

COMMISSION ON SOFTWARE- DEFINED WARFARE

Final Report



REPORT AUTHORS

Whitney M. McNamara, Peter Modigliani, and Tate Nurkin

COMMISSION CO-CHAIRS

Mung Chiang
Mark T. Esper
Christine H. Fox

COMMISSION DIRECTOR

Stephen Rodriguez

PROGRAM DIRECTOR

Clementine G. Starling-Daniels

COMMISSION STAFF

Mark J. Massa
Curtis Lee
Abigail M. Rudolph
Alexander S. Young

Cover: AI-generated image created with ChatGPT. Image of software-defined warfare for the US military.

March 2025

ISBN: 978-1-61977-365-3

© 2025 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

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

ATLANTIC COUNCIL

COMMISSION ON SOFTWARE- DEFINED WARFARE

Final Report

REPORT AUTHORS

Whitney M. McNamara,
Peter Modigliani, and Tate Nurkin

CO-CHAIRS

Mung Chiang
Mark T. Esper
Christine H. Fox

COMMISSION DIRECTOR

Stephen Rodriguez

PROGRAM DIRECTOR

Clementine G. Starling-Daniels

COMMISSION STAFF

Mark J. Massa
Curtis Lee
Abigail M. Rudolph
Alexander S. Young

Forward Defense's Commission on Software-Defined Warfare:

To drive transformative change in the DoD, the Atlantic Council's *Forward Defense* program convened the Commission on Software-Defined Warfare. The commission was chartered to address the key barriers preventing the DoD from adopting and deploying advanced software solutions and to chart a path toward a more effective, agile, survivable, resilient, and future-ready defense infrastructure and force posture. In partnership with national security experts, industry leaders, and the technology sector, this commission developed actionable recommendations for the DoD and US Congress to transform software acquisition, integration, and management practices to improve US defense.



SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

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.

The **Forward Defense (FD)** program, housed within the Scowcroft Center, generates ideas and connects stakeholders in the defense ecosystem to promote an enduring military advantage for the United States, its allies, and partners. Our work identifies the defense strategies, capabilities, and resources the United States needs to deter and, if necessary, prevail in future conflict.

COMMISSIONERS

Steve Bowsher, president and chief executive officer, In-Q-Tel

Gen James E. Cartwright, USMC (ret.), board director, Atlantic Council; eighth vice chairman of the Joint Chiefs of Staff

Gen Joseph F. Dunford, Jr., USMC (ret.), board director, Atlantic Council; nineteenth chairman of the Joint Chiefs of Staff

Francis A. Finelli, managing director, Carlyle Group

James “Hondo” Geurts, former assistant secretary of the Navy for research, development, and acquisition

Susan M. Gordon, former principal deputy director of national intelligence

Lt Gen S. Clinton Hinote, USAF (ret.), former deputy chief of staff, Air Force Futures

Paul Kwan, managing director, global resilience practice, General Catalyst

Ellen Lord, former under secretary of defense for acquisition and sustainment, US Department of Defense

John Ridge, chief adoption officer, NATO Innovation Fund

Nadia Schadlow, senior fellow, Hudson Institute; former US deputy national security advisor for strategy

Lt Gen Jack Shanahan, USAF (ret.), former director, Joint Artificial Intelligence Center

Trae Stephens, general partner, Founders Fund

ADM Scott H. Swift, USN (ret.), thirty-fifth commander, US Pacific Fleet

INDUSTRY COMMISSIONERS

Rob Bassett Cross, founder and chief executive officer, Adarga; nonresident senior fellow, *Forward* Defense, Scowcroft Center for Strategy and Security, Atlantic Council

Prashant Bhuyan, founder and chief executive officer, Accrete AI

Michael D. Brasseur, chief strategy officer, Saab, Inc.

Todd Bryer, vice president for strategic growth, CAE

Jordan Coleman, chief legal and policy officer, Kodiak Robotics

Scott Cooper, vice president, government relations, Peraton

Steven Escaravage, president, Defense Technology Group, Booz Allen Hamilton

Jon Gruen, chief executive officer, Fortem Technologies

Adam Hammer, co-founder and chief executive officer, Roadrunner Venture Studios

Jags Kandasamy, co-founder and chief executive officer, Latent AI

Rob Lehman, co-founder and chief commercial officer, Saronic Technologies

Joel Meyer, president, public sector, Domino

Sean Moriarty, chief executive officer, Primer AI

Nathan Parker, chief executive officer, Edge Case Research

Gundbert Scherf, co-founder and co-chief executive officer, Helsing

Zachary Staples, founder and chief executive officer, Fathom5

Tyler Sweatt, chief executive officer, Second Front Systems

Dan Tadross, head of federal delivery, Scale AI

Jim Taiclet, chairman, president, and chief executive officer, Lockheed Martin

Chris Taylor, founder and chief executive officer, Aalyria Technologies

Mark Valentine, president, global government, Skydio

ADVISORS

LtGen Michael S. Groen, USMC (ret.), former director, Joint Artificial Intelligence Center

Rob Murray, partner, Back Row Angels; nonresident senior fellow, *Forward* Defense and Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, Atlantic Council

MajGen Arnold L. Punaro, USMC (ret.), advisory council member, Scowcroft Center for Strategy and Security, Atlantic Council

Stu Shea, managing partner and strategic advisor, Shea Strategies, LLC

To produce this report, the authors conducted more than seventy interviews and consultations with current and former officials in the US Department of Defense, congressional staff members, allied embassies in Washington, DC, and other academic and think tank organizations. However, the analysis and recommendations presented in this report are those of the authors alone and do not necessarily reflect the views of individuals consulted, commissioners, commission sponsors, the Atlantic Council, or any US government organization. Moreover, the authors, commissioners, and consulted experts participated in a personal, not institutional, capacity.

TABLE OF CONTENTS

- EXECUTIVE SUMMARY1**
- FOREWORD4**
- ENTERPRISE CHALLENGES5**
- RECOMMENDATIONS.....6**
 - 1. Mandate enterprise data and invest in AI enablers.....6**
 - 2. Ensure software interoperability and integration8**
 - 3. Modernize test and evaluation infrastructure9**
 - 4. Enforce commercial as the default approach for software 10**
 - 5. Transform DoD software requirements 12**
 - 6. Remove all restrictions on software funding..... 13**
 - 7. Measure what matters for DoD software 15**
 - 8. Enable software talent across the enterprise 16**
 - 9. Fully establish a DoD software cadre.....17**
- CONCLUSION 19**
- BIOGRAPHIES.....20**
- ACKNOWLEDGEMENTS23**
- SPONSORS24**
- LIST OF ACRONYMS26**

What is software-defined warfare?

Software-defined warfare is a paradigm of the continuous integration and delivery of cutting-edge technology and leading interoperable software into legacy and future defense systems to drive a software-centric, hardware-enabled approach to warfighting.

EXECUTIVE SUMMARY

A profoundly transformed global security environment presents the United States with its most significant geopolitical and geoeconomic challenges since the Cold War—and perhaps since World War II. China, Russia, Iran, and North Korea—together a new “axis of aggressors”—are increasingly collaborating to support their revisionist geopolitical goals and challenge global stability. Meanwhile, US domestic constraints—such as relative-to-inflation flat defense budgets, military recruitment and talent shortfalls, byzantine acquisition processes, and inadequate industrial capacity—severely limit the US ability to adequately deter and address these threats at speed and scale.

During World War II, US industrial strength and manufacturing capacity decisively factored into the Allies’ victory. Today, however, US defense production capacity falls short of potential wartime demands. In contrast, China’s industrial policies, manufacturing prowess, and strategic focus on software-defined technologies—including artificial intelligence (AI); cloud computing; and development, security, and operations (DevSecOps)—have propelled Beijing to rapidly advance its defense capabilities.

Maintaining the Department of Defense (DoD) status quo—anchored to a defense acquisition system ill-suited to the rapid tempo of modern technological innovation—places the United States at significant risk. This approach undermines the nation’s ability to effectively deter near-peer adversaries in the short term and jeopardizes its capacity to prevail in a major conflict.

Addressing these systemic challenges demands a sustained, long-term effort. Meanwhile, there is an urgent need for near-term, high-impact initiatives to bridge existing capability gaps and reestablish an advantage. That is what this report’s concept of software-defined warfare presents.

Why is software-defined warfare key to US military advantage?

A major area of strategic advantage and deterrence of future conflict is the ability to increase the speed, accuracy, and scale of information sharing across US forces for dramatically faster decision-making and maneuvering compared to US adversaries.

To realize that advantage, the United States must prioritize the adoption of software as a foundational military capability commensurate to the role it will play in future conflicts. This means not only adopting robust novel software capabilities but also ensuring timely updates to existing software-enabled platforms and ensuring disparate capabilities across the Joint Force can communicate and collaborate with one another to exponentially expand the capability of the existing US force structure.

Software-defined warfare

Software-defined warfare (SDW) provides a practical means for the DoD to rapidly transform from a hardware-centric organization reliant on Industrial Age practices and legacy software to a software-centric one more prepared to meet the demands of deterring and combating Digital Age threats.

Specifically, embracing SDW across the DoD can deliver three broad advantages. First and most urgently, the DoD can realize efficiencies by modernizing its legacy platforms—the foundation of today’s force—with advanced software upgrades. This approach integrates cutting-edge technology into existing platforms, better supporting warfighters, optimizing costs, and extending the value of current capabilities. Second, SDW is vital to building the force of the future, which will rely on autonomous,

software-driven, and iteratively updated capabilities. Third, more efficient software adoption and use across the enterprise can deliver time and cost efficiencies for a range of administrative and operational processes.

Achieving these benefits requires developing and using new and enhanced technologies and infrastructure, processes, and human capital that individually and collectively facilitate the scalability of software solutions; adoption of common standards, open architectures, and flexible approaches to data rights; and a workforce able to acquire, integrate, and employ software more efficiently.

To succeed in SDW, the DoD must more effectively engage the US commercial software industry, especially in the development of software that incorporates modern development tools and best practices. While the law requires the DoD to prioritize purchasing commercial solutions, DoD culture favors building over buying in practice. This report highlights how the DoD can leverage leading commercial software more efficiently. Importantly, these commercial solutions must meet the stringent security standards required for defense systems, ensuring both operational integrity and resilience.

Allies and partners are an essential source of US strategic advantage and have an important role to play in the success of SDW. This report focuses on how the DoD can improve and accelerate software acquisition, integration, and use across the enterprise while increasing DoD access to the globally leading US commercial software industry. At the same time, the Commission on Software-Defined Warfare's research continually underscored the need for the DoD to better coordinate with allies and partners on software development, experimentation, and best practices for integration and interoperability. Creating mechanisms to align software-related activities and leverage the best capabilities across these partnerships will enable Washington and its allies to harness the scale and interoperability required to meet existing and emerging security threats. This approach is also vital to maintaining the rapid pace of battlefield software innovation, as demonstrated in Ukraine, which will likely characterize future conflicts.

The commission interviewed more than seventy key stakeholders across the DoD, the defense innovation ecosystem, the commercial and dual-use technology industry, and the US Congress to support its extensive research and deliberations. This effort generated the following nine recommendations that will drive the transformation to SDW.

TECHNOLOGY

1. Mandate an enterprise data repository and invest in AI enablers

The deputy secretary of defense should direct the DoD's under secretary for research and engineering (R&E), in partnership with the Chief Digital and Artificial Intelligence Office (CDAO) and the services, to accelerate the ingestion, organization, storage, and analysis of raw data, with well-defined interfaces that permit enterprise-wide data sharing. Furthermore, CDAO, in partnership with the under secretary for R&E and service chief information officers (CIOs), should invest in the pillars of software and AI development—AI-ready data sets, models and model cards, DevOps platforms, and machine-learning operations (MLOps) enterprise tools—to empower end users to efficiently generate and operationalize software and AI with scale, transparency, and reproducibility in mind.

2. Ensure software interoperability and integration

To ensure interoperability, service CIOs, where possible, should enforce interoperability best practices including Modular Open Systems Approach (MOSA) frameworks (in accordance with 10 USC 2466a per the FY17 National Defense Authorization Act (NDAA)), shared application programming interfaces (APIs), and co-developed reference architectures for multi-vendor environments. A designated Program Executive Office (PEO) in each Service should oversee the functionality of mission integration between disparate capabilities, consolidating tools and leveraging simulations to validate technical integration across mission threads to enable system-of-systems (SOS) warfare.

3. Modernize test and evaluation infrastructure

The DoD should empower the Test Resource Management Center (TRMC) to modernize simulation environments and digital testing infrastructure to support the Department's ability to rapidly validate software and AI enabled platforms at scale. TRMC should also establish joint testing teams and adopt industry best practices for DevSecOps pipelines, with an emphasis on data feedback loops to streamline processes, enhance scalability, and improve system performance through continuous feedback and analysis.

PROCESS

4. Enforce commercial as the default approach for software

Adopt a default approach of acquiring commercial software, requiring justification for custom development. Implement early checkpoints in requirements, acquisition, and contracting phases to ensure thorough market research and industry engagement, embedding this approach into DoD policies and training.

5. Transform DoD software requirements

Exempt most software requirements from the Joint Capabilities Integration and Development System (JCIDS) process and establish dynamic, streamlined requirements-management processes that enable rapid, iterative software development. Create a consortium to provide market intelligence on commercial software and hold quarterly technical discussions with allies to align on shared needs and solutions.

6. Remove all restrictions on software funding

The DoD comptroller, in collaboration with service comptrollers and congressional staff, should update the Financial Management Regulations (FMR) to allow flexible use of research, development, test, and evaluation (RDT&E), procurement, or operations and maintenance (O&M) funding for all software activities, enabling rapid acquisition, threat responsiveness, and reduced risks. Issue an interim policy memo to provide immediate guidance to streamline implementation ahead of the next FMR update. Discontinue BA-8 pilots.

7. Measure what matters for DoD software

Develop and track standardized software metrics across all acquisition programs, with regular reporting to drive improvements in delivery speed, interoperability, and quality. Metrics should include deployment frequency, mean time to repair, API usage, and customer satisfaction, among other metrics, with actionable insights shared across the DoD to identify bottlenecks and streamline processes.

PEOPLE

8. Enable software talent across the enterprise

Develop an extensive, connected, layered, and modular software-centric training program that involves both digital and in-person learning and incorporates the specific requirements of different roles and missions. Partner with academia and expand current defense institution training on software to instill a basic-to-intermediate understanding of software best practices and their value to improve software integration and employment. Create opportunities for software talent to gain commercial experience and foster collaboration between operators and industry.

9. Fully establish a DoD software cadre

Recruit software engineers with experience in modern development environments to guide and inform decision-makers on software pipelines, architectures, and leading commercial solutions on either a full-time or a temporary and episodic basis. Individuals should be deployed in prominent roles, including as CIOs and in program management offices, software factories, AI/data organizations, and operational commands. Leverage special hiring authorities—highly qualified experts (HQEs), special government employees (SGEs)—and the reserves to recruit and retain talent. Establish academic partnerships to develop certified talent pipelines, while revising hiring authorities and conflict-of-interest rules to attract and retain top-tier talent.

FOREWORD

The United States stands at the threshold of a new era in defense and national security. Dramatic changes in the global security environment are upending the established world order, presenting new and unexpected challenges. The war in Ukraine, conflict in the Middle East, and rising tensions in the Indo-Pacific underscore shifting power dynamics. At the same time, we are in an age marked by an escalating pace of technological change. Innovations such as the fusion of AI, autonomy, and robotic systems are poised to profoundly influence national security and economic power. This moment demands decisive action to prepare the US military to adapt swiftly to evolving conditions and reclaim its tactical, operational, and strategic advantages.

An impartial assessment of global geopolitics and geoeconomics reveals significant and widening gaps in US capabilities. These gaps not only undermine deterrence but also place the ability of US military forces to prevail in future conflicts at risk. The shifting geopolitical landscape exposes vulnerabilities in the nation's approach to capability design, development, fielding, and sustainment. Addressing these gaps is imperative to prepare for emerging threats, yet immediate solutions are also needed to confront present dangers. While the principle of "speaking softly and carrying a big stick" has long guided US foreign policy, it is now imperative that US military power and economic strength are capable of deterring potential adversaries and, if deterrence fails, prevailing in conflict. Software-defined warfare presents a vital opportunity to bridge these challenges, providing a pathway to both near-term readiness and long-term competitive advantage.

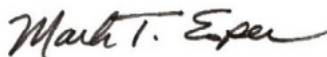
A software-defined mindset and capabilities are essential to modern military readiness. From enterprise solutions to autonomous systems to personnel, software underpins the effectiveness of defense operations. However, Industrial Age, hardware-centric acquisition processes are unsuitable for software systems that need to be updated with the rapid cycle of technological advancement. To preserve its competitive advantages, the DoD must embrace a more agile and integrated approach to software—one that fosters continuous modernization, capitalizes on cutting-edge commercial innovations, and deepens collaboration with allies and partners.

The Atlantic Council's Commission on Software-Defined Warfare was convened to address these challenges and identify solutions. Comprising leaders from government, industry, and academia, the commission identified clear, actionable, and meaningful recommendations that will position the DoD for enduring success. This report's roadmap is organized around three core pillars: technology, process, and people. The recommendations outlined herein propose actionable steps to shape software investments, build a cohesive digital ecosystem, modernize software development practices, and cultivate a skilled and sustainable workforce. Together, these recommendations provide a clear pathway to establishing a software-defined DoD capable of responding rapidly and effectively to emerging threats in an increasingly dynamic security environment.

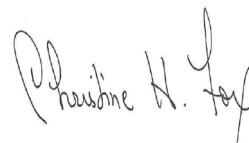
As we present these recommendations, we acknowledge the support and insights of the many contributors who have helped shape this vision. We believe this work will provide leaders with the tools and direction needed to build a DoD that is resilient, innovative, and more fully prepared for the future. Now is the time to build a modern, software-defined defense infrastructure to ensure the safety and security of the United States.



President Mung Chiang



Mark T. Esper



Christine H. Fox

ENTERPRISE CHALLENGES

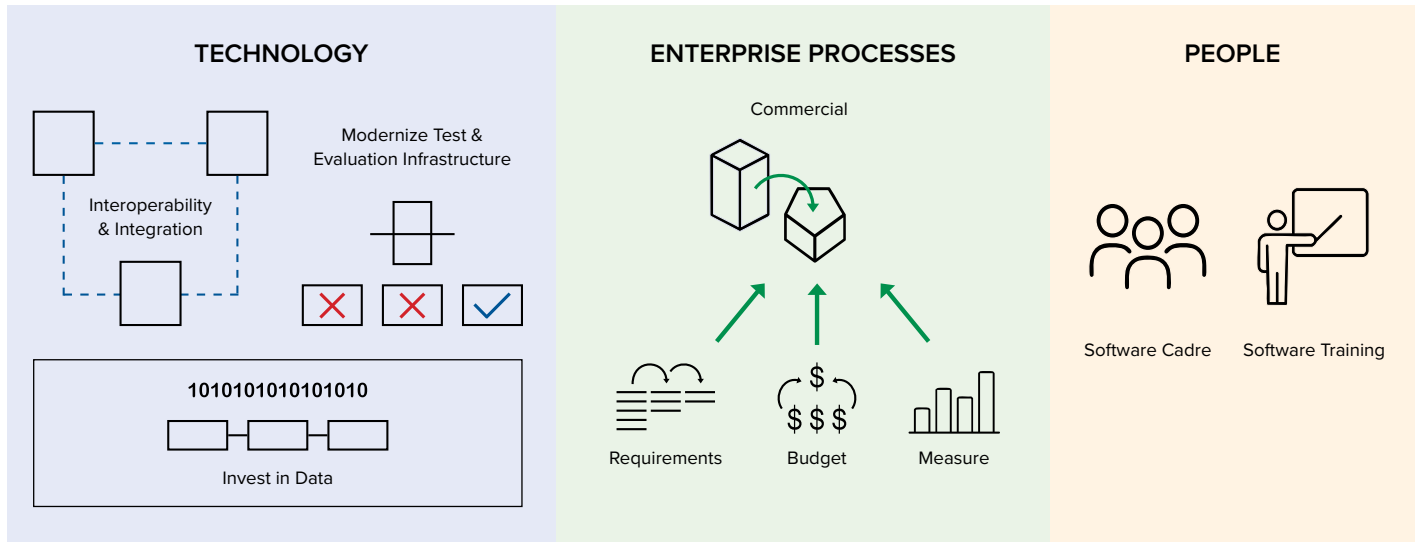
The commission started with a vision for what the future of software-defined modernization and warfare could look like if optimized. Striving to go beyond diagnosing the

challenges facing the DoD enterprise, this commission outlined desired outcomes to help the DoD overcome such challenges.

Challenges (“as-is”)	Outcomes (“to-be”)
The absence of DoD enterprise processes and enablers to rapidly update software with novel capabilities that keep pace with threats.	Enterprise processes, including requirements, acquisition, budget, contracting, and authorities, are aligned to allow the rapid identification and iterative upgrades of software-based systems, capabilities, and platforms.
The DoD has limited processes or proving grounds to allow end users to experiment with, and rapidly adopt and scale, novel software solutions, including AI and autonomy-enabled systems.	End users routinely interact and experiment with novel capabilities leveraging a wide variety of digital infrastructure tools and proving grounds. Testing processes are improved and integrated throughout the capability lifecycle.
The DoD lacks established best practices for developing or buying software.	Department officials better understand software business models and performance outcomes, enabling them to articulate a more predictable demand signal to industry.
The industry faces challenges in providing and deploying its capabilities due to a lack of transparency and predictability, and other bureaucratic hurdles.	A robust ecosystem of software companies regularly delivers software solutions to the DoD. Defense is seen as a desirable market with many more companies competing to provide best-of-breed capabilities.
There is a major shortfall of software pipelines, talent, and resources to meet the demand for software-defined warfare within DoD organizations.	The DoD increases technical and software literacy across the enterprise—from senior leaders to program managers to operators at the edge—through a sustainable, multilayered approach of enhanced training, software career path development, implementation of novel means of targeted recruitment, increased opportunities for engagement with commercial software developers, and collaboration with academia.
Systems, capabilities, and platforms are generated in silos. The disconnect hinders the integration of systems on the battlefield, creation of an interoperable force structure, and the DoD’s goal of a joint warfighting concept, as well as partner and allied collaboration.	Novel systems are developed with integration as a central focus, ensuring seamless compatibility across platforms. Program managers are incentivized to collaborate across programs and Services, aligning their efforts with overarching warfighting goals. Military leaders are equipped with mission integration tools that enable interoperability within existing force structures. This approach allows the United States to achieve a significantly more dynamic force structure, a true Joint Force capability, and the ability to effectively leverage contributions from allies.
The absence of a software-centric culture across the DoD impedes the employment of modern DevSecOps, which fosters rapid iterations.	Through professional development, enhanced industry collaboration, strong leadership, and talent management, the DoD can cultivate a software-centric culture. This shift will drive a middle-out change in how the organization understands and integrates software.

RECOMMENDATIONS

Optimized Software Defined Warfare Conceptual Model



1. Mandate enterprise data and invest in AI enablers

A. Collect and share data across the enterprise

PROBLEM STATEMENT:

Data is the *sine qua non* of modern AI development. Yet, despite progress in recent years, the DoD is still not adhering to its own Data Strategy, which emphasizes the importance of a systematic plan for enterprise-wide data collection, organization, storage, and analysis with well-defined interfaces that permit enterprise-wide data sharing.¹ In 2017 alone, the Pentagon collected twenty-two terabytes of data, or the equivalent of more than 19 million photos, per day.² Given that the volume of data has been projected to double every two years, one can extrapolate that the US military in 2025 is likely to generate around 352 terabytes, or

up to 88 million photos or 17,600 hours of high-definition video, per day.³ The department’s wide variety of platforms and sensors—used to conduct training, tests, joint and coalition exercises, and both peacetime and wartime operations on a global scale—provide it with an extremely high volume of diverse and highly operationally relevant data. DoD leaders must implement and enforce the DoD Data Strategy with regard to the collection, storage, and organization of data to ensure this strategic advantage does not go unexploited.⁴

RECOMMENDATION:

The deputy secretary of defense should direct the DoD under secretary for R&E, in partnership with the CDAO and the services, to accelerate the ingestion, organization, storage, and

1 “Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage,” US Department of Defense, November 2023, https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.
 2 “Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition,” Congressional Research Service, June 4, 2020, <https://sgp.fas.org/crs/intel/R46389.pdf>.
 3 Ibid.
 4 “Executive Summary: DoD Data Strategy,” US Department of Defense, September 30, 2020, <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

analysis of data, with well-defined interfaces that permit enterprise-wide data sharing.

B. Invest in capabilities to develop, deliver, and govern AI solutions at scale

PROBLEM STATEMENT:

Advanced, digitally native companies are delivering transformational impact by building the reusable capabilities that allow these firms to develop, deploy, and govern software and AI solutions rapidly and at scale. By providing their teams with data, tools, and infrastructure—as well as shared repositories of prior projects, pipelines, code, and models—such companies are able to drive innovation and outcomes at scale. Through common, integrated platforms that both span the AI development and deployment lifecycles and unify the growing ecosystem of AI technologies, these groups are able to both accelerate time to value and provide the governance necessary to meet the requirements of exacting, yet evolving, policy with regard to AI safety and observability.

Like large, private-sector companies that are early in their AI maturity, DoD teams that are pursuing digital innovation struggle to access the data, tools, and infrastructure they need to develop and implement solutions. Constrained by legacy systems and fragmented and incomplete tools, and without access to prior work, these teams struggle both to develop and deploy effective solutions. Many projects end with proof-of-concept prototypes that increase institutional skills and learning but typically fail to deliver significant, let alone transformational, change. The result is many individual small-scale digital projects that are mostly bespoke, with no shared code base or documented interfaces that would allow the projects to achieve scale or be reproduced or repurposed. When the leadership turns over, progress is slowed or stopped; in many cases, new leaders restart an innovation cycle.

To ensure that the DoD's investments yield a growing portfolio of robust, operational AI solutions that can be built upon and continuously improved, the CDAO, in partnership with the under secretary for R&E and the services, should lead in acquiring the capabilities to develop, deploy, and govern AI and software solutions—including advanced analytics, machine learning (ML), and generative AI—to be leveraged across the DoD. Key to this effort is creating reusable, secure, and governable capabilities by implementing common platforms that unify the digital ecosystem and span the capability lifecycle. On top of these common platforms, the services should consider their own repositories tailored to address their domain- and service-specific challenges

and should be able to share these securely with each other to foster knowledge sharing and accelerate innovation.

RECOMMENDATION:

- Resource the CDAO, in partnership with the under secretary for R&E and Service CIOs, to acquire and sustain unified, shared platforms that support and accelerate the end-to-end development, deployment, and governance of AI and software solutions—including MLOps capabilities, DevOps platforms, tools for developing, deploying, and reusing models, and reusable AI-ready datasets.
- ▶ The CDAO should consider the best strategy to make these tools accessible to the end-user community across innovation organizations, services, and combatant commands (CCMDs) to empower users to leverage these digital resources to solve mission-critical problems.
- ▶ Services should designate a CDAO liaison that helps them discover what is available to them at the CDAO repository and identify gaps in service-specific investments to ensure department-wide investments are not redundant to better streamline demand for new capabilities.
- Service CIOs, in partnership with CDAO and under secretary for R&E, should be resourced to invest in AI and software enablers that are domain- and Service-specific, and in which the CDAO is unlikely to invest.
- Both the CDAO and the services should maintain unclassified and classified datasets of highly relevant DoD use cases that are available for industry to use to demonstrate capability viability.

Success measure: DoD end users are empowered to leverage their domain expertise to experiment with and operationalize robust and governed AI pipelines with best-of-breed capabilities from industry. AI and software adoption can be scaled faster and more efficiently because capabilities are built with transparency, scale, and reproducibility in mind. The DoD saves money by not buying the same capabilities many times over. There is better coordination and transparency across the department on shared resources for AI and software adoption.

Notional example: The Army's 101st Airborne Division understands the potential of AI and software in addressing operational challenges around an automatic target-recognition problem set and in automating command and control (C2). Instead of building something from scratch, leadership first engages CDAO and the

Army CIO shop to determine what tools are available to them. The Army leverages existing AI-ready data sets on infrared sensors and large language models (LLMs) trained on C2 courses of action (COA) development. Beginning to appreciate the compounding efficiencies in leveraging MLOps enterprise tools for orchestrating multiple work streams and AI pipelines, the 101st considers leveraging an enterprise platform to migrate its existing AI capabilities and workflows.

2. Ensure software interoperability and integration

PROBLEM STATEMENT:

The operational foundation of all warfighting concepts is the underlying information networks, and their digital underpinnings must be integrated to enable data flows across disparate capabilities that make up a kill chain. As capable as these platforms are individually, their ability to share information and collaborate yields greater effects and dynamism than any single platform could achieve independently. Prioritizing the integration of data and machine-to-machine communication can unlock meaningful advantages on the battlefield.⁵

One critical bottleneck hindering effective warfighting is the lack of interoperability between platforms, sensors, networks, and communication links. Capabilities are often developed in silos, with proprietary or bespoke software, and lack interoperability requirements. This results in every platform having a unique way of integrating capabilities into it. Although there are instances in which proprietary software is necessary, it should not be the default.

The links between these capabilities are typically not tested until they deploy for large-scale exercises, which are focused on joint and combined operations and, as such, are not usually the optimum venue to address the complexity of ensuring integration. This challenge becomes exacerbated when operating as a coalition force with allies and partners.⁶ Addressing this problem requires dedicated time in simulated environments or access to digital engineering tools to identify capabilities or

tactics, techniques, and procedures (TTPs) to overcome a lack of organic interoperability.

Service chiefs should identify a PEO charged with ensuring interoperability between systems that make up relevant kill chains for the Service. A program management shop within that PEO should be charged with testing, buying, fielding, and sustaining the mission integration tools that enable these effects.

More dedicated simulation and digital engineering efforts to test integration should help strengthen the demand signal for non-proprietary mission integration tools externally to industry, and the need for better models and model-based system engineering (MBSE) best practices internally.

RECOMMENDATION:

- To ensure interoperability between new capabilities being adopted, Service CIOs, in coordination with Joint Interoperability Test Command (JITC) and the DoD CIO, should mandate
 - ▶ MOSA frameworks applied to the maximum extent practical;
 - ▶ defining modules and leveraging APIs and modular system interfaces to enable data interchange between disparate platforms;
 - ▶ industry and government co-collaborated reference architecture for multi-vendor environments as a best practice; and
 - ▶ industry, where possible, ensuring the capabilities it provides to different parts of the DoD can interoperate with one another.
- To aid in interoperability with allies and partners, these best practices should be shared as early and often as possible with partners through existing allied technical exchanges.

5 Lieutenant General (ret.) John (Jack) N. T. Shanahan, “Reimagining Military C2 in the Age of AI Revolution, Regression, or Evolution,” Special Competitive Studies Project, December 2024, <https://www.scsp.ai/wp-content/uploads/2024/12/DPS-Reimagining-Military-C2-in-the-Age-of-AI.pdf>; Bryan Clark, Dan Patt, and Timothy A. Walton, “Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage,” Hudson Institute, March 3, 2021, <https://www.hudson.org/national-security-defense/implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage>; Todd Harrison, “Battle Networks and the Future Force,” Center for Strategic and International Studies, August 5, 2021, <https://www.csis.org/analysis/battle-networks-and-future-force>.

6 Bryan Clark, et al., “Integrated by Mission—Federated for Execution,” Hudson Institute, September 2024, <https://s3.amazonaws.com/media.hudson.org/Integrated+by+Mission—+Federated+for+Execution+NDIA+ETI+Hudson.pdf>.

- Service chiefs should designate one PEO shop to coordinate service-wide effects.
 - ▶ Consolidate the development, acquisition, management, and modernization of non-proprietary mission integration tools under a dedicated program office within the designated PEO shop to elevate the role of mission integration.
 - ▶ The designated PEO should leverage simulation tools to imitate the feasibility of the technical integration to
 - ensure the successful integration of new and legacy systems, including the use of open-computer architecture to facilitate the deployment of capability on associated hardware;
 - create demand signals for software mission integration tools; and
 - identify new software-enabled capabilities that can enable SoS warfare.

Success measure: Services are incentivized to proactively establish open compute requirements and identify seams between capabilities that would prevent them from carrying out their highest-priority missions and creating acquisition pathways for mission integration tools.

Notional example: The Navy’s PEO for integrated warfare systems (IWS) is designated as the Navy’s “effects” organization. PEO for IWS identifies three relevant operational problems and begins simulating and combining existing force structures to address them. IWS 1.0 stands up with the authority to procure and sustain mission integration tools identified during simulation exercises, as well as to capture TTPs in which end users creatively overcome inorganic integration.

3. Modernize test and evaluation infrastructure

PROBLEM STATEMENT:

As a part of its strategy to maintain military superiority, the DoD is investing tens of billions of dollars to develop and field next-generation warfighting capabilities, including AI-enabled,

software-defined, and autonomous capabilities.⁷ Before fielding, these systems need to be tested and validated to ensure adequate performance and warfighter trust. However, current testing capabilities and infrastructure lag far behind what is required to do this in a rapid, robust manner.⁸

Live training ranges are typically the default for test and evaluation. Although a powerful tool, they have limitations. Having been built decades ago, they are not purposefully built to test digital technologies and concerns around operational security prevent many from freely experimenting. Another challenge is the lack of live test data and the advanced tooling to analyze and learn from it at scale and on relevant timelines.

Although the services have pockets of excellence in simulating or digitally evaluating capability performance, there is a lack of resources for innovation organizations, like the Defense Innovation Unit (DIU), to rapidly test and validate digitally enabled technologies that innovative groups hope to procure in large volumes. Historically, the DoD would buy down risk by injecting significant resources and time into test and evaluation (T&E) before deployment. Today, the DoD must not only field systems on faster timelines but also track performance over system life-cycles. This requires simulation and digital engineering tools to quickly validate the digital underpinnings of capabilities being evaluated, as well as a system in place to feed data being produced back into the product development cycle. The scale and flow of that data are non-trivial, as that resource-intensive feedback loop can greatly accelerate or impede the ability to integrate real-world learning.

Ultimately, a rapid, iterative T&E capability that prioritizes the flow of data can unlock the scale and robustness needed to both support the deployment at scale of these capabilities at deployment and significantly extend the life and performance of these critical systems. Making this capability available to innovation and acquisition organizations at the forefront of software adoption should be imperative.

RECOMMENDATIONS:

In partnership with the under secretary for R&E, CDAO, JITC, and the DIU, charge the TRMC and resource it effectively to provide the digital infrastructure to provide developmental and opera-

7 Department of Defense Releases the President’s Fiscal Year 2025 Defense Budget,” US Department of Defense, press release, March 11, 2024, <https://www.defense.gov/News/Releases/Release/Article/3703410/department-of-defense-releases-the-presidents-fiscal-year-2025-defense-budget/>.

8 “Assessing the Operational Suitability of DoD Test and Evaluation Ranges and Infrastructure,” National Academies, 2022, <https://www.nationalacademies.org/our-work/assessing-the-operational-suitability-of-dod-test-and-evaluation-ranges-and-infrastructure>.

tional testing proving grounds for innovation organizations leading on commercial software adoption.

The TRMC should partner with industry to explore metrics for vendor self-certification for both T&E and verification and validation (V&V) for more mature vendors that have invested in their own state-of-the-art capabilities. This measure will both alleviate the department being a bottleneck to deployment and help to rapidly deploy capabilities that have met the required T&E thresholds co-developed by the TRMC.

The TRMC, in partnership with innovation organizations and Office of the Secretary of Defense (OSD) leaders, should establish joint operational testing and development testing teams that share data, analysis, and tooling across development and deployment stages. This approach should reduce barriers, streamline the test process, and provide continuous system performance improvement, while also incentivizing a DevSecOps pipeline for T&E that is informed by and applies industry best practices for enterprise scalability, advanced analysis, and data sharing.

Success measure: Simulating capability viability becomes a widely accessible and organic part of validating and testing digitally enabled technologies. In addition, metrics are established to drive progress toward the automation of qualification processes and alternative certification paths. This adoption helps create a pipeline that rapidly scales the deployment of robust and trusted software-defined capabilities.

Notional example: The TRMC invests in digital infrastructure focused on testing drones' ability to swarm to overwhelm enemy defenses. The DIU uses this infrastructure to quickly validate compelling candidates for its Commercial Service Openings submissions rapidly and iteratively. The initial testing helps identify existing deficiencies—potentially including adversarial embedded code in a commercial component—as well as best practices for managing the data flows required to monitor the performance of these capabilities, and cross-functional teams organized to begin addressing the problem.

4. Enforce commercial as the default approach for software

PROBLEM STATEMENT:

While a preference for commercial products and services is well established in the Title X statute, the DoD continues to develop new software when there are clear commercial alternatives.⁹ When the DoD decides to develop custom software, this path often results in higher costs, longer schedules, and increased risks. Commercial software is often updated continuously across a broad customer base, of which the DoD could take advantage. Instead, updating software to address threats and bugs or add functionality takes considerable time and funding.

There are growing concerns that many software factories have become bloated, with hundreds of personnel who drive outdated and overly bespoke services instead of service-wide enterprise platforms and services. This approach negates enterprise efficiencies and hinders the adoption of the latest tools and solutions.

RECOMMENDATIONS:

- Requirements, acquisition, and contracting executives install checkpoints in the early phases of software-intensive programs to enforce statutory preferences for commercial software. Require added justification and approvals to pursue a non-commercial software solution.
- Service Chief Technology Officers (CTOs) and the DIU align DoD and industry groups to provide enterprise market intelligence and due diligence for in-depth insights into the commercial software market and include those of allies and partners. These offices should leverage or establish a platform to share these insights. They should publish and maintain a clearer software total addressable market (TAM) by technology segments. This roadmap should outline how they plan to leverage software as part of their annual budget documents to better incentivize and shape industry research and development. This TAM should map to commercial TAMs to identify dual-use or DoD-unique software.
- Update DODI 5000.87 on the software acquisition pathway and related acquisition policies and regulations to require program managers and contracting officers to capture, in

9 "10 USC 3453: Preference for Commercial Products and Commercial Services," US House of Representatives, December 22, 2024, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section3453&num=0&edition=prelim>.

software acquisition and contracting strategies that they pursued commercial solutions to the maximum extent practicable.¹⁰ This should include

- ▶ engaging industry, industry-focused organizations, and consortia to communicate their needs and understand existing solutions;
 - ▶ capturing holistic timelines and costs of buying commercial solutions compared to developing new software (contracting, acquisition, development, integration, test, and updates);
 - ▶ ensuring contracting requirements are captured in a manner that would not preclude viable commercial solutions as partial or whole solutions to address the capability needs;
 - ▶ ensuring contract strategies do not preclude commercial solutions and that they enable leading software vendors and nontraditional defense companies to compete;
 - ▶ enabling DoD users and industry to rapidly demonstrate, prototype, and experiment with commercial solutions for defense applications;
 - ▶ working with testers and certifiers to understand cybersecurity, integration, and other factors to assess the risks and processes of using the software in the defense domain;
 - ▶ ensuring prime contractors and subcontractors default to commercial solutions;
 - ▶ identifying how modular open systems, common interfaces, and standards are leveraged;
 - ▶ publishing the non-commercial item determination in the solicitations for custom software development to allow vendors to appeal that decision, if justified;
 - ▶ ensuring realistic intellectual-property (IP) strategies avoid unrealistic demands for source code while enabling the DoD to update or pivot if costs or performance are unsuitable;
 - ▶ having acquisition sponsors provide supporting justification if commercial solutions are not viable and new development is warranted; and
 - ▶ ensuring requirements and acquisition approving officials or boards must validate the commercial solution analysis early in the process.
- The services, in collaboration with the defense acquisition executive, Defense Acquisition University, DIU, and the CDAO, should expand guidebooks and training for acquisition and requirements professionals on effectively leveraging commercial software. These should be maintained online and regularly updated with insights and resources from across the DoD, government, and industry. They shall include the documentation and compliance tasks avoided by using commercial software. Program offices and portfolio executives should provide regular inputs to guidance and the community on best practices, lessons learned, and adoption metrics.
 - Service CTOs, in partnership with the DIU and the Office of the under secretary for (R&E), should meet quarterly to review software research and development efforts by science and technology (S&T) organizations to minimize duplication with the commercial sector. They should also incentivize organizations charged with developing concepts of operations to do so collaboratively, based on consistent industry engagement, to understand the state of play in commercial technologies that can be leveraged for warfighting missions.
 - Service CTOs and CIOs should have authority to work with the PEOs to co-direct software factory funding. This authorization will ensure the factories focus on the intended objectives and can achieve the performance metrics developed per the Software Modernization Implementation Plan.¹¹ Based on a clear inventory of platforms, services, and personnel, the CTOs and CIOs, in partnership with the PEOs, should adjust investments that maximize efficiencies and effectiveness. These adjustments could include reducing personnel billets and increasing software licenses. These factories should enable increased speed and quality of deploying code to various environments while maximizing interoperability and cybersecurity. PEOs, CTOs, and CIOs should hold software factory leadership accountable to continuously improve per-

10 “DoD Instruction 5000.87: Operation of the Software Acquisition Pathway,” US Department of Defense, October 2, 2020, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF>.

11 “Memorandum for Senior Pentagon Leadership,” US Department of Defense, February 2, 2022, <https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareModStrat.pdf>.

formance metrics and enable software-intensive acquisition programs and operations on the tactical edge. Similarly, the CTOs and CIOs should be accountable to continuously improve enabling policies, resources, authorities to operate, and reciprocity across organizations and the services.

Success measure: The DoD identifies and tracks commercial software acquisition metrics and TAM. The DoD demonstrates a significant increase in commercial software usage, particularly for systems with well-bounded, government-defined modular system interfaces. This measure improves system cost, schedule, and performance.

Notional example: One of the Army's autonomy programs deviates from its strategy of a lengthy government-developed autonomy stack and rapidly acquires commercial software from leading vendors. The program saves years in development and millions in costs, while delivering higher-quality software to operations faster.

5. Transform DoD software requirements

PROBLEM STATEMENT:

The DoD will often spend years defining the initial and detailed requirements, then lock them down for the acquisition program and contractors to execute. This runs counter to modern software requirements, which operate with far greater speed and agility. In modern software development processes, a development team begins with a hypothesis of customer needs, then engages users and stakeholders, mocks up notional solutions, demonstrates existing capabilities, and rapidly prototypes or develops minimum viable products. Based on user feedback, testing, and performance, the scope, requirements, and priorities will change—sometimes drastically. Users, testers, and others will be engaged early and throughout development, with software capabilities delivered rapidly and iteratively. Empowered lower-level officials will regularly shape the scope and priorities of future iterations.

In the event of a conflict this decade, the Joint Force will operate primarily with the current operational systems. Upgrades to many major weapon systems will be driven by software and data on the tactical edge. Given the rapid pace of change in operations, threats, and technologies, the DoD cannot afford to spend years defining software requirements through lengthy, linear bureaucratic processes.

In the FY20 NDAA, Congress exempted any program using the software acquisition pathway from the JCIDS unless a stream-

lined process was agreed upon by all acquisition executives. In the FY24 NDAA, Congress required the department to modernize its requirements system.

RECOMMENDATIONS:

- The DoD should exempt all software requirements below the Major Defense Acquisition Program thresholds from the JCIDS approval processes. This exemption should include requirements for new software capabilities and software upgrades to legacy systems, regardless of the acquisition pathway used.
- Service requirements organizations—in collaboration with Joint Staff J8 forces, acquisition executives, and software leaders—should establish separate, yet complementary, structures, processes, and training to manage software requirements in a streamlined, dynamic, and collaborative environment.
 - ▶ While a high-level document might be used to capture initial operational capability needs, the bulk of software requirements will be managed via dynamic backlogs with active stakeholder engagements.
 - ▶ Policies should delineate hardware and software requirements and enable each to operate on separate timelines and processes. When capabilities reach appropriate maturity levels during system development, use integrated hardware-software testing, digital engineering, modeling, and simulation to verify desired system performance.
 - ▶ Requirements should enable operational agility measured in days and weeks, tailoring for both global and regional needs across the full range of military operations, and should enable operational commands to define and tailor capabilities based on edge-generated data, while providing insight to service software capabilities.
- Service requirements organizations should update policies to require sponsors to provide written justification in an appendix to the requirements document or a companion document, demonstrating that they pursued commercial solutions to the maximum extent practicable. This includes identifying how the requirements community, through the acquisition community, actively engaged industry and the DoD S&T ecosystem to
 - ▶ communicate operational needs, challenges, and environments;

- ▶ understand what commercial solutions exist, the existing applications of these solutions, and the emerging software capabilities that could have military applications;
- ▶ capture requirements in a manner that would not preclude viable commercial solutions as partial or whole solutions to address the capability needs; and
- ▶ foster discussions between the DoD and industry to reduce barriers to buying commercial solutions.

Success measure: Each of the military services updates its software requirements processes to enable greater speed, agility, and quality. Updated training, guidance, and resources enable the requirements and acquisition communities to successfully adopt modern software practices.

Notional example: A major weapons system was unable to detect or react to adversary drones in theater. Through a dynamic software requirements process, this threat becomes the top priority for the next software release. The vendors work closely with operators and testers to rapidly iterate on software upgrades that drastically improve mission operations within weeks.

6. Remove all restrictions on software funding

PROBLEM STATEMENT:

The DoD's FMRs and appropriations constraints drive risks, delays, confusion, and bad strategies to acquire software.¹² The regulations treat software as having a linear development, production, and sustainment lifecycle. How software is acquired—through new development (as an end item or development team services), through a license, or as a commercial item—drives different appropriations. FMR, Volume 2A, Chapter 1 drives considerable debate and confusion about how to properly fund modern software.¹³

“All costs are classified as either an expense or an investment. Expenses are the costs incurred to operate and maintain the organization, such as personal services, supplies, and

utilities. Investments are the costs that result in the acquisition of, or an addition to, end items . . . Costs budgeted in the Operations and Maintenance (O&M) appropriation are considered expenses. Expenses include labor costs of contractor personnel, maintenance, repair, overhaul, rework of equipment . . . and engineering efforts to determine how to satisfy a deficiency.

Costs budgeted in the Procurement and Research Development Test & Evaluation (RDT&E) appropriations include both expenses and investments. Investments are costs to acquire capital assets, equipment, assemblies, support elements such as data, training, support equipment, and contractor support.

Acquiring and deploying a complete system with a cost of \$250,000 or more is an investment and should be budgeted in a Procurement appropriation. Proprietary software financed on an annual fee basis is an expense item properly financed in RDT&E or O&M. Software releases categorized as iterations on the basic release and not involving significant performance improvements or extensive testing are considered a maintenance effort. Commercial Off the Shelf (COTS) systems that require engineering design, integration, test, and evaluation to achieve the objective performance will be budgeted in RDT&E. Commercial items without modification like COTS will be funded in either Procurement or O&M appropriations.”

As the Defense Innovation Board expertly wrote, software is never done.¹⁴ Software must be continuously updated and delivered to provide new features and interfaces, as well as to address bugs, cyber vulnerabilities and technical debt, and to replace outdated components. Acquiring software and platforms as a service is the norm for commercial software and, increasingly, in defense. Rapid updates will be made as threats change. Many organizations and individuals will interpret these regulations differently. Programs can spend months or years debating the interpretation, which increases risks and causes delays. Programs that did not request funding years earlier in the appropriation mix and aligned with an official's FMR interpretation are forced to attempt the difficult process of reprogramming funding through Congress or must pursue suboptimal strategies.

12 “DoD 7000.14-R: Department of Defense Financial Management Regulation (DoD FMR),” Under Secretary of Defense (Comptroller), last updated January 2025, <https://comptroller.defense.gov/fmr/>.

13 “Volume 2A, Chapter 1: ‘General Information’ Summary of Major Changes,” US Department of Defense, October 2008, https://comptroller.defense.gov/Portals/45/documents/fmr/current/02a/02a_01.pdf.

14 “Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage,” US Department of Defense, May 3, 2019, https://media.defense.gov/2019/Apr/30/2002124828/-1/-1/0/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINAL.SWAP.REPORT.PDF.

The DoD and Congress sought to address this issue through budget activity (BA)-8 software funding pilots. However, there were many issues with the pilots selected and unrealistic expectations of the results. The Army recently decided to fund software through RDT&E funds only, yet that imposes additional constraints and issues. Operational commands wanting to upgrade their software have only O&M funding. Shifting all software needs to RDT&E increases competition for limited RDT&E funds between software and hardware needs.

RECOMMENDATION:

- The DoD should immediately discontinue the BA-8 pilots and implement the pilot intent.
 - The DoD comptroller, in collaboration with service comptrollers and congressional appropriations staff, should update the FMR to enable the DoD to acquire, update, operate, and sustain software capabilities with available RDT&E, procurement, or O&M funding appropriated for the capability.¹⁵ This echoes the congressionally directed Planning, Programming, Budgeting, and Execution (PPBE) Reform Commission's recommendation 11A.¹⁶
 - The DoD comptroller should issue a policy memo for immediate action and clarification while adding these changes to the ongoing comprehensive FMR updates per the PPBE Reform Commission.
- DoD and service comptrollers should communicate guidance on implementing the changes across the workforce.

The language would enable any funding appropriated for a software capability to be used regardless of the software activities (e.g., new development versus maintenance) or how it is acquired (e.g., development, COTS, or as a service). This new language should enable

- ▶ rapid acquisition and delivery of leading software capabilities;
- ▶ improved responsiveness to changes in threats, operations, and technologies; and
- ▶ reduced operational, cybersecurity, and programmatic risks.

Success measure: The DoD comptroller issues a software funding directive removing appropriation restrictions and provides clear direction to the workforce on flexible software funding execution.

Notional example: To meet a critical operational requirement, a program explores a range of software acquisition and contracting strategies unburdened by the mix of funding appropriations.

¹⁵ "DoD 7000.14-R."

¹⁶ "Defense Resourcing for the Future," Commission on Planning, Programming, Budgeting, and Execution Reform, March 6, 2024, <https://ppbereform.senate.gov/finalreport/>.

These reports should include the following metrics.

Deployment frequency	The number of software updates deployed to the operational environment (production) in the last year (or time between deployments). Goal: > once per week.
Time to initial deployment	Time from the initiation of software development to the date the initial software capabilities are deployed to an operational environment. Goal: < six months.
Automated testing use and timelines	Program and portfolio use of automated testing and testing timelines. Goal: daily automated testing, development and operational testing timelines declining.
Mean time to restore (MTTR)	The average amount of time it takes to address a critical vulnerability or issue, including testing, certifying, and authority to operate. Goal: < one day.
API use	Total API usage each week or month to enable interoperability and data sharing across applications. Goal: increasing usage each month.
Production software defect density	Defect density of production software in operations each month. Goal: heavily domain dependent.
Security vulnerabilities	Number of security vulnerabilities identified and remediated. Goal: heavily domain dependent.
Change failure rate	Percentage of software changes that resulted in system disruptions, including downtime, errors, or negative impacts on users. Goal: < 10 percent and heavily domain dependent.
Customer satisfaction	Quantitative metrics or qualitative value assessments of customer satisfaction. Goal: > 80 percent of customers rate software high value.
User engagement	Number of user engagements per month by software developers. Goal: end users engaged weekly.
Software reuse	Number of acquisition programs able to reuse software capabilities and infrastructure. Goal: increasing reuse each month.

7. Measure what matters for DoD software

PROBLEM STATEMENT:

All software-intensive systems and all hardware systems with significant amounts of software should be tracked internally and report a modern set of metrics through their chains of command. As many industry leaders have stressed, speed and cycle times are the priority software metrics.

The department made great strides with the rollout of the Software Acquisition Pathway, which requires some metrics and reporting for the nearly seventy-five programs using it.¹⁷ Congress, in Section 846 of the FY23 NDAA, required the DoD to submit a report to Congress on software delivery timelines for programs using the Software Acquisition Pathway or Defense Business Systems. Software metrics, and broader software practices, should apply to programs using any of the acquisition pathways, including the software elements of hardware-intensive weapon systems.

RECOMMENDATIONS:

The acquisition executives’ staff should collaboratively develop new software metrics for most acquisition programs. PEOs, services, agencies, and the OSD should compile and share quarterly or annual reports across the DoD workforce and leadership to provide visibility into trends, best practices, and enterprise issues to drive regular discussions and actions on how to accelerate delivery. These metrics often identify program trends and issues to drive corrective action and continuous improvement. The Navy’s PEO Digital established World-Class Alignment Metrics (WAMS), which are a model for others to follow.¹⁸

The focus of the metrics and subsequent actions at the program, portfolio, and enterprise levels is to continuously deliver impactful software to the user communities to improve mission impact. Each program and organization might have different objectives or challenges to address, such as release velocity, software quality, or user satisfaction. Some of these may have competing forces that must be managed (e.g., quality versus speed). DORA’s annual Accelerate State of DevOps report provides industry-leading metrics for software, including levels for elite, high, medium, and low performance.¹⁹ The DoD should

17 “Software Acquisition,” Adaptive Acquisition Framework, last visited February 19, 2025, <https://aaf.dau.edu/aaf/software/>.

18 “About,” PEO Digital, last visited February 19, 2025, <https://www.peodigital.navy.mil/About/>.

19 “Accelerate State of DevOps Report,” DORA, 2024, <https://dora.dev/publications/>.

strive toward these commercial goals as objectives and tailor performance levels to unique DoD environments.

Major programs and software-intensive portfolios should map out the processes to develop, test, certify, and deploy software, including actual timelines for each phase; key stakeholders involved (by name or organization); key bottlenecks; the opportunities to streamline software delivery timelines; and how stakeholders are accountable to accelerate software delivery speed, manage operational and development risks, and ensure high-quality and secure software. Furthermore, programs and portfolios should identify where additional resources (personnel, tools, and services) at a program, portfolio, or enterprise level would enable speed of delivery. These metrics are more for internal DoD operations, with a subset that might be shared with Congress or publicly.

Success measure: The military services and related organizations track, share, and use a core set of software metrics across the defense enterprise and leverage insights for key decisions, investments, and continuous improvement in speed, quality, reuse, and user satisfaction (mission impact).

Notional example: A PEO of a software-intensive portfolio has an online dashboard of software metrics that is integrated into program and portfolio operations. Program, portfolio, and policy decisions are made based on these metrics, with the workforce culture focused on leaning out processes and barriers to enable rapid, iterative, and quality software deliveries to operations. Acquisition professionals and vendors are incentivized to continuously improve.

8. Enable software talent across the enterprise

PROBLEM STATEMENT

The DoD lacks sufficient software expertise across the DoD workforce to harness software for modern warfare. Absent a software-literate workforce across career fields, the adoption of modern software processes, structures, tools, and strategies will fail to rapidly deliver warfighting capabilities that harness critical technology areas including AI, autonomy, and cyber. While the DoD has taken steps to upskill its existing workforce for the Digital Age, a widely acknowledged software proficiency shortfall remains. While the United States is the world leader in software talent and solutions, the DoD lacks the expertise to effectively acquire, integrate, and use software tools that are central to mission success.

RECOMMENDATIONS

Develop an extensive, connected, layered, and modular software-centric training program that involves both digital and in-person learning and incorporates the specific requirements of different roles and missions across the force. The objective of this effort is to increase awareness of the importance of software to DoD operations, instill a basic-to-intermediate-level understanding of commercial software best practices and agile software development and their value, and build the skills required to more effectively integrate and operate software in specific roles.

Specifically, the DoD should do the following.

- Partner with leading academic institutions in software development to create a curriculum for an approximately week-long in-person or hybrid training course tailored to senior leaders in the DoD. This executive training curriculum should concentrate on commercial software development best practices and the importance of software to mission execution for senior leaders in the DoD. Training emerging and current senior leaders on these topics can help the DoD develop leaders more willing to create the conditions and culture that will facilitate accelerated adoption.
- Leverage and expand existing successful mechanisms and models for software training, such as the Army Software Factory, and access to digital training libraries at both non-DoD and DoD academic institutions.
- Defense education institutions across the DoD should enrich training to deepen understanding of the importance of software, commercial software best practices and development approaches, and integration of software into DoD activities. The course curriculum should engage and harness insights from leading software experts in industry, as well as in academia, to determine the skill sets and knowledge bases most relevant to the defense context.

In addition to enhancing software literacy through training, the DoD needs to scale formal software career fields and paths for military and civilian personnel to harness the software talent for new and expanded roles. For example, in February 2024, the Air Force reestablished warrant officers for information technology (IT) and cyber career fields to improve technical expertise in cyber and information technologies.

As part of this effort, the DoD should increase opportunities for identified DoD software-focused professionals to interact with both traditional defense industry companies and commercial companies involved in developing software for the DoD. This should include, but not be limited to, embedding DoD talent in these companies for several months to gain firsthand experience in software development cycles and challenges associated with software acquisition. The ability to engage more closely with commercial industry should also extend to the CCMDs, which should expand opportunities for operators to train and experiment directly with commercial industry through exercises such as the Army's Scarlet Dragon, among others.

Success measure: The DoD increases software and technical literacy across the enterprise through scalable training tailored to different DoD levels and roles. The DoD creates opportunities for the identification, enhanced training, and deployment of software talent that can be deployed across the organization to drive software adoption and use.

Notional example: A Navy officer with demonstrated software competence is placed in a leading commercial software company that supports the DoD on a six-month rotation or internship. The officer learns from product developers and product managers to understand commercial development and improvement processes and brings this knowledge back to help operators in a CCMD more efficiently and effectively operate software-defined capabilities.

9. Fully establish a DoD software cadre

PROBLEM STATEMENT

The FY22 NDAA directed the DoD to establish a software cadre of experts in software acquisition and adoption to guide and advise the DoD on how best to improve these activities within the department. Only a handful of staff members were resourced for a massive opportunity space. The need to increase the number of software engineers with experience in modern software development environments persists. The objective of this recruitment is not to enhance the DoD's organic capacity to develop software. Rather, it is to bring in "solution architects" who can use their technical proficiency and understanding of operational requirements to guide and inform program management offices, portfolio executives, software factories, AI and data organizations, operational commands, and others across the DoD enterprise on efforts to rapidly and effectively acquire, integrate, and employ software.

This commission recognizes concerns about the DoD's ability to compete for talent with commercial software companies, based on the DoD's compensation, culture, and conflict-of-interest concerns. This issue is especially the case with high-end talent and senior executives. However, one can also observe a growing pool of mission-focused candidates at various stages of their careers, especially early and mid-career professionals with ten to fifteen years of experience. These candidates value public service and could be available either as part of a full-time cadre or in support of short-term engagements if the DoD can create and employ mechanisms and incentives that allow candidates to move more easily from the commercial sector to government.

RECOMMENDATIONS:

The DoD should recruit fifty to one hundred experienced software engineers in modern development environments and place them in key roles across the enterprise. These individuals' expertise will be used to inform decision-makers on software pipelines, architectures, and leading commercial solutions. Members of this cadre can address key software issues and guide efforts to develop software requirements, acquisition strategies, integration, certification, and employment of software. They can be placed in prominent roles across the DoD, including program management offices and portfolios responsible for acquiring software capabilities; CIO, software factories, and AI and data organizations focused on enterprise services, in operational commands that need to rapidly iterate on tactics and software upgrades; and as executives who oversee major programs, shape budgets, and lead combat operations. Members of this cadre would operate as a network, potentially rotating and surging to meet prioritized problems related to software acquisition, integration, and employment, and sharing best practices and insights.

Candidates can be hired in a full-time role using existing hiring authorities such as HQEs. They can also be engaged on a temporary or episodic basis through commercial talent exchange programs such as CDAO's AI and Data Acceleration program or as SGEs to provide iterative specialized services for a restricted number of days throughout the year. The services should also implement direct commissioning of willing experienced software engineers in the reserves, up to and including the general officer level (as is done for specialized roles such as doctors and lawyers) and should also identify and engage leading software talent already serving in the reserves, similar to the Marine Innovation Unit approach. Programs like GigEagle help identify talent in the reserves for short-term problem sets. By leveraging reservists throughout the year, the DoD can capitalize on existing exper-

tise while mitigating financial and professional risks for those working with the DoD.

Increasing reliance on short-term commercial or reservist software talent will necessitate a review and refinement of conflict-of-interest rules to balance the need to protect the DoD from the risk of providing companies unfair advantages and the need to make it easier for top-level talent to move between the DoD and the commercial sector.

In addition to meeting current demand, the DoD should partner with academic institutions to develop talent pipelines of individuals who are educated and certified in commercial software processes and engineering as well as in the DoD processes and requirements. The DoD should work with interested institutions to develop curriculum and certification criteria that will allow students to be fast-tracked into the DoD software cadre positions.

Success measure: The DoD successfully recruits an increased number of software experts and solutions architects over the next two years to advise on software development, acquisition, and adoption within program offices and CCMDs in particular, while also building a pipeline of software-focused talent.

Notional example: Cadre members placed in program offices use their expertise to understand the significance of decisions a vendor has made in its software development process and inform program managers and acquisition officers on the implications that development decisions hold for future integration and certification. This guidance allows acquisition professionals to make decisions better informed by downstream considerations, reducing costs and time associated with integration, certification, and upgrading of critical software systems.

CONCLUSION

The commission's report presents clear, actionable recommendations and outlines the desired outcomes to address a critical aspect of modern defense and security. While the adoption of software-defined warfare currently poses a challenge, it is also an area of a defining opportunity. The rapidly shifting geopolitical landscape, marked by an axis of aggressors, demands immediate and decisive action to maintain US strategic advantage. If these recommendations are fully implemented, the United States will possess a modern, agile, and resilient defense infrastructure that is capable of fostering a robust software foundation that will bolster the capabilities of US hardware, while streamlining interoperability across services, allies, and partners.

However, failure to act will leave the nation vulnerable and unable to adequately adapt to rapidly evolving threats. The time to act is now—while the United States prepares for the challenges of tomorrow, software-defined warfare provides a timely and practical solution to strengthen US defense capabilities today. Leaders in the DoD, Congress, and the private sector should work to implement these recommendations with a sense of urgency—the members of this commission stand by to help them do so. At stake is nothing less than the stability of the US-led, rules-based international order and the decades of unprecedented peace and prosperity it has undergirded.

BIOGRAPHIES

CO-CHAIRS



Mung Chiang is the president of Purdue University and the Roscoe H. George distinguished professor of electrical and computer engineering. Prior to being elected university president in 2022, he was the John A. Edwardson dean of the College of Engineering and executive vice president for strategic initiatives at Purdue University.

Chiang received BS (1999), MS (2000), and PhD (2003) from Stanford University and an honorary doctorate (2024) from Dartmouth College. Before 2017, Chiang was the Arthur LeGrand Doty professor of electrical engineering and an affiliated faculty in computer science and in applied mathematics at Princeton University.

He founded the Princeton EDGE Lab in 2009 and co-founded several startup companies and industry consortia since the early years of edge computing. Most of his twenty-six US patents are licensed for network deployment. He co-authored two textbooks based on massive open online courses: *Networked Life* (2012) and *Power of Networks* (2016). For his research in communication networks, wireless technology, and network optimization, he received the NSF Alan T. Waterman Award (2013), as well as IEEE Founders Medal (2025), IEEE INFOCOM Achievement Award (2022), IEEE Kiyo Tomiyasu Award (2012), and Guggenheim Fellowship (2014). He was elected to the American Academy of Arts and Sciences (Class of Mathematical and Physical Sciences 2024), the National Academy of Inventors (2020), and the Royal Swedish Academy of Engineering Sciences (2020).

In 2020, as the science and technology adviser to the US secretary of state, Chiang initiated tech diplomacy programs in the US government. In 2024, he started serving on the inaugural board of the US Foundation for Energy Security and Innovation, and was elected to the Board of Directors of the US Olympic and Paralympic Committee as an independent director.



Mark T. Esper served as secretary of defense from 2019-2020, and as secretary of the army from 2017-2019. A distinguished graduate of West Point, he spent twenty-one years in uniform, including a combat tour in the Gulf War. Esper earned a PhD from George Washington University while working on Capitol Hill, at the Pentagon as a political appointee, and as a commissioner on the US-China Economic and Security Review Commission. He was also a senior executive at a prestigious think tank, two business associations, and a Fortune 100 technology company. Esper is the recipient of multiple civilian and military awards. He currently sits on several public policy and business boards, including the Atlantic Council board of directors.



Christine Fox is a senior fellow at Johns Hopkins Applied Physics Laboratory (JHU/APL). Previously, she was the assistant director for policy and analysis at JHU/APL, a position she held from 2014 to early 2022. Before joining APL, she served as acting deputy secretary of defense from 2013 to 2014 and as director of Cost Assessment and Program Evaluation (CAPE) from 2009 to 2013. As director, CAPE, Fox served as chief analyst to the Secretary of Defense. Prior to her DoD positions, she served as president of the Center for Naval Analyses from 2005 to 2009, after working there as a research analyst and manager since 1981. Currently, she also serves on many governance and advisory boards including the Strategic Competitive Studies Project, Palantir Technologies, Muon Space, DEFCON AI, and Brown Advisory. Fox holds bachelor's and master's degrees in applied mathematics from George Mason University. She is a three-time recipient of the Department of Defense Distinguished Public Service Medal and of the Army's Decoration for Distinguished Civilian Service.

CO-AUTHORS



Whitney McNamara is a vice president at Beacon Global Strategies. Prior to that, McNamara worked in the Office of the Secretary of Defense for Research and Engineering, where she served as the S&T portfolio lead at the Defense Innovation Board, whose mission is to provide the secretary of defense, deputy secretary of defense, and other senior leaders with recommendations on emerging technologies and innovative approaches that DoD should adopt to ensure US technological and military dominance.



Peter Modigliani is a senior advisor at Govini, advising under secretary of defense for acquisition & sustainment on strategic acquisition initiatives. Prior to that, he was a vice president at Beacon Global Strategies. Modigliani subsequently served as a defense acquisition leader within the MITRE Corporation, enabling the DoD and intelligence community to deliver innovative solutions with greater speed and agility. He works with acquisition and CIO executives, program managers, the Section 809 Panel, congressional staffs, industry, and academia to shape acquisition reforms, strategic initiatives, and major program strategies. Prior to MITRE, he was an assistant vice president with Alion Science and Technology. Modigliani began his career as an Air Force program manager for command, control, communications, computers, intelligence, surveillance, and reconnaissance programs.



Tate Nurkin is a nonresident senior fellow with the Atlantic Council's *Forward Defense* and *Indo-Pacific Security Initiative* in the Scowcroft Center for Strategy and Security. He is the founder of OTH Intelligence Group (OTH), which provides research, analysis, and consulting on defense technology, the global defense industry and markets, and Indo-Pacific security as well as wargaming and scenario planning support. Nurkin is also a partner with One Defense where he works with public and private sector organizations to accelerate the transition of emerging technologies into the defense industrial base. Before establishing OTH in March 2018, Nurkin spent twelve years at defense intelligence firm Janes where he served in a variety of roles, including executive director of strategic assessments and futures studies. He previously worked for Joint Man

agement Services, the Strategic Assessment Center of SAIC, and the Modeling, Simulation, Wargaming, and Analysis team of Booz Allen Hamilton. Nurkin holds a master of science degree in international affairs from the Sam Nunn School of International Affairs at Georgia Tech and a bachelor of arts in history and political science from Duke University. He lives in Charlotte, NC.

COMMISSION DIRECTOR



Stephen Paul Rodriguez is the founder of One Defense, a technology-enabled consulting firm that identifies advanced commercial capabilities and accelerates their transition into the defense industrial base. He was a senior leader at an artificial intelligence growth-stage company and a global defense corporation. He has also been in and out of the US government throughout his career, including operational service in Colombia, Armenia, Azerbaijan, and Afghanistan. Rodriguez serves on the Boards of fourteen venture-backed companies, including Applied Intuition, Chariot Defense, Firestorm, Kela Systems, Smack Technologies, Ursa Major Technologies, and ZeroMark. He is also a commission director at the Atlantic Council, chairman of Blue Forge Alliance, and a life member at the Council on Foreign Relations. Rodriguez received his BBA from Texas A&M University and an MA from Georgetown University's School of Foreign Service. He has been published in the *Wall Street Journal*, *Foreign Policy*, *WarOnTheRocks*, and *National Review*.

PROGRAM DIRECTOR



Clementine G. Starling-Daniels is the director of the Atlantic Council's *Forward* Defense program and a resident fellow within the Scowcroft Center for Strategy and Security. In her role, she shapes the center's US defense research agenda and produces thought leadership on US security strategies and the evolving character of warfare.

Her research focuses on long-term US thinking on issues like China and Russia's defense strategies, space security, defense industry, and emerging technology. Prior to launching *Forward* Defense, Starling-Daniels served as deputy director of the Atlantic Council's Transatlantic Security team, specializing in US security policy toward Europe and NATO. During her time at the Atlantic Council, Starling-Daniels has written numerous reports and commentaries on US space strategy, deterrence, operational concepts, coalition warfare, and US-Europe relations. Outlets that have featured her analysis include *Bloomberg*, *Defense One*, *Defense News*, *RealClearDefense*, *the National Interest*, *SpaceNews*, *NATO's Joint Air and Space Power Conference*, *the BBC*, *National Public Radio*, and *ABC News*, among others. Starling-Daniels previously worked in the UK Parliament focusing on technology, defense, and Ukraine. She graduated with honors from the London School of Economics with a BSc in international relations and history and she received her Master of Arts in Security Studies from Georgetown University's School of Foreign Service.

COMMISSION STAFF

Mark J. Massa is the deputy director of the *Forward* Defense program of the Scowcroft Center for Strategy and Security at the Atlantic Council. He leads *Forward* Defense's work on strategic forces policy. He holds an MA in security studies and a BSFS in science, technology, and international affairs from Georgetown University.

Curtis Lee is a program assistant in the *Forward* Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security. His work focuses on defense innovation and policy. He holds a MS in public policy and management, a BS in policy and management, and a BA in Chinese studies from Carnegie Mellon University.

Abigail M. Rudolph is a program assistant in the *Forward* Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security. Her work focuses on defense industrial policy, defense innovation, and emerging technology. She holds a BA in national security with a minor in sustainability from Baldwin Wallace University.

Alexander S. Young is a project assistant in the *Forward* Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security. His work focuses on defense industry, emerging technologies, and national security policy. He holds a BA in political science and global studies from the University of California, Santa Barbara and a MSc in global politics from the London School of Economics and Political Science.

ACKNOWLEDGEMENTS

This report was written and prepared with the support and input of its authors, commissioners on the Atlantic Council's Commission on Software-Defined Warfare, and the *Forward* Defense program of the Atlantic Council's Scowcroft Center for Strategy and Security.

This effort was conducted under the supervision of Commission Director Stephen Rodriguez, *Forward* Defense Director Clementine Starling-Daniels, Deputy Director Mark J. Massa, Program Assistant Curtis Lee, Program Assistant Abigail Rudolph, and Project Assistant Alexander Young. Thank you to Kathryn Levantovskaia and Holly Ryan for earlier contributions. Special thanks to Atlantic Council CEO Fred Kempe and Matthew Kronig for their support of this effort.

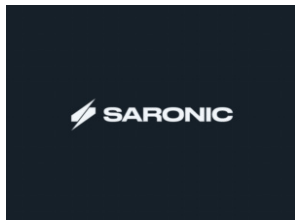
This effort has been made possible through the generous support of Booz Allen Hamilton, CAE, Helsing, Lockheed Martin, and Second Front Systems as foundational sponsors, as well as sponsorship from Aalyria Technologies, Accrete, Adarga, Domino Data Lab, Edge Case Research, Fathom5, Fortem Technologies, Kodiak Robotics, Latent AI, Peraton, Primer AI, Saab, Saronic Technologies, Scale AI, and Skydio.

FOUNDATIONAL SPONSORS

Booz | Allen | Hamilton



SPONSORS



LIST OF ACRONYMS

AI: Artificial intelligence	MOSA: Modular Open Systems Approach
API: Application programming interface	NDAA: National Defense Authorization Act
BA-8: Budget activity eight	O&M: Operations and maintenance
C2: Command and control	OSD: Office of the Secretary of Defense
CCMD: Combatant command	PEO: Program executive officer/office
CDAO: Chief Digital and Artificial Intelligence Office	PPBE: Planning, programming, budgeting, and execution
CIO: Chief information officer	R&E: Research and engineering
COA: C2 courses of action	RDT&E: Research, development, test, and evaluation
COTS: Commercial off the shelf	S&T: Science and technology
CTO: Chief technology officer	SDW: Software-defined warfare
DevSecOps: Development, security, and operations	SGE: Special government employees
DIU: Defense Innovation Unit	SOS: Systems-of-systems
DoD: US Department of Defense	T&E: Test and evaluation
FMR: Financial Management Regulations	TAM: Total addressable market
HQE: Highly qualified experts	TRMC: Test Resource Management Center
IP: Intellectual property	TTP: Tactics, techniques, and procedures
IT: Information technology	V&V: Verification and validation
IWS: Integrated warfare systems	WAMS: World-Class Alignment Metrics
JCIDS: Joint Capabilities Integration and Development System	
JITC: Joint Interoperability Test Command	
LLM: Large language model	
MBSE: Model-based system engineering	
MLops: Machine-learning operations	

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

Alain Bejjani

Colleen Bell

Sarah E. Beshar

Karan Bhatia

Stephen Biegun

John Bonsell

Linden P. Blue

Brad Bondi

Philip M. Breedlove

David L. Caplan

Samantha A. Carl-Yoder

*Teresa Carlson

*James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

*George Chopivsky

Wesley K. Clark

*Helima Croft

Ankit N. Desai

Dario Deste

*Lawrence Di Rita

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Richard Edelman

Stuart E. Eizenstat

Tara Engel

Mark T. Esper

Christopher W.K. Fetzer

*Michael Fisch

Alan H. Fleischmann

Jendayi E. Frazer

*Meg Gentle

Thomas Glöcer

John B. Goodman

Sherri W. Goodman

Marcel Grisnigt

Jarosław Grzesiak

Murathan Günal

Michael V. Hayden

Robin Hayes

Tim Holt

*Karl Hopkins

Kay Bailey Hutchison

Ian Ilnatowycz

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

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mark Machin

Marco Margheri

Michael A. Margolis

Chris Marlin

William Marron

Roger Martella

*Judith A. Miller

Dariusz Mioduski

*Richard L. Morningstar

Georgette Mosbacher

Majida Mourad

Mary Claire Murphy

Julia Nesheiwat

Edward J. Newberry

Franco Nuschese

Joseph S. Nye

*Ahmet Ören

Ana Palacio

*Kostas Pantazopoulos

Alan Pellegrini

David H. Petraeus

Elizabeth Frost Pierson

*Lisa Pollina

Daniel B. Poneman

Robert Portman

*Dina H. Powell

McCormick

Michael Punke

Ashraf Qazi

Laura J. Richardson

Thomas J. Ridge

Gary Rieschel

Charles O. Rossotti

Harry Sachinis

Curtis Michael

Scaparrotti

Ivan A. Schlager

Rajiv Shah

Wendy R. Sherman

Gregg Sherrill

Jeff Shockey

Kris Singh

Varun Sivaram

Walter Slocombe

Christopher Smith

Clifford Sobel

Michael S. Steele

Richard J.A. Steele

Mary Streett

Nader Tavakoli

*Gil Tenzer

*Frances F. Townsend

Melanne Verveer

Tyson Voelkel

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

William H. Webster

**Executive Committee Members*

List as of February 1, 2025



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.

© 2025 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council
1400 L Street, NW, 11th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org