AY 2024-2025

THE AI FAULT LINE: DRIVING MILITARY POWER AND SHAPING GLOBAL ORDER

INDUSTRY STUDY COURSE GROUP PAPER

DR. JAMES KEAGLE

Seminar 2: Artificial Intelligence
Cohort Submission

SEMINAR #2

Word Count: 8756

May 14, 2025

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

Artificial Intelligence Industry Seminar Faculty

Dr. James Keagle (USAF, Ret.), Artificial Intelligence Industry Seminar Lead
Col G. John David, United States Marine Corps
Mr. Bruce Lichtman (USAF, Ret./Department of Homeland Security (DHS) Chair)
Dr. Robert Williams, National Geospatial Intelligence Agency

Seminar Members

Mr. Clay Allen, Department of State
Lt Col, Nacereddine Benhamla, Algerian Territorial Air Defense Forces Command
Mr. Eric William Tevis Boulware, Booz Allen Hamilton
Mr. Nicholas DiFiore, Joint Staff
COL Maureen Giorio, U.S. Army
Mr. Matthew Godwin, Defense Information Systems Agency
LTC Joshua Hayward, U.S. Army
Lt Col Leigh "PERV" Irwin, U.S. Marine Corps
Colonel Marco Mangini, Italian Air Force
LTC Florangel J. Merten, U.S. Army
CAPT Daisuke Nakagawa, Japan Maritime Self-Defense Force
Ms. Ashley O'Keefe, U.S. Air Force
Colonel Adam Olsen, U.S. Air Force
Mr. SunJun Park, Boeing
Mr. Gregory Patrick, Department of Homeland Security
Lt Col Dan Piper, U.S. Air Force
Brig Gen Zion Razon, Israel, Army
Ms. Fiona Lee Saunders, IBM
CDR Robert Seader, U.S. Navy
Lt Col Matthew Verdin, U.S. Marine Corps

Field Study Visit Locations, Hosts, and In-Class Guest Speakers

Local Visits

- **Airbus**
  - Feodora (Dora) Kurtz, Head of Corporate Strategy
  - Mr. Jaysen Yochim, Senior Director, Autonomy and AI Systems
- **DoD OT&E**
  - Dr. Christopher Palmer, Principal Director (CTO), DoD Research & Engineering, OUSD (R&E)
- **Air Force Research Lab (AFRL)**
  - Dr. Gilbert "Bert" Peterson, Professor of Computer Science, Associate Dean for Academic Affairs, Air Force Institute of Technology
- **Scale AI**
  - Mr. Dan Tadross, Head of Public Sector
  - Mr. Sandip "Sonny" Sarkar, Public Sector Strategy and Revenue Lead
  - Mr. G. Andrew Otterbacher, Director - GSP
- **AWS** (Amazon Web Services)
  - Mr. Mo Shahin, Joint Defense Agencies business – Fourth Estate
  - Mr. Blaine Little, Account Manager
  - Ms. Hannah Marlowe, Sr. Manager Model Customization
  - Mr. Matthew Marcus, AI Powered Modeling, Simulation and Test and Evaluation
  - Mr. Eric Topp, AWS Supply Chain – Application, Air Logistics Optimization (ALO)
  - Ms. Heather Hopkins, AI/ML Technology Development and Regulatory Changes
  - Ms. Sandra El Ashry, Gen AI Innovation Center
- **Google**
  - Mr. Kevin Mulligan, Senior Manager, U.S. Federal Policy and Outreach, Government Affairs and Public Policy
- **Allen Institute for Brain Science**
  - Dr. Nuno Maçarico da Costa, Associate Investigator
  - Dr. Casey Schneider-Mizell, Assistant Investigator
- **Booz Allen Hamilton**
  - Mr. Chris Bogden (USAF, Ret.), EVP
  - Mr. Brian MacCarthy, SVP, Booz Allen Ventures
  - Mrs. Holly Levanto, VP, Advana Lead
  - Mr. Elliot Mandel, SA, Digital Twins
  - Mrs. Sarah Smith, SA, AI Capabilities to the Combatant Commands
  - Mr. Aaron Sant-Miller, Director, Deployment of AI Models in Cyber Pipelines
  - Mrs. Catherine Ordun, VP, Adversarial AI Threats

- **JHU/APL** (Johns Hopkins University Applied Physics Laboratory)
    - Mr. Conrad Grant, Chief Engineer
    - Mr. Jeff Brown. Project Manager
- **Technology Advancement Center / Dream Port**
    - Mr. Gregg Smith, CEO
    - Mr. Thomas 'TC' Hoot, VP of Contracts
- **Alsop Louie Partners**
    - Mr. Gilman Louie, Chief Executive Officer America's Frontier Fund/Partner
- **Oracle**
    - **Oracle Reston**
    - Mr. Mark Tatum, Distinguished Technologist / Oracle GDI
    - Mr. Ezra Gere, Data Science Lead/Research Engineering
    - Mr. Brandon Anderson, Cloud Account Manager
    - Mr. Christopher Lowe, Government, Defense, Intelligence (GDI)
    - Mr. Stephen Buck, DoD Business Development
    - **Oracle Data Center (Loudoun, VA)**
    - Mr. Christopher Lowe, Government, Defense, Intelligence (GDI)
- **Shield AI**
    - Mr. Brandon Tseng, Shield AI Co-Founder, President; Former SEAL & Surface Warfare Officer
- **Palantir**
    - Ms. Mia Stender, BD Lead, USMCR, Marine Innovation Unit
    - Mr. Ben Radford, Applied AI
    - Mr. Charlie Cleveland, Senior Counselor, Major General, US Army (Retired)
- **Anduril**
    - Dr. Lance Lewis, Anduril Naval S&T Portfolio Director

Pittsburgh

- Carnegie Mellon University (CMU)
    - Hon. Tim McNulty, Associate Vice President, Government Relations
    - Dr. Rita Singh, Associate Research Professor Language Technologies Institute
    - Mr. Steven Wray, Executive Director, Block Center for Technology and Society
- Aurora Innovations
    - Mr. Matt Blackburn, Government Relations
- Alpha Gear Lab
    - Ms. Afshan Khan, Investor / Strategist / Mentor
- Innovation Works
    - Ms. Afshan Khan, Investor / Strategist / Mentor
- Human Engineering Research Laboratories (HERL), University of Pittsburgh

- Dr. Rory Cooper, Assistant Vice Chancellor for Research for Health Sciences and STEM Collaboration, University of Pittsburgh

NYC

- **IBM Watson Center**
  - Dr. George Tulevski, Senior Manager, Think Lab
  - Mr. Matt Reichman, IBM Research Executive, AI & Emerging Technology
  - Dr. Maria Chang, Senior Research Scientist
  - Ms. Cait Crawford, IBM Fellow
- **Stevens Institute for Technology**
  - George Calhoun, Director Quantitative Finance
  - Mr. Steve Yang
  - Dr. Ionut Florescu, Director of the Hanlon Financial Systems Lab
  - Mr. Justin Murray, Early Stage Investor, NJ FAST, Plug and Play Tech Center
  - Mr. Arshad Saied, Chief Online Learning Officer & Dean of the College of Professional Education
  - Mr. Zachary Feinstien, AI Compliance Officer
  - Mr. Gregory P. Prastacos, Professor and Co-Director, Center for Research to Advance Financial Technologies, School of Business at Stevens Institute of Technology
  - Mr. Tyler Lange, Venture Capital, Corporate Innovation, NJ FAST, Director, New Jersey, Plug and Play Tech Center

Silicon Valley

- **HP**
  - Dr. Tommy Gardner, Chief Technology Officer
  - Dr. Kimberly Brenik
  - Ms. Bettina Bunton, Sustainability Manager
  - Mr. Stephen (Mushizero) Pieraldi, Distinguished Technologist, Guru of Guesswork
- **Lawrence Livermore National Laboratory**
  - Mr. Reg Beer, Defense Systems Program Leader and Director of Collaborative Autonomy
  - Mr. Alexx Perloff, Research Scientist
  - Mr. Michael Schneider, Associate Program Leader and Group Leader
  - Mr. Mark Piscotty, Software Engineering
  - Ms. Sara E. Harrison, R&D Engineer
  - Mr. Jim Leek, Computer Scientist
- Apple, Inc.

    - Mr. Jon McCormack, Senior Director American Multinational Corporation and Technology Company headquartered in Cupertino, California
- Plug and Play
    - Mr. Justin Murray, Early Stage Investor, NJ FAST, Plug and Play Tech Center
    - Mr. Tyler Lange, Venture Capital, Corporate Innovation, NJ FAST, Director, New Jersey, Plug and Play Tech Center
- **NVIDIA**
    - Mr. Kevin Berce, Senior Director, Federal
    - Mr. Shane Shaneman, Senior AI Strategist - NVIDIA Federal
    - Mr. Jack Dahlgren, NVIDIA Executive Briefing Center Producer
    - Mr. Kris Keith
    - Mr. Tim Woodard, Principal Solutions Architect
- In-Q-Tel
    - A.J. Burtone
- Defense Innovation Unit (DIU)
    - CDR Cullen Greenfield, Program Manager in the Space Portfolio
    - Lt Col Nicholas DuPre, Material Leader, Acquisition
    - Mr. Tom Horan, AI/ML Portfolio Director
- IBM
    - Ms. Christina Howell, Executive Client Briefing Center Manager
    - Ms. Marina Danilevsky, Senior Research Scientist – Language Technologies
    - Dr. Ruoyi Zhou, Director, Strategic Research Partnerships
    - Mr. Kevin Roche, Engineer/Scientist at IBM Research and IBM Quantum Ambassador
- Stanford University
    - Dr. Alex “Sandy” Pentland, Stanford University
    - Dr. Matthew Fuhrmann, Texas A&M
    - Dr. Alexandre Debs, Yale University

Taiwan

- Microsoft Taiwan
    - Mr. Michael Chang
- LINE Taiwan
    - Ms. Jofan Lin
- National Science and Technology Council (NSTC)
    - Dr. Zsehong Tsai
- Meta Taiwan
    - Mr. Max Chen
- TSMC

    - Ms. Nina Kao
    - Ms. Carol Wu
    - Mr. Paul Loughran
- MediaTek
    - Ms. Beth Chien
    - Mr. Wen-Tang Su
- ITRI
    - Dr. Stephen Su
- Micron Taiwan
    - Mr. Rado Wang
- MODA
    - Honorable Herming Chiueh
- E-Tron
    - Dr. Nicky Lu, President, Owner and Cofounder

Table of Contents

Executive Summary

Artificial Intelligence (AI) and quantum technologies are rapidly transforming the character of warfare and the foundations of international power. This paper contends that the United States (U.S.) faces an urgent imperative: preserve its military-technological edge not only through AI superiority but also through institutional transformation, innovation surges, and strengthened international partnerships. Strategic competitors—especially China—are aggressively investing in AI and quantum computing with the intent to outpace U.S. capabilities, reshape global norms, and erode American deterrence.

China's military-civil fusion strategy, backed by state-driven funding and industrial-scale intellectual property theft, has enabled accelerated development of quantum-enhanced AI systems. These advancements are poised to challenge U.S. advantages in cryptography, cyber operations, logistics, and decision-making speed. Chinese investments in quantum communications, sensing, and algorithmic warfare reflect a holistic strategy to achieve dominance across physical and digital domains.

This paper organizes its analysis around four critical Lines of Effort (LOEs):

1. Cognitive Dominance: AI agent ecosystems and advanced human-machine teaming can give the U.S. a decisive cognitive advantage in high-speed operations. Brain-computer interfaces (BCIs) offer a path to preserve human judgment amid accelerating machine decision cycles—critical for maintaining ethical and legal control over autonomous systems.

2. Computing the Future: Quantum computing is emerging as a strategic disruptor. Quantum-AI convergence will unlock exponential improvements in intelligence fusion, threat detection, and mission planning. Edge AI platforms will ensure mission continuity in degraded or

denied environments. Digital twins and predictive maintenance will transform sustainment and readiness strategies across the force.

3. Reengineering Defense Acquisition: U.S. defense acquisition must evolve to meet the pace of algorithmic warfare. Expanding flexible acquisition pathways (e.g., OTAs, PIAs), launching a dedicated AI acquisition track, and incentivizing non-traditional industry partnerships are essential to unlocking innovation. These reforms must be paired with investments in digital engineering and workforce reskilling to institutionalize adaptability.

4. International Competition and Cooperation: AI and quantum are becoming central battlegrounds in the U.S.-China rivalry. China's authoritarian AI model and quantum advances threaten to outflank U.S. capabilities if left unchecked. In response, democratic allies must deepen interoperability, co-develop ethical standards, and align strategic investments through platforms like AUKUS and NATO. These coalitions will be vital in shaping responsible AI use and countering autocratic norms.

This paper calls for a wartime-level innovation surge: a national mobilization to integrate AI and quantum capabilities into U.S. military doctrine, infrastructure, and alliances. Strategic leadership will require public-private partnerships, secure and scalable energy and data systems, updated IP and export controls, and a concerted international effort to promote democratic values in algorithmic warfare. The nation that leads in quantum-AI integration will not only win future conflicts—it will define the rules of global order in the 21st century.

1.0 INTRODUCTION

> *"Victory smiles upon those who anticipate the change in the character of war, not upon those who wait to adapt after the changes occur."*
> – Early airpower theorist Giulio Douhet

Imagine a scenario where shipping containers arriving at U.S. ports on the West and East Coasts suddenly release swarms of Chinese drones, overwhelming critical infrastructure, disabling military systems, and targeting personnel. At the same time, hundreds of thousands of autonomous munitions are released from high-altitude balloons drifting across American skies, striking nuclear facilities and defense installations. Legacy air superiority platforms like the F-22 or the future Next Generation Air Dominance fighter were never designed to counter such an asymmetric, massed, and distributed threat. Perhaps more alarming, neither the U.S. military nor the American public is psychologically prepared for a battle fought on homeland soil.

This terrifying scenario is no longer confined to fiction. Fueled by artificial intelligence (AI), the accelerating convergence of autonomy, sensors, and decision support systems is reshaping the character of warfare more swiftly than any previous military revolution. Unlike past transformations that unfolded over decades, today's breakthroughs emerge in months, demanding immediate adaptation. While cultural and bureaucratic barriers matter, they pale in comparison to the unprecedented velocity at which this technology is evolving and the profound and unpredictable ways it will redefine how wars are fought.

As AI transforms warfare at unprecedented speed, the nation that can integrate AI-enabled capabilities across its military will gain decisive cognitive dominance. The window for U.S. leadership in military AI is rapidly closing. Seizing this moment requires wartime-level urgency, innovative public-private partnerships, and preservation of human judgment in critical decisions. Maintaining a technological edge demands focused investment in AI development,

rapid prototyping, and expanded use of agile acquisition authorities. The U.S. must build new collaboration models, establish a technical reserve corps, and reform intellectual property policies to close the gap between government and industry. America's future security will hinge not just on acquiring advanced AI but on transforming military institutions, doctrine, and culture to wield it more effectively than our adversaries.

The race for AI supremacy represents the most consequential technological competition in human history. This contest will determine not just military advantage but also the very structure of global order in the 21st century.[1] We are at a pivotal moment where the nation that most effectively weaponizes AI will gain decision dominance across all domains, reshaping the global balance of power. For the U.S., failing to secure a leading edge in this AI arms race would amount to strategic surrender, risking the erosion of the western-led international order by authoritarian rivals.

This paper explores how AI is reshaping the future of warfare and the implications for U.S. defense strategy. It argues that America's security will depend not only on technological superiority but on transforming its military culture, acquisition systems, and alliance structures to wield AI more effectively than its rivals.

2.0 STRATEGIC ENVIRONMENT

AI is accelerating the transformation of warfare, not incrementally, but exponentially. Within a few years, AI has evolved from narrow applications to complex agent ecosystems that can analyze, decide, and act with minimal human intervention. This shift is compressing the traditional Observe-Orient-Decide-Act (OODA) loop, forcing militaries to operate at machine speed and rethink the foundations of operational planning.

[1] Robert Work and Shawn Brimley, "20YY: Preparing for War in the Robotic Age," Center for a New American Security, January 2014, 20-22.

The influence of AI and autonomous systems is already evident on today's battlefields. In Ukraine, both sides have deployed drones for reconnaissance and strike missions, showcasing how precision capabilities have been democratized. Ukrainian forces, in particular, have used low-cost drones to conduct accurate, high impact strikes on Russian targets, imposing significant costs on a militarily superior adversary.[2]

Similarly, in Gaza, the Israel Defense Force employed systems like "Gospel" and "Lavender" to accelerate the targeting process by analyzing vast datasets and recommending targets with unprecedented speed.[3] Brigadier General Yossi Sariel observed in 2021, "The speed and complexity of modern warfare require decision-making at a pace and scale that exceed unaided human capability." These systems exemplify effective human-machine teaming, dramatically accelerating battlefield decision cycles while maintaining critical human oversight.[4]

These battlefield AI systems represent only the first wave of AI-enabled warfare. This is the beginning of a more profound technological revolution that extends from quantum computing systems to the tactical edge, fundamentally transforming how military forces process information, make decisions, and execute operations across all domains.

Our adversaries' approach to AI in warfare underscores the strategic importance of not just acquiring advanced technology but fully integrating it into new warfighting concepts. For example, rather than merely layering AI onto legacy systems, China is pursuing a wholesale shift toward cognitively driven operations, treating AI as a foundation for reshaping how the People's Liberation Army (PLA) fights. This reflects a broader trend: strategic advantage in the AI era

[2] "How AI Is Changing Warfare," *The Economist*, June 20, 2024, accessed August 17, 2024, https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare.
[3] Harry Davies, Bethan McKernan, and Dan Sabbagh, "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza," The Guardian, December 1, 2023, sec. World news, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.
[4] Yossi Sariel, *The Human-Machine Team: How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World* (Independently published, 2021).

will belong to nations that can align technological innovation with doctrinal adaptation and institutional agility. For the U.S., the challenge is not one of innovation capacity, but of speed, integration, and willingness to rethink conventional paradigms before an adversary capitalizes on them.

The fusion of AI, quantum computing, autonomous systems, and edge capabilities is not simply evolving warfare—it is driving a paradigm shift that renders traditional doctrine increasingly irrelevant. [5] In this new era of algorithmic warfare, cognitive speed and decision advantage eclipse conventional firepower, compressing decision cycles beyond human limits. The future battlefield will favor those who can process data, decide, and act at machine speed. [6]

3.0 U.S. ARTIFICIAL INTELLIGENCE POLICIES

3.1 Biden Administration's AI Policies (2023-2025)

President Biden's Executive Order 14110 seized the initiative with America's first comprehensive AI governance framework, compelling industry to disclose safety test results before deploying powerful systems. His administration mobilized the federal bureaucracy by installing chief AI officers and mandated aggressive "red-teaming" to expose critical AI vulnerabilities. Biden's final executive action—EO 14141— set the stage for U.S. AI infrastructure leadership by streamlining data center permitting and mandating the Department of Defense (DoD) and the Department of Energy (DoE) to build federal AI facilities by 2027.[7]

[5] Clay Allen, *The Quantum Leap to Superintelligence: When Machines Outthink Their Masters,* (Dwight D. Eisenhower School, 2025).
[6] Harry Davies, Bethan McKernan, and Dan Sabbagh, "The Gospel: How Israel Uses AI to Select Bombing Targets in Gaza," *The Guardian*, December 1, 2023, sec. World news, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.
[7] Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Federal Register 88, no. 199 (October 30, 2023): 75191-75225, accessed May 6, 2025, https://www.federalregister.gov/documents/2023/10/30/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

3.2 The Trump Administration's Bold AI Deregulation (2025-Present)

President Trump quickly dismantled Biden's regulatory approach, nullifying EO 14110 through Executive Order 14148 and branding it part of "unpopular, inflationary, illegal, and radical practices."[8] Within days, Trump issued Executive Order 14179, declaring "the policy of the United States is to sustain and enhance America's global AI dominance" through aggressive deregulation and unfettered market competition.[9] The White House dismissed Biden's framework as "unnecessarily burdensome requirements" that would "stifle private sector innovation and threaten American technological leadership."[10] Yet Trump strategically preserved EO 14141's emphasis on AI infrastructure development, recognizing its critical importance to national power projection.[11]

David Sacks—Trump's handpicked "AI and Crypto Czar"—now drives a comprehensive AI Action Plan to cement American leadership through market-driven innovation. The administration's new Energy Dominance Council is confronting AI's massive energy demands by mobilizing resources—from natural gas to small modular reactors—to ensure U.S. AI infrastructure outpaces global rivals.[12]

---

[8] Donald J. Trump, "Executive Order 14148: Revocation of Certain Executive Orders Concerning Federal Regulation," Federal Register 90, no. 18 (January 25, 2025): 4759-4761, accessed May 6, 2025, https://www.federalregister.gov/documents/2025/01/25/2025-01574/revocation-of-certain-executive-orders-concerning-federal-regulation.

[9] Donald J. Trump, "Executive Order 14179: Removing Barriers to American Leadership in Artificial Intelligence," The White House, January 23, 2025, accessed May 6, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

[10] White House Press Office, "Fact Sheet: President Donald J. Trump Takes Action to Enhance America's AI Leadership," The White House, January 24, 2025, accessed May 6, 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/.

[11] Michael E. Kenneally and Rachael K. Plymale, "January 2025 AI Developments — Transitioning to the Trump Administration," Inside Government Contracts (blog), February 12, 2025, accessed May 6, 2025, https://www.insidegovernmentcontracts.com/2025/02/january-2025-ai-developments-transitioning-to-the-trump-administration/.

[12] White House Press Office, "Energy Dominance Council: Meeting America's AI Infrastructure Challenge," The White House, February 28, 2025, accessed May 6, 2025, https://www.whitehouse.gov/briefings-statements/energy-dominance-council-meeting-americas-ai-infrastructure-challenge/.

4.0 STAKEHOLDER INTERESTS

The rapid advancement of AI has mobilized diverse stakeholders, each with distinct motivations, capabilities, and strategic priorities. From government agencies and defense institutions to tech firms, allies, and adversaries, these actors are shaping the trajectory of AI development and deployment in ways that will define the future of military and economic power.

U.S. Government: AI is viewed as vital to national security, economic strength, and global leadership. Agencies like the Defense Advanced Research Projects Agency (DARPA), National Science Foundation, DoE, and the Strategic Capital Office drive funding and policy to build critical infrastructure, scale chip manufacturing, and sustain America's technological edge.[13]

Department of Defense: The DoD sees AI as key to battlefield dominance and is pushing through institutional inertia to modernize. The Chief Digital and AI Office (CDAO) leads efforts while each service branch develops tailored AI capabilities to maintain operational superiority.[14]

U.S. Technology Sector: Private tech companies like OpenAI, Anthropic, and Google DeepMind are accelerating AI innovation, especially in generative models and autonomy. Their competitive edge comes from talent, computing power, and vast data, often outpacing government adoption cycles.[15]

[13] National Security Commission on Artificial Intelligence, "Final Report," March 1, 2021, accessed May 5, 2025, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.
[14] U.S. Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," February 12, 2019, accessed May 5, 2025, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
[15] PricewaterhouseCoopers, "Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise?," PwC Global, 2017, accessed May 5, 2025, https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.

Defense Industrial Base: Traditional defense firms are integrating AI into legacy systems and platforms, emphasizing digital twins, predictive maintenance, and system optimization. However, they often require acquisition reform to match commercial innovation speed.[16]

Allies and Partners: Allies and partners seek to enhance interoperability, uphold ethical standards, and maintain technological relevance through shared AI development. Their goals include strengthening collective defense, accelerating dual-use innovation, and shaping global norms around responsible AI use.

Competitor Nations: Strategic competitors view AI as a decisive tool for gaining economic dominance, controlling information, and shifting the global balance of power. Their interests center on using AI to modernize military forces, exploit asymmetries against technologically superior adversaries, and reduce reliance on foreign technologies. These actors often pursue state-directed AI development, integrating civil, commercial, and military capabilities to accelerate deployment and blunt the strategic advantages of rival nations.

5.0 MAJOR CHALLENGES

Amid rapid, commercially driven innovation, much of it globally available shortly after development, the U.S. defense procurement system remains too slow, fragmented, and bureaucratic to respond effectively. Today's acquisition timelines average 10 to 20 years from concept to fielding, four times longer than in the 1950s.[17] This antiquated and cumbersome process, originally designed to regulate government-industry relationships, now obstructs the

[16] U.S. Department of Defense, "National Defense Industrial Strategy Implementation Plan for FY2025," Office of the Under Secretary of Defense for Acquisition and Sustainment, June 15, 2024, accessed May 5, 2025, https://www.acq.osd.mil/asda/dpc/ndis-implementation-plan-fy2025.pdf.
[17] Roger F. Wicker, *Restoring Freedom's Forge: America's Innovation Unleashed* (Washington, DC: Office of Senator Roger F. Wicker, 2024).

U.S. from effectively adopting cutting-edge technologies and threatens its ability to compete in the AI era.[18]

5.1 Cultural Resistance to Military Transformation

Despite a strong innovation ecosystem, deep-seated cultural resistance within the U.S. military threatens to undermine national security. It must be addressed to preserve strategic advantage in an era of accelerating global competition. History shows that technological breakthroughs alone are not enough. Successful military transformation demands both disruptive visionaries and institutional leaders willing to champion change from within.

A century ago, Brigadier General Billy Mitchell confronted similar resistance when advocating for airpower. After World War I, Mitchell recognized that aircraft would render battleships vulnerable and fundamentally alter the character of naval warfare. His demonstration in 1921—successfully sinking decommissioned battleships with bombers—should have forced a doctrinal reckoning. [19] He embodied the quintessential military disruptor, challenging entrenched doctrine and forcing recognition of emerging threats. Instead, entrenched naval leadership dismissed the tests, clung to battleship dominance, and marginalized Mitchell, who was ultimately court-martialed for his outspoken criticism of military leadership. [20]

While Mitchell pushed from the outside, Franklin D. Roosevelt played the equally vital role of an enabler from within. As Assistant Secretary of the Navy, he rejected calls to create a

[18] RAND Corporation, *Improving Defense Acquisition: Insights from Three Decades of RAND Research* (Santa Monica, CA: RAND Corporation, 2022); Jeffrey "Shady" LaFleur (Director of the Senior Acquisition Course and Professor of Innovation and Entrepreneurship in Defense Acquisition, Eisenhower School, National Defense University; former Air Force acquisition professional with extensive experience at SOCOM and the Rapid Capability Office), interview by author, May 1, 2025.

[19]Thomas Wildenberg, "Billy Mitchell Takes on the Navy," Naval History Magazine 27, no. 5 (September 2013), U.S. Naval Institute, https://www.usni.org/magazines/naval-history-magazine/2013/september/billy-mitchell-takes-navy.

[20] Thomas Wildenberg, "Billy Mitchell Takes on the Navy," Naval History Magazine 27, no. 5 (September 2013), U.S. Naval Institute, https://www.usni.org/magazines/naval-history-magazine/2013/september/billy-mitchell-takes-navy.

separate air force, instead insisting that naval aviation be developed as an integrated component of the fleet. His support helped institutionalize airpower within the Navy, enabling the United States to rapidly adapt and leverage carrier aviation in World War II, just in time to shift the tide in the Pacific. [21] [22]

This historical case demonstrates a critical lesson: revolutionary military technologies require both visionary disruptors like Mitchell, who challenge institutional thinking, and insightful organizational leaders like Roosevelt, who channel disruptive innovation in ways that strengthen rather than fracture military capabilities.

As we face our own technological revolution, we need both the disruptive vision of today's "Mitchells" and the judicious leadership of modern "Roosevelts" to integrate revolutionary capabilities while preserving core institutional strengths. The most successful military transformations occur not when disruptors work alone, but when organizational leaders recognize disruptive potential and create structures to nurture and integrate those capabilities within existing institutions, navigating between resistance to necessary change and wholesale restructuring that might discard valuable organizational expertise.

5.2 Technical and Operational Challenges

Quantum-AI Security Vulnerabilities: The convergence of quantum computing and AI introduces powerful capabilities but also serious risks. Existing cryptographic systems may be rendered obsolete, while adversaries could exploit AI-specific vulnerabilities through data

[21] Jeffery S. Underwood, "The Wings of Democracy: The Influence of Air Power on the Roosevelt Administration, 1933-1941" (1991), 11.
[22] Thomas Wildenberg, "Billy Mitchell Takes on the Navy," Naval History Magazine 27, no. 5 (September 2013), U.S. Naval Institute, https://www.usni.org/magazines/naval-history-magazine/2013/september/billy-mitchell-takes-navy.

poisoning, adversarial attacks, or system manipulation. Ensuring resilience will require rapid adoption of quantum-safe encryption and hardened AI architectures.[23]

Edge Computing in Contested Environments: AI systems must operate reliably in degraded, denied, or disconnected conditions, yet most current platforms depend on connectivity to centralized infrastructure. Building edge-capable systems that can sense, decide, and act independently in hostile environments is essential for maintaining decision advantage.[24]

Tactical Edge Revolution: Non-traditional firms are pioneering operational edge capabilities, but scaling these solutions across the force remains challenging. Platforms like Anduril's Lattice and Shield AI's autonomous aircraft demonstrate what's possible, but integration with legacy systems, doctrine, and acquisition processes lags behind.[25] [26]

Acquisition Bottlenecks: The current acquisition system cannot keep pace with AI innovation. Federal Acquisition Regulations (FAR) impose timelines and oversight mechanisms that are incompatible with rapid prototyping and fielding. Flexible pathways like OTAs and partnership intermediaries have shown promise but remain underutilized.[27] [28]

---

[23] National Security Agency and National Institute of Standards and Technology, "Post-Quantum Cryptography Transition Strategy," Joint Publication, March 15, 2024, accessed May 5, 2025, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3612875/nsa-releases-post-quantum-algorithms-for-national-security-systems/.

[24] Edge Industry Review, "Tactical Edge Cloud Computing: Enhancing Military Battlefield Efficiency," Special Report, October 18, 2023, accessed May 5, 2025, https://edgeindustryreview.com/reports/tactical-edge-cloud-computing-enhancing-military-battlefield-efficiency/.

[25] Anduril Industries, "Lattice: Operating at the Edge in Denied Environments," Technical Brief, March 2025, accessed May 5, 2025, https://www.anduril.com/technologies/lattice-edge-computing/.

[26] Shield AI, "V-BAT Autonomous Operations in GPS-Denied Environments," Shield AI Blog, January 15, 2025, accessed May 5, 2025, https://shield.ai/blog/autonomous-operations-gps-denied/.

[27] Executive Office of the President, "Restoring Common Sense to Federal Procurement," Federal Register 90, no. 81 (April 15, 2025): 23674-23689, accessed May 5, 2025, https://www.federalregister.gov/documents/2025/04/15/2025-08215/restoring-common-sense-to-federal-procurement.

[28] Technology Advancement Center, "About TAC: Accelerating Innovation for National Security," Organizational Overview, April 29, 2025, accessed May 5, 2025, https://thetac.tech/.

Human-Machine Teaming: As autonomy accelerates decision cycles, maintaining meaningful human oversight becomes more difficult. New approaches are needed to ensure that commanders remain in control, whether through intuitive interfaces, doctrinal shifts, or emerging technologies like BCI.[29]

Energy Requirements: The AI arms race is driving unprecedented energy demand. Training a single advanced AI model can consume more electricity than some small towns use in a month.[30] This surge strains the national power infrastructure and creates a critical vulnerability. Without reliable and scalable power, America's most advanced AI capabilities could fail at decisive moments. Meeting this demand requires not just more capacity, but innovation in energy delivery, cooling, and distributed systems.[31]

Cost Imposition Strategies: AI lowers the barriers to high-impact capabilities, enabling adversaries to deploy low-cost, attritable systems that can impose outsized costs on U.S. forces. To respond, the U.S. must shift from exquisite platforms to distributed, scalable systems designed for mass and resilience.[32]

Ethical AI Governance: Rapid deployment of autonomous capabilities raises urgent questions about accountability, proportionality, and compliance with the law of armed conflict. Embedding ethical constraints at the design and deployment stages—not just in policy—will be essential to preserve legitimacy and effectiveness.

---

[29] Defense Advanced Research Projects Agency, "Six Paths to the Nonsurgical Future of Brain-Machine Interfaces," DARPA News and Events, May 20, 2019, accessed May 5, 2025, https://www.darpa.mil/news-events/2019-05-20.
[30] Department of Energy, "Executive Order 14141: Advancing United States Leadership in Artificial Intelligence Infrastructure," Association for the Advancement of Business AI, January 19, 2025, accessed May 6, 2025, https://www.aab-ai.org/2025/01/19/latest-eo-on-ai/.
[31] U.S. Department of Energy, "Strategic Framework for AI Infrastructure Development," DOE Office of Science, March 15, 2025, accessed May 6, 2025, https://www.energy.gov/science/articles/strategic-framework-ai-infrastructure-development,.
[32] William Roper, "Attritable Systems: Redefining Platform Economics for Great Power Competition," Defense Advanced Systems Journal 15, no. 2 (March 2025): 45-67, accessed May 5, 2025, https://www.defensesystemsjournal.org/articles/attritable-systems-redefining-platform-economics/.

Systematic IP Theft by China: China's industrial-scale intellectual property theft continues to erode the U.S. innovation edge. Military-civil fusion policies turn stolen commercial technology into military capability, accelerating PLA modernization while undermining U.S. firms and allies.

6.0 PROBLEM STATEMENT

The American military technological edge, the cornerstone of its global influence, erodes at an alarming speed as peer competitors, particularly China, pursue comprehensive national strategies to achieve AI dominance. The PLA, guided by Beijing's civil-military fusion doctrine and fueled by systematic intellectual property theft, is rapidly developing "intelligentized warfare" capabilities designed specifically to neutralize American conventional advantages.[33] While the U.S. maintains significant innovation capacity, its fragmented approach to AI development, bureaucratic acquisition processes, and cultural resistance to change, threatens to squander this increasingly tenuous lead.[34]

The DoD faces an existential challenge: how to rapidly integrate AI capabilities across all military domains while maintaining human oversight, ethical boundaries, and allied interoperability. This integration must occur within a fractured acquisition environment unsuited to the pace of technological change, hampered by outdated security protocols, and constrained by traditional requirements-based procurement models.[35] Simultaneously, quantum computing breakthroughs threaten to break existing cryptographic systems while enabling new forms of

[33] Commission on the Theft of American IP, *Update to the IP Commission Report* (Seattle: National Bureau of Asian Research, February 2017), 1; Scott Tosi, "Steal the Firewood from Under the Pot: The Role of IP Theft in Chinese Global Strategy," *Military Review* 100, no. 5 (September-October 2020): 96.
[34] Executive Office of the President, *Restoring Common Sense to Federal Procurement* (Washington, D.C.: April 2025), https://www.whitehouse.gov/presidential-actions/2025/04/restoring-common-sense-to-federal-procurement/.
[35] Stan Soloway, "The President's Procurement Order Offers a Real Opportunity. Let's Not Squander It," *Nextgov*, April 17, 2025, https://www.nextgov.com/ideas/2025/04/presidents-procurement-order-offers-real-opportunity-lets-not-squander-it/404645/.

cyber warfare,[36] while military operations increasingly require edge computing that can operate in contested environments with degraded or denied communications.[37] The window for establishing U.S. leadership in military AI is rapidly closing. Meeting this moment requires wartime-level mobilization of America's full innovation ecosystem before rivals with opposing values seize the technological advantage and reshape the global order.[38]

Seizing the initiative requires a coordinated response across four interdependent fronts. First, the U.S. must establish cognitive dominance through AI agent ecosystems and advanced human-machine teaming (Line of Effort (LOE) 1). Second, it must invest in quantum computing, edge AI, and digital sustainment to ensure computational superiority at every echelon of conflict (LOE 2). Third, the defense acquisition system must be reengineered to field AI-enabled capabilities at speed and scale, unlocking innovation from across the commercial sector (LOE 3). And finally, the U.S. must lead in shaping international AI norms and alliances to counter authoritarian models and ensure strategic advantage through collective AI-enabled deterrence (LOE 4). Together, these lines of effort constitute a wartime-level innovation surge essential to preserving U.S. military leadership in the AI era.

7.0 LOE 1: COGNATIVE DOMINANCE: AGENT ECOSYSTEMS AND HUMAN-MACHINE TEAMING

Emerging AI technologies promise unprecedented cognitive speed and operational adaptability, redefining how militaries sense, decide, and act across all domains. This section

[36] NSA and NIST, "Post-Quantum Cryptography Transition Strategy," 2024.
[37] Edge Industry Review, "Tactical edge cloud computing: Enhancing military battlefield efficiency," October 18, 2023.
[38] Department of Defense, *National Defense Industrial Strategy Implementation Plan for FY2025* (Washington, DC: Office of Prepublication and Security Review, June 2024).

explores how agent-based architectures and neurotechnology can serve as cognitive force multipliers and strategic enablers on the future battlefield.

7.1 The Evolution of Military AI: From Algorithms to Agent Ecosystems

The evolution of military AI has progressed from algorithms to models and now to agent ecosystems. AI agents distinguish themselves through four key characteristics: autonomy, goal-directedness, tool use, and planning.[39] Unlike traditional AI systems that passively process inputs to generate outputs, agents operate autonomously with minimal supervision, pursue defined goals, coordinate with external tools and AI systems, and develop multi-step strategies to dynamic environments.

An effective military agent ecosystem requires a coherent architecture that supports cross-domain integration while addressing domain-specific requirements. The proposed architecture organizes agents into five primary categories designed for interoperability:

1. **Intelligence-gathering agents** function as the sensory system for military operations, collecting, analyzing, and processing information from multiple sources. These include signals intelligence agents monitoring communications, imagery agents processing visual data, open-source agents synthesizing public information, and fusion agents integrating data across streams.
2. **Decision-support agents** enhance human decision-making by generating options, evaluating courses of action, and identifying potential outcomes. This includes planning agents that develop operational approaches, wargaming agents that simulate potential scenarios, risk assessment agents that identify vulnerabilities, and recommendation agents that propose optimal solutions to commanders.

[39] Stuart Russell and Peter Norvig, "Artificial Intelligence: A Modern Approach," 4th ed. (Hoboken, NJ: Pearson, 2021), 34-56.

3. **Logistics and resource management agents** streamline sustainment by optimizing supply chains, predicting maintenance needs, coordinating transportation routes, and managing energy use within operational constraints.[40]
4. **Cyber-defense agents** protect military networks and systems from sophisticated attacks. Detection agents identify anomalies, response agents neutralize attacks, deception agents deploy honeypots and decoys, and attribution agents trace threat actors.[41]
5. **Training and simulation agents** enhance readiness through personalized instruction and realistic scenarios. Tutoring agents adapt instruction to individual needs, scenario generators create mission-relevant environments, assessment agents track performance gaps, and red-team agents simulate adversary tactics.[42]

7.1.1 Strategic Value of Agent Ecosystems in Military Operations

Cognitive Force Multiplication: Agent ecosystems provide a powerful strategic advantage by serving as cognitive force multipliers. While traditional force multiplication emphasizes enhancing physical capabilities through technology or tactics, AI agents expand cognitive capabilities, enabling personnel to process more data, assess more options, and control more assets than otherwise possible.[43] This multiplication effect is particularly valuable in information-dense environments, where human cognitive limitations become operational constraints. They can help the commander cut through the fog of war and enhance his

[40] Scott Tosi, "Steal the Firewood from Under the Pot: The Role of IP Theft in Chinese Global Strategy," *Military Review* 100, no. 5 (September–October 2020): 96, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-20/Tosi-Intellectual-Property-Theft-1.pdf
[41] Glenn Chafetz, "How China's Political System Discourages Innovation and Encourages IP Theft," *SAIS Review of International Affairs*, July 31, 2023, https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/.
[42] Reuters. "Russia's Sberbank Plans Joint AI Research with China as DeepSeek Leaps Forward." *Reuters*, February 6, 2025, accessed May 12, 2025, https://www.reuters.com/technology/artificial-intelligence/russias-sberbank-plans-joint-ai-research-with-china-deepseek-leaps-forward-2025-02-06/.
[43] Christy Lee, "Russia Turns to China to Step up AI Race against U.S.," Voice of America, January 9, 2025, https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html.

Clausewitzian inner eye. By augmenting human intelligence with agent ecosystems, commanders can effectively operate across multiple domains simultaneously, maintaining situational awareness and decision advantage against numerically superior forces.

Decision Speed and Quality: Agent ecosystems accelerate and enhance military decision-making by processing and synthesizing diverse data streams at machine speed, reducing the loop.[44] They rapidly generate, assess, and recommend multiple courses of action, often identifying options human planners might overlook. Studies show that human-agent teams consistently outperform humans or AI alone in complex decision environments.[45] The ideal model for military decision-making pairs agents' data-driven analysis with human strategic insight and ethical judgment.

Data Processing and Adaptive Response: Agent ecosystems excel at processing diverse data streams, extracting relevant patterns, and presenting actionable intelligence to human operators. Unlike conventional analytics tools, agents can autonomously filter noise, extract key patterns, and present relevant intelligence aligned with operational goals without needing explicit instructions for every situation.[46]

This ability to prioritize and adapt in real-time makes them especially valuable in fast-changing, contested environments. As adversaries seek to disrupt command and control, agent ecosystems offer a resilient edge by being able to reconfigure dynamically to sustain decision advantage.

[44] Robert Work and Shawn Brimley, "20YY: Preparing for War in the Robotic Age," Center for a New American Security, January 2014, 20-22.
[45] Mary L. Cummings et al., "Human-Agent Teaming Performance in Military Decision Tasks," "Military Psychology" 34, no. 6 (2023): 522-538.
[46] David Danks and Alex John London, "Algorithmic Bias in Autonomous Systems," "Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence" (2022): 4691-4697.

7.2 Maintaining Human Control: Brain-Computer Interfaces and the Human-Machine Team

As military platforms grow more autonomous and operate at machine speed, brain-computer interfaces (BCI) offer a critical means to preserve human control and decision-making superiority. An advanced BCI removes the physical intermediary between mind and machine, enabling system control at the speed of thought. In a contested environment, this essential link could fundamentally transform military command and control (C2), allowing warfighters to direct unmanned vehicles, initiate cyber operations, and manage battlefield communications without the bottleneck of conventional controls and displays. DARPA emphasizes future conflicts will unfold too fast "for humans to manage effectively with current technology," and BCIs offer a path to keeping commanders meaningfully engaged.[47]

While the U.S. currently leads in BCI research, China is aggressively pursuing its own programs, integrating disruptive neurotechnology into its Military-Civil Fusion strategy for both human enhancement and military applications, including neurocognitive warfare.[48] Unlike U.S. efforts, which are fragmented and constrained by regulatory, ethical, and sociocultural barriers, China's state-directed approach provides a clearer articulation of dual-use intent and accelerates both development and fielding.[49] The China Brain Project explicitly emphasizes brain-machine technologies for military and civilian use, aligning closely with the PLA vision of human-machine hybrid intelligence. This competition has critical strategic implications: the nation that

[47] **"**Six Paths to the Nonsurgical Future of Brain-Machine Interfaces," DARPA, May 20, 2019, https://www.darpa.mil/news/2019/nonsurgical-brain-machine-interfaces.
[48] Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington DC, 2024), 27, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/military-and-security-developments-involving-the-peoples-republic-of-china-2024.pdf.
[49] Joy Putney, "Neurotechnology for National Defense: the U.S. and China," The Cipher Brief, July 1, 2021, https://www.thecipherbrief.com/column_article/neurotechnology-for-national-defense-the-u-s-and-china.

matures BCI technology first may gain a decisive OODA-loop advantage to outpace adversaries and seize the initiative in high-speed, multidomain operations.

As this technological revolution transforms warfare at unprecedented speed, the nation that most effectively integrates AI agent ecosystems into its military will gain decisive cognitive advantage across all domains, from intelligence gathering to battlefield operations. The window for establishing leadership in military AI is rapidly closing, demanding a wartime-like mobilization that bridges the government-tech divide through innovative partnership models while preserving human judgment in consequential decisions. America's future security and global influence depend not merely on possessing advanced AI capabilities, but on our ability to adapt our military institutions, doctrine, and culture to harness this transformative technology before our adversaries do.

8.0 LOE 2: COMPUTING THE FUTURE: QUANTUM, EDGE AI, AND DIGITAL SUSTAINMENT

Next generation computing capabilities, from quantum systems to edge AI and digital twins, have the potential to redefine the technical foundation of military power. These technologies promise to enhance speed, precision, and resilience across decision-making, logistics, cybersecurity, and maintenance. This section examines how quantum computing could revolutionize information processing, why edge platforms are essential for contested environments, and how AI-enabled digital twins are transforming sustainment and readiness.

8.1 The Potential of Quantum Computing

The convergence of quantum computing and AI marks a transformative shift in national security. With the ability to process information at unprecedented scales, quantum computing unlocks a new era of AI capabilities with profound implications for military decision-making,

cybersecurity, logistics, and intelligence. Recent milestones, such as International Business Machine's (IBM) 1,000-qubit systems and Google's quantum supremacy experiments, demonstrate tangible progress toward scalable quantum systems.[50]

Quantum computing leverages qubits' superposition and entanglement properties to process information exponentially faster than classical computers. When applied to AI, this creates several critical accelerations:

- **Quantum Parallelism** allows AI to simultaneously evaluate vast solution spaces, enabling faster optimization of logistics, mission planning, and adversary strategies.
- **Quantum Machine Learning (QML)** architectures, such as quantum neural networks, can recognize complex patterns invisible to classical systems, enhancing surveillance, threat detection, and strategic forecasting.[51]
- **Recursive AI Enhancement** raises the prospect of rapid self-improvement cycles, potentially outpacing human cognitive capacity.[52] For example, research suggests a 10,000-logical-qubit system could synthesize centuries of scientific advancement in hours.[53]

These accelerations compress operational timelines, potentially creating both opportunities for strategic surprise and risks of catastrophic failures.

Quantum-enhanced AI offers decisive advantages across several key domains. In cybersecurity and cryptography, quantum computers could break current encryption standards while enabling superior cyber defense through enhanced anomaly detection. The National

[50]Clay Allen, *The Quantum Leap to Superintelligence: When Machines Outthink Their Masters,* (Dwight D. Eisenhower School, 2025).
[51]Fiona Saunders, Quantum AI in Military Decision-Making -- Strategic Considerations for National Security (Dwight D. Eisenhower School, 2025).
[52] Future of Life Institute, "Policy Recommendations for Managing Existential Risks from Quantum AI," 2025.
[53] Clay Allen, *The Quantum Leap to Superintelligence: When Machines Outthink Their Masters,* (Dwight D. Eisenhower School, 2025).

Security Agency and National Institute of Standards and Technology's efforts to develop quantum-resistant cryptography are vital to future-proofing secure communications.[54] In intelligence analysis, quantum AI enables real-time fusion of vast intelligence inputs, improving target identification, predictive analysis, and deception detection. DARPA's Quantum Computing Applications for National Security exemplifies U.S. efforts to harness quantum capabilities for intelligence dominance.[55] For logistics, quantum algorithms can dynamically optimize resource allocation, forecast equipment failures, and streamline supply chains, enhancing resilience and efficiency.[56]

Looking ahead, quantum-enhanced AI could power future autonomous systems capable of adapting in real time and operating effectively under degraded or denied conditions, fundamentally reshaping the character of warfare.

8.2 The Edge Computing Imperative for Military Operations

While quantum computing holds long-term potential, today's operational demands require reliable computing at the tactical edge, especially in contested environments where connectivity is limited or denied. Edge computing, which processes data near the source rather than relying on centralized clouds, has become a critical enabler for advanced military capabilities.[57] For military operations, where connectivity, latency, and security are paramount, edge AI enables capabilities such as autonomous navigation and real-time threat detection in degraded conditions.[58] This transforms distributed operations by enabling autonomous decision-making when command links are disrupted.

---

[54] NSA and NIST, "Post-Quantum Cryptography Transition Strategy," 2024.
[55] DARPA, "Quantum Computing Applications for National Security," 2024.
[56] Ernst & Young, "Quantum Logistics Optimization for Defense," 2024.
[57] Clay Allen, *The Quantum Leap to Superintelligence: When Machines Outthink Their Masters* (Dwight D. Eisenhower School, 2025).
[58] Edge Industry Review, "Tactical edge cloud computing: Enhancing military battlefield efficiency," (October 18, 2023).

8.2.1 Service-Specific Applications of Edge AI

Each service has adopted edge AI to address domain-specific challenges:

- **Army:** Project Convergence demonstrates the integration of edge AI into land warfare operations, enabling autonomous target recognition and battlefield coordination among dispersed units operating with degraded communications. These systems utilize ruggedized computing platforms capable of running complex AI algorithms without requiring continuous network connectivity.[59]
- **Navy:** The Unmanned Campaign Framework emphasizes autonomous maritime systems operating in contested environments where remote control is impossible. Edge computing enables unmanned surface and underwater vessels to maintain situational awareness and mission effectiveness despite communications interference.[60]
- **Air Force:** The Autonomous Collaborative Platforms program requires edge AI for coordinated unmanned aerial vehicle operations beyond human control timelines. These platforms must process sensor data and make tactical decisions locally when communications with command centers are compromised.[61]

8.2.2 Unique Military Requirements for Edge Computing

Unlike commercial applications, military edge AI must meet strict operational requirements:

[59] DefenseMagazine.com, "Project Convergence Capstone 5: Shaping the Future of Warfare," Defense Magazine, March 15, 2025, https://www.defensemagazine.com/article/project-convergence-capstone-5-shaping-the-future-of-warfare.
[60] Seapower Staff, "Navy, Marine Corps Release Unmanned Campaign Plan," Seapower (blog), March 16, 2021, https://seapowermagazine.org/navy-marine-corps-release-unmanned-campaign-plan/.
[61] "Autonomy, Collaboration, and Experimentation," Air & Space Forces Magazine, accessed April 21, 2025, https://www.airandspaceforces.com/article/autonomy-collaboration-and-experimentation/.

1. **Resilience in denied, degraded, intermittent, and limited environments:** Military edge platforms must operate reliably despite electronic warfare and communications disruption. Companies including Shield AI are pioneering systems with these capabilities, developing systems like its V-BAT unmanned aerial vehicle.
2. **Security against adversarial attacks:** Edge AI systems must resist physical and cyber compromise attempts targeting their algorithms and hardware.
3. **Joint interoperability:** Standardized interfaces and protocols are essential for integration across services and coalition partners.
4. **Low SWaP profiles:** Edge hardware must be compact and energy-efficient to suit forward-deployed platforms.

8.2.3 Operationalizing Cybersecurity for Edge AI

Effective integration of AI cybersecurity requires securing the entire stack from tactical edge devices to enterprise-level defense networks.

1. **Tactical integration:** Edge systems must incorporate lightweight AI models for real-time threat detection and autonomous patching, particularly in contested communications environments.
2. **Strategic integration:** Centralized defense networks should leverage AI for continuous monitoring, automated threat detection, and rapid incident response and recovery.

Programs like the Joint Artificial Intelligence Center's Cyber Autonomy Security Initiative highlight both the promise and current limitations of scaling AI across operational networks.

Barriers such as organizational resistance, data silos, and inflexible acquisition pathways hinder broad adoption.[62]

As operational demands evolve, maintaining technological superiority in edge AI platforms will require synchronization between defense requirements and commercial innovation cycles. The path to enduring advantage lies not in developing the most advanced algorithms in isolation but in creating integrated operational platforms that function effectively in the challenging environments that characterize modern warfare.

8.3 Digital Twins and Predictive Maintenance

One of the most strategically consequential applications of AI is in the long-term sustainment of defense acquisition platforms. In an era where readiness and responsiveness are paramount, predictive maintenance powered by AI is not merely a cost-saving measure but a strategic capability. Conventional maintenance models rely on time-based schedules or reactive repairs.[63] These approaches, while serviceable in peacetime, cannot keep pace with the demands of high-tempo operations, contested logistics, or aging platforms under strain.

The DoD has been investing heavily in the digital twin domain. The Air Force has implemented Condition Based Maintenance Plus programs—developed in partnership with C3.ai—that incorporate AI models analyzing flight hours, vibration signatures, temperature trends, and maintenance logs to predict the health of key systems.[64]

---

[62] Mark Pomerleau, "Pentagon AI Team Sets Sights on Information Warfare," C4ISRNet, July 22, 2020, https://www.c4isrnet.com/smr/information-warfare/2020/07/22/pentagon-ai-team-sets-sights-on-information-warfare/.

[63] Booz Allen Hamilton, "Artificial Intelligence for Predictive Maintenance," accessed April 19, 2025, https://www.boozallen.com/markets/defense/indo-pacific/artificial-intelligence-for-predictive-maintenance.html.

[64] U.S. Air Force Materiel Command, "Rapid Sustainment Office's Condition-Based Maintenance Plus, Artificial Intelligence Program Boosts Aircraft Readiness," *Air Force Materiel Command News*, May 3, 2023, https://www.afmc.af.mil/News/Article-Display/Article/3382942/rapid-sustainment-offices-condition-based-maintenance-plus-artificial-intellige.

Digital twins—virtual replicas of physical systems that evolve with real-time data—further expand the utility of AI in acquisition lifecycle management. These models are capable of simulating stress conditions, operational wear, and sustainment needs across an entire platform's lifespan. Booz Allen Hamilton has supported the construction of the DoD's largest-ever digital twin, enabling continuous monitoring and real-time insights into complex infrastructure and weapon systems.[65]

9.0 LOE 3: REENGINEERING DEFENSE ACQUISITION FOR THE AI ERA

The pace of AI innovation has exposed critical shortcomings in the DoD's legacy acquisition system, particularly its rigidity, complexity, and inability to adapt at machine speed. To meet the demands of algorithmic warfare, the DoD must modernize how it acquires both AI-enabled tools and the infrastructure that supports them. Recognizing the urgency for reform, the White House recently issued an executive order aimed at restoring "common sense" in federal procurement, calling for acquisition practices that are faster, more adaptable, and innovation driven.[66] This requires embracing flexible acquisition pathways, integrating AI into procurement and sustainment workflows, and expanding partnerships beyond the traditional defense industrial base. At stake is the ability to compete in a strategic environment where advantage depends not just on what the U.S. can build, but how fast it can field it.

9.1 Modernizing Acquisition Pathways for Defense AI Integration

Flexible mechanisms such as Other Transaction Authorities (OTA) and Partnership Intermediary Agreements (PIA) provide alternatives to the traditional Federal Acquisition

[65] Booz Allen Hamilton, "Building DoD's Largest-Ever Digital Twin of Its Kind," accessed April 19, 2025, https://www.boozallen.com/insights/digital-twin/building-dods-largest-ever-digital-twin-of-its-kind.html.
[66] Executive Office of the President, *Restoring Common Sense to Federal Procurement* (Washington, D.C.: April 2025), https://www.whitehouse.gov/presidential-actions/2025/04/restoring-common-sense-to-federal-procurement/.

Regulations (FAR) based model. These pathways can speed delivery, expand competition, and lower barriers for non-traditional vendors, helping the DoD regain tempo and agility in the face of peer competition. These tools provide legal and structural flexibility to work with non-traditional firms, academic institutions, and consortia in ways that traditional procurement vehicles cannot.[67] By streamlining oversight and tailoring terms to mission outcomes rather than bureaucratic compliance, OTAs and PIAs support faster prototyping and iterative development cycles.[68]

OTAs allow federal agencies to conduct research and develop prototypes outside standard procurement rules that govern FAR-based contracts. The National Security Agency has used OTAs to acquire AI-enabled language translation and machine learning tools from non-traditional providers with specialized technical expertise and rapid innovation cycles, capabilities often missing in the legacy defense industrial base.[69]

Beyond speed, OTAs also foster co-development environments that bring together mission owners, technical experts, and vendors to collaborate directly. The CDAO, for instance, recently awarded Scale AI an OTA to deliver advanced data curation and annotation tools through the Tradewinds Solutions Marketplace. The agreement was finalized in under three weeks, an unprecedented pace in the defense contracting world.[70]

While OTAs remove barriers to entry, PIAs expand the aperture of discovery. PIAs allow designated intermediaries—often nonprofit organizations or state-chartered entities—to connect

[67] Nick Wakeman, "Lines Blur Between Traditional and Non-Traditional Players," *Washington Technology*, January 15, 2020, https://www.washingtontechnology.com/2020/01/lines-blur-between-traditional-and-non-traditional-players/354595/.
[68] Justin Doubleday, "Intel Agencies See 'Appealing' Use Cases for OTAs," Federal News Network, March 13, 2023, https://federalnewsnetwork.com/contracting/2023/03/intel-agencies-see-appealing-use-cases-for-otas/.
[69] Justin Doubleday, "Intel Agencies See 'Appealing' Use Cases for OTAs," Federal News Network, March 13, 2023, https://federalnewsnetwork.com/contracting/2023/03/intel-agencies-see-appealing-use-cases-for-otas/.
[70] "Scale AI Awarded a New OTA by the Department of Defense," *Tradewinds AI*, accessed April 29, 2025, https://www.tradewindai.com/blog/scale-ai-awarded-a-new-ota-by-the-department-of-defense.

federal agencies with the innovation ecosystem.[71] This enables faster engagement, reduced costs, and quicker transition of emerging technologies into operational use. U.S. Special Operations Command has led the way through its SOFWERX platform—a designated partnership intermediary—executing hundreds of collaborative events, assessments, and prototype transitions. SOFWERX has facilitated over $180 million in contracts, transitioning nearly half of its Small Business Innovation Research Phase II projects into advanced development or acquisition programs.[72]

Other organizations, such as the Technology Advancement Center (TAC), are extending this model across the federal landscape. As a nonprofit intermediary, TAC partners with small businesses and academic researchers to surface dual-use technologies in areas like cybersecurity, security communications, AI, and other national defense challenges. With half of its ecosystem composed of small firms, TAC lowers the barriers to entry for innovative solutions and helps deliver operational capabilities to the field faster.[73]

9.2 AI-Driven Acquisition and Procurement Optimization

AI is transforming defense procurement by improving speed, accuracy, and decision-making throughout the acquisition lifecycle. AI tools now assist with contract evaluation, market research, vendor selection, and real-time data analysis, functions once limited by manual processes. For example, the DoD uses AcqBot, an AI-powered contract writing tool, to help contracting officers manage larger workloads more efficiently.[74] Similarly, the General Services

[71] "The Other Transactions & Partnership Intermediary Connection," Strategic Institute for Innovation in Government Contracting, August 30, 2022, https://strategicinstitute.org/other-transactions/ot-pia-connection/.
[72] USSOCOM, "SoftwareX Executive Info Brief," SOFWERX, January 10, 2024.
[73] Technology Advancement Center, "About TAC," accessed April 29, 2025, https://thetac.tech/.
[74] AcqBot, "AI Talking Points," accessed April 19, 2025, https://acqbot.com/blog/ai-talking-points.

Administration's Procurement Copilot uses natural language processing to interpret acquisition needs and suggest vendor and pricing options based on historical solicitations.[75]

AI is also being applied in decision-making for source selection. The U.S. Army is pursuing an AI-enabled source selection evaluation Software-as-a-Service tool that uses algorithms to quickly and objectively score proposals based on mission-specific criteria.[76] This supports faster decisions and greater agility, aligning with current federal modernization policies.[77] Meanwhile, in the private sector, companies like SAP offer AI procurement tools that are already being used to manage public-sector supply chains. These tools automate spending analysis, monitor supplier reliability, and flag anomalies before contracts are awarded.[78] By streamlining pre-award processes, they reduce the time and workload required to initiate programs, ultimately saving the government money.

Beyond procurement, AI is playing a growing role in acquisition planning and system design. Digital twins are increasingly used to simulate performance, forecast maintenance needs, and reduce lifecycle risk. According to Northrop Grumman's Brian Schmidt, digital twins are "vital for weapon systems, logistics, maintenance and readiness" throughout the DoD ecosystem.[79] The DoD has formally institutionalized this approach through directive 5000.97, which mandates digital engineering methodologies and practices across the entire lifecycle of

[75] U.S. General Services Administration, "Procurement CoPilot: Resources," *Acquisition Gateway*, accessed April 20, 2025, https://acquisitiongateway.gov/procurementcopilot/resources/33096.
[76] U.S. Army Small Business Innovation Research (SBIR), "AI-Enabled Source Selection Solution for Contract Proposal Evaluation," accessed April 19, 2025, https://www.armysbir.army.mil/topics/ai-enabled-source-selection-solution-for-contract-proposal-evaluation/.
[77] White House, *Fact Sheet: President Donald J. Trump Modernizes Defense Acquisitions and Spurs Innovation in the Defense Industrial Base*, April 2025, https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-president-donald-j-trump-modernizes-defense-acquisitions-and-spurs-innovation-in-the-defense-industrial-base/.
[78] SAP, "AI in Procurement," accessed August 18, 2024, https://www.sap.com/resources/ai-in-procurement.
[79] Joe O'Halloran, "Digital Twins Critical for Digital Transformation to Fly in Aerospace," *Computer Weekly*, April 28, 2025, https://www.computerweekly.com/news/366623100/Digital-twins-critical-for-digital-transformation-to-fly-in-aerospace.

defense acquisition programs.[80] This enables the government to reduce development risk, improve lifecycle cost forecasting, and accelerate fielding of more reliable systems.

Together, these AI-enabled tools reduce workload, shorten timelines, improve cost forecasting, and increase transparency and auditability, positioning the DoD to better match acquisition speed with technological change.

9.3 Opening the Aperture: Shaping the Future of the Defense AI Industry

As innovation in AI accelerates, the DoD's ability to modernize its acquisition strategy increasingly depends on deep, agile collaboration with the private sector. This means moving beyond the traditional defense industrial base to engage with dynamic technology firms, venture-backed startups, and non-traditional suppliers.[81] A broader view of the commercial AI landscape, including the competitive dynamics and barriers to entry, is provided in Appendix 1, which outlines a five forces and PESTLE analysis of the AI industry and profiles leading firms such as OpenAI, Anthropic, and Scale AI.

Non-traditional defense vendors, especially those working through OTA-enabled partnerships, are reshaping how the government acquires and fields technology. Software-native firms like Palantir exemplify this shift. Unlike legacy defense primes that focus on hardware-intensive systems with long development cycles, Palantir delivers modular, scalable software platforms optimized for national security missions. Operating on rapid product cycles and commercial cloud infrastructure, these companies offer AI tools that are both adaptable and deployable at speed.

[80] Joe O'Halloran, "Digital Twins Critical for Digital Transformation to Fly in Aerospace," *Computer Weekly*, April 28, 2025, https://www.computerweekly.com/news/366623100/Digital-twins-critical-for-digital-transformation-to-fly-in-aerospace.
[81] Executive Office of the President, *Restoring Common Sense to Federal Procurement*.

Palantir has become a key player in military analytics and sustainment planning by integrating intelligence, logistics, and procurement data into operational platforms.[82] These tools not only improve decision-making but also reduce manual workloads by automating data processing and accelerating insight generation.[83] This shift toward digital-first defense solutions reflects a broader momentum that challenges the traditional acquisition model and aligns with the evolving needs of modern warfare.[84]

9.4 AI in the Workforce and National Innovation

AI technologies are reshaping both public and private sectors, creating new opportunities while also posing significant workforce challenges. Research shows that AI tends to increase demand for high- and medium-skilled labor while potentially displacing workers in routine, lower-skilled roles.[85] According to McKinsey & Company, this transition will require "targeted re-skilling and upskilling," particularly for low-skilled workers. Even high-income professionals, such as writers, creatives, lawyers, and consultants, will need to adapt as generative AI transforms key aspects of their jobs .[86]

[82] Brian Deagon, "Palantir Stock: Defense Software Maker Builds Military AI Business," *Investor's Business Daily*, accessed April 20, 2025, https://www.investors.com/news/technology/palantir-stock-pltr-software-defense-military/.
[83] Liu, Florent. "Unlocking Enterprise Insights: How Palantir's AI Knowledge Database Transforms B2B Decision-Making," LinkedIn, February 28, 2025, https://www.linkedin.com/pulse/unlocking-enterprise-insights-how-palantirs-ai-knowledge-florent-liu-qku0e/.LinkedIn+2LinkedIn+2.
[84] Maria Deutscher, "Report: Palantir and Anduril Join Forces to Try and Secure U.S. Government Defense Contracts," *SiliconANGLE*, December 22, 2024, https://siliconangle.com/2024/12/22/report-palantir-anduril-join-forces-try-secure-u-s-government-defense-contracts/.
[85] "Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems", GAO. February 17, 2022. https://www.gao.gov/products/gao-22-104765.
[86] Department of Defense, *DoD Strategy and Implementation Plan for ICT and Services Supply Chain Risk Management Assurance* (Washington, DC: Office of Prepublication and Security Review, June 2024).

Leading companies are already responding. IBM has invested over $1 billion in since 2016, [87] and Amazon is transitioning employees into higher skill and higher demand positions.[88] The DoD is taking a similar approach upskilling its current workforce through comprehensive AI training, while simultaneously recruiting world-class AI talent to build future-ready capabilities.[89]

AI is also accelerating research and innovation. From rapid prototyping to high-speed digital simulation, AI tools enable breakthroughs across sectors. National laboratories use AI to analyze scientific data, evident in how "AI-powered systems identified potential COVID-19 treatments within days rather than the months or years traditional methods would require."[90] In healthcare and finance, AI helps researchers discover new drugs and predict efficacy, detect fraud, and improve risk management."[91]

Public-private partnerships are key to advancing this innovation. For example, Booz Allen Hamilton and Shield AI are partnering to deliver "a new era of AI-enabled, software-defined autonomous solutions for the DoD" that provide faster decision-making capabilities in contested environments, giving the U.S. military essential decision advantage.[92]

---

[87] U.S. House of Representatives, *Bipartisan House Task Force Report on Artificial Intelligence*, 118th Congress, (December 2024).
[88] Amazon Pledges to Upskill 100,000 U.S. Employees for In-Demand Jobs by 2025, Amazon, July 11, 2019, https://press.aboutamazon.com/2019/7/amazon-pledges-to-upskill-100-000-u-s-employees-for-in-demand-jobs-by-2025.
[89] "Summary of the 2018 DOD AI Strategy, Harnessing AI to Advance Our Security and Prosperity," Office of the Under Secretary of Defense for Research and Engineering, February 12, 2019.
[90] Amandeep Singh, "AI-powered systems identified potential COVID-19 treatments within days rather than the months or years traditional methods would require." Pharma Phorrum, accessed April 20, 2025, https://pharmaphorum.com/views-analysis-digital/how-ai-is-fighting-covid-19-the-companies-using-intelligent-tech-to-find-new-drugs.
[91] Department of Defense, *National Defense Industrial Strategy Implementation Plan for FY2025* (Washington, DC: Office of Prepublication and Security Review, June 2024).
[92] Nicholas Jordan and Jennifer Mapp, "In the Dark: How the Pentagon's Limited Supplier Visibility Risks U.S. National Security," War on the Rocks, June 14, 2023.# AI Military Integration: Transforming Defense in the Era of Strategic Competition.

10.0 LOE 4: INTERNATIONAL COMPETITION AND COOPERATION

AI is becoming a cornerstone of global power, shaping competition and cooperation across economic, military, and diplomatic domains. The defining contest is between the U.S. and China, with each viewing AI leadership as vital to national strength. Yet a broader international landscape is emerging as allies and regional actors integrate AI into their defense capabilities, creating competition between democracies and autocratic regimes over who will set the norms for AI in future warfare.

10.1 Strategic Competition: China and Russia's Bid for Defense AI Dominance

China aims to lead in AI by 2030, embedding it within industrial policy and military modernization.[93] Its civil-military fusion, backed by state-backed investments and loans, ensures commercial AI breakthroughs are fed into the PLA This supports Beijing's vision of AI-enabled military dominance. The PLA is pursuing "intelligentized warfare," envisioning using AI to accelerate decision cycles, enable swarming tactics, and integrate joint operations to neutralize U.S. conventional advantages. PLA doctrine emphasizes an "algorithm-centric" warfare model, where AI and data dominance are seen as more decisive than traditional hardware advantages.[94]

China's pursuit of AI dominance is powered by an innovation model that blends top-down state direction with intense domestic market competition, backed by over $180 billion in government investment.[95] Chinese tech firms, shielded by the Great Firewall and operating under

[93] Wanyu Zhang Luo Yan, "Spotlight Series on Global AI Policy — Part III: China's Policy Approach to Artificial Intelligence," Global Policy Watch, February 8, 2024, https://www.globalpolicywatch.com/2024/02/spotlight-series-on-global-ai-policy-part-iii-chinas-policy-approach-to-artificial-intelligence/.
[94] "The PLA and Intelligent Warfare: A Preliminary Analysis," accessed April 29, 2025, https://www.cna.org/reports/2021/10/the-pla-and-intelligent-warfare-preliminary-analysis; "New PLA Unit Underscores Intelligentized Warfare Shift - Asia Times," accessed April 29, 2025, https://asiatimes.com/2024/04/new-pla-unit-underscores-intelligentized-warfare-shift/
[95] Kai-Fu Lee, *AI Superpowers China, Silicon Valley, and the New World Order*, 1st ed. (Boston: Houghton Mifflin Harcourt, 2018); Robert D. Atkinson, "China Is Rapidly Becoming an Innovator in Advanced Industries" (Information Technology & Innovation Foundation, September 16, 2024),

minimal privacy constraints, benefit from access to massive, centralized datasets, giving them a distinct advantage in training AI models.[96]

China's efforts to accelerate AI development are also fueled by systematic intellectual property (IP) theft. China's acquisition of U.S. IP costs the U.S. around $600 billion annually, approximately 1-3% of U.S. GDP.[97] In fact, China is responsible for 50-80% of all IP theft against the United States, with 80% of economic espionage prosecutions involving conduct benefiting the Chinese state.[98] As explained in more detail in Appendix 2, Beijing employs comprehensive acquisition strategies including cyber espionage, forced technology transfers, strategic investments, and talent recruitment programs.[99] Worse yet, China's new Anti-Foreign Sanctions Law explicitly authorizes seizure of foreign IP assets, weaponizing its legal system against foreign companies.[100] The consequences to U.S. national security are profound. China's acquisition of AI technologies directly accelerates PLA military modernization in autonomous systems and cyber operations that challenge U.S. AI and battlefield supremacy.[101] Chinese

https://itif.org/publications/2024/09/16/china-is-rapidly-becoming-a-leading-innovator-in-advanced-industries/; Martin Beraja, "Government as Venture Capitalists in AI," Working Paper, Working Paper Series (National Bureau of Economic Research, July 2024).

[96] Kai-Fu Lee, *AI Superpowers China, Silicon Valley, and the New World Order*; Robert Lee and Jasmine Lyu, "Tencent Equity Research - Tencent's AI Progress Makes It a Likely Future Leader: React," *Bloomberg Intelligence*, n.d.

[97] Commission on the Theft of American IP, *Update to the IP Commission Report* (Seattle: National Bureau of Asian Research, February 2017), 1, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf.

[98] Scott Tosi, "Steal the Firewood from Under the Pot: The Role of IP Theft in Chinese Global Strategy," *Military Review* 100, no. 5 (September–October 2020): 96, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-20/Tosi-Intellectual-Property-Theft-1.pdf.

[99] Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, May 6, 2019), 4–5, https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

[100] Lester Ross, "China Further Formalizes Its Anti-Foreign Sanctions Legal Arsenal: the Regulations on Implementation of the Anti-Foreign Sanctions Law," WilmerHale, March 31, 2025, https://www.wilmerhale.com/en/insights/client-alerts/20250331-china-further-formalizes-its-anti-foreign-sanctions-legal-arsenal-the-regulations-on-implementation-of-the-anti-foreign-sanctions-law.

[101] Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, May 6, 2019), 4–5,

companies undercut American competitors by avoiding research and development (R&D) costs, forcing U.S. firms to accept diminished margins or abandon markets entirely.[102]

Russia, while more economically constrained, is also pursuing advantages from AI-enabled military capabilities, focusing on electronic warfare, intelligence rurveillance and reconnaissance (ISR), and autonomous combat vehicles. The Russian military seeks to integrate AI to process battlefield data, automate target selection, and enhance cyber operations. The Russian armed forces are accelerating development by leveraging the war in Ukraine to rapidly field, test, and evaluate AI innovations on the battlefield.

Russia and China are deepening cooperation in defense AI as part of their broader "no limits" strategic partnership. Facing western sanctions and limited access to advanced chips, Russia has turned to China for joint AI development, with Sberbank leading collaboration efforts.[103] Both countries have discussed the military applications of AI, including autonomous weapons and enhanced battlefield decision-making.[104] China, in turn, may benefit from Russian wartime data and defense technologies to advance its own military AI systems.

10.2 Allied Advantage: Building AI Coalitions for Defense

Faced with authoritarian advances in AI, the U.S. and like-minded democracies are pursuing collaborative AI development to ensure interoperability and uphold democratic values through forums like AUKUS and NATO.

---

https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

[102] Lester Ross, "China Further Formalizes Its Anti-Foreign Sanctions Legal Arsenal: the Regulations on Implementation of the Anti-Foreign Sanctions Law," WilmerHale, March 31, 2025, https://www.wilmerhale.com/en/insights/client-alerts/20250331-china-further-formalizes-its-anti-foreign-sanctions-legal-arsenal-the-regulations-on-implementation-of-the-anti-foreign-sanctions-law.

[103] Gleb Bryanski, "Russia's Sberbank Plans Joint AI Research with China as DeepSeek Leaps Forward," *Reuters*, February 6, 2025, sec. Artificial Intelligence, https://www.reuters.com/technology/artificial-intelligence/russias-sberbank-plans-joint-ai-research-with-china-deepseek-leaps-forward-2025-02-06/.

[104] Christy Lee, "Russia Turns to China to Step up AI Race against U.S.ini," Voice of America, January 9, 2025, https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html.

AUKUS, an alliance between the U.S., United Kingdom, and Australia, focuses in part on joint development of advanced military technologies, including AI. Each partner brings complementary strengths: the U.S. contributes scale and defense AI investment; the UK offers world-class research institutions; and Australia provides Indo-Pacific test ranges and regional context. Since 2023, joint AUKUS trials have demonstrated AI-enabled coalition ISR and strike coordination, with real-time model sharing and platform integrations across the three nations.[105] [106] This integration promises a decisive edge by enabling coalition forces to act as a unified, AI-enabled warfighting system.

NATO is advancing allied cooperation on artificial intelligence through ethical alignment, policy coordination, and joint innovation. In 2021, all member states adopted NATO's first AI strategy, which included a shared commitment to the Principles of Responsible Use—covering lawfulness, accountability, explainability, reliability, governability, and bias mitigation.[107] The NATO Defense Innovation Fund and the Defense Innovation Accelerator for the North Atlantic support the development of multinational AI applications for joint use, such as target recognition and decision support systems.

At its core, allied AI cooperation aims to keep pace with adversaries like China and Russia while reinforcing democratic values. Ally and partner AI cooperation focuses on three goals:

1. **Interoperability:** Integrating AI into coalition operations with compatible models and data structures, enabling seamless communication between AI-enabled systems.

[105] Ministry of Defence (UK), "World First as UK Hosts Inaugural AUKUS AI and Autonomy Trial" (UK Government, May 2023); "AUKUS Partners Demonstrate Advanced Capabilities AI Trial," Department of Defence, May 26, 2023, https://www.defence.gov.au/media-room/media-releases/aukus-partners-demonstrate-advanced-capabilities-ai-trial.
[106] "AUKUS Pillar II Milestones Hint at Future Integrated Autonomous, Artificial Intelligence Operations," U.S. Department of Defense, August 9, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3484698/aukus-pillar-ii-milestones/.
[107] NATO, "Summary of NATO's Revised Artificial Intelligence (AI) Strategy," NATO, accessed April 29, 2025, https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

2. **Norm Setting:** Promoting ethical AI principles, including human-in-the-loop control and legal accountability.
3. **Strategic Advantage:** Pooling data, research, and technological tools to offset national limitations and build collective strength.

By demonstrating ethical restraint and lawful application of AI in defense, allied democracies seek to distinguish themselves from authoritarian actors like China and Russia, who are known to export AI-enabled surveillance and autonomous weapons with minimal oversight.

10.3 Regional AI Developments and Implications

While the U.S.-China rivalry dominates the defense AI discourse, AI is reshaping regional security dynamics worldwide. Several key examples illustrate this trend:

In Europe, Russia's 2022 invasion of Ukraine catalyzed a push for AI-enabled defense innovation.[108] The European Union's (EU) Strategic Compass calls for coordinated investment in emerging technologies, while the European Defense Fund supports joint AI R&D.[109] Despite fragmented investment and limited defense-industrial consolidation, Europe aims to lead in normative frameworks through initiatives like the EU AI Act, which emphasizes ethical, human-centric AI values.[110]

In the Indo-Pacific, Japan exemplifies how U.S. allies integrate AI to enhance operational efficiency. The Japan Maritime Self-Defense Force is exploring how AI could be used for predictive maintenance and logistics optimization to support more extended deployments and

[108] "Russia's Threats against Ukraine Are a Wake-up Call for Europe, MEPs Say | News | European Parliament," February 16, 2022, https://www.europarl.europa.eu/news/en/press-room/20220210IPR23007/russia-s-threats-against-ukraine-are-a-wake-up-call-for-europe-meps-say.
[109] "A Strategic Compass for Security and Defence | EEAS," April 19, 2025, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.
[110] "AI Act | Shaping Europe's Digital Future," April 15, 2025, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

faster resupply in response to Chinese naval activity.[111] Projects like the Global Combat Air Program (with the UK and Italy) and AI-enabled drone wingmen for F-35s[112] highlight Tokyo's dual domestic innovation and international collaboration strategy.

Middle powers like Algeria demonstrate a third approach, leveraging AI to modernize defenses through geopolitical balancing, sourcing AI-enabled systems from China, Russia, and Europe to maximize bargaining leverage while avoiding overdependence. This hedging underscores how AI proliferates through strategic partnerships, not just indigenous innovation.

10.4 Strategic Implications: Instability and Bifurcation

The acceleration of AI competition between the U.S. and China, expanding allied cooperation, and diffusion to smaller states mark a turning point in international security. AI accelerates the speed of operations, enabling systems to identify, target, and engage faster than humans can respond. This raises the risk of inadvertent escalation, especially if AI systems interact in unforeseen ways. Maintaining human oversight becomes increasingly complex in time-sensitive scenarios.

The proliferation of advanced AI to middle-tier militaries and non-state actors lowers barriers to fielding autonomous weapons, complicating deterrence and increasing the likelihood of conflict. Unlike nuclear weapons, AI is not a singular system but a diffuse, embedded technology that defies traditional arms control. Efforts at the UN to regulate lethal autonomous weapons have stalled, suggesting that voluntary norms and confidence-building measures are the most viable near-term options.[113]

---

[111] "Acquisition, Technology and Logistics Agency: New Generation Equipment Research Institute," accessed April 29, 2025, https://www.mod.go.jp/atla/shinsouken.html.
[112] Elio Calcagno Douglas Barrie, "The New Partnership among Italy, Japan and the UK on the Global Combat Air Programme (GCAP)," Text, IAI Istituto Affari Internazionali, March 14, 2025, https://www.iai.it/en/pubblicazioni/c04/new-partnership-among-italy-japan-and-uk-global-combat-air-programme-gcap.
[113] Morgan et al., "Military Applications of Artificial Intelligence."

AI is also bifurcating the global technology ecosystem. As democratic allies align their AI efforts and authoritarian states develop rival systems, incompatible standards emerge. Competing models—ethical, interoperable AI versus surveillance-based autocracy—will shape how AI is adopted worldwide. This geopolitical contest is also a soft-power competition, with nations in Africa, Asia, and Latin America choosing between China's "Digital Silk Road" or Western initiatives like the Global Partnership on AI.

In this volatile landscape, forging trusted coalitions will be essential to navigating the opportunities and perils of AI-enabled warfare. Coalitions of like-minded nations will be required to establish norms of ethical use while maintaining strategic advantage. The choices made today will define not just military advantage, but the rules, values, and stability of the AI-driven international system to come.

11.0 CONCLUSIONS AND RECOMMENDATIONS

11.1 The AI Fault Line: Shaping the Future of Global Order

AI is becoming a central fault line in global security, shaping the pace and character of future warfare and the structure of international order. The intensifying AI arms race between the U.S. and China reflects deeper strategic, ideological, and technological divides, with each side racing to harness AI for military and economic advantage. At the same time, democratic allies are coalescing around cooperative frameworks, like AUKUS, NATO, and regional partnerships, to develop interoperable AI capabilities and promote ethical norms. Yet, the global diffusion of AI to middle powers and non-state actors threatens to erode traditional deterrence, accelerate decision cycles, and create new escalation risks. In this volatile landscape, forging trusted coalitions will be essential to navigating the opportunities and perils of AI-enabled warfare. These international coalitions will also establish the norms of ethical use of AI in warfare, such

as maintaining human oversight. The choices made today will define not just military advantage but the rules, values, and stability of the AI-driven international system to come.

11.2 Recommendations for Military Capabilities and Concepts

The DoD must develop a comprehensive Multi-Domain AI Integration Strategy that creates a framework for integrating AI agents across all military domains. This strategy should establish clear roles, responsibilities, and human oversight mechanisms, while addressing how AI can enhance existing capabilities and enable new operational concepts. To ensure effective adoption, the future force will require extensive AI-enabled joint training programs that prepare military personnel to operate effectively with AI systems, emphasizing human-machine teaming, rapid decision-making, and adaptability in high-pressure, dynamic environments.

As autonomy increases, maintaining meaningful human control will be critical. This will require accelerated investment in BCI research, emphasizing non-invasive solutions that function reliably in contested environments. Alongside technical development, the DoD must develop comprehensive ethical guidelines and rigorous testing protocols to ensure AI systems operate within legal and moral boundaries without compromising operational effectiveness.

11.3 Recommendations for Platforms, Operations, and Infrastructure

The potential national security implications of quantum computing, especially when paired with AI, require the DoD to dedicate research focusing on decision support, cryptography, and intelligence analysis applications. At the same time, the growing importance of edge computing in tactical environments calls for developing technical standards for ruggedized AI systems, emphasizing interoperability, cybersecurity, and reliance in denied, degraded, intermittent, and limited conditions.

The DoD should expand digital twin capabilities across the defense enterprise to strengthen platform resilience and lifecycle performance. These tools enhance platform design, testing, and predictive maintenance, enabling data-driven sustainment strategies.

However, greater reliance on AI also increases exposure to cyber and algorithmic threats. The DoD must pair these advancements with robust cybersecurity frameworks explicitly tailored for military AI applications, addressing model, data, and communication channel vulnerabilities. These efforts must be integrated across services and domains to create a unified, secure, and resilient foundation for AI-enabled operations.

11.4 Recommendations for Acquisition, Supply Chain, and Dual-Use

To fully leverage AI as a national security force multiplier, the DoD must move beyond incremental acquisition reforms and adopt a systemic, future-ready approach. This requires aggressive expansion of flexible acquisition mechanisms such as OTAs and PIAs. These frameworks should not merely supplement but systematically replace outdated FAR-driven procurement processes in areas demanding rapid innovation. These mechanisms should be the primary pathways for rapidly onboarding non-traditional, agile technology providers. To accelerate AI integration in defense acquisition, rigid, requirements-based models must be replaced by flexible, problem-solution approaches that empower Program Executive Officers (PEOs) to reallocate funding across portfolios and respond dynamically to evolving mission needs.

Additionally, scaling these agile pathways demands dedicated funding streams and long-term partnerships with industry leaders and startup ecosystems. Implementation will require coordinated leadership across the Office of the Secretary of Defense, CDAO, and the services to institutionalize these reforms across acquisition portfolios, supported by targeted training, policy

guidance, and incentives for contracting officers and PEOs. Congress should align appropriations and oversight frameworks with these flexible pathways to enable speed while preserving accountability.

Establish a dedicated AI Acquisition Pathway within the DoD to accelerate the delivery of mission-relevant AI capabilities. This pathway should be tailored to the unique characteristics of AI development, including rapid iteration, data dependencies, and validation requirements, and enable deployment within weeks or months. It must include streamlined documentation, modular contracting tools, flexible data rights frameworks, and embedded checkpoints for ethics, testing, and human oversight. The approach should align with existing rapid procurement mechanisms, such as OTAs, while supporting agile prototyping and enterprise scaling.

Supply chain modernization must also be prioritized. The government should invest in AI-driven supply chain monitoring tools, emphasizing real-time risk assessment and predictive logistics capabilities to ensure the uninterrupted flow of critical materials. Simultaneously, DoD should mandate interoperable data standards across acquisition and supply chain management platforms to integrate AI-driven analytics seamlessly throughout procurement lifecycles and supply chain operations.

A centralized AI governance framework should be established to ensure integrity and trust in this ambitious transformation. This structure must be empowered with the authority, resources, and accountability mechanisms to enforce ethical AI standards, ensuring uncompromising transparency and security despite accelerated acquisition timelines.

11.5 Recommendations for International Cooperation and Competition

The U.S. must strengthen existing multinational frameworks like AUKUS and NATO to deepen collaboration on AI-enabled defense capabilities. This includes developing shared

technical standards, ensuring interoperability across systems, and conducting combined exercises that build trust and capability. The U.S. should also lead in establishing global norms for responsible military AI use, advocating principles such as human oversight, algorithmic transparency, and accountability in all applications of autonomous systems.

At the same time, the U.S. must counter China's pervasive and systematic theft of American and allied AI IP. A comprehensive policy framework must immediately establish a multi-tiered security framework for AI technologies, incorporating enhanced cyber defenses, mandated security protocols for defense contractors, and strengthened counterintelligence against Chinese talent recruitment. The U.S. must also strengthen legal frameworks by enacting targeted IP protection reforms, increasing resources for the Department of Justice prosecution support, and implementing targeted sanctions against entities benefiting from stolen IP. The strategy must work with multi-national organizations to harmonize IP protection standards, coordinate investment screening protocols, and establish collective response mechanisms for major theft incidents. This unified and coordinated approach would disrupt China's technology acquisition efforts more effectively while preserving the innovation advantage of the U.S. and its democratic partners in the emerging AI arms race.

11.6 The Path Forward: An Innovation Surge

America's military-technological edge is eroding under the pressure of accelerating global innovation and intensifying strategic competition. To reverse this trend, the U.S. must urgently initiate an "innovation surge" – a bold, coordinated effort to dramatically increase R&D funding, accelerate prototyping and experimentation, expand alternative acquisition authorities to bypass bureaucracy, and establish dedicated AI and autonomy units across each military Service.

This surge must leverage the full spectrum of national innovation capacity, drawing on the capabilities of government, industry, and academia.

Since much of today's innovation originates in the commercial sector, the DoD must forge stronger partnerships with tech companies, startups, and universities. This includes expanding innovation hubs, creating national technical talent reserves, reforming intellectual property policies, and developing secure rapid-testing environments. These partnerships should emphasize dual-use technologies, creating a sustainable solution pipeline that meets both civilian and defense needs.

The U.S. also has a unique opportunity to lead in shaping ethical guidelines for AI in warfare. This requires clear policies on autonomy in weapon systems, close coordination with allies to shape shared AI norms, active engagement in international forums, and investment in technologies that embed compliance with the law of armed conflict. By demonstrating responsible leadership in developing and employing these technologies, America can help shape an international order that harnesses AI's potential while preserving human judgment in the most consequential conflict decisions.

History underscores the importance of institutional adaptability. Successful transformations, like the Polaris missile program, were driven by clear strategic vision, internal coalitions of support, and novel organizational structures that linked disruptive technology to operational outcomes. In contrast, efforts like Billy Mitchell's advocacy for airpower floundered in the face of entrenched resistance and fragmented leadership.

The lesson is clear: disruptive technologies frequently confront institutional resistance from those preparing to fight the last war. Today, the convergence of AI and autonomous systems fundamentally alters warfare, creating capabilities that parallel history's most revolutionary

military innovations. If the U.S. is to maintain its strategic edge, it must break from outdated models, enact institutional reform, and commit to sustained, innovation-driven transformation. In this new era of algorithmic warfare, embracing change is not optional; it is essential to national survival and victory.

Appendix 1 – Industry Analysis Artificial Intelligence

Appendix 1

Industry Analysis
Artificial Intelligence

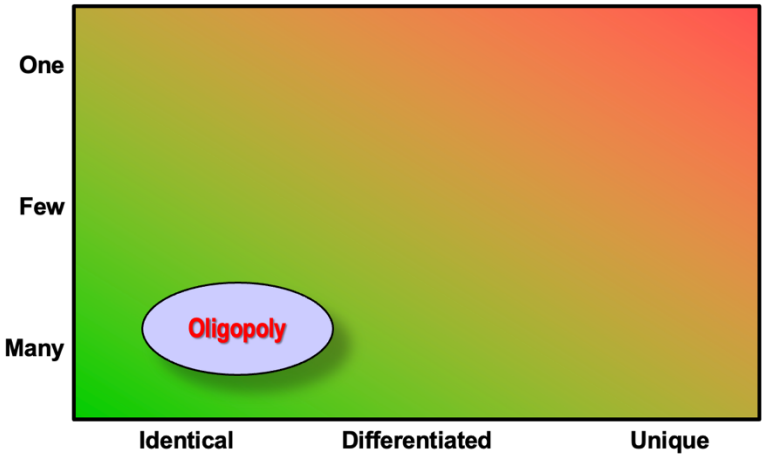
Seminar 2
NDU Eisenhower School

Industry Analysis: *Artificial Intelligence*

Number of Sellers

Many Sellers with Some Dominant Firms

OpenAI
Anthropic
Alphabet
Meta
Scale AI



Products/Services Sold

Large Language Models (LLMs), Generative AI (text, images, video), AI-powered cloud services, and Custom enterprise AI solutions

NDU Eisenhower School

Five Forces: *Artificial Intelligence*

Threat of New Entry
- High upfront costs (talent acquisition, computing infrastructure)
- Strong IP protections and proprietary algorithms
- High regulatory scrutiny
- Barrier lowered slightly by cloud computing and open-source models

Bargaining Power of Suppliers
- Few providers of specialized hardware (GPUs, TPUs)
- Dominance by major cloud infrastructure suppliers
- High switching costs between infrastructure providers
- Dependence on limited semiconductor manufacturers
- Risk of hardware supply constraints

Rivalry Among Existing Competitors
- Intense competition among leading firms
- Rapid innovation and frequent technology updates
- Aggressive talent acquisition and retention efforts
- Significant R&D by major industry players
- High stakes for market leadership and first-mover advantage

Bargaining Power of Customers
- Increasing buyer influence (large enterprise customers)
- Moderate substitutability among standardized AI services
- High switching costs for customized AI solutions
- Growing customer reliance reduces long-term bargaining leverage
- Significant negotiating power for high-volume buyers

Threat of Substitutes
- Viable substitutes (traditional software, analytics tools) for simpler tasks
- Quantum computing
- Limited alternatives for complex AI-driven tasks
- Effectiveness of AI solutions limits substitution
- Cloud-based automation and traditional software remain viable for simpler workflows

Porter, *Competitive Strategy*

NDU Eisenhower School

Five Forces: *Artificial Intelligence*

High Impact
Medium Impact
Low Impact

Force:	Rivalry	Entrants	Substitution	Supplier power	Customer power
Industry –	Artificial Intelligence				
Select factors associated with this force	• Intense competition among key players • Rapid innovation cycles leading to frequent technology obsolescence • High stakes competition for market leadership and talent acquisition • Aggressive investment in R&D is driving ongoing innovation • Fierce product marketing and nonstop innovation	• Large upfront capital and infrastructure costs • Extensive regulatory oversight with increasing complexity • Reduced barriers via cloud computing and open-source availability • High costs associated with skilled AI talent acquisition	• Limited current alternatives matching AI's capabilities • Moderate risk due to fast technological advances • High effectiveness of AI solutions reduces substitution threats • Quantum computing emerging	• Limited providers of specialized hardware (GPUs, TPUs) • Dependence on the limited number of semiconductor makers • Dominant cloud providers control key infrastructure • High switching costs • Potential vulnerabilities due to hardware supply constraints	• Increasing leverage for large corporate and government customers • High switching costs for customized AI solutions • Dependence on AI reduces leverage • Growing influence of big business customers
Impact	**HIGH**	**MEDIUM**	**LOW**	**HIGH**	**MEDIUM**
Analysis of the Factors	Intense competition among major players like OpenAI, Google, Microsoft, and Meta is fueled by rapid innovation, aggressive R&D investment, and a battle for AI talent. Frequent model updates and marketing pressure increase operational and strategic urgency.	Barriers to entry remain high due to the cost of infrastructure, talent, and regulatory compliance. However, cloud-based tools and open-source frameworks have lowered the entry threshold for niche players and startups.	Substitutes like traditional analytics and software exist for simpler tasks, but few current alternatives can match AI's capabilities in language, vision, or autonomy. Quantum computing may pose a future threat but remains early-stage.	Supplier power is elevated due to the limited number of GPU and TPU providers (e.g., NVIDIA, Google) and dominant cloud infrastructure platforms (AWS, Azure). High switching costs and geopolitical instability further amplify supplier leverage.	Large enterprise and government customers like AWS and xAI can negotiate based on scale, but lock-in effects, complex integrations, and dependency on leading AI models reduce their leverage over time.

NDU Eisenhower School

PESTLE: *Artificial Intelligence*

Political	Economic	Social	Technological	Legal	Environmental
• Rising geopolitical competition shaping national AI policies • Growing governmental investment in AI-driven defense capabilities • International cooperation and tensions influencing AI standards • Increased global regulatory oversight and compliance demands • AI export controls and national security restrictions	• Rapid growth and high market valuation (expected over $1T by 2030) • Increasing venture capital and corporate investments in AI • Significant economic disruption potential across industries • High demand driving up talent and infrastructure costs	• Widespread adoption of AI increasing public interaction and dependence • Rising public concern around ethical use, bias, and transparency • Increased consumer expectations for AI-driven personalization • Growing societal debate on AI's impact on employment	• Rapid advancements in computing power and algorithms • Breakthroughs in generative AI and large-scale language models • Accelerated innovation cycles and rapid product iterations • Emerging integration with other technologies (quantum computing, IoT)	• Evolving international privacy and data protection laws (e.g., GDPR, AI Act) • Increasing litigation around intellectual property and AI-generated content • Enhanced scrutiny on algorithmic transparency and accountability • Complex regulatory landscape complicates global AI deployment	• Significant energy demands from AI training and data centers • Increasing pressure for sustainable, energy-efficient computing practice • Growing public and regulatory emphasis on environmental responsibility • Innovations aimed at reducing AI's environmental footprint • Training large models (e.g., GPT-4) consumes significant energy, prompting regulatory and social concern

NDU Eisenhower School

Citations

- Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2024* (Stanford, CA: Stanford University, 2024), https://aiindex.stanford.edu/report/.
- McKinsey & Company, "The State of AI in 2024," *McKinsey Analytics*, February 2024, https://www.mckinsey.com/business-functions/quantumblack/our-insights/the-state-of-ai-2024.
- Boston Consulting Group, "AI Market Outlook and Trends," *BCG*, January 2025, https://www.bcg.com/publications/ai-market-outlook-trends-2025.
- OECD, "Artificial Intelligence Policy Observatory," *OECD.AI*, accessed April 10, 2025, https://oecd.ai/en/.
- European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," COM(2021) 206 final, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
- U.S. White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
- World Economic Forum, *Global AI Action Alliance: AI Governance Frameworks and Recommendations* (Geneva: World Economic Forum, 2023), https://www.weforum.org/reports/global-ai-action-alliance-2023/.
- DCF Modeling, "OpenAI Five Forces Analysis," *DCF Modeling*, January 2025, https://dcfmodeling.com/products/openai-porters-five-forces-analysis.
- StrategyPunk, "PESTLE Analysis: Artificial Intelligence," *StrategyPunk*, October 2024, https://www.strategypunk.com/content/files/2024/10/StrategyPunk.com—PESTLE-Analysis-AI.pdf.
- NVIDIA Corporation, "NVIDIA AI Infrastructure Overview," *NVIDIA*, accessed February 4, 2025, https://www.nvidia.com/en-us/data-center/products/ai-infrastructure/.

NDU Eisenhower School

Appendix 2 – Intellectual Property (IP) in AI – Definitions and Global Legal Frameworks

A2.1 IP Types and Definitions

Patents: Legal rights granted to inventors for novel, non-obvious, and useful inventions. Patents provide 20-year exclusive rights to make, use, or sell the invention in exchange for public disclosure of the technical information.[114]

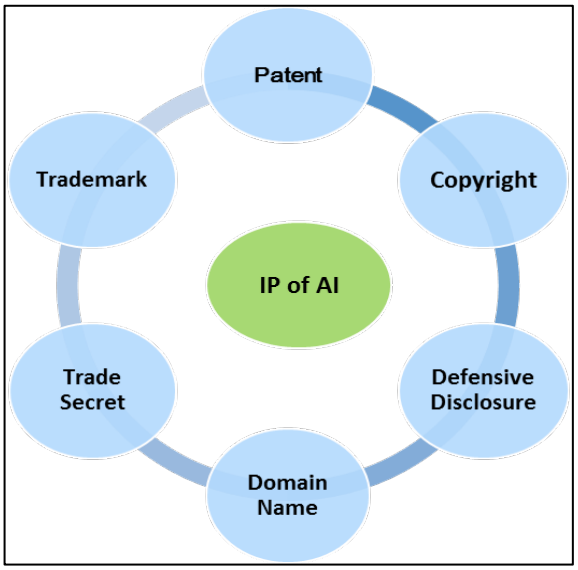


Figure 1: Comprehensive intellectual property protection framework for AI, illustrating the six key protection mechanisms that must work in concert to secure AI innovations.

Copyrights: Automatic protections for original works fixed in tangible form, including software code, documentation, and creative content. Protection extends for the creator's lifetime plus 70 years, granting exclusive rights to reproduce, distribute, display, and create derivatives.[115]

Trademarks: Distinctive signs, symbols, names, or slogans used to identify and distinguish products or services in the marketplace. Unlike patents, trademark protection can be maintained indefinitely with proper renewal and continued commercial use.[116]

Trade Secrets: Confidential business information that provides a competitive advantage, including formulas, processes, and proprietary techniques. Trade secrets require no registration but demand reasonable measures to maintain secrecy and have no expiration date as long as secrecy is preserved.[117]

[114] "Intellectual Property Law: A Brief Introduction," Congressional Research Service, April 13, 2022.
[115] "IP Law," CRS.
[116] "IP Law," CRS.
[117] "IP Law," CRS.

A2.2 IP Overview

IP in AI encompasses legally protected intangible assets resulting from human innovation. Patents protect novel algorithms and hardware designs for 20 years, granting exclusive manufacturing and distribution rights.[118] Copyrights automatically protect original expressions, including software code and datasets, for the creator's lifetime plus 70 years.[119] Trademarks safeguard brand identifiers for AI products and services indefinitely with proper renewal.[120] Trade secrets protect confidential business information that provides a competitive advantage, including proprietary training techniques and model parameters, requiring no registration but demanding reasonable secrecy measures.[121]

The AI technology stack requires comprehensive protection across multiple layers: data collection methodologies (patents/trade secrets), algorithms and model architectures (patents/copyrights/trade secrets), training methodologies (trade secrets), model weights and parameters (trade secrets), and model outputs and applications (patents/copyrights).[122] Hardware dependencies, particularly Taiwan's semiconductor production, create critical chokepoints in the global AI supply chain, with TSMC producing approximately 90% of advanced chips required for AI training and inference.[123]

---

[118] "Intellectual Property Law: A Brief Introduction," Congressional Research Service, April 13, 2022, https://crsreports.congress.gov/product/pdf/IF/IF10986.
[119] Dr. Gary L. Deel, "What Is Intellectual Property Law? And Why Does it Matter?" American Public University, July 13, 2023, https://www.apu.apus.edu/area-of-study/security-and-global-studies/resources/what-is-intellectual-property-law/.
[120] Will Kenton, "What Is Intellectual Property and What Are Some Types?" Investopedia, June 7, 2024, https://www.investopedia.com/terms/i/intellectualproperty.asp.
[121] Brian T. Yeh, "Protection of Trade Secrets: Overview of Current Law and Legislation," Congressional Research Service, April 22, 2016.
[122] World Intellectual Property Organization, "WIPO Technology Trends 2019: Artificial Intelligence," Geneva: WIPO, 2019, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.
[123] Semiconductor Industry Association, "SIA State of the Industry Report," Washington, DC: SIA, 2024, https://www.semiconductors.org/wp-content/uploads/2024/10/SIA_2024_State-of-Industry-Report.pdf.

A2.3 Global IP Legal Frameworks

A2.3.1 United States: Architect of Innovation

The U.S. has established a robust IP framework grounded in the U.S. Constitution, which empowers Congress "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[124] This system has become a cornerstone of America's technological advancement and global AI leadership. For AI innovation, patent law safeguards novel algorithms and applications, trade secret protection shields proprietary training techniques, and copyright law protects software code and creative outputs.[125] The U.S. IP regime is strengthened by export controls restricting advanced technology shipments to potential adversaries while preserving domestic innovation advantages.[126]

A2.3.2 China: Acquisition Over Innovation

While China has developed comprehensive IP laws that resemble Western standards on paper, enforcement remains elusive.[127] China's political system creates fundamental disincentives for true innovation, with the Chinese Communist Party's emphasis on control and lack of genuine rule of law

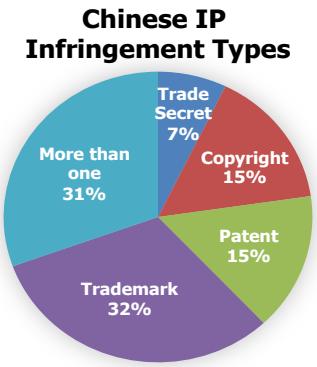


Figure 2: Distribution of Chinese intellectual property infringements by type.

[124] Rich Stim, "Overview of Intellectual Property Laws," Stanford Libraries, accessed April 2025, https://fairuse.stanford.edu/overview/introduction/intellectual-property-laws/.
[125] National Security Commission on Artificial Intelligence, "Final Report" (Washington, DC: NSCAI, 2021), 173-181.
[126] Ana Swanson, "Trump Targets Chinese Tech Firms, Citing National Security," *The New York Times*, March 25, 2025.
[127] "China's IP Protection Development: A Comprehensive Overview," China Briefing, August 13, 2024, https://www.china-briefing.com/news/chinas-ip-protection-development-a-comprehensive-overview/.

encouraging acquisition over original creation.[128] Many Chinese firms face strong incentives to appropriate intellectual property—both domestic and foreign—rather than invest in risky, expensive R&D.[129]

China's Military: Civil Fusion strategy deliberately blurs the lines between commercial and military technology development, enabling the repurposing of acquired foreign AI innovations for military applications.[130] This systematic approach includes state-sponsored cyber espionage, forced technology transfers, and strategic investments designed to access proprietary intellectual property.[131]

The recent implementation of China's Anti-Foreign Sanctions Law (AFSL) in March 2025 further complicates IP protection by explicitly authorizing the seizure of foreign IP.[132] The regulation empowers Chinese authorities to freeze or seize assets within China, including IP held by targeted individuals or entities, restrict critical IP-related activities, including banning

[128] Glenn Chafetz, "How China's Political System Discourages Innovation and Encourages IP Theft," *SAIS Review of International Affairs*, July 31, 2023, https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/.
[129] Chafetz, "How China's Political System Discourages Innovation."
[130] Rose Tenyotkin et al., "How China Legally Accesses Foreign Technologies to Build Military Capabilities," *CNA Report*, June 1, 2020, https://www.cna.org/reports/2020/08/economic-statecraft-china.
[131] Sean O'Connor, How Chinese Companies Facilitate Technology Transfer from the United States (Washington, DC: U.S.-China Economic and Security Review Commission, May 6, 2019), 4-5.
[132] Lester Ross, "China Further Formalizes Its Anti-Foreign Sanctions Legal Arsenal: the Regulations on Implementation of the Anti-Foreign Sanctions Law," *WilmerHale*, March 31, 2025.

technology exports and limiting data transfers, and creates a private right of action allowing Chinese organizations to sue foreign companies that comply with international IP protections.[133] This legal framework effectively weaponizes China's legal system against foreign companies attempting to safeguard their innovations and creates a mechanism for state-led appropriation of AI technologies.[134]

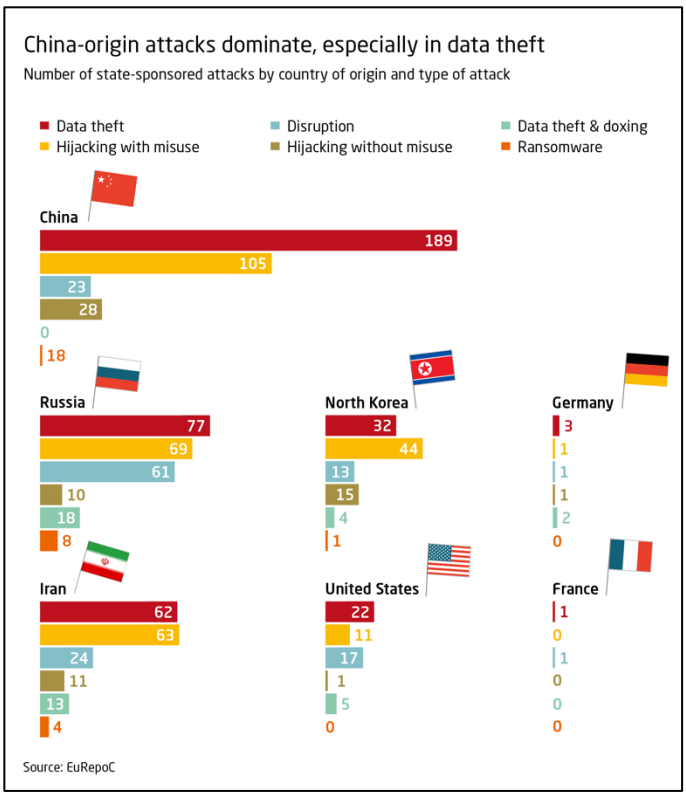


Figure 3: China-origin cyberattacks dominate global state-sponsored data theft activities, representing the primary vector for AI intellectual property acquisition.

[133] Jacob Harding, "China Passes Anti-Foreign Sanction Law," Winston & Strawn, July 31, 2021, https://www.winston.com/en/blogs/regulating-the-digital-world/china-passes-anti-foreign-sanction-law.html.
[134] Reuters, "China rolls out new rules to step up countermeasures to foreign sanctions," *Reuters*, March 24, 2025, https://www.reuters.com/world/china/china-rolls-out-new-rules-step-up-countermeasures-foreign-sanctions-2025-03-24/.

Appendix 3 – Wargaming in the AI Era – Implications for National Security

Wargaming is increasingly essential to understanding and integrating artificial intelligence (AI) into national security planning. Long used to simulate military conflict and stress-test strategy, wargames are now evolving to address the complexity, speed, and unpredictability that AI introduces across defense and commercial domains. AI-enabled wargames allow military planners to experiment with new operational concepts, simulate human-machine teams, and assess the performance of autonomous systems under battlefield conditions. They provide a flexible, low-risk environment to test assumptions, reveal vulnerabilities, and identify paths to advantage before these systems are fielded in real-world operations. By rapidly iterating across thousands of scenarios, modern wargaming compresses learning cycles and supports more adaptive strategy development.[135]

These simulations are not confined to combat modeling. Defense organizations now use wargaming to inform procurement, capability development, and command-and-control arrangements, especially when evaluating AI-enabled systems. For instance, planners can model how a swarm of autonomous drones coordinates with human pilots, or how command structures must adapt when decisions are made at machine speed. AI agents embedded in wargames simulate adversary adaptation, providing more dynamic red-teaming than traditional human-led scenarios.[136] This allows participants to engage with fast-evolving challenges that mirror real-world adversaries' increasing use of AI to exploit decision cycles and degrade U.S. advantage.

Commercial and policy actors have also embraced wargaming as a strategic foresight tool. Technology firms and think tanks employ scenario-based exercises to explore how AI

[135] Jon Harper, "Air Force Sees Opportunities for AI to Improve Wargaming," *Defense Scoop* (blog), April 12, 2024, https://defensescoop.com/2024/04/12/ai-wargaming-air-force-futures-mit/.
[136] Patrick Hinton, "Generative AI and Wargaming: What Is It Good For?," *The RUSI Journal* 168, no. 7 (November 10, 2023): 34–41, https://doi.org/10.1080/03071847.2023.2282863.

disruption might unfold through cyberattacks, misinformation campaigns, or supply chain manipulation.[137] These games help identify second- and third-order effects of AI proliferation that traditional risk assessments might overlook. Importantly, they also build shared mental models among industry, government, and academic stakeholders—facilitating the kind of cross-sector collaboration that AI integration demands.

Wargames are also critical to navigating the ethical and legal dilemmas surrounding AI in warfare. Simulated crises—such as autonomous targeting failures or AI system escalation—allow decision-makers to debate policies before those scenarios become reality. [138] These exercises surface practical issues like accountability, explainability, and the thresholds for human override in high-speed engagements. They also help refine human-machine interfaces and training protocols by revealing how operators interpret, trust, or override AI-generated recommendations under stress.

As the character of warfare evolves, wargaming offers the Department of Defense and its partners a uniquely adaptable platform for anticipating technological disruption. By simulating contested, algorithm-driven environments in advance, these exercises reduce surprise, support agile decision-making, and ensure ethical oversight is embedded early in concept development. In an era defined by AI competition, wargaming is not a legacy tool—it is a strategic necessity.

[137] Kristoffer Lie Eide et al., "Perspective Chapter: How Artificial Intelligence (AI) Fundamentally Changes Crisis Management Training and Exercises," in *Crisis Management Dynamics - Strategies, Challenges, and Best Practices* (IntechOpen, 2025), https://doi.org/10.5772/intechopen.1008950.
[138] Sara Goudarzi, "Wargames and AI: A Dangerous Mix That Needs Ethical Oversight," *Bulletin of the Atomic Scientists* (blog), December 4, 2023, https://thebulletin.org/2023/12/wargames-and-ai-a-dangerous-mix-that-needs-ethical-oversight/.

Appendix 4 – AI Appendix

Not required by James Keagle – Instructor.