its own testing at its research and development center in Texas, where the company allows engineers and farmers to exchange insights.[46] Through the company's centralized John Deere Operations Center Mobile, it can notify users of performance issues and machine health updates. While the number of deployed autonomous tractors appears to be limited and the rollout has been slow, the company's "handholding" approach to product rollout is intended to ensure sufficient evaluation of system performance and build human trust.[47] Company press releases and content have framed autonomy as augmentative to farm labor, not substitutional, to allay fears of human replacement by machines.[48]

Tesla's approach to cultivating user trust and confidence differs. It can collect data from millions of vehicles across numerous driving scenarios, helping the company to develop robust resources for more common driving scenarios and edge cases. This should in theory make the AI subcomponents that power Tesla automobiles' self-driving performance able to handle unexpected circumstances encountered on the road.[49] Tesla has spent in the low billions of dollars on research and development in roughly the last two years to improve its fleet's AI capabilities and to develop compute infrastructure.[50]

However, the company's approach to rolling out its AI-enabled "full self-driving" (FSD) mode—one of Tesla's driver-assistance systems—appears to have had mixed results when it comes to building driver trust in the system. FSD began with a beta rollout that pushed updates directly to users' vehicles. FSD, which is a human-supervised system and advertised as "requiring minimal intervention," incorporates automated steering useful for urban environments, accounting for frequent turns, stop signs, pedestrians, and other obstacles.[51] Tesla's vast customer fleet positioned it strongly to collect and use data to make model improvements, but an academic study of Tesla drivers from 2024 comparing user trust in the less-sophisticated "autopilot" mode and FSD beta features found that 93 percent of participants reported trust in autopilot, while only 42 percent reported trusting FSD and 36 percent did not trust it.[52] Crash data released by Tesla suggests that FSD mode with human supervision is nearly twice as safe compared to full-human driver performance in North America (though statistics on this data may have significant limitations for one-to-one comparisons, and metrics are provided by the company).[53] However, human complacency in self-driving modes led the National Highway Traffic Safety Administration (NHTSA) to compel a recall of more than two million Tesla vehicles following an over-the-air update to autopilot mode that the NHTSA viewed as creating driver disengagement risk.[54] This led Tesla to incorporate driver-oriented cameras in vehicles to deter driver passivity.[55]

45. "How Deere Plans to Build a World of Fully Autonomous Farming by 2030," CNBC, October 2, 2022, https://www.cnbc.com/2022/10/02/how-deere-plans-to-build-a-world-of-fully-autonomous-farming-by-2030.html.
46. "Research & Development Center," John Deere, n.d., https://www.deere.com/en/stories/featured/research-dev-center/#:~:text=It%20started%20with%20a%20laptop,Kyle%20Leinaar%2C%20test%20site%20manager.
47. Richard Bishop, "Ag Autonomy Grows Ever Bigger With John Deere CES Announcements," Forbes, January 16, 2025, https://www.forbes.com/sites/richardbishop1/2025/01/16/ag-autonomy-grows-ever-bigger-with-john-deere-ces-announcements/; and Bob Woods, "How Deere Plans to Build a World of Fully Autonomous Farming by 2030," CNBC, updated October 4, 2022, https://www.cnbc.com/2022/10/02/how-deere-plans-to-build-a-world-of-fully-autonomous-farming-by-2030.html.
48. John Deere, "John Deere 8R Autonomous Tractor," via Furrow, March 2025, https://thefurrow.co.uk/john-deere-8r-autonomous-tractor/.
49. "Full Self-Driving (Supervised)," Tesla, n.d., https://www.tesla.com/fsd.
50. "Tesla Research and Development Expenses 2010–2025," Macrotrends, https://www.macrotrends.net/stocks/charts/TSLA/tesla/research-development-expenses.
51. "Full Self-Driving (Supervised)," Tesla.
52. Sina Nordhoff, "Drivers' Reflections on Their Use of Partial Driving Automation, Trust, and Perceived Safety," Transportation Research Part F: Traffic Psychology and Behaviour 107 (2024): 1105–1124, https://www.sciencedirect.com/science/article/pii/S1369847824002729.
53. Brad Templeton, "Tesla Finally Releases FSD Crash Data That Appears More Honest," Forbes, November 14, 2025, https://www.forbes.com/sites/bradtempleton/2025/11/14/tesla-finally-releases-fsd-crash-data-that-appears-more-honest/.
54. "Part 573 Safety Recall Report 23V-838," National Highway Traffic Safety Administration, December 12, 2023, https://static.nhtsa.gov/odi/rcl/2023/RCLRPT-23V838-8276.PDF.
55. Kirsten Korosec, "Tesla Has Activated Its In-Car Camera to Monitor Drivers Using Autopilot," TechCrunch, May 27, 2021, https://techcrunch.com/2021/05/27/tesla-has-activated-its-in-car-camera-to-monitor-drivers-using-autopilot/.

Tesla and John Deere present useful analogs for military technology developers and adopters. John Deere's emphasis on cultivating user trust and integrating new technological capabilities into legacy systems may be especially relevant. The company has also embraced a Startup Collaborator program with smaller precision ag companies that is roughly similar to Other Transaction Authorities-based prototype work in the defense industry. Iterative development and user participation before full rollout appear to have built confidence with target consumers and facilitated adoption. Tesla's ability to swiftly propagate updates throughout its fleet is notable for the goals of creating a seamless user-update experience and ensuring its AI-enabled systems are operating at the cutting edge. However, it also highlights the challenge of automation bias relevant for military users.

These examples' limitations for military contexts are also important. John Deere and Tesla's systems operate in comparatively pristine environments where intentional adversarial challenges are atypical. The pacing considerations in these environments are market pressures, not strategic and military competition pressures, and both companies arguably enjoy advantages in terms of first movement and scale. Furthermore, while the stakes in terms of human lives and well-being in these use cases are not insignificant, broadly speaking they are lower than in combat environments. "Handholding" rollout models like Deere's for edge AI in deployed environments would almost certainly entail risks to embedded developers. Nonetheless, both cases show how providing hands-on learning for edge users, iteratively incorporating feedback, and building confidence through adoption can provide value.

Conclusion and future considerations

Many of the benefits of AI-enabled systems ultimately turn on human decisions: when to judge a system operationally ready, when to deploy it in contested conditions, when to trust or question its outputs, and where to set the bounds of acceptable use in line with strategic priorities and under the laws of war and rules of engagement. Realizing AI's advantages in DDIL environments will depend not only on technological solutions but also on whether human roles, processes, and structures can adapt accordingly.

The necessity for adaptation for DDIL conditions extends beyond the tactical level. The DDIL challenges identified in this report, like degraded communications, model drift, and cognitive overload, require broader engagement from the services to be addressed effectively. The services have an important role to play in setting acquisition and testing standards, owning baseline model data, and developing doctrine, PME, and training; leaders in combatant commands must be aware of any advanced models or AI-enabled capabilities deployed within their area of operations. Preparing for AI-enabled operations in contested environments therefore requires service- and operational-level process and even doctrinal changes away from the edge.

Across DOD initiatives, technical goals and policy have largely outpaced the integration work needed to cultivate fielded capabilities. DDIL environments will threaten or even eliminate the connectivity that lets operators and commanders mitigate integration shortfalls in more permissive conditions. As the US military confronts the high likelihood that future fights will unfold under DDIL conditions, the steps outlined in this report to facilitate effective AI adoption at the edge are summarized as follows:

Delineating authorities (national authorities, services, combatant commands)

- Map authorities across the AI life cycle (e.g., data governance, model updates, deployment, repatriation) and specify in advance which echelon holds each; consider clear Rickover-style models for security-related authorities.
- Set explicit model-update and retraining timelines for peacetime and wartime (e.g., two to four weeks in peacetime, twenty-four to forty-eight hours in conflict), with updates executed where security can be verified.

Iterative development (services and acquisition bodies)

- Tie iterative development to doctrine, training, and TTP updates, not just capability refinement, and make contested-environment conditions explicit requirements in demonstrations and sprints.
- Expand embedded, user-facing development models such as Thunderforge, and develop contracting mechanisms that allow contractor support closer to deployed units, including in wartime.

Testing and experimentation (services, operational test community)

- Adopt life cycle TEVV built around the four pillars and resource it in service budgets, both before and after deployment.
- Incorporate robust red-teaming of AI applications intended for use in DDIL conditions.
- Consider operational-tester billets closer to the edge for AI-specific roles, such as testing and evaluating deployed models set to be used in new contexts.
- Explore how operational research teams can enable rapid, effective testing and model adjustments at the edge in the event of a conflict.
- Experiment at scale under simulated denied conditions, using synthetic data and LVCT environments such as Project Tripoli to surface human-machine integration concerns and critical mission considerations for users.

PME and training (services, PME institutions)

- Services and PME institutions need to build DDIL-relevant curricula addressing automation bias, calibrated trust, and skill preservation.
- PME should complement hands-on, unit-level training.

Finally, several issues fall beyond this paper's scope but warrant attention. Continued progress on model compression, quantization, and faster retraining will be central to what edge AI can realistically do under size, weight, and power constraints. While this paper has focused on protecting US capabilities, the United States is not the only power pursuing AI-enabled information dominance. Complementary work should examine how US forces can impose reciprocal DDIL conditions and costs on adversary systems through data denial, vulnerability exploitation, and the disruption of edge performance in contested spaces.

Regardless of the pace of technical progress, the human element highlighted in this paper will remain central. Most effectively capitalizing on AI capabilities requires human judgment, organizational structure, and doctrine to adapt at pace.

About the author

Owen J. Daniels is a nonresident senior fellow in the Forward Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security. His upcoming book, *AI and the Future of War*, will be available from Polity Press in early 2027. Daniels is also the associate director of analysis and Andrew W. Marshall fellow at Georgetown's Center for Security and Emerging Technology. Previously, he worked in the Joint Advanced Warfighting Division at the Institute for Defense Analyses, where he researched issues including the ethical implications of AI and autonomy, autonomous weapons norms, and joint operational concepts. He has also worked as an associate director in the Atlantic Council's Scowcroft Center for Strategy and Security and as a defense researcher at Aviation Week. He attended Princeton University, where he majored in international relations with minors in Arabic and Near Eastern studies. He has a master's in public policy from Georgetown University's McCourt School of Public Policy.

Acknowledgments

The author thanks project advisers James Cartwright, retired Marine Corps general, Jack Shanahan, retired Air Force lieutenant general, and Douglas Small, retired Navy rear admiral, as well as all of those who participated in consultations to contribute to this report and its recommendations.

The Atlantic Council is grateful to Leidos, Primer AI, Latent AI, and Edge Case for their support of this report. This report was written and published in accordance with the Atlantic Council's policy on intellectual independence, which requires all donors to agree to the council maintaining independent control of the content and conclusions of its work. The author is solely responsible for its analysis and recommendations.

Atlantic Council Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Ilker Baburoglu
Alain Bejjani
Colleen Bell
Peter J. Beshar
*Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
R. Nicholas Burns
Kurt M. Campbell
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
Christopher Cavoli
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
George Chopivsky
Wesley K. Clark
Kellyanne Conway
*Helima Croft
Ankit N. Desai
*Lawrence Di Rita
Dante A. Disparte
Denelle Dixon
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Joseph Durso
Richard Edelman
Stuart E. Eizenstat
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
William E. Grayson
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
*Robin Hayes
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Keoki Jackson
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Karen Karniol-Tambour
*Andre Kelleners
John E. Klein
Ratko Knežević
C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Diane Leopold
Andrew J.P. Levy
Jan M. Lodal
Douglas Lute
Jane Holl Lute
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Judith A. Miller
Dariusz Mioduski
Richard Morningstar
Georgette Mosbacher
Majida Mourad
Mary Claire Murphy
Scott Nathan
*Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Robert O'Brien
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
David H. Petraeus
Elizabeth Frost Pierson
Radu Pițurlea
*Lisa Pollina
Daniel B. Poneman
Robert Portman
Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Laura J. Richardson
*Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
*Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Frances F. Townsend
Melanne Verveer
Kemba Walden
Michael F. Walsh
*Peter Weinberg
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik

**Executive Committee Members*

List as of July 1, 2026

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org