AY 2024-2025

BYTES BEFORE BULLETS: FORGING A COHERENT AND INTEROPERABLE C4ISR ECOSYSTEM

C4ISR INDUSTRY STUDY

MR. GEORGE LASKEY, MR. CHARLES KENT MAY

SEMINAR 6

COL MATTHEW BALLANCO, USAF
CDR DAN BELLE, USN
MR. FREDERICK DAVENPORT, NRO
LT COL SARAH DOWD, USAF
LTC JON HATHAWAY, USA
COL JOSH JOHNSON, USA
MRS. JANET MADDOX, DAF
LT COL JEN MALATESTA, USAF
MS. MEGAN MALONE, USA
LTC J. MIKE MCLEAN, USA
CDR MICHAEL MILLER, USN
CDR SEAN ROCHA, USN
LTC DAVID TAVARES, ARNG
LT COL JOSH TYSON, USAF

WORD COUNT: 8664

19 MAY 2025

The Dwight D. Eisenhower School
for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Executive Summary

In the 21st-century armed conflict, strategic battlespace advantage increasingly belongs to the belligerent who can control and exploit the flow of digital information. That strategic battlespace is rapidly shifting. Russia's use of electronic warfare and drone-enabled rapid targeting in Ukraine and China's pursuit of "intelligentized" warfare through Artificial Intelligence (AI) and integrated data systems exemplify how adversaries are adapting faster than traditional acquisition timelines allow. U.S. operations in the Red Sea and Indo-Pacific also reveal persistent shortcomings in joint and coalition interoperability, bandwidth constraints, and vulnerable space-based infrastructure. These trends underscore the need for a Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) posture that is not only technologically advanced but resilient, agile, and designed from the outset for allied collaboration.

C4ISR capabilities represent the digital backbone of national defense, enabling decision advantage at all levels of war. As adversaries develop asymmetric tools to blind, jam, and paralyze U.S. and allied forces, the Department of Defense (DoD) faces a strategic imperative: transform its C4ISR enterprise to remain effective in contested, data-saturated, multi-domain environments.

This paper analyzes the C4ISR industry through field research, stakeholder engagement, and applying analytical models such as Strengths, Weaknesses, Opportunities, and Threats (SWOT). The C4ISR Industry Study seminar's visits to U.S. and foreign commercial firms, research labs, academia, and government entities provided a multidimensional view of how C4ISR capabilities are developed, acquired, and integrated into operations. The seminar's research reveals that while the United States holds significant technological advantages, systemic barriers inhibit the speed and scale of innovation adoption necessary to sustain that edge.

The current global C4ISR industry is growing—valued at more than $146 billion and expected to expand steadily—but faces structural constraints. Legacy acquisition models, overclassification, disjointed oversight, and proprietary system lock-in continue to stifle innovation adoption and integration across domains. Supply chain dependencies, especially in microelectronics and space technologies, present mission assurance risks that adversaries continue to exploit. Equally urgent is the growing delta in digital fluency across the military workforce. Without targeted investment in data-centric skills, the DoD risks fielding advanced tools without operators trained to leverage them.

Addressing these challenges requires a coherent modernization approach integrating policy reform, commercial innovation, and human capital development. Central to this is the institutionalization of data and metadata standards, unlocking cross-domain and allied interoperability while enabling advanced capabilities such as AI and autonomous ISR. Reforming Foreign Military Sales (FMS) to support multilateral C4ISR data-sharing architectures will strengthen coalition resilience and reduce strain on U.S. forces abroad.

To ensure future warfighting dominance, the DoD must forge agile partnerships with commercial industry, expanding efforts like the Commercial Space Augmentation Reserve (CSAR), adopting continuous Authority to Operate (ATO) frameworks, and fielding hybrid ISR architectures. These partnerships accelerate delivery, expand surge capacity, and inject cutting-edge capabilities at the speed of relevance. Building a digitally fluent workforce—through embedded commercial certifications, AI-enabled training tools, and data-centric enlisted specialties—will ensure C4ISR roles remain agile in data-intensive environments.

This transformation demands bold leadership, deliberate scaling, and sustained investment to evolve America's fragmented C4ISR ecosystem into a coherent, resilient, interoperable, and decisive information advantage.

Preface

Introduction to Group Paper

"Future conflicts could well be decided by information advantage, success going to the side that transforms vast amounts of data from distributed sensors and weapons systems across multiple domains into actionable information for better, faster decision making and precision effects."

- David Norquist, Former Deputy Secretary of Defense in the 2020 C3 Modernization Strategy[1]

In today's battlespace, where wars are won by bytes before bullets, America's C4ISR network is the digital nervous system driving modern warfighting dominance and securing national defense. The Joint Warfighting Concept 2034-2044 reveals a stark reality: we are entering a period of defensive dominance where the ability to "fuse and distribute data faster than the adversary" will determine battlefield outcomes.[2] As adversaries like China and Russia develop capabilities to paralyze military forces through systems destruction warfare, the United States faces a critical imperative to revolutionize its approach to information dominance.[3]

The evolving nature of warfare, particularly as observed in recent conflicts, underscores the necessity of this transformation. The compression of the sensor-to-shooter timeline has redefined military engagements. In Russia's war against Ukraine, Ukrainian forces demonstrated this evolution during a December 2024 attack near Lyptsi, where they employed drones and ground-based unmanned systems to identify and strike enemy targets with remarkable speed and

[1] David Norquist, 2020 *C3 Modernization Strategy,* Department of Defense, September 2020, i, https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf
[2] T.X. Hammes and Mark Montgomery, "Joint Warfighting Concept 2034–2044" (Washington, D.C.: Institute for National Strategic Studies, 2024), 13, https://inss.ndu.edu/Media/News/Article/4015624/joint-warfighting-concept-2034-2044/.
[3] Hammes and Montgomery, 17.

precision[4]. Machine-gun-equipped ground drones and kamikaze aerial drones drastically reduced the time between target acquisition and engagement, exemplifying the advancements in sensor-to-shooter processes.[5]

During an April 2025 TED Talk in Vancouver, Anduril CEO Palmer Luckey underscored that a prospective People's Liberation Army (PLA) invasion of Taiwan would be shaped by the lessons of Ukraine—where the rapid integration of commercial technologies, particularly in AI and electronic warfare, has redefined the modern battlespace.[6] Luckey's insights on the convergence of AI and defense underscore a critical trend: adversaries, including China, are dynamically adapting their strategies from lessons learned in the Ukraine conflict and are likely to apply those lessons in the future to situations like a potential Taiwan conflict, leveraging asymmetric tactics to disrupt and disable key U.S. and allied systems. The DoD has taken notice of these key trends by publishing a Combined Joint All-Domain Command and Control (CJADC2) strategy. However, fully implementing this high-tech roadmap is still a work in progress.[7] In this paper, the seminar first examines the C4ISR strategic environment and the interests of stakeholders across multiple sectors. The attention then turns to analyzing the C4ISR market and influences therein, concluding with recommendations to achieve incremental steps toward data and metadata interoperability.

---

[4] David Ignatius, "What a Russian and Ukrainian General Agree on: This War Is Different," *The Washington Post*, February 6, 2024, https://www.washingtonpost.com/opinions/2024/02/06/russia-ukraine-drone-war-technology-stalemate/.

[5] Samuel Bendett and David Kirichenko, "Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine," *Modern War Institute*, January 10, 2025, https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/.

[6] *The AI Arsenal That Could Stop World War III* (Vancouver, BC, Canada: TED Conferences, LLC, 2025), https://www.ted.com/talks/palmer_luckey_the_ai_arsenal_that_could_stop_world_war_iii.

[7] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy" (Washington, DC: Department of Defense, March 2022), https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

Who We Are

The AY 2024-25 C4ISR Industry Study Seminar comprised 14 students from the Dwight D. Eisenhower School for National Security and Resource Strategy at the National Defense University. This group, pictured in Figure 1, provided diverse professional perspectives from across the government and contributed unique policy, functional, and operational expertise.

Figure 1:C4ISR Industry Study Seminar Students and Professors

CAPT George Laskey (United States Navy, retired) and Mr. Kent May (Department of State) directed the academic program. They guided the development of an analytic framework to assess the state and relevance of the C4ISR economic-industrial sector to national security. The seminar conducted in-depth analyses of leading C4ISR firms as part of a companion course, Industry Analysis, facilitated by Mr. Kent May.

Field Study Visits

The C4ISR research team visited a wide variety of industry firms, government entities, and academia, depicted in Figure 2, in support of this industry study. Domestically, the seminar

visited Boston, MA; Fort Worth, TX; San Diego, CA; and Honolulu, HI. Internationally, the group traveled to Canberra, Australia. These visits aided the seminar in assessing capability, capacity, and compatibility across the C4ISR industry.

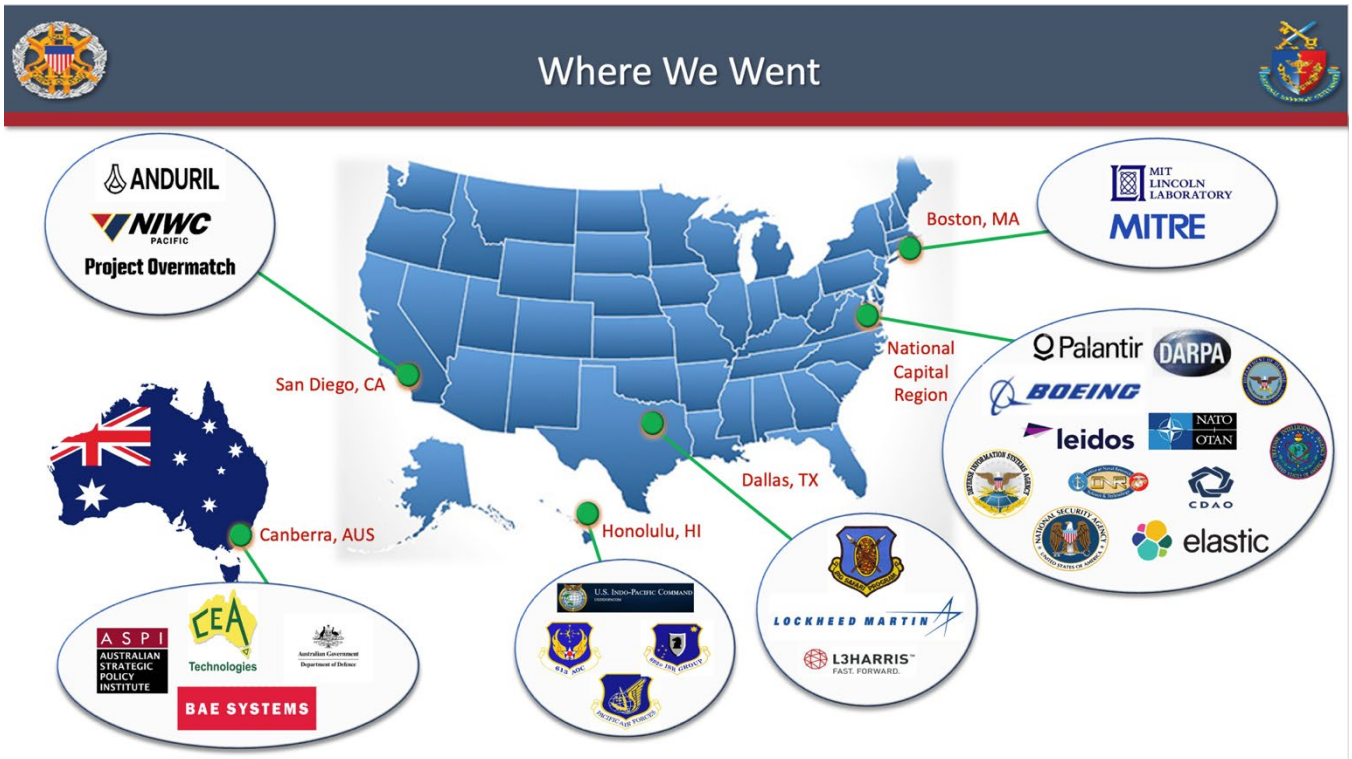


Figure 2: C4ISR Visits and Guest Speakers

Thesis

To ensure strategic advantage in a contested global environment, the DoD must adopt a coherent C4ISR modernization approach that advances joint data interoperability, enhanced public-private partnerships, and scalable workforce data literacy readiness. The DoD can achieve a resilient and interoperable C4ISR ecosystem capable of countering 21st-century threats by fusing policy innovation, expanding commercial-defense interaction, and pursuing multilateral data integration architectures.

A detailed assessment of the strategic environment is essential to properly frame the urgency of C4ISR modernization. Emerging operational patterns and adversary adaptations—

particularly in Ukraine and other contested domains—offer critical insights into the future character of warfare the United States must be prepared to confront.

Strategic Environment

Emergent Trends in Modern Warfare

The war in Ukraine has served as a transparent proving ground to the world for rapid innovation and adaptation, where the seamless integration of surveillance and strike capabilities—often via drones costing as little as $500—has enabled the destruction of high-value targets like tanks and artillery systems worth millions.[8] Such examples highlight how technological innovation and affordability can revolutionize warfare, reinforcing the urgency for the United States to prioritize advancements in its C4ISR industrial base.

Beyond Ukraine, the strategic environment reveals additional challenges. A National Defense University analysis of a potential conflict scenario with Russian forces in the Suwalki Gap highlights Russia's emphasis on electronic warfare (EW) as a primary tool for disrupting NATO's communication and command structures. Russia aims to create confusion and delay adversarial responses by deploying nonlethal EW effects early in a conflict, underscoring the importance of robust ISR, resilient communications, and effective electronic countermeasures.[9]

In the maritime environment, the Eisenhower Carrier Strike Group's (CSG) deployment in the Red Sea in 2024 showcases the Navy's innovative application of the Composite Warfare Commander (CWC) construct across distributed operations. The CSG Commander, RADM

[8] Mariano Zafra et al., "How Drone Combat in Ukraine Is Changing Warfare," Reuters, March 26, 2024, https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.
[9] Jan E. Kallberg, Stephen S. Hamilton, and Matthew G. Sherburne, "Electronic Warfare in the Suwalki Gap: Facing the Russian 'Accompli Attack,'" *Joint Force Quarterly* 97 (April 1, 2020), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106498/.

Marc Miguez, explained in a July 2024 *USNI Proceedings* article that his "warfare commanders run their domains across the CSG's wide area of operation" while "the integrated air and missile defense commander works consolidated area defense for the entire sector...hand in hand with coalition partners and the Combined Air Operations Center (CAOC)."[10] What remains unaddressed, however, is the precarious nature of this coordination between the maritime component CSG and the air component AOC. The relationship relies on fragile connectivity channels that could easily be disrupted in a contested environment. While the AOC possesses the bulk of intelligence fusion capabilities and air battle management expertise with Air Force personnel, the strike group retains the primary sensors, contextual understanding, and operational authorities. This disconnect creates an ad hoc joint C2 arrangement sustained primarily through personal relationships and the cumbersome exchange of numerous liaison officers rather than robust systems integration. Despite the article's emphasis on "highly integrated planning," the absence of resilient, integrated systems described in the DoD CJADC2 strategy leaves this critical synchronization vulnerable to all communications disruption.[11]

China and Russia are deliberately developing sophisticated counter-space capabilities to degrade or destroy U.S. and coalition forces' ability to operate effectively in and through space. The Defense Intelligence Agency's "Challenges to Security in Space" report from 2022 documents Russia's testing of direct-ascent anti-satellite weapons and China's deployment of co-orbital satellite technologies designed to interfere with or damage critical space infrastructure.[12] Similarly, a RAND analysis reveals how these nations pursue electronic warfare systems capable

[10] Marc Miguez, "Ike Carrier Strike Group and the Red Sea Crisis," *Proceedings* 150, no. 7 (July 2024), https://www.usni.org/magazines/proceedings/2024/july.
[11] Miguez.
[12] Defense Intelligence Agency, "Challenges to Security in Space – 2022" (Washington, DC: United States Department of Defense, 2022), 4, https://media.defense.gov/2022/Apr/12/2002976239/-1/-1/0/CHALLENGES-TO-SECURITY-IN-SPACE-2022.PDF.

of jamming or spoofing satellite communications and positioning signals, the backbone of modern military operations.[13]

China's increasing risk tolerance in space further complicates the strategic landscape. RAND's analysis indicates that the PLA is willing to escalate conflicts in space to achieve strategic objectives, reflecting a shift in their deterrence calculus.[14] This willingness to accept higher risks highlights the imperative for the United States to maintain technological superiority and deter aggression by ensuring the reliability and redundancy of its C4ISR systems.

Both Russia and China have demonstrated capability and intent to exploit U.S. and allied vulnerabilities through EW, space-based disruption, and traditional kinetic kill chains. The rapid deployment of commercial technologies into military applications, as demonstrated in Ukraine, showcases the potential for public-private collaboration to bolster national defense capabilities. Creating affordable, mass-producible systems will ensure scalability and readiness in future conflicts.[15]

Current Industry Status, Key Issues, and Forecast

The C4ISR market combines command, control, communications, computers, intelligence, surveillance, and reconnaissance. It is a complex market system overlapping numerous other industries comprising platforms, payloads, sensors, and systems designed to provide and analyze information for government personnel and commercial customers. The C4ISR framework is crucial in modern combat environments, helping operators gain a decision-

[13] H. Wang, G. Graff, and A. Dale-Huang, "China's Growing Risk Tolerance in Space: People's Liberation Army Perspectives and Escalation Dynamics" (Santa Monica, CA: RAND Corporation, 2024), 4, https://www.rand.org/pubs/research_reports/RRA2313-2.html.
[14] Wang, Graff, and Dale-Huang, 7.
[15] *The AI Arsenal That Could Stop World War III*.

making advantage, enhance situational awareness, and effectively engage hostile forces. Analysts typically describe the market by key segments, including geography/platform (land-based, airborne/space-based, naval, etc.) and/or application (ISR, C2, etc.).[16] C4ISR is in high demand for both commercial and national security applications, ensuring secure communication and surveillance and enabling data-driven decision-making.

The global C4ISR market was valued at $146.5 billion in 2023 and is expected to grow to $171.6 billion by 2028. This represents an incremental growth of $25.1 billion, growing year-on-year within a narrow range of 3.1% to 3.4% between 2023 and 2028. Growth is driven by factors like policy support in certain sectors, high demand for outsourcing services from specific regions, and the rise of low-cost hubs.[17] However, challenges like economic slowdowns, reduced enterprise IT budgets, increased in-house sourcing, and intense competition can constrain growth in mature markets. Recent global events, such as the Russia-Ukraine war, have also underscored the critical role of C4ISR and are expected to increase demand.

The DoD JADC2 strategy and Chief Digital and Artificial Intelligence Office (CDAO) emphasize standardized data architectures, coalition cybersecurity frameworks, modular systems, and strategic reforms.[18] Historically, the DoD treated software like hardware, applying traditional acquisition models ill-suited for iterative, rapid technological advancement. However, the industry's trajectory demands a pivot from hardware-centric acquisition models toward continuous, modular software development processes.

[16] Technavio, "Global C4ISR Market 2024-2028" (Chicago, IL: Infiniti Research Limited, 2024), 38, https://www-emis-com.nduezproxy.idm.oclc.org/php/url-sharing/route?url=7430e7b38e11e1c3&.
[17] Technavio, 42.
[18] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy."

Modern warfighting requires bandwidth-optimized architectures capable of supporting real-time, multi-domain operations.[19] Legacy systems, reliant on inefficient data pipelines and centralized control, are incompatible with emerging requirements like AI-enabled targeting, autonomous swarms, and coalition-based ISR integration. The shift from "data abundance" to "data sufficiency" emphasizes the importance of transmitting the right data to the right node rather than overwhelming tactical networks.[20] Success in future conflicts depends on scalable, federated C2 solutions supported by resilient supply chains and modular open systems.

The DoD JADC2 strategy supports a federated, government-owned "data fabric" supporting open application programming interfaces (APIs), modular designs, and zero-trust cybersecurity models to enable real-time, secure information sharing across domains and allied forces.[21] The CDAO reinforces these goals by decoupling data from applications, ensuring that government-owned data architectures remain accessible and interoperable regardless of vendor. Through modular, scalable platforms, private-sector innovators like Palantir and Anduril demonstrate this approach's benefits, enabling coalition partners to "plug and play" seamlessly across security domains.[22] However, inconsistent data and metadata standards and remnants of legacy systems like Link-16 inhibit interoperability and slow the adoption of advanced tools such as AI and real-time decision-making platforms.[23] Despite recent strategies advocating for

[19] United States Army Training and Doctrine Command (TRADOC), "The Operational Environment to 2035," 2023.
[20] Chief Digital and Artificial Intelligence Office, "2023 DoD Data, Analytics, and Artificial Intelligence (AI) Adoption Strategy" (Washington, DC: U.S. Department of Defense, 2023), https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.
[21] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy."
[22] Mark Pomerleau, "Key to the Pentagon's Concept for Modern War Is Standardization," *DefenseScoop*, August 12, 2024, https://defensescoop.com/2024/08/12/key-pentagon-cjadc2-concept-modern-war-standardization/.
[23] U.S. Department of Defense, "DoD Metadata Guidance" (Washington, DC: Department of Defense, 2023), https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Metadata%20Guidance.pdf.

standardized, machine-readable data, progress remains slow due to institutional inertia, proprietary vendor interests, and disjointed oversight.

Innovation Trends

Commercial Technologies. Commercial technologies are increasingly central to C4ISR advancements due to faster development cycles and cutting-edge capabilities. Examples include AI/machine learning (ML)-enabled ISR fusion tools, Low Earth Orbit (LEO) satellite communications, and modular open system architectures.

AI/ML tools are crucial for transforming raw intelligence into operational insights and enhancing situational awareness. Since C4ISR revolves around data, high-quality, interpretable data is essential to unlock the potential of AI, potentially streamlining tasks such as arms export reviews, autonomous ISR operations, and reducing dependency on centralized infrastructure. Data is the currency that flows through the C2 structure to finance decision-making. Deploying these tools at the tactical edge is also a priority for the PLA. In support of their Multi-Domain Precision Warfare (MDPW) concept, the PLA seeks to integrate big data and AI to rapidly identify key vulnerabilities in the U.S. operational system and then combine joint forces across domains to launch precision strikes against those vulnerabilities.[24]

LEO satellite communications are another vital commercial innovation. Advances in digital tech, cheaper components, and reduced launch costs have led to proliferated LEO constellations, providing resilient communications in Denied, Degraded, Intermittent, or Limited (DDIL) environments. Companies like Black Sky, Capella, Maxar, and Planet offer high-

[24] U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2024" (Washington, DC: Office of the Secretary of Defense, 2024), https://media.defense.gov/2024/Oct/20/2003323520/-1/-1/1/2024-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

resolution Earth imagery to support ISR missions.[25] Integrating commercial and military assets creates hybrid architectures that enhance operational adaptability, although vulnerabilities in ISR supply chains and surge procurement planning remain challenges.

Modular open architectures and software-defined systems mark a shift from proprietary to interoperable solutions. These include software-defined radios and leverage open systems standards like Open Mission Systems (OMS) and Future Airborne Capability Environment (FACE), which promote flexibility and integration. These standards, such as the Block 4 updates in the F-35 program, have taken ten years to implement and are now reaching service to help the F-35 more efficiently accept applications. This adoption promotes flexibility and integration by using open architectures and common standards to enable various vendors' software and hardware components to interoperate.[26] Non-traditional defense companies are leading in adopting these standards, offering software solutions that connect siloed data and reduce vendor lock-in. Software-defined networking (SDN) allows for dynamic reconfiguration of tactical networks to meet mission demands, even in contested bandwidth environments.

Experimentation Accelerating Delivery Cycles. Experimentation allows the DoD to identify gaps and adapt to technological advances faster than traditional acquisition models. The CDAO has leveraged its Global Information Dominance Experiments (GIDE) series to create a dynamic environment for testing and validating emerging technologies, particularly benefiting non-traditional defense contractors. By conducting iterative experiments every 90 days, GIDE enables rapid prototyping and real-time feedback, facilitating the transition of innovative

[25] National Reconnaissance Office, "NRO Announces Largest Award of Commercial Imagery Contracts" (Chantilly, VA: National Reconnaissance Office, May 25, 2022), https://www.nro.gov/Portals/135/documents/news/press/2022/press_release_05-22.pdf.
[26] Joseph Trevithick, "More Top Secret F-35 Stealth Fighter Data Given To NATO Members," The War Zone, August 2, 2024, https://www.twz.com/air/more-top-secret-f-35-stealth-fighter-data-given-to-nato-members.

solutions into programs of record. A notable success story from this initiative is Anduril Industries' Lattice Mesh, a decentralized networking capability that allows for seamless data distribution across various platforms and domains. Through GIDE, Lattice Mesh was rigorously tested, demonstrating its ability to enhance interoperability among legacy systems within the Joint Force. This validation led to a $100 million production agreement awarded to Anduril, underscoring the effectiveness of GIDE in accelerating the adoption of cutting-edge technologies.[27]

Data Ecosystems for Situational Awareness. C4ISR fundamentally relies on managing data (collection, processing, and interpretation) and demands high-quality, metadata-tagged information for ML and cross-domain interoperability. The DoD has recently published a set of strategy documents that collectively establish goals for data standardization. At the highest level, the FULCRUM Information Technology strategy states that "trustworthy data is indispensable for achieving strategic dominance."[28] It includes specific goals to increase data quality, improve the use of metadata, and improve data curation. The DoD's 2020 C3 strategy also addresses data standardization through the lens of message formats. Specifically, it aims to "adopt a single modern and efficient machine-to-machine C2 messaging standard… to improve interoperability and understandability at the data objective level."[29] The 2022 JADC2 strategy states that to create a decision advantage, the Joint Force, allies, and partners must be able to discover and

[27] Sydney J. Freedberg Jr., "Decentralizing Battle Data: CDAO, Anduril Open Tactical 'Mesh' to Third-Party Developers," *Breaking Defense*, December 13, 2024, https://breakingdefense.com/2024/12/decentralizing-battle-data-cdao-anduril-open-tactical-mesh-to-third-party-developers/.
[28] U.S. Department of Defense, "FULCRUM: The Department of Defense Information Technology Advancement Strategy" (Washington, DC: Department of Defense, 2024), https://dodcio.defense.gov/Portals/0/Documents/Library/FulcrumAdvStrat.pdf.
[29] U.S. Department of Defense, "Command, Control, and Communications Modernization Strategy" (Washington, DC: Department of Defense, 2020), https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf.

access any necessary data.[30] To do that, the department's objectives must be to establish minimum metadata criteria and adopt data standardization.

Communications and Computers Supply Chain Vulnerabilities

In a contested global environment where peer competitors actively target U.S. space and cyberinfrastructure, the lack of contracted surge capacity and mission assurance in commercial satellite communication (SATCOM) and ISR supply chains represents a critical vulnerability. While traditional concerns about semiconductor dependencies and globalization remain valid, the more immediate and operationally consequential challenge is the DoD's insufficient integration of commercial computing and communications capabilities into assured wartime frameworks.

Commercial LEO satellite communication networks have expanded rapidly, offering revolutionary redundancy and global coverage potential for C4ISR systems operating in DDIL environments.[31] However, these networks, notably exemplified by firms such as SpaceX, Amazon (Project Kuiper), and others, are not currently subject to binding mission assurance requirements during military conflict. Unlike legacy military communications satellites, there is no guarantee that commercial SATCOM providers would prioritize DoD traffic during conflict, nor are there contractual obligations for surge launch or replacement of critical nodes under adversarial attack conditions.[32] This absence of binding agreements exposes a dangerous gap

[30] U.S. Department of Defense, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy."
[31] Michelle K. Donahue, "The C2 Fix Initiative: What It Means for Sustainment Forces" (U.S. Army, January 22, 2025), https://www.army.mil/article/282485/the_c2_fix_initiative_what_it_means_for_sustainment_forces.
[32] Jonathan P. Wong and et al., "Leveraging Commercial Space Services: Opportunities and Risks for the Department of the Air Force" (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/research_reports/RRA1724-1.html.

between the peacetime integration of commercial assets and their availability when contested operations commence.

The United States' heavy reliance on global suppliers for microelectronics, semiconductors, and printed circuit boards (PCBs) creates critical vulnerabilities. More than 80 percent of the world's semiconductors are produced in East Asia, with Taiwan alone accounting for most advanced microchips.[33] Supply disruptions in this region, whether through natural disasters or military conflict, would have cascading effects on C4ISR systems dependent on these components. Even more concerning is the documented presence of Chinese-manufactured components within U.S. military systems, raising the specter of sabotage or espionage via "kill switches" or latent vulnerabilities embedded deep within hardware architectures.[34]

While the proliferation of commercial ISR capabilities — particularly in Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), and SATCOM — has expanded options for surge support, the existing Planning, Programming, Budgeting, and Execution (PPBE) process, even with recent modifications for 'urgent capability acquisition,' remains too slow to meet the demands of high-intensity conflict. As seen in the commercial imagery sector, firms like Maxar, BlackSky, and Planet possess "good enough" capabilities for many ISR tasks. Still, without streamlined authorities and standing agreements, the DoD cannot guarantee the timely

[33] Defense Business Board, "Supply Chain Illumination in the Department of Defense" (Washington, DC: Department of Defense, January 7, 2025), https://dbb.defense.gov/Portals/35/Documents/Reports/2025/DBB%20Supply%20Chain%20Illumination%20Report%20CLEARED.pdf.
[34] "Ex-DoD Official Says Chinese-Made PCBs Plague U.S. Systems," EE Times, March 22, 2024, https://www.eetimes.com/ex-dod-official-says-chinese-made-pcbs-plague-u-s-systems/.

availability of commercial ISR capabilities or prioritize national defense needs over commercial customers during crises.[35]

Production Factors and Latent Capacity and Innovation Opportunities

Despite operating within a thriving innovation ecosystem, the DoD faces persistent difficulties in converting leading-edge research into deployable C4ISR solutions at scale.[36] The combination of outdated acquisition processes, risk-averse organizational culture, and slow adoption of open architectures prevents the fast exploitation of new technologies.[37] This stagnation contrasts China's civil-military fusion strategy, where commercial and state resources are deliberately integrated to deliver operational capabilities at high speed.[38]

The U.S. innovation base faces an additional challenge due to inadequate integration between its civil and military sectors. Military technology advancement lags because DoD interactions are restricted by outdated contracting methods and intellectual property disputes, while commercial industries have progressed in areas like cloud computing and satellite communication.[39] Unfortunately, the defense sector fails to keep pace with the momentum of America's broader technology ecosystem, especially in critical areas like AI-enabled sensor fusion and adaptive networking.

[35] Donahue, "The C2 Fix Initiative: What It Means for Sustainment Forces."
[36] United States Government Accountability Office, "Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework" (Washington, D.C.: U.S. Government Accountability Office, April 8, 2025), https://www.gao.gov/products/gao-25-106454.
[37] Michael T. Klare, "A New Military-Industrial Complex Arises: The Secret War Within the Pentagon," Fair Observer, March 20, 2025, https://www.fairobserver.com/business/technology/a-new-military-industrial-complex-arises-the-secret-war-within-the-pentagon/.
[38] U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2024," 24.
[39] Chief Digital and Artificial Intelligence Office, "2023 DoD Data, Analytics, and Artificial Intelligence (AI) Adoption Strategy."

The United States has significant unused productive potential that could be activated through increased partnerships with trustworthy international entities. The Government Accountability Office (GAO) revealed inefficiencies in current Foreign Military Sales (FMS) procedures which hinder U.S. allies from obtaining necessary C4ISR capabilities and reduce coalition preparedness.[40] Streamlining FMS procedures and adopting more agile licensing models could allow U.S. partners to co-develop, co-produce, and co-operate advanced ISR systems without sacrificing security or strategic advantage.

The C4ISR industrial base can grow to scale and become more resilient through strategic co-production agreements, particularly with Five Eyes partners alongside NATO members and close Indo-Pacific partners. Implementing collaborative manufacturing with regional maintenance hubs and shared R&D efforts will enable defense structures to become more interoperable while reducing supply chain weaknesses, which is crucial for multi-domain operational success.[41] For example, the F-35 Lightning II fighter program, developed and produced by a consortium of allied nations, demonstrates the benefits of armaments co-production by pooling resources and expertise across countries to deliver a cutting-edge system.[42] Likewise, the National Technology and Industrial Base (NTIB) expansion to include trusted allies mirrors the successful Five Eyes intelligence framework to foster defense industrial integration.[43] More recently, the Australia, United Kingdom, and United States (AUKUS)

[40] United States Government Accountability Office, "Foreign Military Sales: DoD Should Improve Planning to Address Workforce and Other Challenges" (Washington, D.C.: U.S. Government Accountability Office, February 2024), https://www.gao.gov/products/gao-24-106321.
[41] United States Department of Defense, "2024 Indo-Pacific Strategy Report," January 20, 2024, https://media.defense.gov/2024/Jan/20/2003369972/-1/-1/1/INDO-PACIFIC-STRATEGY-REPORT-2024.PDF.
[42] Edward Lundquist, "F-35 Industrial Base Relies on International Participation," *National Defense*, January 1, 2015, https://www.nationaldefensemagazine.org/articles/2015/1/1/2015january-f35-industrial-base-relies-on-international-participation.
[43] Stew Magnuson, "US-UK-Canada-Australia Industrial Base Initiative Yet to Gather Steam," *National Defense*, September 9, 2019, https://www.nationaldefensemagazine.org/articles/2019/9/9/us-ukcanada-australia-industrial-base-initiative-yet-to-gather-steam.

security pact exemplifies how joint innovation efforts can reshape the strategic landscape.[44] Opportunities exist to embed flexible FMS "fast lanes" for ISR systems, automating portions of the export review process through AI-enabled compliance tools and incentivizing commercial companies to design products with coalition interoperability by default to unlock significant latent industrial power.

Stakeholder Interests

State of Business-Government Relations

The relationship between the U.S. government and the defense industrial base (DIB) in the C4ISR sector is increasingly complex, shaped by rapid technological change, evolving acquisition policy, and shifting operational demands. Historically, the relationship has been described through concepts like the "iron triangle" of government, congress, and industry or the "triple helix" of government, industry, and academia, highlighting their crucial interaction.[45][46] More so than in other defense fields, the DoD relies heavily on industry to develop, produce, and sustain advanced C4ISR platforms and software. The increased reliance on industry is driving changes in how the government and industry interact. The C4ISR market is mature, with a higher-than-average technical degree of change and many active competitors.[47] Projected increases in DoD spending are expected to drive incumbent defense firms to pursue emerging

[44] Robert Peters and Wilson Beaver, "AUKUS Is a Good First Step, But It Needs to Go Further" (Washington, D.C.: The Heritage Foundation, March 4, 2024), https://www.heritage.org/defense/report/aukus-good-first-step-it-needs-go-further.
[45] Gordon Adams, The Politics of Defense Contracting: The Iron Triangle (New York: Council on Economic Priorities, 1981).
[46] Henry Etzkowitz, *The Triple Helix, University-Industry-Government Innovation in Action* (Routledge, 2008), https://mguntur.id/files/ebook/ebook_1605608206_cf742d707b4e0bf22bf3.pdf
[47] Frost and Sullivan, Global Aerospace & Defense Research Team, "US DoD C4ISR Growth Opportunities, Sharp Spending Increases in Command & Control and Communications Research," Frost & Sullivan, KA77-22, June 2024

requirements more aggressively while attracting new entrants eager to compete for future contracts.[48] Today, military leaders openly acknowledge that no single contractor has all the innovation needed for military C2 and insist that government data must be a government-owned asset accessible across platforms.[49] This insistence is a significant reason why the DoD still struggles to incentivize commercial firms to participate.

The DoD prioritizes engaging industry partners to improve joint force effectiveness with cutting-edge technology.[50] Recent policy directives emphasize acquisition reform, rapid capability acquisition, and the adoption of commercial technology. These policy changes attempt to improve access and participation by the C4ISR industry. However, the C4ISR industry is experiencing high growth, rapid change, and fragmentation across "sense" and "make sense" business units. This volatility has led to a reliance on a smaller pool of defense primes who often act as integrators rather than primary innovation hubs. Even so, a notable trend of new entrants, particularly in software, is challenging the traditional oligopoly. Companies like Palantir and Anduril are challenging traditional defense primes and carving out significant market share through the government's creation of consortia. "We are working together to provide a new generation" of defense contractors, one consortium participant noted, describing a collective bid to supply the U.S. military with efficient, cutting-edge capabilities by pooling their technologies.[51] There is a recognized need for the defense market to open to more players and

[48] Frost and Sullivan, "US DoD C4ISR Growth," 16
[49] Mark Pomerleau, "Key to the Pentagon's Concept for Modern War Is Standardization," DefenseScoop, August 12, 2024, https://defensescoop.com/2024/08/12/key-pentagon-cjadc2-concept-modern-war-standardization.
[50] Michael T. Klare, "A New Military-Industrial Complex Arises: The Secret War Within the Pentagon," Fair Observer, March 20, 2025, https://www.fairobserver.com/business/technology/a-new-military-industrial-complex-arises-thesecret-war-within-the-pentagon.
[51] Reuters, "Palantir, Anduril Join Forces with Tech Groups to Bid for Pentagon Contracts, FT Reports," Reuters, December 22, 2024, https://www.reuters.com/markets/deals/palantir-anduril-join-forces-with-tech-groups-bidpentagon-contracts-ft-reports-2024-12-22.

ideas and streamline the transition from concept to capability. Despite strategies emphasizing partnership, there are gaps in integrating industry perspectives in several areas.

Intellectual Property (IP) conflicts and regulatory compliance deter commercial participation.

The DoD has made a solid effort to broaden firm participation. However, intellectual property (IP) constraints and regulatory burdens still discourage commercial entrants, especially non-traditional defense contractors (NTDCs). While IP rights are important, their rigid enforcement without considering diverse technology layers (open source, proprietary, government custom code) complicates interoperability efforts.[52] In addition, with few competitors in some areas, primes and NTDCs may engage in conduct that protects their market position, such as leveraging intellectual property (IP) rights to block aftermarket or third-party entrants. The DoD has noted instances where contractors use proprietary data rights to induce "vendor lock," limiting competition for sustainment or upgrades.[53]

Furthermore, Federal Acquisition Regulation (FAR) contracts present complex requirements, including thousands of pages, complicated contracting and certification requirements, stringent security demands, intricate data and IP rights, and specialized cost accounting standards. However, NTDCs are not subject to all regulatory requirements. This policy change was instituted to attract NTDCs into the defense market by relaxing some regulatory requirements (such as cost accounting) and using commercial determination and Other Transaction Authority (OTA) contracts to reduce the burden on NTDCs.[54] However, it

[52] Defense Innovation Board, "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage," Washington, DC: Defense Innovation Board, May 3, 2019.
[53] Department of Defense, "State of Competition within the Defense Industrial Base / Office of the Under Secretary of Defense for Acquisition and Sustainment." [EBook]. Jan. 2022, 6-7, EBSCOhost, research.ebsco.com/linkprocessor/plink?id=78cebc42-1458-3518-9c6f-5d414281b09d.
[54] Jennifer Stewart, et al., "Vital Signs 2025: The Health and Readiness of the Defense Industrial Base," Arlington, VA: NDIA, 2025

does not protect NTDCs from regulatory requirements if they grow into Traditional Defense Contractors (TDCs).[55] This distinction serves as a deterrent to NTDC retention.

DoD Data Standards

Even with the recent acquisition reform initiatives, many C4ISR programs still fail to incentivize contractors to design systems that integrate easily with others. This leads to vendors preferring proprietary designs and architectures, maintaining a competitive edge and potentially creating vendor lock-in.[56] Open standards initiatives (such as Data, Applications, and Governance Interoperability Reference Architecture ((DAGIR)) and JADC2) are reshaping the defense technology landscape for the future, but entrenched legacy systems and institutional inertia limit complete industry alignment.[57] In addition, the details of interoperability standards matter and must be clearly articulated by the government to industry. One area explored during this industry study is data and metadata standards. The DoD's lack of consistency and weak enforcement of data and metadata standards results in system incompatibility when sharing information. Industry may also resist data standardization due to concerns that DoD standards won't keep pace with technology, would limit engineering flexibility, or would render investments in proprietary products moot.[58] There is also a belief that new standards will add to existing legacy standards rather than replace them.[59] Finally, "no one is responsible for sponsoring or managing capabilities needed to achieve joint integration."[60] As a result,

[55] Stewart, "Vital Signs," 22
[56] U.S. Department of Defense, Summary of the Joint All-Domain Command and Control (JADC2) Strategy, March 2022.
[57] Mark Pomerleau, "Key to the Pentagon's Concept for Modern War Is Standardization," DefenseScoop, August 12, 2024, https://defensescoop.com/2024/08/12/key-pentagon-cjadc2-concept-modern-war-standardization.
[58] Discussion with the author as part of industry site visits, various locations, January-April 2025.
[59] Discussion with the author as part of industry site visits, various locations, January-April 2025.
[60] Bryan Clark and Dan Patt, "Joint Integration Emerging as the Solution for CJADC2," RealClearDefense, Sep 30, 2023

communication among the many government entities working C4ISR and industry often provides conflicting messages.

Rapid Acquisition and Innovation Cells

Initiatives like the Defense Innovation Unit (DIU), CDAO, and Rapid Capabilities Offices are crucial intermediaries between commercial technology sectors and military needs. These frameworks are intended to help bridge the "valley of death," the funding gap where promising prototypes fail to reach full-scale production due to fiscal pressures. Despite the successes in prototyping and experimentation, challenges remain in scaling DIU activities and investments. As of fiscal year 2023, DIU reported that since its inception in 2016, 62 prototypes transitioned into production or service contracts with the DoD, resulting in a declining transition rate of approximately 13.8 percent.[61] Additionally, budgetary constraints, security requirements, and institutional resistance contribute to scalability limitations. Finally, the traditional PPBE process can impact technology transition, making new technology programs vulnerable in budget execution, especially when they require fiscal flexibility.[62] These factors ultimately limit industry participation and innovation in the C4ISR market.

Modeling and Simulation (M&S) and Experimentation

M&S, experimentation, and emulation have become essential pre-acquisition tools, enabling earlier detection of integration issues and fostering more agile development. Leveraging M&S can streamline development and testing, reduce the need for costly physical

[61] Courtney Albon, "Pentagon Technology Hub Sees Lower Transition Rate, Higher Value Deals," Defense News, May 2, 2024, https://www.defensenews.com/battlefield-tech/2024/05/02/pentagon-technology-hub-sees-lowertransition-rate-higher-value-deals/.
[62] Baroni Center for Government Contracting, "Improving Technology Transition Through a More Flexible PPBE Process" (Arlington, VA: George Mason University, September 2024), 1, https://mstm.gmu.edu/news/2024-09/newwhite-paper-identifies-how-make-it-easier-transition-defense-technologies.

prototypes, and identify integration issues earlier. In addition, experimentation is another effective tool for fostering innovation and provides a playing field for the military (U.S. and allies/partners) and industry. Several C4ISR experimentation efforts now exist, including Project Convergence, Project Overmatch, and Joint Fires Network. These efforts are testing for seams in operations while leading to new requirements that inform future acquisition programs. This link to future programs serves as a key incentive for industry participation.[63] The trajectory of C4ISR experimentation is increasing, allowing acquirers to gain deeper insight into the market and industry participants while also allowing industry insight into DoD C4ISR concepts and challenges.

The current state of business-government collaboration in C4ISR reflects uneven progress shaped by persistent cultural, structural, and policy constraints. While some advances have narrowed the gap between innovation and fielded capability, integration remains inconsistent. At the same time, the DoD faces the growing challenge of 21st-century mobilization, characterized by the need to generate and scale capabilities rapidly across domains and partners in an increasingly contested, information-driven environment.

21st Century Mobilization Preparedness

Mobilization preparedness for 21st-century conflict faces mounting challenges across multiple dimensions: fielding critical capabilities at speed, scaling a data-centric force, integrating joint and coalition operations, and adopting emerging technologies at scale. Although pilot efforts and limited successes exist, systemic barriers continue to constrain the DoD's ability to transition rapidly from peacetime posture to wartime demands in an information-driven

[63] Kimberly Underwood, "Project Convergence Breaks More Ground," AFCEA Signal, Mar 6, 2024, https://www.afcea.org/signal-media/defense-operations/project-convergence-breaks-more-ground

battlespace. Without deliberate acceleration, the United States risks losing its decision advantage against increasingly capable adversaries. Meeting these demands requires more than peacetime readiness; it requires a different kind of whole-of-government and industry response.

What distinguishes mobilization from routine force generation is the expanded participation it requires across government, industry, and allied partners. It demands more than just surge capacity—it involves identifying and preparing additional developers and warfighters, fielding adaptable equipment for contested environments, and accelerating the development of mission-critical skills to meet the challenges of war. These dynamics introduce friction across planning, procurement, and operational execution that is rarely encountered in steady-state defense activities. These pressures are evident in the ISR enterprise, where surge requirements and procurement timelines collide with outdated assumptions, brittle contracts, and unaligned acquisition processes.

ISR Surge and Scalable Procurement Pathways

As peacetime transitions into conflict, ISR requirements escalate sharply, demanding faster collection, higher revisit rates, and persistent coverage to maintain decision advantage in DDIL environments.[64] However, the United States lacks a coherent plan to surge ISR capabilities during crisis or conflict. While commercial space and SATCOM services offer potential surge capacity, most contracts lack enforceable obligations for wartime access, introducing operational risk. Leveraging commercial space imagery and commercially available information (CAI) remains underdeveloped, requiring more responsive policy frameworks.

[64] U.S. Department of Defense, Joint Concept for Command and Control of the Joint Aerial Layer Network (JCC2JALN) (Washington, DC: Department of Defense, March 2015), accessed April 17, 2025, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_aerial_layer_network.pdf?ver=2017-12-28-162026-103.

Compounding the challenge, critical C4ISR supply chains—including microelectronics, PCBs, and rare earth minerals—are concentrated in high-risk regions like Taiwan and China, creating dependencies that slow response times and introduce security vulnerabilities.[65] Production delays in systems like the F-35, caused by reliance on Chinese-sourced materials, illustrate the risks inherent in fragile supply chains.[66] Although initiatives like the CHIPS Act and Defense Production Act (DPA) Title III investments aim to rebuild domestic industrial capacity, these efforts are long-term.[67]

Legacy acquisition systems like PPBE and Joint Capabilities Integration and Development System (JCIDS) remain too slow to meet surge demands.[68] Industry partners have shown the ability to accelerate capability development when freed from elements of conventional acquisition oversight. Industry collaboration and acquisition reform are essential to enabling scalable ISR mobilization. However, even if ISR capacity can surge and supply chain risks be mitigated, mobilization will require a workforce capable of exploiting the information advantage at machine speed.

Mobilizing a Data-Centric Force

Building a force capable of exploiting information dominance is critical to 21st-century mobilization. C4ISR is fundamentally about data: collecting, transmitting, processing, and interpreting it to enable decision advantage. Data is increasingly viewed as a strategic asset and decisive instrument of national power. Achieving and maintaining advantage in strategic

[65] IATF for Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States
[66] Defense News, "Pentagon suspends F-35 deliveries over Chinese alloy in magnet," Sept 7, 2022 defensenews.com
[67] International Defense, Security & Technology, "Strengthening domestic rare earth supply chains: a Defense priority," February 16, 2025
[68] Defense Innovation Board. Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage. Washington, DC: Defense Innovation Board, May 3, 2019.

competition hinges on the ability to operate at machine speed, and adversaries like China have aggressively embraced this approach. China's military modernization focuses on evolving from informatized to intelligentized, AI-enabled operations, leveraging integrated data ecosystems and AI to gain algorithmic battlefield advantage.[69] Russia has similarly invested in electronic warfare and counter-space operations to disrupt ISR and communications networks.

Despite growing recognition of this need, U.S. efforts to build and sustain a data-centric force remain fragmented. While companies such as Lockheed Martin, Leidos, and Anduril have developed internal training pipelines, they are limited in scale and poorly integrated with DoD career pathways. Pilot programs like SkillBridge and Indo-Pacific upskilling initiatives show promise but lack enterprise-wide coordination.

This absence of standardized credentialing, unified qualification frameworks, and sustained investment mechanisms creates a widening readiness gap. Without operators skilled in managing mission-critical data, initiatives like CJADC2 risk faltering operationally despite technological advances. Mobilization in the information age demands human capital development equal to materiel production. Yet building a data-centric force alone is not enough; without seamless interoperability, information and decision advantages risk being fragmented across services and coalition partners.

Interoperability Challenges to Joint and Coalition Operations

Despite ISR collection and workforce development improvements, mobilization would remain incomplete without resolving interoperability barriers. Effective C4ISR operations require seamless information exchange across services, agencies, and coalition partners.

[69] Kevin Pollpeter, Amanda Kerrigan, and Andrew Ilachinski, "The PLA and Intelligent Warfare: A Preliminary Analysis" (Arlington, VA: Center for Naval Analysis, October 2021).

However, technical challenges—including incompatible data formats, proprietary vendor architectures, inconsistent metadata standards, and limited automated tagging—impede rapid data sharing and integration.[70] Data created with few standards limits ML, cross-domain collaboration, and decision-making at speed.

Policy barriers further exacerbate these challenges. Export controls such as the International Traffic in Arms Regulations (ITAR) and strict classification rules slow technology and intelligence sharing, even with trusted allies. Fragmented acquisition policies and oversight inconsistencies complicate enforcement of interoperability requirements across programs. Different services and commands often develop redundant but incompatible systems, draining resources and further fragmenting the C4ISR architecture.[71]

Operational realities in DDIL environments demand resilient, hybrid communications architectures blending commercial and military networks. Commands like the United States Southern Command stress that "zero trust" architectures enabling secure, dynamic data collaboration are essential for coalition operations across varying trust levels.[72]

Recent experimentation, including U.S.-led Project Convergence, demonstrates that progress in interoperability is achievable under controlled conditions. However, scaling these advances across the joint force and coalition partners remains incomplete. Without consistent enforcement of common standards and open system architectures, future mobilization risks fragmentation, delayed decision cycles, and degraded coalition effectiveness. Even with

[70] U.S. Department of Defense, Summary of the Joint All-Domain Command and Control (JADC2) Strategy.
[71] John R. Hoehn, Caitlin Campbell, and Andrew S. Bowen, Defense Primer: What Is Command and Control, IF11805, version 4 (Washington, D.C.: Congressional Research Service, November 14, 2022), https://crsreports.congress.gov.
[72] Laura Heckmann, "Southcom Searching For Secure Comms, Long-Range Sensors," National Defense Magazine, November 22, 2023, https://www.nationaldefensemagazine.org/articles/2023/11/22/southcom-searching-for-secure-comms-long-range-sensors.

improved interoperability frameworks, mobilization efforts must adapt to integrate rapidly evolving emerging technologies that will define future battlefields.

Emerging Technologies: Opportunities and Gaps

Emerging technologies present significant opportunities and challenges for mobilization preparedness, particularly in C4ISR operations under contested conditions. AI, ML, edge computing, resilient mesh networks, and autonomous systems are advancing rapidly, offering the potential to revolutionize C2 by accelerating data transport and processing, enhancing situational awareness, and supporting decision-making at the tactical edge.

Pilot programs like Project Convergence have demonstrated that AI-enhanced targeting, automated ISR fusion, and dynamic spectrum management can significantly increase operational tempo under controlled conditions. Concepts like carrier strike groups evolving into "super edge nodes," equipped with AI/ML processing capabilities, illustrate how decentralized battle management could sustain operational effectiveness even in degraded or denied communications environments.[73]

However, efforts to institutionalize emerging technologies across the force remain limited. Traditional, risk-averse culture, reliance on legacy systems, fragmented operational testbeds, and limited flexible fielding authorities hinder rapid adoption. The recent emphasis on the software-specific acquisition pathway may accelerate some efforts, but adapting DoD acquisitions to the demands of C4ISR requires tackling broader cultural and skills misalignments.[74]

---

[73] "US Navy Unveils 'Sea Strike' Vision of Future Warfare," Navy Leaders 2022, accessed April 19, 2025, https://www.navyleaders.com/news/navy-unveils-sea-strike-vision-future-warfare.
[74] Shaun Waterman, "Meeting the Software Challenge: Acquisition Reform Brings Its Own Complications," *Air and Space Forces Magazine*, May 5, 2025, https://www.airandspaceforces.com/software-acquisition-reform-challenges-part-three/

Meanwhile, adversaries are aggressively integrating emerging technologies. China is leveraging AI, autonomy, and space-based systems to pursue information dominance through 'intelligentized warfare,' while Russia continues to expand electronic warfare and counter-space capabilities.[75] Without deliberate acceleration, modernization, and scalable fielding of emerging technologies, the United States risks losing the decision advantage critical to success in future conflicts. Collectively, these mobilization challenges expose critical vulnerabilities that government and industry stakeholders must urgently address to sustain operational advantage in future conflicts.

Analysis

Analyzing the DoD C4ISR Market in a CJADC2-Focused Environment

The following section presents a comprehensive analysis of the DoD C4ISR industry within the context of CJADC2-driven strategic competition. The analysis employs multiple strategic frameworks – SWOT, Political, Economic, Social, Technological (PEST), and Porter's Five Forces – to systematically evaluate the external environment and industry dynamics shaping C4ISR innovation. The evaluation is informed by contemporary defense industry analyses and authoritative sources, ensuring alignment with current operational and strategic realities. Crucially, the analysis explicitly considers the implications for U.S. strategic competition with China and Russia – examining how the United States can strengthen C4ISR advantages and what risks must be mitigated considering adversaries' efforts. The ultimate goal is to inform policies that will drive a more agile and resilient C4ISR industrial base – one capable of delivering the

[75] Kevin Pollpeter, Amanda Kerrigan, and Andrew Ilachinski, "The PLA and Intelligent Warfare: A Preliminary Analysis" (Arlington, VA: Center for Naval Analysis, October 2021).

components for integrated “kill chains” and information dominance foundational for 21st-century deterrence and warfighting.

SWOT

The U.S. enters the CJADC2 era with formidable strengths: a cutting-edge tech base supported by massive investment, the synergy of allied networks, an experienced industrial and military workforce, and significant accumulated know-how. These strengths provide a solid foundation to build upon if they are properly leveraged through good policy (e.g., maintaining alliances, encouraging innovation, and training the workforce). They are also valuable and hard for adversaries to replicate – China cannot overnight create allies with trust or an open innovation culture like the U.S. enjoys, making these true competitive advantages.

For all its strengths, the U.S. C4ISR/CJADC2 ecosystem is weighed down by bureaucratic inertia, human capital and process inefficiencies, and structural frailties like supply chain risks. These weaknesses are widely recognized – indeed, many current reforms (acquisition reform, data strategy implementation, workforce upskilling, supply chain resilience efforts) are aimed at addressing them. However, they remain challenges that require sustained effort. Identifying these weaknesses allows us to target them in our later recommendations since mitigating them would unlock a greater advantage from the strengths noted.

The environment is rich in opportunities: technological leaps to exploit, reform energy to harness, allies to integrate further, lessons to implement, and commercial synergies to tap. Capitalizing on these could significantly enhance U.S. C4ISR effectiveness and offset weaknesses. Many of these opportunities align with or respond to the threats and weaknesses identified, meaning they can be seen as part of the solution set going forward.

STRENGTHS
Technological Leadership and Innovation Base: Robust tech edge in software, semiconductors, AI, networking; strong national innovation system.
Scale of Defense Spending and Market Size: Largest defense budget globally (~$800B), enabling simultaneous investments and risk tolerance in advanced technology.
Alliances and Global Partnerships: Extensive network of global allies and partner integration (Five Eyes, NATO, AUKUS) providing substantial operational and strategic advantage.
Experienced Defense Industrial Base & Workforce: Proven industry capability with institutional knowledge to deliver complex integrated systems effectively.
Operational Experience and Data: Rich experience from operational deployments (Gulf Wars, Ukraine, etc.) providing practical insights and battle-tested data to improve and refine future C4ISR systems.
WEAKNESSES
Bureaucratic Acquisition Processes and Slow Fielding: Slow and cumbersome procurement that hampers agile technology adoption and innovation.
Interoperability Gaps and Legacy Systems: Multiple legacy systems with limited native interoperability, lacking unified data architectures and standardized interfaces.
Workforce and Skills Gaps: Digital literacy gaps and difficulty recruiting/retaining top software talent; cultural resistance to agile and innovative methodologies.
Supply Chain Vulnerabilities: Heavy reliance on foreign suppliers and single-point vulnerabilities in key components such as semiconductors.
Over-classification and Information Sharing Limits: Excessive classification barriers prevent effective innovation, broad data sharing, and collaborative development.
Cost Growth and Sustainment Challenges: High lifecycle and sustainment costs for advanced C4ISR platforms strain budgets and threaten sustainability.
OPPORTUNITIES
Emerging Technologies and Innovation Momentum: AI, ML, 5G/5.5G/6G, quantum computing, autonomy, cloud computing, and edge technologies provide opportunities to significantly enhance capability.
Reform Initiatives and Policy Windows: Ongoing defense budgeting and acquisition reform efforts (PPBE reform, FoRGED Act, Office of Strategic Capital) create opportunities to streamline procurement and technology adoption.
Allied Integration and Export Opportunities: Further integration of allied networks presents opportunities for co-development, interoperability, and export markets for U.S. technologies.
Lessons from Recent Conflicts (Ukraine) and Experiments: Real-world operational lessons (Ukraine war) and experiments (Project Convergence) provide valuable insights to quickly iterate and enhance system designs.
Commercial Collaboration and Dual-Use Tech: Expanding public-private partnerships like Trusted Capital, commercial satellites, Software as a service (SaaS), Infrastructure as a service (IaaS) provide cost-effective means of rapid capability augmentation.
THREATS
Near-Peer Adversaries' Advancements: Rapid modernization of China's and Russia's C4ISR capabilities, including intelligent warfare, cyber warfare, electronic warfare, and anti-satellite technologies. Long Range strike capabilities also put US analysis, C2, and Sustainment capabilities at risk.
Electronic and Cyber Warfare in Conflict: High likelihood of severe electronic and cyber-attacks (jamming, spoofing, network sabotage) that could degrade or disable key C4ISR systems during conflict.
Supply Chain Disruptions and Economic Shocks: Vulnerabilities in global supply chains for critical components (e.g., Asian semiconductor reliance) could disrupt programs significantly in crisis scenarios.
Allied Reluctance or Divergence: Risk of allied divergence in technology standards or procurement strategies, potentially hindering comprehensive interoperability.
Domestic Political or Budget Instability: Political shifts or budget constraints could negatively impact consistent long-term funding and policy support for JADC2 initiatives
Security Breaches and Counterintelligence: Persistent espionage threats from adversaries aiming to steal technology or sabotage programs internally.

Table 1: SWOT Analysis

The threats facing the C4ISR/CJADC2 effort are sobering. Advanced adversaries are not standing still – they threaten to undermine or outpace the United States technologically and to destroy or blind U.S. networks in wartime. Meanwhile, systemic shocks from supply chains or shifts in geopolitical focus can derail progress. These threats underscore why maintaining the momentum of innovation and addressing weaknesses is an urgent matter of national security. The SWOT analysis paints a picture of critical imperatives: leverage strengths (tech, alliances, funds) and opportunities (reforms, new tech) to overcome internal weaknesses and guard against or neutralize external threats (adversary moves, disruptions).

PEST

The DoD's industrial base is intensifying efforts to modernize, integrate, and innovate C4ISR capabilities to maintain strategic advantage in military-industrial competition and armed conflict. Facing hostile rivalry, evolving multi-domain operational demands, and an increasingly contested information environment, modernization prioritizes data-centric architectures, resilient communications, and agile development processes. Efforts include fostering public-private partnerships, acquisition policy reform, and leveraging emerging technologies to build a more interoperable, resilient, and adaptive C4ISR enterprise that aligns technological innovation with the DoD's operational imperatives.

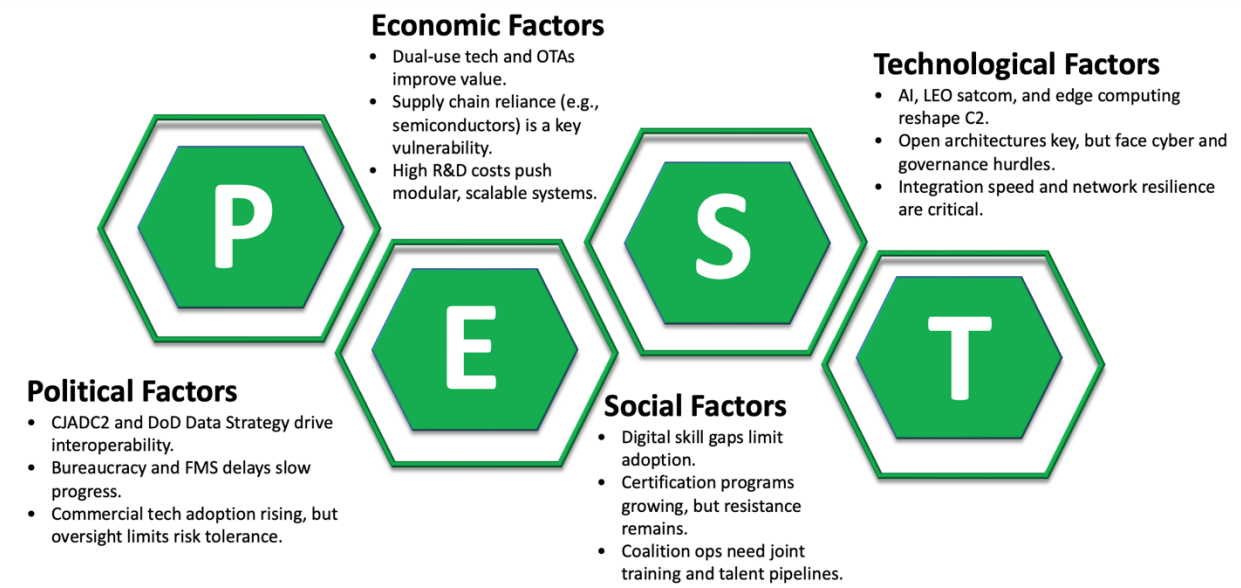


Figure 3: PEST Analysis

Political Implications

Political factors influence C4ISR innovation and modernization decisions and processes. Bureaucratic inertia, outdated FMS processes, and plodding acquisition cycles have hampered timely C4ISR deployment and undermined coalition interoperability.[76] Recent policy initiatives, including the 2020 DoD Data Strategy, the 2022 CJADC2 strategy, and the 2024 Data and AI strategy, emphasize data-centric operations and cross-domain interoperability to overcome political fragmentation.[77] Furthermore, strategic frameworks such as NATO, AUKUS, and other bilateral/multilateral security pacts are collaboratively oriented to support tactical C4ISR

[76] US Government Accountability Office, Defense Trade: Better Information Needed to Support Decisions Affecting Proposed Weapons Transfers, GAO-20-63 (Washington, DC: GAO, December 2019). https://www.gao.gov/products/gao-20-63.
[77] US Department of Defense, DoD Data Strategy, October 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF. And US Joint Chiefs of Staff, Joint All-Domain Command and Control Strategy, March 2022, https://media.defense.gov/2022/Mar/17/2002958400/-1/-1/0/JADC2-STRATEGY.PDF.

architecture interoperability as strengthened by political alliances.[78] Domestically, political support is shifting toward promoting commercial-sector integration and faster acquisition pathways through the CDAO.[79] However, long Congressional oversight timelines and security concerns complicate expedient technological adoption, which requires a delicate balance between defense-specific innovation and political risk acceptance.

Economic Implications

Economically, U.S. and allied defense industrial bases are reshaping defense and security approaches to C4ISR. Increased civilian investment and research and development (R&D) efforts to deliver smart-sensing and data-integrated technologies have expanded the DoD's access to dual-use technologies as cost-efficient delivery mechanisms for defense capabilities. Economic competition fosters diversification but exposes vulnerabilities, such as supply chain risks linked to semiconductor dependencies and rare-earth elements. Programs like the CHIPS Act aim to strengthen domestic supply resilience through reshoring, which is critical to C4ISR supply chains.[80] Moreover, public-private partnerships and flexible acquisition models like OTAs (Other Transaction Authority) economically incentivize innovation.[81] However, budgetary constraints and rising R&D costs demand that DoD balance investments across traditional

[78] US GAO, Defense Trade: Better Information Needed to Support Decisions Affecting Proposed Weapons Transfers. And Robert Peters and Wilson Beaver, "AUKUS Is a Good First Step, but It Needs to Go Further," *The Heritage Foundation*, 15 February 2022, https://www.heritage.org/defense/report/aukus-good-first-step-it-needs-go-further.

[79] US Department of Defense, "CDAO Overview," Chief Digital and Artificial Intelligence Office, accessed 18 April 2025, https://www.ai.mil/about.html. And CDAO, "Data and AI for Coalition Interoperability," Defense Innovation Forum Brief, 2024.

[80] International Defense, Security & Technology, *"Strengthening domestic rare earth supply chains: a Defense priority,"* 16 February 2025. And DBB.defense.gov, "Supply Chain Illumination in the Department of Defense," January 7, 2025. https://dbb.defense.gov/Portals/35/Documents/Reports/2025/DBB%20Supply%20Chain%20Illumination%20Report%20CLEARED.pdf.

[81] "Department of Defense Data Strategy" (Washington, DC, 2020), https://www.defense.gov/News/News-Stories/Article/Article/2383405/dod-unveils-data-strategy/.; Kathleen Hicks, "Creating Data Advantage" (Washington, DC: Department of Defense, 5 May 2021), https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/deputy-secretary-of-defense-memorandum.pdf.

platforms and emergent C4ISR architectures. Future fiscal strategies must prioritize scalable, modular solutions over bespoke, expensive systems to sustain technological advantage affordably.

Social Implications

Workforce skillset development represents a critical social challenge to C4ISR modernization. The "digital readiness gap" among military personnel underscores the difficulty in operating advanced C4ISR systems without sufficient data literacy and technical expertise.[82] Initiatives like digital skill designators and commercial certification programs (e.g., CompTIA Data+) are beginning to close this gap.[83] Moreover, generational shifts in the force composition, where digital natives expect seamless, user-friendly systems, are reshaping operational demands that are growing due to a forecasted generational deficit in technical talent interest and development pathways.[84] However, cultural resistance within the acquisition community and operational units still hamper technology adoption.[85] Additionally, greater multinational operations amplify linguistic and cultural interoperability challenges across coalition C4ISR systems, necessitating enhanced training and doctrine harmonization.[86] Investment in public-private educational programs will be crucial for operationalizing cutting-edge C4ISR technologies across the future force.

[82] US Government Accountability Office, Actions Needed to Improve DOD's Workforce Management, GAO-24-105645 (2024), pg. 12–14.
[83] US Department of Defense. Artificial Intelligence Education Strategy. Washington, DC: 2020, pg. 4–6

[84] Eric V. Larson, *Force Planning Scenarios*, 1945–2016, pg. 195. National Security Commission on Artificial Intelligence, Final Report (Washington, DC: 2021), pg. 14–15.
[85] OUSD R&E. "Digital Engineering Capability to Automate Testing and Evaluation," May 2024. https://dsb.cto.mil/wp-content/uploads/2024/08/DSB_DE_Final-Report_050124_Stamped.pdf#.
[86] Angela O'Mahony et al., Prioritizing Security Cooperation with Highly Capable US Allies: Framing Army-to-Army Partnerships, RR-A641-1 (Santa Monica, CA: RAND Corporation, 2022).

Technological Implications

Technologically, C4ISR modernization is driven by industry-led technical innovation in dual-use technologies, specifically in space-based sensing and communications via proliferated low-earth orbit satellites, AI-enabled data processing, and resilient networking architectures.[87] Next-generation C4ISR networks are moving towards edge computing, AI-enabled data fusion, and modular open system architectures to support CJADC2 requirements.[88] The integration of commercial innovations like Anduril's autonomous ISR platforms and Starlink's SATCOM constellations is revolutionizing battlefield data transport and resilience.[89] However, these advances introduce vulnerabilities—including cybersecurity risks, supply chain sabotage, and dependency on often fragile and vulnerable commercial systems—which adversaries like China and Russia actively assess for exploitation.[90] Furthermore, inconsistent metadata and data governance standards threaten interoperability across joint and coalition forces.[91] To fully leverage technological gains, DoD must institutionalize rigorous data governance, adopt modular

[87] National Reconnaissance Office. "NRO Announces Largest Award of Commercial Imagery Contracts." Press release no. 05-22. Chantilly, VA: National Reconnaissance Office, May 25, 2022. https://www.nro.gov/Portals/135/documents/news/press/2022/press_release_05-22.pdf. And Jason Weiss and Dan Patt, Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era (Washington, DC: Hudson Institute, December 2022).

[88] US Joint Chiefs of Staff, Joint All-Domain Command and Control Strategy, March 2022, https://media.defense.gov/2022/Mar/17/2002958400/-1/-1/0/JADC2-STRATEGY.PDF.

[89] Feldstein, Steven. "Why Catching up to Starlink Is a Priority for Beijing." Carnegie Endowment for International Peace, September 3, 2024. Accessed April 17, 2025. And Frost and Sullivan, Global Aerospace & Defense Research Team, "Assessment of the US DoD C4ISR Market, Forecast to 2025," Frost & Sullivan, K4D9-15, August 2020.

[90] IATF for Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. And Defense Intelligence Agency, "Challenges to Security in Space – 2022" (Washington, D.C.: United States Department of Defense, 2022), 9, https://media.defense.gov/2022/Apr/ 12/2002976239/-1/-1/0/ CHALLENGES-TOSECURITY-IN-SPACE-2022.PDF.

[91] US Department of Defense, *Command, Control, and Communications Modernization Strategy,* (Washington, DC: Department of Defense, 2020), 25, https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf. And "Improving System Interoperability with a Data-Centric Universal C2 Language," Carnegie Mellon University Software Engineering Institute, accessed April 10, 2025, https://insights.sei.cmu.edu/annual-reviews/2021-year-inreview/improving-system-interoperability-with-a-data-centric-universal-c2-language/.

and adaptive system designs, and accelerate public-private R&D collaboration focused on speed, resilience, and mission adaptability.

The future of U.S. C4ISR modernization requires integrating political commitment, economic incentives to industry, workforce readiness, and technological agility into a unified approach. Bureaucratic delays, supply chain vulnerabilities, and workforce skill gaps must be addressed through streamlined acquisition, public-private partnerships, and targeted digital upskilling. Rapid integration of commercial technologies like autonomous ISR and proliferated SATCOM demands standardized data governance and modular, open architectures to mitigate security risks. Sustained C4ISR advantage will belong to those who adapt faster, integrate smarter, and lead coalition efforts across domains.

Porter's Five Forces Analysis

Porter's Five Forces framework provides a structured lens to assess the competitive dynamics of the C4ISR industry under JADC2. The five forces—(1) rivalry among existing competitors, (2) threat of new entrants, (3) bargaining power of suppliers, (4) bargaining power of buyers, and (5) threat of substitutes—reveal the market's unique structure and shifting power relationships. While the defense sector is not a free market in the classical sense (given the DoD's monopsony position and heavy regulation), it remains subject to evolving competitive pressures. The C4ISR industry is characterized by high barriers to entry, long-standing incumbents with proprietary systems, and tight coupling with government acquisition practices. [92] Rivalry is relatively moderate but intensifying in areas like commercial space, where dual-use

[92] Technavio, Global C4ISR Market 2024-2028 (Chicago, IL: Infiniti Research Limited, 2024), 101, https://www-emis-com.nduezproxy.idm.oclc.org/php/url-sharing/route?url=7430e7b38e11e1c3&.] [Jennifer Stewart, et al., Vital

technologies and venture-backed firms are lowering costs and increasing innovation. Although regulatory constraints continue to limit substitution and new entrants, emerging firms like Palantir have demonstrated that disruptive innovation is possible—even within this tightly controlled space. [93] Meanwhile, supplier power is reinforced by vertical integration and proprietary architectures, and buyer power—though centralized in the U.S. government—has shifted slightly toward collaboration via multinational research and development partnerships. Collectively, these dynamics underscore the complex, adaptive nature of competition in the defense C4ISR ecosystem.

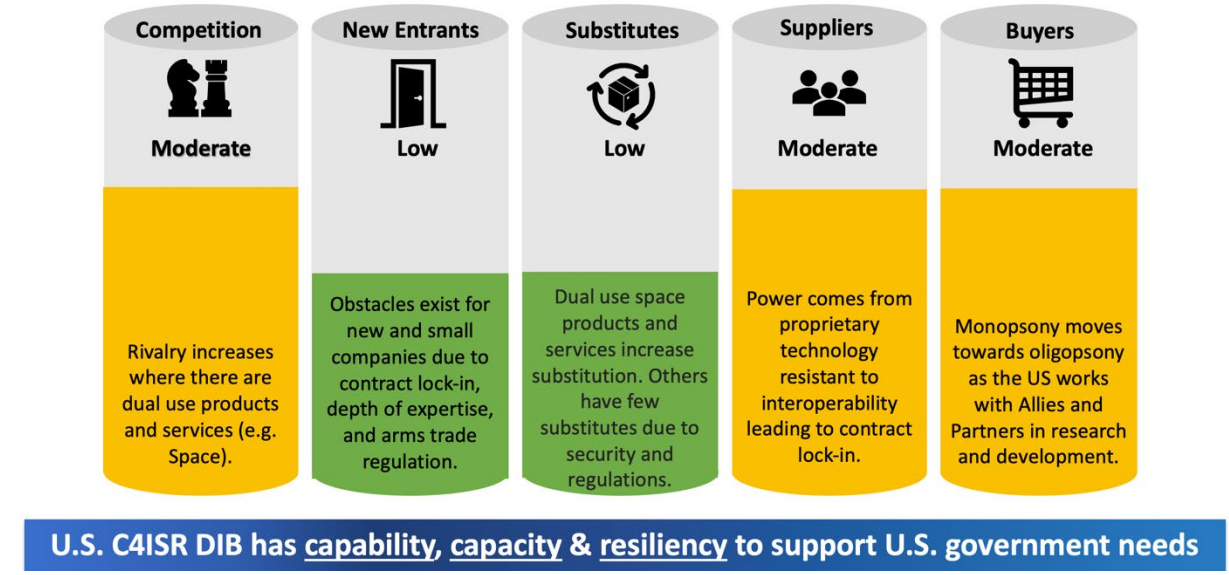


Figure 4: C4ISR Industry Competitiveness (Porter's Five Forces Analysis)

Signs 2025: The Health and Readiness of the Defense Industrial Base (Arlington, VA: NDIA, 2025), https://www.ndia.org/-/media/sites/ndia/policy/vital-signs/2025/vitalsign_2025_final.pdf?download=1?download=1.

[93] Michael T. Klare, "A New Military-Industrial Complex Arises: The Secret War Within the Pentagon," Fair Observer, March 20, 2025, https://www.fairobserver.com/business/technology/a-new-military-industrial-complex-arises-the-secret-war-within-the-pentagon.

Problem Statement

Despite recent strategic emphasis, DoD C4ISR modernization demands a more coherent approach that synchronizes acquisition reform, data standardization, workforce development, and public-private collaboration, hindering its ability to effectively partner with industry to build a resilient, interoperable ecosystem capable of sustaining strategic advantage in a contested global environment.

To enhance coherence in DoD C4ISR modernization, the following section presents seven recommendations organized into three thematic areas. These proposals are informed by the seminar's collective expertise, original research, and insights gained through engagements with U.S. and allied industry, academia, military institutions, and government agencies.

Recommendations

Despite abundant strategy and guidance, U.S. C4ISR modernization remains disjointed, delayed, and uninspired. The following recommendations are not a panacea but a set of targeted micro catalysts intended to accelerate the long-overdue shift toward a more coherent and integrated C4ISR enterprise.

Standardize the Data, Empower the Network: Reforming DoD and FMS for Coalition Interoperability

1. Institutionalizing and Enforcing Data and Metadata Standards

Inconsistent data governance and metadata practices significantly threaten achieving data interoperability across joint and coalition forces. Expanding and enforcing common data and metadata standards is essential for enhancing information security, enabling advanced analytics

and AI applications, and facilitating automated, cross-domain information sharing with allies and partners.

However, data standardization remains a persistent challenge due to the DoD legacy technology debt and industry resistance to externally imposed constraints. To overcome these obstacles, the DoD should expand collaborative efforts with the private sector through established consortia such as the Sensor Open Systems Architecture (SOSA), ensuring that standards are co-developed to reflect operational needs and commercial viability. Thoughtfully crafted standards—developed with meaningful industry input—can reduce vendor lock-in while preserving incentives for innovation, ultimately increasing long-term profitability for participating firms and potentially lowering barriers to entry for new firms.

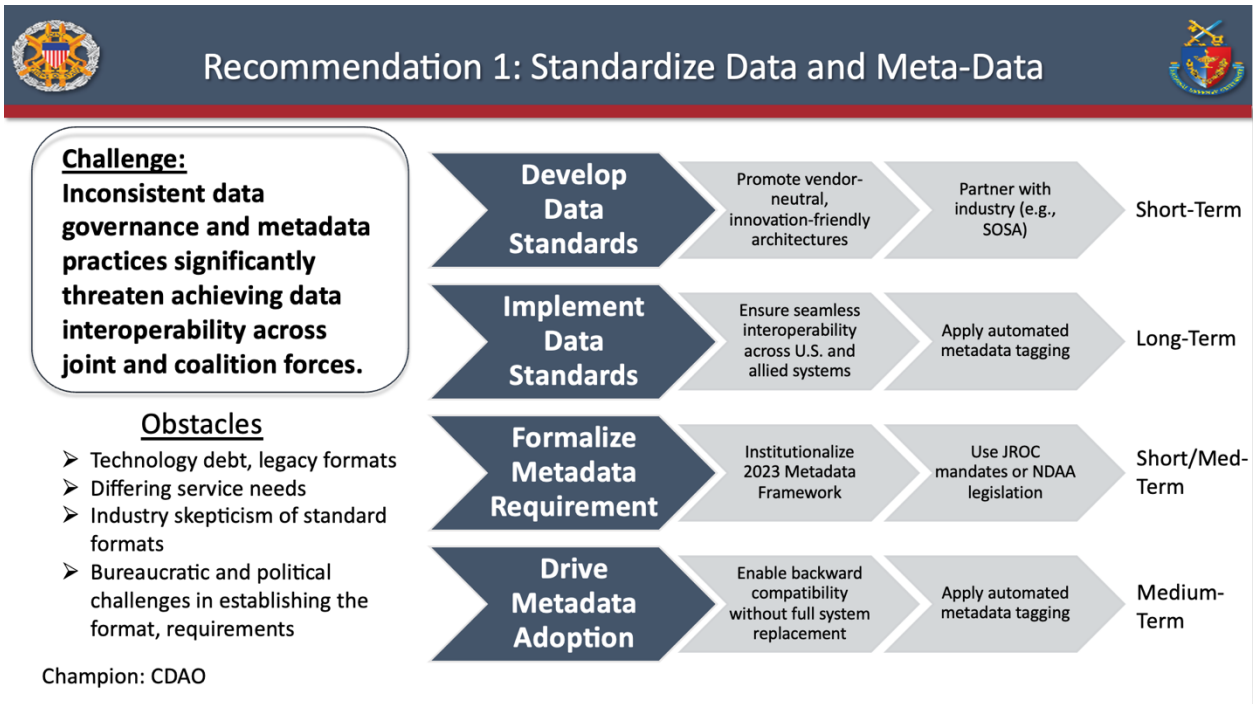


Figure 5: Recommendation 1 - Standardize Data and Metadata

Metadata standardization, in particular, represents a high-payoff opportunity to modernize the DoD's data layer. Automated metadata tagging at the point of data ingestion can

retrofit legacy systems to meet contemporary operational requirements. This capability offers a new vector for public-private partnership and aligns with the CDAO 2023 Metadata Guidance. The DoD should move aggressively to operationalize this guidance by formalizing metadata tagging as a requirement through the Joint Requirements Oversight Council (JROC) or securing legislative mandates through a future National Defense Authorization Act (NDAA). Any legislative action should incorporate agile compliance pathways to avoid delaying acquisitions, ensuring data modernization efforts keep pace with technological and operational demands.

2. Expand C4ISR Data-sharing and Ease U.S. Equipment Demands Through Reformed FMS

Amid rising inflation and outdated security protocols, FMS has devolved into a narrow relationship maintenance tool, sidelining its potential for advancing multilateral cooperation, C4ISR data integration, and equitable security burden-sharing. To remedy this and take full advantage of FMS opportunities, OSD Policy (P) and the State Department should coordinate a proposal to remove or significantly increase current Congressional notification monetary limits for FMS procedures to match today's inflation rates and security requirements to modernize the process and expand U.S. operational reach. These measures would eliminate unnecessary and deleterious bureaucratic delays without impinging necessary oversight. The FMS administrative process is overdue for streamlining, such as simplified approval procedures and digital tools that enable faster decision timelines while maintaining complete transparency. Modernization efforts should prioritize integrating secure, interoperable data-sharing technologies into allied and partner forces, fostering multilateral information-sharing agreements centered around U.S. C4ISR systems. The creation of common technological systems by the United States would allow allies to function autonomously while decreasing their dependency on American military

resources in Middle Eastern regions and enhance network resiliency throughout coalition operations.

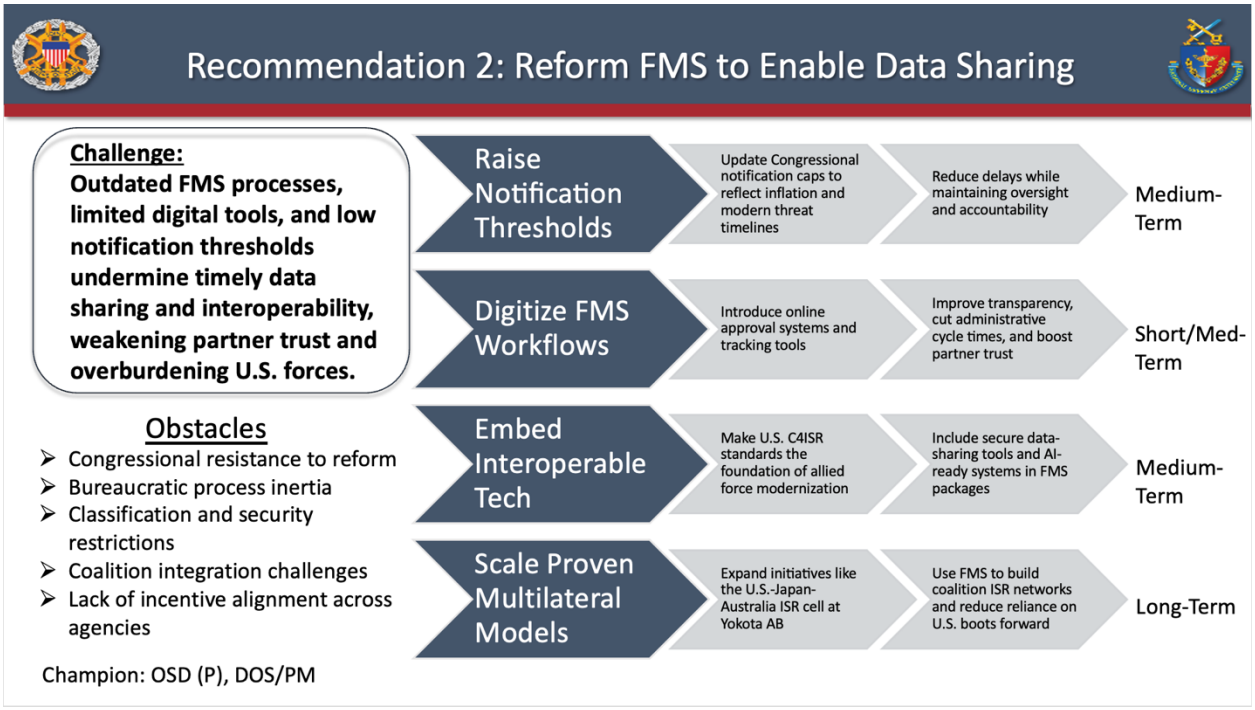


Figure 6: Recommendation 2 - Reform FMS to Enable Data Sharing

Furthermore, the Indo-Pacific region, where U.S. allies and partners are increasingly inclined to advance their cooperative efforts, offers significant potential for expanding these agreements. The launch and success of the Bilateral Intelligence Analysis Cell between the United States and Japan (later adding Australia) on Yokota Air Base is a portent of the potential available through FMS-based C4ISR cooperative initiatives[94]. Multilateral data sharing in the

[94] "U.S., Japan Hold Bilateral Intelligence Analysis Cell Opening Ceremony," U.S. Indo-Pacific Command, accessed May 7, 2025, https://www.pacom.mil/Media/News/News-Article-View/Article/3233497/us-japan-hold-bilateral-intelligence-analysis-cell-opening-ceremony/https%3A%2F%2Fwww.pacom.mil%2FMedia%2FNEWS%2FNews-Article-View%2FArticle%2F3233497%2Fus-japan-hold-bilateral-intelligence-analysis-cell-opening-ceremony%2F; "Joint Statement of the 2023 U.S.–Japan Security Consultative Committee ('2+2')," U.S. Department of Defense, accessed May 7, 2025, https://www.defense.gov/News/Releases/Release/Article/3265559/joint-statement-of-the-2023-usjapan-security-consultative-committee-22/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3265559%2Fjoint-statement-of-the-2023-usjapan-security-consultative-committee-22%2F.

Indo-Pacific region would enhance collective defense systems while making enemy targeting more complex and establishing foundations for wider security networks. Expanding FMS transactions for C4ISR technologies will deliver essential funding to the U.S. defense industrial base to drive innovation and production capacity while promoting burden sharing through collective investment.

Enhanced Public-Private Partnerships

3. Leverage Commercial Capabilities and Data Infrastructure

To strengthen public-private partnerships and accelerate the integration of commercial innovation into national defense, the United States must better harness existing commercial space-based ISR and data infrastructure. A key step is operationalizing the U.S. Space Force's Commercial Strategy, particularly through developing the Commercial Space Augmentation Reserve (CSAR). Modeled after the Civil Reserve Air Fleet (CRAF), CSAR would enable the rapid contracting of commercial providers for SATCOM, imagery, and radar services during crises, significantly enhancing ISR surge capacity. Additionally, a forward-leaning policy must authorize the use of commercial technologies developed "to the edge" without requiring bespoke government specifications, accelerating access to disruptive capabilities. Digital communications infrastructure—including fiber and satellite pathways—should be treated as a strategic asset, with regulatory mechanisms to prioritize national security data flows during contingencies. Establishing a hybrid architecture that integrates commercial and military systems, particularly in domains like SATCOM, will improve resilience, complicate adversary targeting, and reduce vulnerability. This effort should be championed by the Under Secretary of Defense for Policy, with coordination across the United States Space Force (USSF), CDAO, DoD Chief Information

Officer, and the National Security Council. Despite high costs and classification barriers, the technical feasibility and strategic necessity are clear.

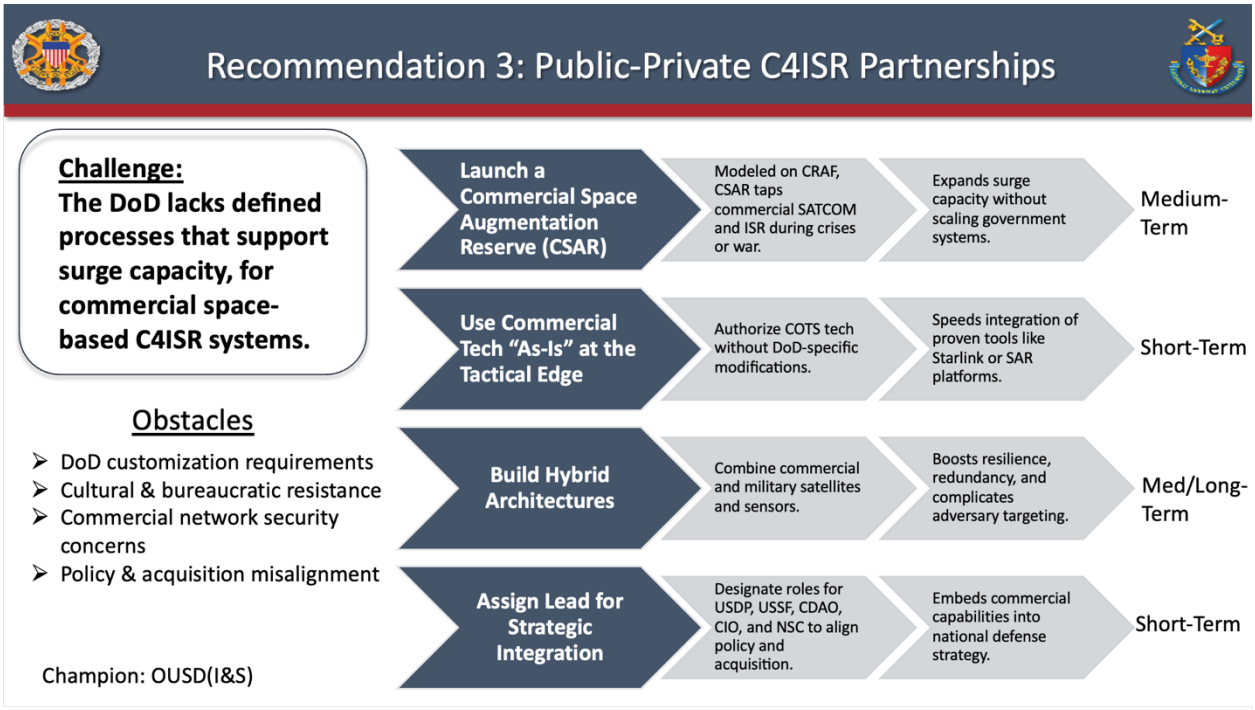


Figure 7: Recommendation 3: Public-Private C4ISR Partnerships

4. Adopt Continuous Authority to Operate (ATO) Models

The DoD must shift from the current static ATO process toward a continuous ATO model to accelerate software deployment and maintain technological relevance.[95] The legacy approach—often requiring months of documentation and review—creates debilitating bottlenecks that hinder the rapid delivery of software updates essential for operational agility. During a recent roundtable, a senior software and design engineer from the U.S. Navy's Project Overmatch underscored the urgency of this transition, noting that a continuous ATO framework

[95] ATO is "Authorization granted by a DAA/AO for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented required security controls and that the residual risk is acceptable," in Defense Information Systems Agency (DISA), *DISN Connection Process Guide*, Appendix K (Fort Meade, MD: DISA, 2022), https://disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/DISN-Glossary.pdf.

is indispensable for aligning defense software development with the pace and practices of the commercial tech sector. [96] Unlike the traditional one-time certification model, a continuous ATO would integrate ongoing security monitoring and compliance validation through advanced tools such as digital twins, which simulate real-time software performance and vulnerabilities. This approach preserves the ATO's original intent—ensuring cybersecurity and operational standards—while drastically reducing deployment timelines. Implementation should begin with policy changes at the service level, championed by the Under Secretary of Defense for Acquisition and Sustainment (USD [A&S]) and supported by the Services' Program Executive Officers (PEOs). Broader legislative reforms should be proposed in the FY26/27 National Defense Authorization Act (NDAA) to enshrine the model across the defense enterprise. Key investments will include modernizing the acquisition workforce, reforming legal and compliance frameworks, and funding the infrastructure required to support digital twin technologies. However, institutional resistance and incompatibility with legacy systems present real risks. Overcoming these challenges will require strong leadership, clear incentives, and a recognition

[96] Senior Software and Design Engineer, U.S. Navy Project Overmatch, comment during industry study visit, San Diego, CA, March 31, 2025.

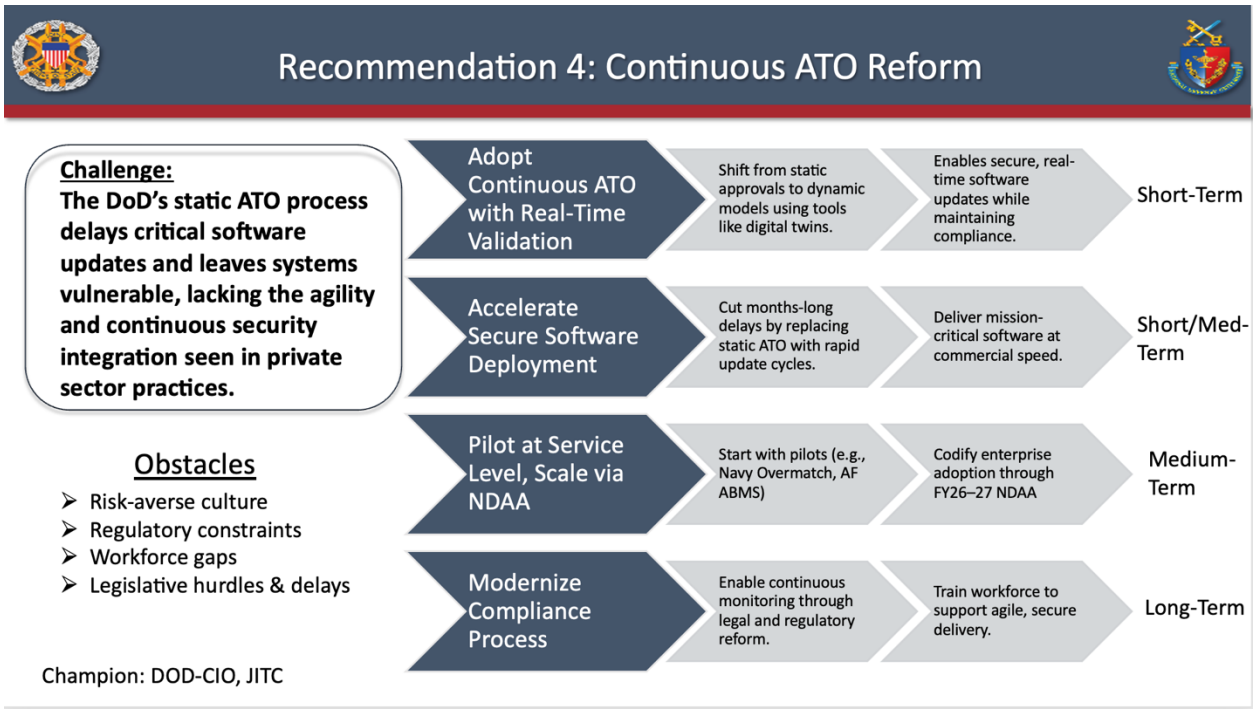
that sustained information advantage depends not only on the software itself—but on the speed and security with which it can be delivered to the fight.

Scalable Workforce Data Literacy Readiness

5. Build Scalable Workforce Readiness Through Certifications, Embedded Training Tools, and Enlisted Data-Centric Specialties

To close the growing digital readiness gap in C4ISR operations, the DoD must build a scalable, integrated workforce development approach. While commercial certifications and AI-enabled training tools exist in limited pockets, they remain underutilized across operational billets and overtasked in others. This recommendation bridges that gap by embedding certification-granting training into PME and initial skills training while co-developing modular, AI-driven tools that deliver on-the-job training within C4ISR work centers and platforms. The result is a more technically fluent force—less dependent on contractor support, more resilient,

Figure 8: Recommendation 4 - Continuous ATO Reform



and better equipped to operate in contested, data-driven environments—aligned with current DoD innovation and mobilization priorities. As a pilot program, the services should analyze their enlisted ranks for specialties most likely to benefit from AI and automation-enabled data management skills to reshape the force.

5A. Integrate Commercial Certifications for Key Workforce Segments

The DoD should expand the use of commercial credentials—such as CompTIA Data+, AWS Cloud Practitioner, and Elastic Certified Analyst—across Professional Military Education (PME), initial skills training, and continuing education pipelines. These industry-recognized certifications reinforce C4ISR-related competencies, including data mining, cloud-based command and control, and real-time data analysis. They improve warfighter proficiency while reducing reliance on contractor field representatives for basic tool usage. Target populations should initially include enlisted personnel and warrant officers in intelligence, cyber, communications, and operations specialties, with eventual expansion to junior officers and government civilians involved in acquisition or analysis. Key digital specialists, such as data scientists, engineers, and developers assigned to the CDAO, Combatant Command J2/J6/J8 staffs, or service software organizations, should also be prioritized. This approach enhances interoperability with commercial platforms, reduces the long-term contractor support burden, and builds enduring, in-house digital capability. Tailored certification and training efforts are particularly vital for intelligence, IT/communications, and command and control personnel (See Table C). Acquisition professionals, systems engineers, and EW/space operators must also achieve digital fluency to field and fight with interoperable C4ISR tools. Investing in these communities accelerates adoption, fosters readiness, and fortifies the force for contested, data-rich environments.

5B. Embed Modular, AI-Enabled Training Tools in C4ISR Platforms

To move beyond certification and ensure true operational fluency, the DoD should co-develop modular, AI-enabled microtraining applications embedded directly into C4ISR software and hardware systems. These adaptive tools deliver progressive, job-specific instruction with intuitive interfaces and real-time feedback, enabling training at the point of need while reducing the burden on centralized instruction pipelines. For example, an E-5 sensor operator could receive real-time guidance on fusing ISR inputs during a live mission—building muscle memory without interrupting operational tempo. Over time, these capabilities would evolve into persistent training layers across platforms fielded through programs like PEO C3T and C3BM. This effort should be championed by the Office of the Under Secretary of Defense for Personnel and Readiness, in coordination with the CDAO, Joint Staff J1, and supported by DIU, PEO C3T, PEO C3BM, and NAVWAR. Pilots in high-demand fields could begin by FY26–27, with full integration by FY30. The cost is low to moderate, funded initially via OTA or procurement and sustained through O&M. If not pursued, the risk is high—data fluency is essential to joint operations. This initiative modernizes training for an information-dominant fight, fostering a digitally fluent force aligned with CJADC2 and JADC2 priorities.

Category	Example Career Fields	Why It Matters
Intelligence (ISR, GEOINT, SIGINT, All-Source)	USAF: 1N, 14N | Army: 35F, 35G, 35N | Navy: IS | USMC: 0231, 0202	Operate and analyze ISR systems; requires data fluency and real-time tools
Cyber & Information Warfare	USAF: 1B4, 17X | Army: 17C, 255 | Navy: CW, IT | USMC: 1721, 1799, 0600	Defend and exploit digital terrain; integrate AI/cyber/data capabilities
Command & Control / Battle Management	USAF: 1C5, 13B | Army: 13-series, 14-series | Navy: SWO (C2) | USMC: 7200, 0602	Direct tactical decisions; need fast, intuitive tools with embedded training
Communications / IT / Network Ops	USAF: 3D1X2/3, 17D | Army: 25-series, 255N | Navy: IT, CTN | USMC: 0600	Maintain C4ISR backbone; manage cloud, data, and network operations
Acquisition, Logistics & Engineering	All Services: 63A, FA 51, PMs, Engineers, GS Acquisition Civilians	Shape acquisition decisions; ensure interoperability and software integration
Space Ops & Electronic Warfare	USSF: 13S | USAF: 1B4 | Army: 29E, 17-series | Navy: EW Officers	Operate in contested space/spectrum; require agile, autonomous systems training
Data Science & Software Development	Civilians (GS-13/14 Data Scientists, Developers at CDAO, CCMD J6/J8); Military billets at Kessel Run, Platform One	Build, manage, and scale AI/ML-enabled systems, data pipelines, and digital ops critical to CJADC2

Table 2: Prospective AI/Data Training Benefit to Military Specialties

5C. Start Shaping the Data Force Now for Future Conflict

Even with data-focused education integrated into milestone training and daily operations, specific work centers—those tasked with processing large volumes of data under continuous operational pressure—will remain hampered by critical data literacy gaps. Armed conflict with a peer adversary will only magnify this challenge. To address it, the DoD should rapidly identify enlisted specialties in the active and reserve components where skills conversion training would yield the greatest operational return. Those performing data-intensive tasks likely to surge in

conflict—well-suited to AI-enabled processing—should be prioritized. These servicemembers will form the foundation of battlespace awareness, enabling faster, more informed decisions for commanders.

The United States Air Force offers a proven template for cultivating operational data expertise. The Air Force Research Lab grants master's degrees in data science to officers who are then embedded in staff and field commands to drive analytics-informed decision-making. In 2025, Air Combat Command—the Air Force's largest operational command—will activate the Studies and Analysis Squadron, a dedicated unit to provide data science support across combat units[97]. This model should inform the rapid development of an enlisted cadre of data managers capable of enabling real-time decision advantage under fire. Intelligence and battle management specialties are prime candidates. Delaying this effort risks a critical shortfall in digital fluency

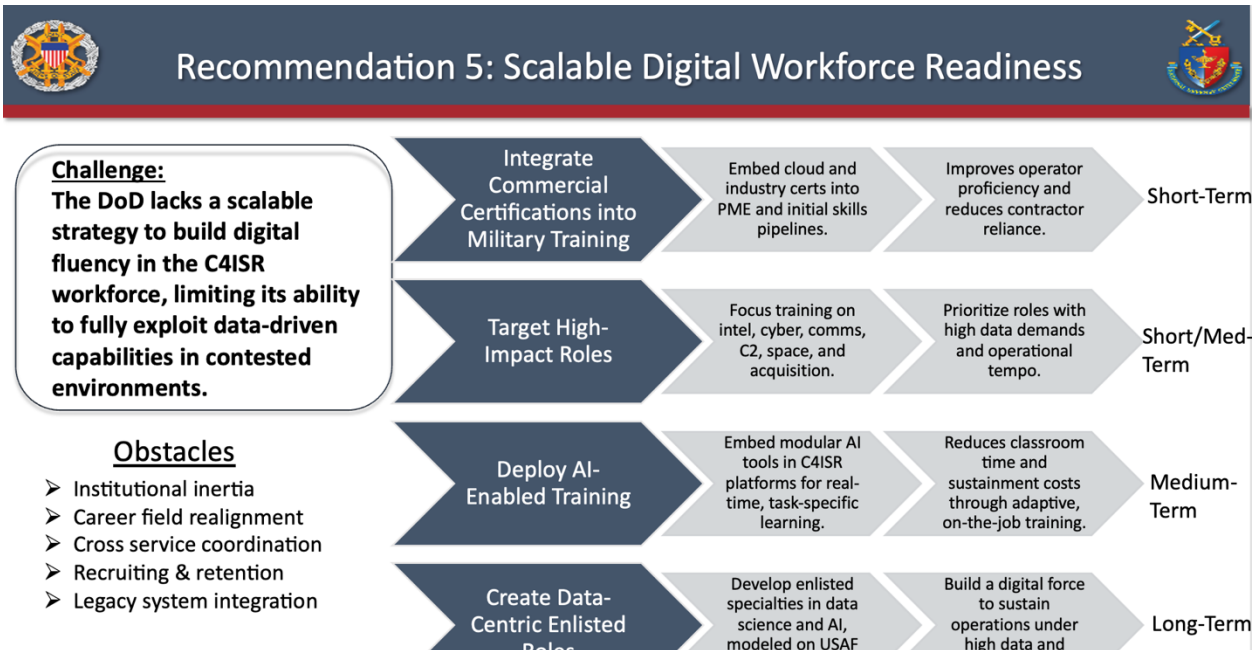


Figure 9: Recommendation 5 - Scalable Digital Workforce Readiness

[97] "Det 4 Provides a Data Analysis Capability for ACC Units," Air Combat Command, October 12, 2023, 4, https://www.acc.af.mil/News/Article-Display/Article/3555752/det-4-provides-a-data-analysis-capability-for-acc-units/https%3A%2F%2Fwww.acc.af.mil%2FNews%2FArticle-Display%2FArticle%2F3555752%2Fdet-4-provides-a-data-analysis-capability-for-acc-units%2F.

just as timelines accelerate toward a potential Taiwan contingency. Beijing is not waiting—and neither can we.

Conclusion

National security and technological transformation intersect at the core of the C4ISR enterprise. The DoD must quickly transform and update its C4ISR capabilities to face operational requirements in today's unstable and contested world environment. The nature of modern warfare, as displayed in the ongoing Russia-Ukraine conflict and China's military advancements, reveals a paradigm shift: The ability to acquire and process information rapidly determines modern warfare effectiveness. Despite its technological capabilities, the United States must address structural, cultural, and procedural barriers to maintain its information superiority and achieve successful joint and coalition combat operations.

The results from field studies alongside stakeholder engagements and industry models demonstrate that outdated acquisition methods, supply chain weaknesses, and excessive classification impede quick technological progress and system compatibility. The U.S. C4ISR industrial base maintains strong technological leadership, a skilled workforce, and a dynamic commercial partner network, yet faces difficulties in quickly combining these assets for contemporary battle requirements. To address these challenges, this study has outlined a comprehensive modernization framework centered on three imperatives: Joint and coalition operations require data and technology standardization, while enhanced public-private partnerships should leverage commercial innovations to support scalable workforce readiness and digital fluency across military forces.

Establishing data and metadata standards is an essential starting point for building interoperability across systems. AI implementation with agile C2 and automation initiatives remain fragmented and vulnerable due to the absence of unified data architectures. Accelerating multilateral data-sharing capabilities through Foreign Military Sales process reform enhances alliance strength and achieves fairer operational burden distribution throughout the Indo-Pacific region. These measures must be combined with reforms that eliminate vendor lock-in while developing open system architectures to support agile coalition activities.

Commercial ISR assets integration through proliferated Low Earth Orbit satellite communications and AI-enabled situational awareness creates real-time chances to grow operational resilience and responsiveness. The Commercial Space Augmentation Reserve and continuous Authority to Operate models highlight DoD strategies to utilize commercial space while maintaining security and operational control. Implementing embedded training tools and commercial certifications for data-centric enlisted specialties will bridge the digital readiness gap while matching technological capabilities with operational proficiency.

Maintaining U.S. warfighting dominance in the information age requires a comprehensive transformation of our approach to conceptualizing, acquiring, operating, and training for C4ISR capabilities beyond new platforms and systems. This transformation must be deliberate but unrelenting. Effective leadership, strategic funding, and dedicated coalition interoperability commitments will prove crucial. The United States must future-proof its C4ISR enterprise to ensure military superiority in future power conflicts, which will be determined before combat begins.

Appendices

Appendix A: National Security Impacts and Trends of Artificial Intelligence in C4ISR

Intelligence Analysis and Predictive Analytics. AI significantly enhances intelligence analysis by rapidly processing multi-source intelligence, including imagery, signals, human reports, and open sources. The National Security Commission on AI (NSCAI) highlights improvements across the intelligence cycle due to AI's ability to detect patterns and anomalies unnoticed by human analysts.[98] For example, the DoD's Project Maven demonstrates AI's capability to automate object detection from drone video feeds, greatly improving intelligence fusion and situational awareness.[99]

Autonomous ISR Platforms. Autonomous surveillance and reconnaissance platforms increasingly utilize AI to interpret sensor data instantly, allowing autonomous navigation and threat response. Examples include drones using reinforcement learning for target tracking and obstacle avoidance.[100] The Air Force's "loyal wingman" drones and the Navy's Sea Hunter unmanned vessels illustrate how AI extends ISR capabilities with minimal human intervention, significantly enhancing persistent surveillance and rapid information dissemination.[101]

Decision-Support Systems for Command and Control. AI-driven decision-support systems substantially boost command and control efficiency. Deputy Secretary of Defense Kathleen Hicks notes AI's role in enhancing commanders' decision-making speed and

[98] Eric Schmidt, et al., "Final Report: National Security Commission on Artificial Intelligence" (Washington, DC: National Security Commission on AI, 2021), https://www.nscai.gov/2021-final-report/.
[99] Gregory C. Allen, "Six Questions Every DOD AI and Autonomy Program Manager Needs to Be Prepared to Answer," May 15, 2023, https://www.csis.org/analysis/six-questions-every-dod-ai-and-autonomy-program-manager-needs-be-prepared-answer.
[100] "Overwatch Imaging | AI-Driven ISR Sensors and Software Solutions | Aerial Mapping and Inspection," Overwatch Imaging, accessed May 5, 2025, https://www.overwatchimaging.com/.
[101] Eric Schmidt, et al., "Final Report: National Security Commission on Artificial Intelligence." 109.

accuracy.[102] For instance, Project Convergence experiments have leveraged AI to shorten the sensor-to-shooter timeline from 20 minutes to under one minute, highlighting AI's transformative potential in operational contexts.[103]

Future AI Trends in C4ISR. Emerging efforts, particularly with Generative AI and Large Language Models (LLMs), are expected to revolutionize defense intelligence and command structures. Initiatives like Task Force Lima and the AI Rapid Capabilities Cell (AI RCC) aim to accelerate generative AI adoption for tasks including intelligence summarization, language translation, and decision support.[104] Additionally, future ISR will feature AI-coordinated drone swarms and robotic systems performing wide-area surveillance and targeting, enabling advanced multi-domain operations such as the Combined Joint All-Domain Command and Control (CJADC2).[105]

Scaling AI for Strategic Advantage. The CDAO's strategy emphasizes transitioning from limited pilots to broad AI deployments using cloud-based development and secure, enterprise-wide platforms. This scalable approach supports rapid model validation and deployment across defense networks. AI's operational integration, particularly in adaptive planning and real-time

[102] Joseph Clark, "DOD Releases AI Adoption Strategy," U.S. Department of Defense, November 2, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F3578219%2Fdod-releases-ai-adoption-strategy%2F.
[103] "Inside the Army's Futuristic Test of Its Battlefield Artificial Intelligence in the Desert," accessed May 6, 2025, https://www.c4isrnet.com/artificial-intelligence/2020/09/25/the-army-just-conducted-a-massive-test-of-its-battlefield-artificial-intelligence-in-the-desert/?utm_source=chatgpt.com.
[104] "CDAO and DIU Launch New Effort Focused on Accelerating DOD Adoption of AI Capabilities," U.S. Department of Defense, accessed May 5, 2025, https://www.defense.gov/News/Releases/Release/Article/3996199/cdao-and-diu-launch-new-effort-focused-on-accelerating-dod-adoption-of-ai-capab/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3996199%2Fcdao-and-diu-launch-new-effort-focused-on-accelerating-dod-adoption-of-ai-capab%2F.
[105] "The Pentagon Is Planning a Drone 'Hellscape' to Defend Taiwan | WIRED," accessed May 6, 2025, https://www.wired.com/story/china-taiwan-pentagon-drone-hellscape/?utm_source=chatgpt.com.

analytics, could dramatically alter campaign strategies by enabling unprecedented synchronization across joint forces.[106]

AI's integration into C4ISR provides strategic, operational, and tactical advantages, bolstering deterrence, accelerating operations, and ensuring information dominance. However, these benefits depend on effectively managing challenges related to reliability, cybersecurity, and personnel training to maintain competitive superiority in the AI-enhanced battlefield.

[106] Clark, "DOD Releases AI Adoption Strategy."

Appendix B: Wargaming in the C4ISR Industry

The DoD has multiple levels of representing new and emerging technologies in an artificial environment to provide the warfighter with the best command, control, computers, communication, intelligence, surveillance, and reconnaissance (C4ISR) technology before they use them in conflict. Three of these areas are strategic wargaming, modeling and simulation (M&S), and experimentation.

Strategic Wargaming

The military services and Office of the Secretary of Defense, Cost Assessment and Program Evaluation (OSD CAPE) regularly conduct wargames to develop future concepts, future force structure, technology gaps, etc.[107] They include experts with operational and technical experience in wargaming, including the intelligence community, theater planners, and experts in the focus capabilities.[108] Firms within the C4ISR sector of the defense industrial base do parallel strategic wargaming to develop capabilities within the context of a Joint and Combined fight with interoperable technology against various threats. In some cases, the DoD gives them wargame readouts to supplement their internal work. However, industry partners miss the dialog during the war game where warfighters express pain points. The opportunity to interject with an innovative, technological solution is minimal by the time the clean, processed notes arrive.

Recommendation: OSD CAPE instantiates an industry team similar to the red team, where firms compete to fill positions to supply industry perspectives in strategic wargames.

Modeling & Simulation

[107] Committee on Armed Services and Cary B. Russell, Defense Analysis: Additional Actions Could Enhance DoD's Wargaming Efforts §, GAO-23-105351 (2023), 11-13.
[108] Committee on Armed Services and Cary B. Russell, Defense Analysis, 18.

M&S in the defense context refers to creating digital models of systems or environments and running simulations to observe their behavior over time. These allow stakeholders to prototype "in the computer" and gain insights without needing a full physical system. M&S has become indispensable to defense acquisition and innovation. First, it enables faster experimentation that iterates designs in hours on a computer versus months or years to build and test in hardware.[109] Second, M&S allows for risk reduction: identifying flaws or failure modes before committing to production, thereby avoiding rework. Third, it provides a safe and controlled means to test edge cases or dangerous scenarios, such as cyberattacks or electronic jamming, to develop countermeasures. Finally, M&S promotes interoperability and collaboration with Allies by serving as a common reference.[110] Overall, using M&S has proven to save time and resources in defense programs while unlocking innovative solutions.

Recommendation: Mandate, expand, and integrate M&S into development cycles.

Experimentation

Several experimental efforts support the delivery of CJADC2, an essential element of C4ISR. Experimentation is a process that advances knowledge and allows for the development of new capabilities.[111] "Campaigns of experimentation" build upon each other, share information and findings, and iterate towards transformational discovery and results.[112] The DoD has four primary experimentation efforts. Project Convergence is the Army's "campaign of learning" to further integrate the Army into the Joint Force.[113] The Navy's Project Overmatch

[109] "Test and Evaluation—Where the Rubber Meets the Road in Digital Engineering | Www.Dau.Edu." Accessed April 17, 2025. https://www.dau.edu/library/damag/november-december2021/test-and-evaluation#.
[110] Demarest, Colin. "US, UK Partner on Command and Control as Project Convergence Wraps." C4ISRNet, November 22, 2022. https://www.c4isrnet.com/battlefield-tech/c2-comms/2022/11/22/us-uk-partner-on-command-and-control-as-project-convergence-wraps/.
[111] David S. Alberts and Richard E. Hayes, *Campaigns of Experimentation, Pathways to Innovation and Transformation* (CCRP Publications 2005), 18, http://www.dodccrp.org/files/Alberts_Campaigns.pdf
[112] Alberts and Hayes, *Campaigns of Experimentation*, 19
[113] Andrew Feickert, "The Army's Project Convergence," Congressional Research Service, IF11654, June 2, 2022

"focuses on delivering reliable communications for a widely distributed hybrid force."[114] The JFN is "USINDOPACOM's mechanism to integrate, command, control, synchronize, and deliver effects across the battlespace."[115] Finally, mixing experimentation and exercise testing JFN, Valiant Shield is a "biennial exercise focused on integration between the services in a multi-domain environment in the Pacific region."[116]

Recommendation: Appoint a CJADC2 lead at the defense level to coordinate Joint and Combined experimentation efforts.

[114] Elisha Gamboa, "Project Overmatch Achieves Historic Milestone with Five Eyes Agreement," NAVWAR Media, 26 February 2025, https://www.navwar.navy.mil/Media/Article/4077984/project-overmatch-achieves-historic-milestone-with-five-eyes-agreement/
[115] John C. Aquilino, "Statement of Admiral John C. Aquilino, U.S. Navy Commander, U.S. Indo-Pacific Command," U.S. Congress, 20 March 2024
[116] Mark Pomerleau, "Joint force, international partners, contractors test command and control capabilities in the Pacific exercise," *Defense Scoop*, July 19, 2024. 2.