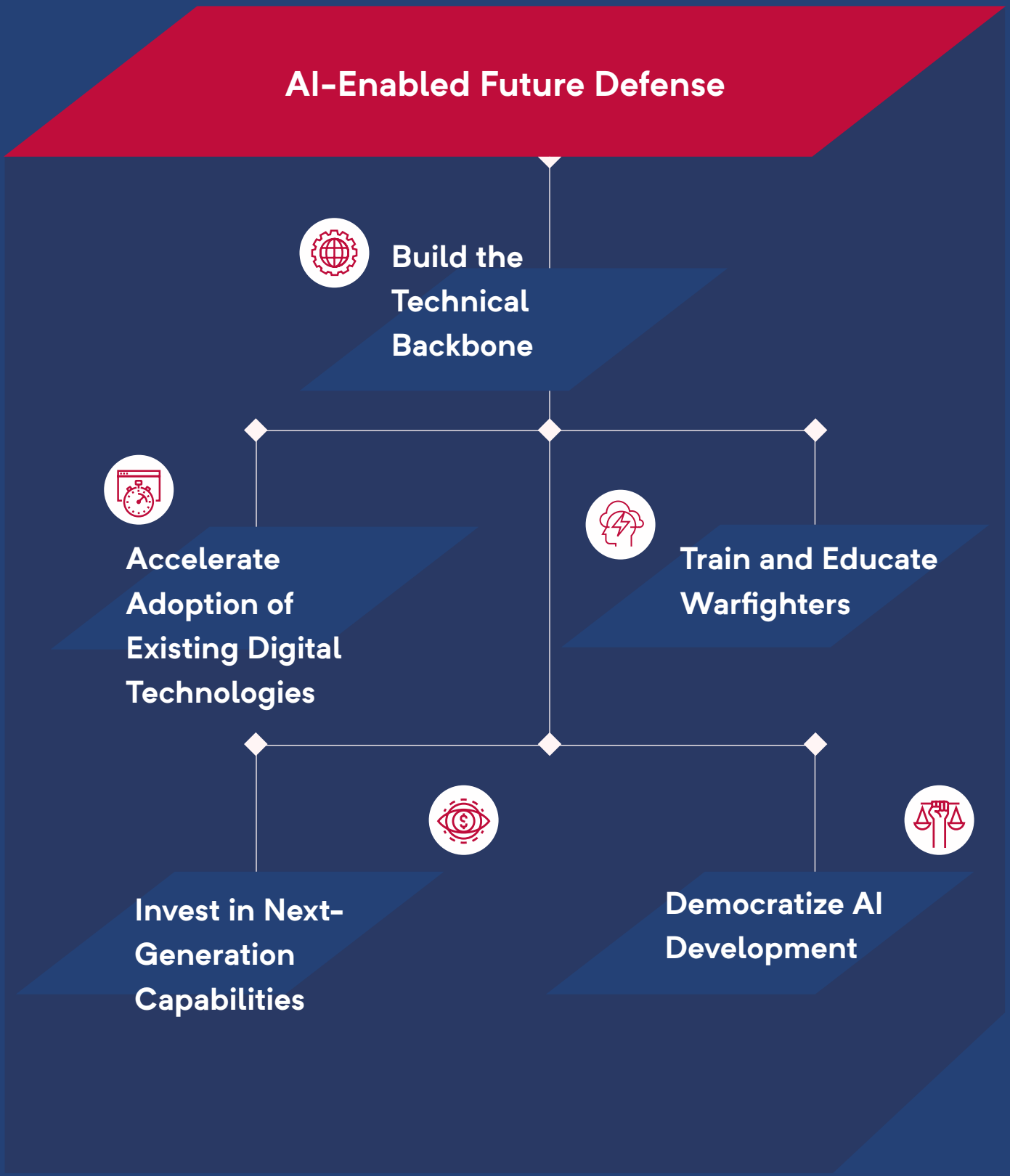
Chapter 2: Foundations of Future Defense


AI-Enabled Future Defense
Build the Technical Backbone
Accelerate Adoption of Existing Digital Technologies
Train and Educate Warfighters
Invest in Next-Generation Capabilities
Democratize AI Development

The U.S. military has enjoyed military-technical superiority over all potential adversaries since the end of the Cold War. Now, its technical prowess is being challenged, especially by China and Russia. Senior military leaders have warned that if current trend lines are not altered, the U.S. military will lose its military-technical superiority in the coming years.[1] Artificial intelligence (AI) is a key aspect of this challenge, as both of our great power competitors believe they will be able to offset our military advantage using AI-enabled systems and AI-enabled autonomy. In the coming decades, the United States will win against technically sophisticated adversaries only if it accelerates adoption of AI-enabled sensors and systems for command and control, weapons, and logistics.

The Department of Defense (DoD) must set an ambitious goal. By 2025, the foundations for widespread integration of AI across DoD must be in place. Those foundations include a common digital infrastructure that is accessible to internal AI development teams and critical industry partners alike, a digitally literate workforce, and modern AI-enabled business practices that improve efficiency. All are prerequisites to achieving a state of military AI readiness, which is discussed in Chapter 3 of this report.

“By 2025, the foundations for widespread integration of AI across DoD must be in place.”

DoD lags far behind the commercial sector in integrating new and disruptive technologies such as AI into its operations. Pockets of excellence started to emerge in 2017 when Project Maven was launched with the aim to simplify work for intelligence analysts by recognizing objects in video footage captured by drones and other platforms.[2] Other promising initiatives are occurring in defense labs and agencies, and proof-of-concept demonstrations are ongoing in service-level tests.[3] However, visionary technologists and warfighters largely remain stymied by antiquated technology, cumbersome processes, and incentive structures that are designed for outdated or competing aims.[4] Successes are usually based on workarounds––in spite of the system.

"... visionary technologists and warfighters largely remain stymied by antiquated technology, cumbersome processes, and incentive structures that are designed for outdated or competing aims."

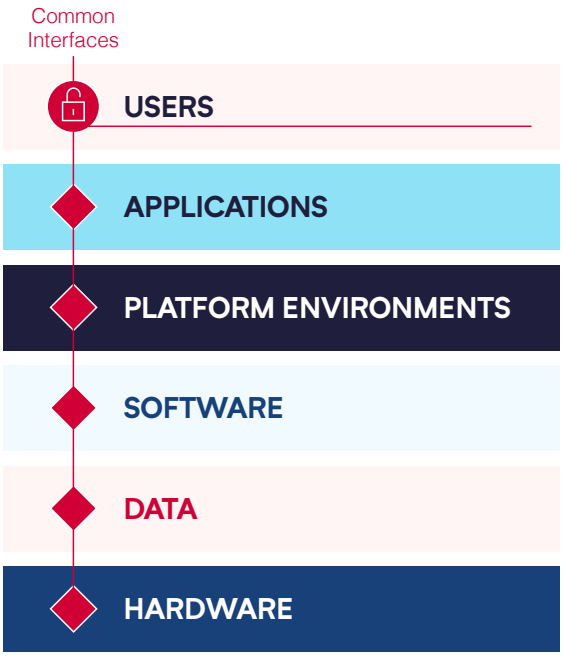
The obstacles to integrating AI are many. DoD has long been hardware-oriented toward ships, planes, and tanks. It is now trying to make the leap to a software-intensive enterprise. Spending remains concentrated on legacy systems designed for the industrial age and Cold War.[5] Many Departmental processes still rely too much on PowerPoint and manually driven work streams. The data that is needed to fuel machine learning (ML) is currently stovepiped, messy, or often discarded. Platforms are disconnected. Acquisition, development, and fielding practices largely follow rigid, sequential processes, inhibiting early and continuous experimentation and testing critical for AI. Even promising AI programs have not yet delivered as hoped and often remain bound to proprietary software and data storage of commercial vendors. Steps such as building the cloud infrastructure necessary to scale AI applications proceed slowly. Data-sharing agreements and software updates that take hours or days in industry turn into months-long delays. Service members at every level lack the technical education and experience to employ AI.

Meanwhile, bureaucracy hinders partnerships with technology firms and critical efforts to expand the National Security Innovation Base.[6] The prospect of bureaucratic snarls deters companies from working with DoD; it is economically irrational for many startups to even try. Traditional defense companies will continue to play a central role in building and integrating large systems for AI-enabled warfare.[7] However, even these contractors, who have the resources and expertise to navigate the system, face process and technical roadblocks that slow efforts to build and integrate AI systems.

As a result, change will not be easy. It will require a Secretary of Defense who focuses the Department on speeding the adoption of new technologies, and a dedicated Steering Committee on Emerging Technology to drive implementation and align priorities between the DoD and the Intelligence Community. The Secretary should direct action in five areas:

Recommendation

1. Build the technical backbone. DoD should make foundational investments to support a Department-wide technical infrastructure for ubiquitous development and fielding of AI. It took a promising first step in 2020 with the issuance of a DoD Data Strategy.[8] However, the Department lacks the modern digital ecosystem, collaborative tools and environments, and broad on-demand access to shared AI resources that it needs to integrate AI across the organization.[9] The Department should avoid reinventing core infrastructure for each new AI-driven program or capability, and it should look to leverage and interoperate with proven solutions from the Intelligence Community (IC) wherever possible. A broader platform that could be used across the Department would enable more dynamic development and employment of AI and would more efficiently utilize scarce technical expertise.[10]



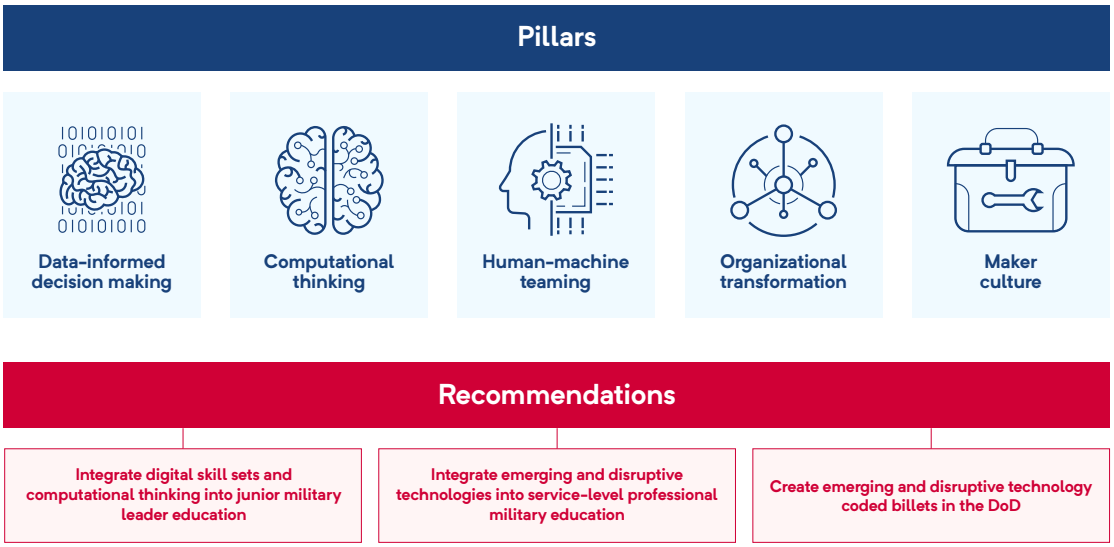
AI Digital Ecosystem.

The Secretary of Defense should direct the establishment of a DoD-wide digital ecosystem. The Secretary should require that all new joint and service programs adhere to the design of this ecosystem and that, wherever possible, existing programs become interoperable with it by 2025.[11] Key elements should include:

- Data architecture composed of a secure, federated system of distributed repositories linked by a data catalog and appropriate access controls[12] that facilitates finding, accessing, and moving desired data across the DoD.[13]
- Packaged AI environments[14] that enable agile and iterative AI capabilities development,[15] testing, fielding, and updating in support of a diverse set of stakeholders.[16]
- A marketplace of shared AI resources[17] that builds upon federated repositories of data, software, and trained models,[18] along with pre-negotiated computing and storage services from a pool of vetted cloud providers.
- A bolstered network and communications backbone to provide bandwidth to support transport and data fusion, secure processing, continuous development and fielding of AI applications, and software system integration at all levels.
- Common interfaces that allow swift integration of mission-oriented investments.

“Warfighters cannot change the way they fight without also changing the way they think.”

Train and Educate Warfighters.



Recommendation

2. Train and educate warfighters. Warfighters cannot change the way they fight without also changing the way they think. Most service members only use the powerful computers they have to create PowerPoint presentations, build spreadsheets, or send emails. Our service members need to develop core competencies in building, using, and responsibly teaming with machine systems to recognize AI’s potential for building a faster and more effective force. In particular, they need to know:

- How to use data in decision-making in ways that complement intuition and experience.
- How to use information processing agents and how to get a computer to perform calculations and analytics that could not be done efficiently by a human.
- How to develop and thrive in a “maker” culture that encourages continuous contact and regular experimentation with and development of new tools.
- How to move toward a “teammate model” for interacting with autonomous systems and navigate issues of delegated authority, observability, predictability, directability, and trust.
- How to bring organizations into the AI era—including when and how to integrate AI-related tasks into priority missions, allocate resources to build and maintain the AI stack, oversee new systems, and support the careers of technical experts.

To improve training and education along these lines, DoD should:

- Identify service members who excel at computational thinking during the accession process;
- Invest in upskilling its workforce through self-guided education courses and coding language incentives;
- Teach junior leaders about problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making as part of their pre-commissioning requirements and initial training;
- Integrate emerging and disruptive technology training into professional military education courses; and
- Create emerging technology coded billets and an emerging technology certification program comparable to the joint billet and qualification system.

Recommendation

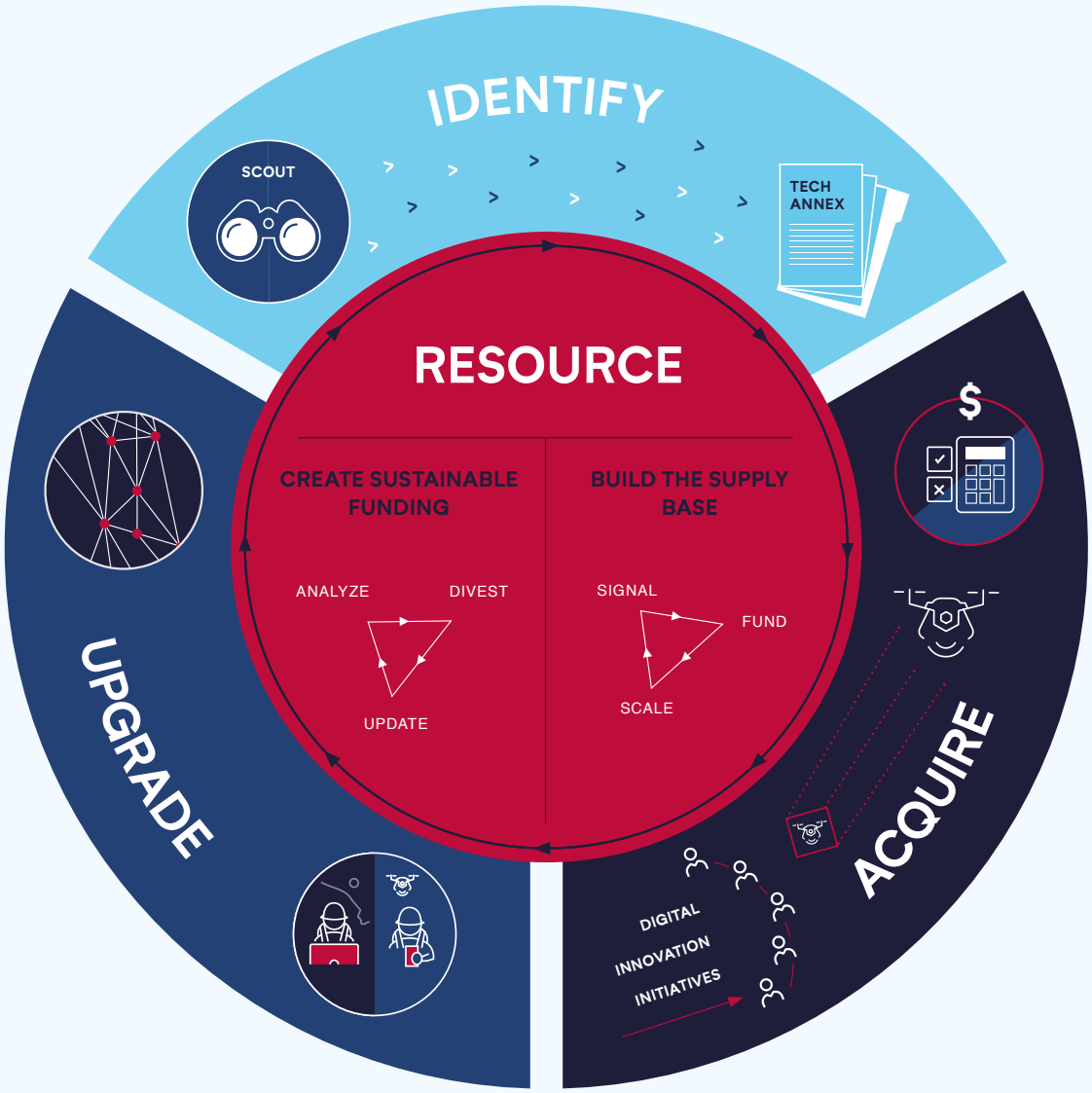
3. Accelerate the adoption of existing digital technologies. DoD has largely relied on workarounds to adopt new technologies, while the core acquisition processes remain sclerotic. There are some bright spots, including the release of the Department's tailorable acquisition framework, contracting resources,[19] and approaches taken by certain programs within the Air Force.[20] The Department must scale these innovative practices and take further steps to align acquisition workforce training, program incentives, budget, and organizational structures to better support the delivery of digitally enabled capabilities.

A number of the Department's digital innovation initiatives have delivered results,[21] but they are uncoordinated and under-resourced. DoD signaling of technology priorities is ad hoc and is not supported by a track record of significant DoD investments in digital technology with non-traditional vendors. As a result, national security AI applications attract less private-market investment. The Department should focus on four actions:

- **Integrate commercial AI to optimize core business processes.** DoD should embrace proven commercial AI applications and incentivize their use to generate labor and cost savings, speed administrative actions, and inform decision-making.[22] As a critical first step, DoD should prioritize construction of enterprise data sets across core administration areas.
- **Network digital innovation initiatives to scale impact.** Pockets of bottom-up innovation need to be married with top-down leadership. The Department should harmonize its innovation initiatives to carry out a coordinated go-to-market strategy for commercial technology solutions. The Under Secretary of Defense for Research and Engineering, working closely with the Under Secretary of Defense for Acquisition and Sustainment, the military services and other headquarters counterparts, should provide strategic direction for this effort.
- **Expand use of specialized acquisition pathways and contracting approaches.** DoD should accelerate efforts to train acquisition professionals on the full range of available options for acquisition and contracting and incentivize their use for AI and digital technologies.[23]

- **Update the budget and oversight processes.** DoD's resource allocation process is nearly identical to what was put in place in 1961. It is incompatible with AI and other digital technologies. DoD and Congress should institute reforms that enable the advancement of software and digital technologies by accounting for speed, uncertainty, experimentation, and continuous upgrades.

An integrated and strategic approach to technology that aligns the process, incentives, and organizational culture of the DoD and the National Security Innovation Base as a pipeline to resource, prioritize, acquire and iterate capabilities critical to sustain the competitive advantage



Delivering AI at Speed and Scale.

“At every level, technologists, operators, and domain experts should function as integrated teams.”

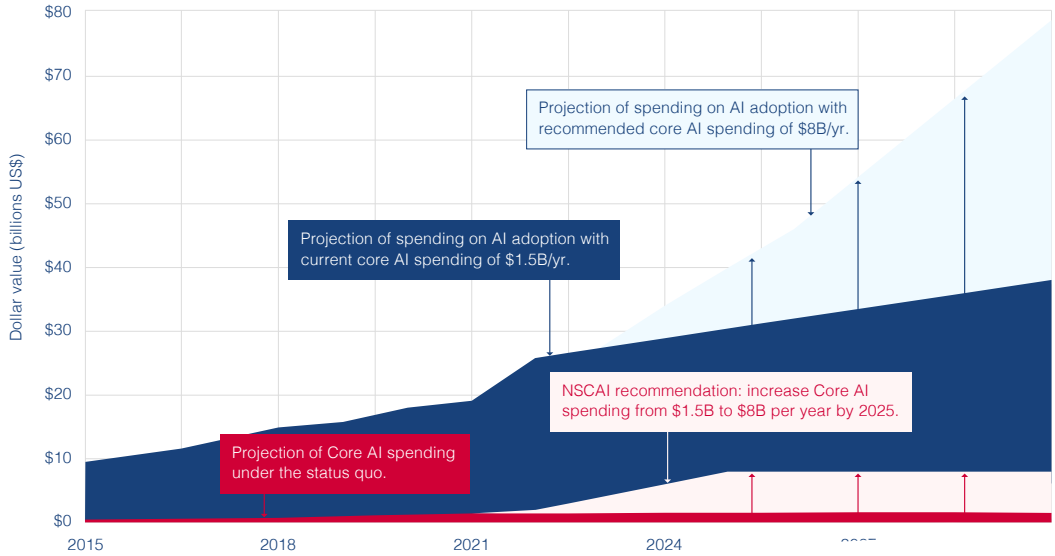
Recommendation

4. Democratize AI development. The Department must promote bottom-up AI development.[24] At every level, technologists, operators, and domain experts should function as integrated teams.[25] This would facilitate user feedback and improve trust and confidence in AI systems. DoD should:

- **Designate the Joint Artificial Intelligence Center (JAIC) as the Department’s AI Accelerator.** The JAIC cannot identify every potential use for AI in the Department, but it can and should serve as a central hub of AI expertise. In this “accelerator” model, JAIC would coordinate with relevant acquisition, technology, and governance offices to inform strategy; develop AI applications that address shared challenges at the Combatant Commands; and provide resources that enable distributed AI development across the Department and the military services.[26]

Enhanced AI R&D Investment, FY 2015-2030
Source: Govini and NSCAI

Enhanced AI R&D Investment, FY 2015-2030.



This figure illustrates the correlation between R&D investment in Core AI technologies and AI adoption projected to the year 2030. Two scenarios are represented in this figure. In the first, the DoD maintains its current level of investment in core AI (~1.5B/year). In the second scenario, the DoD increases its

investments in core AI to $8B/year. A significant increase in core AI spending is required to drive the rate of AI adoption higher.

NSCAI staff teamed with two external partners to analyze historical and planned DoD investments in AI RDT&E. The source data for the analysis is DoD's annual RDT&E budget expenditures (for FY2015 – FY 2020) and annual RDT&E budget requests (for FY2021-FY2025). For the methodology employed and lessons learned from this work, see Analysis of DoD RDT&E Investments in AI, NSCAI (on file with the Commission). Disclaimer: We believe this analysis yields important insights into general trends in AI spending and solutions for better future analyses, but caution that quality issues in the source data detailed in our on file report mean that the spending level estimates presented contain significant, difficult to estimate margins of error.

AI-enabled programs develop (in the case of RDT&E programs) and field (in the case of procurement programs) the gamut of DoD warfighting and business systems, incorporating Core AI applications for analyzing, automating, communicating, maneuvering, monitoring, sensing, and many other tasks. While AI spending is usually a small percentage of these programs, their system's performance may be critically dependent upon the incorporation of core AI.

AI-enabling programs include technologies such as cloud computing and advanced microelectronics required to support the deployment of effective AI capabilities at scale.

- **Establish integrated AI delivery teams at each Combatant Command.** These commands have specific operational needs that routinely outpace centralized development. AI delivery teams should be embedded at each Combatant Command and capable of supporting the full lifecycle of AI development and fielding, including data science, engineering, testing, and production—leveraging common resources through the digital ecosystem.[27] Teams should include forward-deployable components to act as the local interface with operational units.[28]

5. Invest in next-generation capabilities. DoD leaders anticipate flat or declining defense budgets for the coming years.[29] Despite potential budgetary pressures, DoD must continue accelerating its modernization programs by prioritizing emerging and disruptive technologies such as AI.[30]

Recommendation

- **Fund AI research and development.** The Department should commit to spending at least 3.4% of its budget on science and technology and allocate at least $8 billion toward AI R&D annually.[31] Additional resources should be focused on organizations with significant AI expertise, such as the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research (ONR), the Air Force Office of Scientific Research (AFOSR), the Army Research Office (ARO), and the service laboratories.

“To make AI ubiquitous throughout its business processes and military systems, DoD must make tough budget tradeoffs and prioritize modernization.”

- **Retire legacy systems ill-equipped to compete in AI-enabled warfare.** To make AI ubiquitous throughout its business processes and military systems, DoD must make tough budget tradeoffs and prioritize modernization.[32] DoD should pursue a balanced approach to update existing systems with leading-edge technologies to buy time for investments in longer-term bets. Further, to guard against bias in favor of defending the status quo, DoD should require an evaluation of AI alternatives prior to funding Major Defense Acquisition Programs (MDAP).[33]
- **Produce a technology annex to the National Defense Strategy.** To link DoD’s technology investment strategy to future operational needs, the annex should include roadmaps for designing, developing, fielding, and sustaining critical technologies that are needed to address the operational challenges identified in the strategy.

Chapter 2 - Endnotes

[1] General Joseph Dunford, then Chairman of the Joint Chiefs of Staff, testified in 2017 that "The U.S. military's competitive advantage against potential adversaries is eroding [...] I assess that within five years we will lose our ability to project power; the basis of how we defend the homeland, advance U.S. interests, and meet our alliance commitments." Posture Statement of General Joseph Dunford, Chairman of the Joint Chiefs of Staff before the Senate Armed Services Committee, *Senate Armed Services Budget Hearing* at 2 (June 13, 2017), https://www.armed-services.senate.gov/imo/media/doc/Dunford_06-13-17.pdf.

[2] *Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare*, Modern War Institute (Aug. 25, 2020), https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/; Cheryl Pellerin, *Project Maven to Deploy Computer Algorithms to War Zone by Year's End*, DoD (July 21, 2017), https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/. Project Maven now includes detecting, classifying, and tracking objects within full motion video images (e.g., person, vehicle, and weapon) and other AI algorithms for text-based projects. *PE 0305245D8Z: Intelligence Capabilities and Innovation*, Office of the Secretary of Defense (Feb. 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/D/0305245D8Z_187.pdf.

[3] For example, the Army's Project Convergence exercise in September 2020 demonstrated use of AI at multiple stages of the targeting process. Jen Judson & Nathan Strout, *At Project Convergence, the US Army Experienced Success and Failure—and It's Happy About Both*, Defense News (Oct. 12, 2020), https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergence-the-us-army-experienced-success-and-failure-and-its-happy-about-both/. The Air Force has held similar exercises, most notably as part of its efforts associated with the Advanced Battle Management System—the technical infrastructure which will support the DoD's Joint All-Domain Command and Control concept. Theresa Hitchens, *ABMS Demo Proves AI Chops For C2*, Breaking Defense (Sept. 3, 2020), https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

[4] This includes the traditional process by which concepts of operation interact with technology development. Chapter 3 of this report offers recommendations to adapt this approach and ensure that technological advancements inform concepts as much as concepts drive technology development.

[5] As one observer has noted: "While DoD's investment accounts have grown substantially in the last three years, this growth has been highly concentrated in buying systems from existing production lines and doing prototypes of military systems." Testimony of Andrew Hunter, Director, Defense-Industrial Initiatives Group, CSIS, before the U.S. House of Representatives Armed Services Committee, *Hearing on DoD's Role in Competing with China* at 6 (Jan. 15, 2020), https://armedservices.house.gov/_cache/files/5/8/5818cc1f-b86f-4dca-8aee-10ca788e6f43/9F4A03ABF1DEAB747AF2D1302087A426.20200115-hasc-andrew-hunter-statement-vfinal.pdf.

[6] The National Defense Strategy highlights the importance of the National Security Innovation Base in maintaining the Department's technological advantage. *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. The Center for Strategic and International Studies offers a useful definition of the term, noting that the "[National Security Innovation Base] is a significant expansion in scope [...] compared to the traditional concept of the defense industrial base" and includes tech firms out of innovation hubs such as Silicon Valley, Boston, and Austin. See Andrew Hunter, *A Strategic Approach to Defense Investment*, CSIS (March 26, 2018), https://www.csis.org/analysis/strategic-approach-defense-investment.

[7] "The largest six prime defense suppliers (Lockheed Martin, Boeing, Northrop Grumman, Raytheon, General Dynamics, and BAE Systems) [...] represented 32 percent of all DoD prime obligations in 2019." *Fiscal Year 2020: Industrial Capabilities*, U.S. Department of Defense at 40 (Dec. 23, 2020), https://www.businessdefense.gov/Portals/51/USA002573-20%20ICR_2020_Web.pdf?ver=o3D76uGwxcg0n0Yxvd5k-Q%3d%3d.

[8] The strategy lays the foundation for the Department to treat data as a strategic asset and details the goals to make DoD data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept. 30, 2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

Chapter 2 - Endnotes

[9] In recent years the Department has made promising initial steps to establish managed services constructs for platforms, cloud infrastructure, and software development. For example, the Air Force's CloudOne and PlatformOne offerings (https://software.af.mil/dsop/services/); the Navy's Black Pearl (https://blackpearl.us/); and the Army's Coding Repository and Transformation Environment (CReATE). Further, the Office of the Secretary of Defense has built a data management platform, ADVANA, with the goal to establish it as the single authoritative source for audit and business data analytics. See Written Statement for the Record of David L. Norquist, Deputy Secretary of Defense before the U.S. Senate Armed Services Committee Subcommittee on Readiness at 6 (Nov. 20, 2019), https://www.armed-services.senate.gov/imo/media/doc/Norquist_11-20-19.pdf.

[10] Components of this platform are underway as a result of the Joint Artificial Intelligence Center (JAIC)'s Joint Common Foundation initiative—particularly the marketplace of shared AI resources including data, algorithms, and trained AI models.

[11] Use of a common technical infrastructure will vastly improve DoD's ability to ensure interoperability and increase the effectiveness of the joint force. However, it is important to note that even without such critical technical infrastructure, the Department is taking important policy steps to drive interoperability and AI readiness for programs designed to meet joint capability needs. See Aaron Mehta, *Hyten to Issue New Joint Requirements on Handling Data*, Defense News (Sept. 23, 2020), https://www.defensenews.com/pentagon/2020/09/23/hyten-to-issue-new-joint-requirements-on-handling-data/. Chapter 3 of this report outlines additional recommendations for achieving a state of military AI readiness by 2025.

[12] Secured access to data sets as well as other shared resources should be managed by user- and role-based authentication facilitated by an end-to-end identity, credential, and access management infrastructure.

[13] This hinges on implementation of the DoD's new data strategy. *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept. 30, 2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[14] These are platform environments with ready-made workflows that can be tailored and launched depending on user type (e.g., researcher, industry partner, operator) and use case (e.g., development, TEVV [test, evaluation, validation, and verification], fielding).

[15] In other words, the DevSecOps application lifecycle. "DevSecOps improves the lead time and frequency of delivery outcomes through enhanced engineering practices, promoting a more cohesive collaboration between Development, Security, and Operations teams as they work towards continuous integration and delivery." *Understanding the Differences Between Agile & DevSecOps—From a Business Perspective*, GSA (last accessed Jan. 1, 2021), https://tech.gsa.gov/guides/understanding_differences_agile_devsecops/.

[16] Stakeholders could include embedded development teams working at the tactical edge; private-sector partners contributing pre-trained models; academic researchers working on open, relevant challenge problems; government science and technology (S&T) researchers working within a service lab; or international partners co-developing interoperable AI capabilities.

[17] Shared AI resources should be managed with continuous Authorization to Operate (ATO) frameworks and with mandated default ATO reciprocity across the Department.

[18] Similar to or relying upon the platform delivery and features of Git (https://git-scm.com), GitHub (https://github.com), and GitLab (https://about.gitlab.com).

[19] The Pentagon acquisition office's Adaptive Acquisition Framework and Contracting Cone mark important steps by the Department to promote the use of alternate authorities for acquisitions and contracting. These include, for example, other transaction authorities, middle-tier acquisitions, rapid prototyping and rapid fielding, and specialized pathways for software acquisition.

[20] For example, the Air Force's Advanced Battle Management System (ABMS), which is managing systems intended to support the new Joint All-Domain Command and Control concept as a portfolio and based heavily on experimentation to drive innovation and an iterative approach to requirements. Notably, the Department of Defense Appropriations Bill for Fiscal Year 2021 expresses concern with various aspects of the Air Force's approach, including the "absence of firm requirements, acquisition

strategy, or cost estimate" and system of systems integration. See H. Rept. 116-453, at 294-295 (July 16, 2020), https://www.congress.gov/116/crpt/hrpt453/CRPT-116hrpt453.pdf.

[21] The term "digital innovation initiatives" is used here to describe the various entities across the Office of the Secretary of Defense and the military services––such as the Defense Innovation Unit (DIU), AFWERX, NavalX, and Army Applications Laboratory (AAL)––that are focused on bridging the gap with the commercial technology sector, especially startups and non-traditional vendors, and accelerating the delivery of best-of-breed technology solutions.

[22] The Defense Innovation Unit (DIU) is currently pursuing a number of AI projects to optimize business processes in the DoD, ranging from using AI-driven Robotic Process Automation to reduce labor costs for the Army Comptroller to improving Air Force readiness with AI-driven predictive maintenance and leveraging AI-constructed knowledge graphs to rapidly identify supply chain risks for the Defense Intelligence Agency. See *JAIC Partners with DIU on AI/ML Models to Resolve Complex Financial Errors*, JAIC (Oct. 1, 2020), https://www.ai.mil/blog_10_01_20-jaic_partners_with_diu_on_aiml_models_to_resolve_complex_finanical_errors.html; *U.S. Defense Department Awards C3.ai $95M Contract Vehicle to Improve Aircraft Readiness Using AI*, Business Wire (Jan. 15, 2020), https://www.businesswire.com/news/home/20200115005413/en/US-Defense-Department-Awards-C3.ai-95M-Contract-Vehicle-to-Improve-Aircraft-Readiness-Using-AI; *Accelerate.AI Accelerates Growth and Product Adoption with Defense Innovation Unit Contract*, Accrete.ai (April 23, 2020), https://blog.accrete.ai/newsroom/accrete.ai-wins-million-dollar-contract-with-the-defense-innovation-unit.

[23] As an example, DIU uses several acquisition pathways and contracting strategies that could help improve both the adoption and operational relevance of AI solutions and also expand the National Security Innovation Base. DIU pioneered the Commercial Solutions Opening with Army Contracting Command–New Jersey, which leverages section 2371b of title 10 U.S.C. Other Transaction authority to create a "fast, flexible, and collaborative" contract vehicle to prototype capabilities for the Department. DIU has also used Section 2374a of title 10 U.S.C. Prize Challenge authority to advance various AI-related priorities for DoD and the broader AI research community.

[24] The Department-wide digital infrastructure described above is critical to enabling this approach, but structural changes are also required to maximize its utility.

[25] There are notable examples of warfighter-technologist pairings within DoD, such as the Air Force's software factories and the forward-deployed tactical data teams used by Special Operations and Army Futures Command. They found that partnering technologists (such as data scientists) with operators or analysts at the tactical edge: 1) significantly reduces the time it typically takes a contractor to understand the problem set and deploy a solution; 2) incentivizes iterative development techniques and fast-fielding of minimum viable products that yield higher-impact solutions on an accelerated timeline; and 3) generates increased buy-in to data and AI technologies as critical mission enablers. NSCAI Engagements (Nov. 2020). To ensure U.S. forces maintain overmatch in the long-term, DoD must scale this user-centered development.

[26] Important offices for coordination with the JAIC include but are not limited to USD(R&E), USD Acquisition & Sustainment (USD(A&S)), Director Operational Test & Evaluation (DOT&E), and the DoD Chief Information Officer (CIO) and Chief Data Officer (CDO). Within USD(R&E), DIU is a key enabler of the JAIC that pursues a project-based approach by transitioning commercial prototypes for specific applications. The JAIC currently serves the Combatant Commands through its Component Mission Initiatives (CMIs), including a Mission Initiative for Joint Warfighting Operations. See *Mission Initiatives*, JAIC (last accessed Dec. 28, 2020), https://www.ai.mil/mi_joint_warfighting_operations.html.

[27] Such applications could be developed by other Combatant Commands, Service software factories, or the JAIC and discoverable via the recommended digital ecosystem. Each Combatant Command should ensure that the AI delivery teams are staffed with the appropriate talent to manage the full lifecycle of AI solutions, including in disciplines such as data science, AI testing and model training, software engineering, product management, and full stack development.

[28] As an example, both Army Futures Command (AFC) and Army Special Operations Command (USASOC) use a model known as "tactical data teams." This model brings AI/ML expertise forward to the field in the form of three- to six-person teams to build AI solutions for real-time operational problems. Executed by a small business, Striveworks, under contract with AFC and USASOC, they are currently supporting efforts in Central Command and Indo-Pacific Command Areas of Responsibility.

Chapter 2 - Endnotes

[29] Jim Garamone, *Chairman Discusses Future Defense Budgets*, U.S. Department of Defense (Dec. 3, 2020), https://www.defense.gov/Explore/News/Article/Article/2433856/chairman-discusses-future-defense-budgets/.

[30] *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 6 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[31] The Defense Science Board has proposed the level of 3.4% in the past to mirror typical practices in the private sector. *Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure*, Congressional Research Service at 12 (Oct. 7, 2020), https://fas.org/sgp/crs/natsec/R44711.pdf.

[32] The Future of Defense Task Force report similarly stated that "policy makers, industry, and the Pentagon must work together to identify trade-offs within the defense apparatus to include legacy systems and operations, which will allow for investment in technology and operational concepts to address future challenges." *Future of Defense Task Force Report 2020*, House Armed Services Committee at 18 (Sept. 23, 2020), https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/424EB2008281A3C79BA8C7EA71890AE9.future-of-defense-task-force-report.pdf.

[33] This should utilize wargaming, experimentation, and live-virtual-constructive environments wherever feasible, and should mandate interoperability with the digital ecosystem. This point echoes the Future of Defense Task Force, which recommended that every Major Defense Acquisition Program (MDAP) should be required "to evaluate at least one AI or autonomous alternative prior to funding." *Id.* at 7.