Hudson Institute

POLICY MEMO

Compiling Advantage: Unlocking the Competitive Power of Software Adaptability

ELLEN LORD
DAN PATT
Hudson Institute Center for Defense Concepts and Technology

March 2024

Introduction: A Call to Action

In an era of strategic competition among technologically advanced powers, software will shape the nature of deterrence and define national security advantages. Software is now ubiquitous, with powerful implications for economic productivity, governance, cybersecurity, and the character of modern warfare. From the systems that power our weapons platforms and command and control (C2) networks to the tools that enable our intelligence analysts and logisticians, software is now integral to every aspect of national defense. As the United States finds itself engaged in a long-term strategic competition with the People's Republic of China, America's success hinges on the US military's ability to rapidly adopt and adapt technology in response to evolving threats and opportunities. The Department of Defense (DoD) needs to harness the power of software to quickly assemble, effectively deploy, and continually update its military capabilities. If it fails to do so, America risks ceding the military advantage to its adversaries.

The central theme of this policy memo is the critical importance of software adaptability in enabling the DoD to outpace and outmaneuver its competitors. We argue that the ability to rapidly develop, deploy, and update software is not merely an enabler of military capabilities, but an emerging foundation of military advantage itself in the digital age. Adaptability is not an inherent feature of software; all too often we are victims of stale, outdated software that stands in the way of our desired outcomes. The DoD needs to carefully cultivate its ability to deploy, update, and integrate software and software-defined systems.

Despite the clear imperative for getting software right, the DoD faces a range of challenges and roadblocks that hinder

its ability to achieve this vision. In particular, the DoD needs to remove the bureaucratic bottlenecks of its mishandled Authority to Operate (ATO) process, shore up a lack of in-house technical expertise, facilitate easier access to data and interfaces, and reform inflexible resourcing processes that were built for an earlier era. These challenges are not merely technical in nature. Rather, they reflect deeper structural and cultural barriers that the US needs to address head-on to compete effectively with its adversaries.

This memo will explore the urgency of "getting software right" for the DoD.[1] The memo draws on insights from our testimony before the House Armed Services Subcommittee on Cyber, IT, and Innovation and our extensive interactions with the technology and broader defense communities.[2] We will identify the key roadblocks in the current system, highlight promising developments and best practices, and offer actionable recommendations for policymakers, DoD leadership, and industry partners to drive the necessary reforms.

The stakes could not be higher. If the DoD fails to prioritize adaptability in its software delivery and unleash the latent forces of innovation, the department could stumble into conflict equipped with brittle systems and be unable to respond effectively to sprawling and advanced threats. To fall short now would not be just a bureaucratic debacle. It would pose an imminent threat to the US military's ability to deter, fight, and win.

The Imperative for Adaptability

The military dimensions of long-term competition between the US and China depend on the DoD's evolution: its advancement through continuous move-counter-move cycles. America's success hinges on its ability to adopt and adapt technology rapidly in response to evolving opportunities and threats. Nearly every US system, both military and commercial, is powered by software. Therefore, *an upper hand in strategic competition necessitates getting software right*.

It is essential to understand the dual nature of software: fluid and frozen. During development, software is fluid— like wet potter's clay, it can be molded and adapted quickly by programmers adding new features, fixing bugs, and optimizing performance. However, once software is compiled and deployed, it becomes brittle and frozen—inflexible and only able to run on specific hardware configurations, severed from its source code and development environment.

Regrettably, the Department of Defense's mainline approach to software development and acquisition largely treats software as a frozen, finished product. This mindset is exemplified by the F-35 Joint Strike Fighter program. The F-35 program remains mostly locked in a "waterfall" development cycle for its core operational software.[3] This is a consequence of early program decisions that sought performance from a highly integrated system. The process of planning, testing, and delivering a new software block can take years, as evidenced by the lengthy progression from Block 3 to 3B to Tech Refresh 3 and Block 4.[4] While the newer blocks' capabilities may be impressive, the drawn-out process to achieve such capabilities severely hinders the US military's ability to adapt to emerging threats or seize fleeting opportunities to gain a tactical advantage. This is software done wrong—brittle and frozen, causing the DoD to field an unadaptable force.

Once a conflict begins, adaptability and scaling drive outcomes. The Pentagon needs to seize the current moment to prepare. For an example of how conflict drives adaptation, consider that the lifecycle of a radio in Ukraine is only about three months. By then, radios typically need to be reprogrammed or swapped out as the Russians have optimized their electronic warfare against them. A new weapons system reaches peak efficiency about two weeks before countermeasures emerge.

For an example of a superior weapons system handicapped by unadaptable software, consider that Excalibur precision

artillery rounds initially had a 70 percent efficiency rate when Ukraine first used them. After six weeks, Excalibur's efficiency declined to only 6 percent as the Russians adapted their electronic warfare to counter the system.[5] This shows how quickly adversaries can adjust to new technologies.

This lack of adaptability is not an inherent property of software; rather, it is a consequence of how we choose to manage software. Ukrainian units with organic programming capability that can rapidly adapt their unmanned aerial vehicle (UAV) software have about 50 percent efficiency, while units reliant on longer supply chains where feedback must be flowed back to an original manufacturer to make changes struggle to hit 20 percent efficiency. Keeping software in a pliant, fluid state is the only way to maintain tactical innovation.

Encouragingly, a handful of leaders inside the DoD are pioneering the kinds of practices the US needs. We can learn from their success. To exploit the fluid nature of software and unlock its potential for rapid adaptation, the department needs to embrace a fundamentally different approach.

This approach should be guided by five key principles:

a. lower the barriers to entry to get software and updates on operational systems and networks,

b. create a culture of *doers* by encouraging organic technical talent in the department and giving talented staff autonomy and flexible resourcing,

c. allow access to the department's vast troves of data by exposing system interfaces,

d. use contracts and agreements to invite a diverse community of partners and industry experts to participate in progress, and

e. adopt resourcing reforms that accommodate the continual nature of software development.

By removing bureaucratic barriers, the DoD can foster a culture of innovation and agility, and possibly unleash a new industrial base.

Challenges and Roadblocks

While the imperative for software adaptability is clear, the Department of Defense faces a range of challenges and roadblocks that hinder its ability to achieve this vision. These obstacles span the lifecycle of software development, from initial deployment to ongoing testing and acquisition, and are deeply rooted in the DoD's organizational culture, processes, and workforce. Years after the Defense Innovation Board (DIB) made key recommendations to the department in its software acquisition and practices (SWAP) study, implementation remains slow and incomplete.[6] Top-level department policy documents remain dreadfully out of date, not accommodating incremental refinement approaches.[7]

Software differs fundamentally from hardware systems in that the boundaries between development, acquisition, and operational usage are often blurred. In a hardware procurement scenario, such as purchasing body armor, the processes of specification, purchasing, and testing are generally distinct from the actual use of the items in the field. This separates the decision-makers involved with development from those involved with managing operational risk to missions or forces. In contrast, a software feature can be developed and immediately deployed to enable new functionality, and the decision to accept or forgo an update beyond a proven baseline must be weighed against the potential risks and rewards of mission success or failure.

This unique characteristic of software also complicates resourcing, as there is often no clear distinction between operations and maintenance (O&M) activities and research, development, test, and evaluation (RDT&E) activities. This paradigm similarly challenges classical approaches to test, evaluation, and risk management. As a result, the

consideration and management of operational risk become closely intertwined with feature development.

Unfortunately, DoD planners frequently overlook this crucial aspect, as there are strong incentives to adopt a compliance-first mindset. Acquisition personnel tend either to focus on meeting requirements as in a traditional hardware system without considering the potential missed opportunities to immediately impact mission outcomes; or to resist continuous software updates under the guise of maintaining security compliance. While security and risk management are undeniably paramount, a narrow focus on compliance can lead to a false sense of security and hinder the adaptability that is essential for mission success in a rapidly evolving threat landscape.

Roadblock 1: Granting Software Authority to Operate

The commercial software industry once treated software delivery much like a hardware product, placing disks in boxes on store shelves. Software was tested, shipped, and sold, with functionality and features frozen in time. Over time, consumers have grown accustomed to over-the-air updates, frequent patches, and app store delivery models. Even hardware products like cars and appliances are increasingly built to accept updates. While not all software in the Department of Defense needs constant updating, the mechanisms for update delivery will vary, and the risks for national security software differ significantly from those of a mobile app, the government can still learn much from the commercial technology industry. In particular, the shift to over-the-air updates was enabled by large-scale automation in testing, continuous integration and continuous delivery (CI/CD) pipelines, and an increasing focus on security throughout the development process.

Automated testing and in situ analytics have been game-changers in the commercial software industry. Likewise, CI/CD pipelines have played a crucial role in enabling rapid software delivery. These pipelines automate the process of building, testing, and deploying software, ensuring that every change goes through a rigorous validation process before being released to users. Moreover, like some forward-leaning defense organizations, risk-sensitive software developers are beginning to embrace a shift-left approach to security, where security considerations are integrated throughout the development lifecycle rather than being an afterthought. This includes practices like threat modeling, secure coding guidelines, and regular security audits, which all help to identify and mitigate potential security risks early on.

The process by which the Department of Defense decides whether software is safe to deploy and use on a system or network is called the Authority to Operate (ATO) process. Unfortunately, the mainline implementation of ATOs still treats software as though it were a boxed product. Though the ATO process was intended to ensure the security and reliability of software systems, it has instead become a bureaucratic bottleneck that slows down the deployment of new capabilities, stifles innovation, and aggravates security problems.[8] Currently, the process often involves lengthy reviews and documentation requirements that can take months or even years to complete, by which time the software may be outdated or no longer meet evolving mission needs.

Moreover, the ATO process has unintentionally created a new form of vendor lock-in, wherein companies that have successfully navigated the arduous process can use their ATO as a barrier to entry against competitors. This lock-in effect stifles competition and hinders the DoD's ability to tap into the latest innovations from across the commercial sector. Smaller, more agile companies with cutting-edge software solutions may be deterred from working with the DoD altogether due to the time and resource demands of the ATO process. Perhaps most shockingly, the DoD lacks ATO reciprocity within and between programs, services, and agencies, hindering the sharing of software platforms and rapid integration of capabilities,[9] which means that long timelines are not a one-time obstacle—they repeat as software is deployed onto one system after another.

Forward-leaning pioneers have created continuous ATO (cATO) processes and incorporated technology tools like CI/CD pipelines and continuous monitoring to improve overall risk posture.[10] Instead of focusing on one snapshot in time of software, cATOs focus on the process that delivers software. cATOs enable real-time, risk-based decision-making, significantly reducing deployment timelines for new and updated software capabilities. By implementing a DoD-wide cATO framework and establishing mechanisms for ATO reciprocity, the DoD can streamline the authorization process and facilitate the sharing of software platforms and components across the enterprise. But moving in this direction would require a cultural shift within the DoD: the department would need to emphasize risk management over risk elimination and move from a mindset of compliance to one that looks to mission outcomes and operational security.

Roadblock 2: Resourcing

Another major roadblock to software adaptability is the DoD's struggle to allocate resources effectively and respond quickly to evolving software needs.[11] The department's budgeting and acquisition processes are still largely geared toward traditional hardware programs with rigid requirements and long lead times. This mismatch makes it difficult for software development teams to secure the funding and support they need to iterate rapidly and deliver capabilities in a timely manner. As a result, promising software initiatives may languish or fail to scale, while legacy systems continue to consume a disproportionate share of DoD resources.

The inability to use a single appropriation to fund software improvements creates significant management challenges for business system upgrades, as illustrated by the case of the Defense Enterprise Accounting and Management System (DEAMS).[12] When DEAMS had technical issues that needed a software patch, financial managers and attorneys had to spend considerable time determining which parts of the patch represented a capability upgrade (RDT&E funded) versus basic sustainment (O&M funded) even though this distinction is meaningless to the software developer. The funding realignment process delayed execution and put added pressure on the program because O&M funds were nearing expiration.

The fiscal year (FY) 2020 National Defense Authorization Act (NDAA) and appropriations bills established a new Budget Activity 8 (BA-8) appropriation for software. The DIB SWAP study recommended this new appropriation to provide the DoD greater flexibility in funding software development, deployment, and sustainment. However, the BA-8 pilot has faced implementation hurdles and has not expanded beyond the original eight programs. Key personnel who championed the initiative have departed, and the program never delivered rigorous metrics regarding its implementation and effectiveness to appropriators, hindering its wider adoption.

The recent report from the congressionally directed Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform offers a simpler and more comprehensive approach to address these resourcing challenges.[13] The commission recommends transforming the budget structure by allocating funding first to programs and then delegating the management of funds across funding categories (RDT&E, O&M, procurement, etc.) to individual program managers (PMs), while still ensuring strong accountability. This approach would provide PMs with the flexibility to allocate resources based on the specific needs of their software programs, enabling faster responses to evolving requirements and technologies. However, the implementation of this systemic solution will require cooperation between the executive and legislative branches and may not happen quickly.

Roadblock 3: Talent Gaps

A severe talent deficit within the DoD's software workforce compounds these challenges. The department struggles to attract and retain top digital talent because it competes with the private sector for a limited pool of skilled professionals.[14]

Government hiring processes can be slow and cumbersome, often taking six to eight months to onboard a highly qualified candidate, even when agency leaders are fully supportive. Also, the DoD's bureaucratic culture and rigid career paths may strip away the job autonomy needed to recruit and retain talented technical leaders into important roles. This talent gap leaves the DoD without the in-house expertise it needs to manage software programs effectively, make informed technical decisions, and drive innovation.

Moreover, acquisition personnel receive insufficient training on the software acquisition pathway, the diverse means of contracting, commercial practices in software, the differences in requirements between software and hardware, and the nature of ATOs and who should be responsible for them. This knowledge gap further hinders the DoD's ability to effectively acquire and manage software programs.

Roadblock 4: Data

Finally, there are persistent misconceptions and knowledge gaps within the DoD around key software concepts such as data rights, interface rights, and the appropriate role of industry in the software innovation process. These misunderstandings can lead to suboptimal contracting strategies, intellectual property disputes, and a lack of effective collaboration between government and industry stakeholders. For example, the DoD may mistakenly pursue a strategy of seeking to own all software source code, rather than focusing on owning the right application programming interfaces (APIs) and other interfaces to ensure interoperability and avoid vendor lock-in.[15]

There is also increasing attention on the coming impact of artificial intelligence (AI). Many expect that AI will increase overall economic productivity, enhance the efficiency of the defense workforce, and directly deliver military capability advantages. But it is important to remember that the DoD can only realize the promise of AI under the right conditions. The first condition is the aforementioned ability to deploy software updates quickly and securely, because data structures and AI-enabled tools depend on frequent updates to remain relevant and accurate. *We cannot lead in AI if we do not get software right*.

The second condition is increased access to data. To train mission-oriented models effectively, software developers need both one-time and ongoing access to libraries of mission-relevant data. This access can be granted in a secure manner that is consistent with today's government security standards. Providing a readily available corpus of relevant data is a necessary condition to create a vibrant ecosystem of software providers. It is also a key incentive for private capital, founders, and employees to enter the defense market. Even as the DoD ensures that industry can hold intellectual property rights to software and algorithms, decision-makers need to make sure that system interfaces and the data that flows across them can support mission needs. With increasing emphasis on joint operations, the department needs to break down its data and system silos between disparate services and program offices.

Addressing these challenges and roadblocks will require a concerted effort from DoD leadership, policymakers, and industry partners. It will involve streamlining bureaucratic processes, updating acquisition strategies, investing in workforce development, and fostering a culture of experimentation, doing, and calculated risk-taking. While daunting, these reforms are essential if the DoD is to harness the full potential of software for adaptive military advantage in an era of strategic competition.

Promising Developments and Best Practices

Amid the roadblocks the Department of Defense faces in its pursuit of software adaptability, there are also reasons for optimism. In recent years, the DoD has taken important steps to improve its software acquisition and development practices, and pockets of excellence have emerged across the services that offer valuable lessons and models for success. Legislation or process alone cannot drive exceptional outcomes; it is

important to recognize the creativity and ingenuity of the department's leaders and seek to amplify and replicate their success.

Conventional acquisition processes emphasize trying to get up-front predictions right: requirements, system specifications, schedules, and cost estimates. Decades ago, in commercial development, problems with estimation were well acknowledged because software development is inherently non-routine work;[16] it is instead a matter of ongoing creative problem-solving. But modern development methods have offered new ways to solve these problems. Acquisition officials now use a suite of tools and tactics to replace monolithic estimation that includes prototyping, breaking work down into small tasks, and setting intermediate milestones.

Officials are also better able to monitor progress thanks to milestones, burndown charts, and even agile management tasks.[17] But technology alone does not guarantee good outcomes and even good programs can fall victim to hype-driven quick-fixes—using Kubernetes, getting on the cloud, consolidating to one software factory, pursuing agile development, or simply hiring Silicon Valley, for example. Each of these is a great tool, but none are one-size-fits-all solutions.[18] To navigate the complexity of software acquisition to fulfill specific program requirements, officials need judgment and organic technical talent.

One of the most significant developments has been the establishment of the Adaptive Acquisition Framework (AAF).[19] The AAF represents a major shift in the DoD's approach to acquisition, moving away from a one-size-fits-all model toward a more flexible, tailored approach that recognizes the unique characteristics of individual acquisition programs. The framework includes a dedicated software acquisition pathway as outlined in DoD Instruction 5000.87 and promoted by the FY2020 NDAA and the DIB SWAP study,[20] which emphasizes the use of modern development practices, including DevSecOps,[21] and encourages greater collaboration between government and industry.

The AAF is a crucial step in the right direction, but its impact will depend on how effectively it is implemented across the DoD. To date, the adoption of the framework has been uneven, with some organizations moving quickly to embrace its principles and others lagging. Only about 50 efforts across the department are using it to date,[22] and it is often viewed as unconventional or high-risk. It will be important for DoD leadership to continue to prioritize and incentivize the use of the AAF, and provide organizations the necessary resources, education, and support to enable its success.

Encouragingly, there are pockets of excellence within the DoD where forward-leaning leaders are already putting these principles into practice. The Navy's Program Executive Office for Digital and Enterprise Services (PEO Digital) is restructuring its portfolio to deliver on modern metrics like adaptability, resilience, time lost, and cost per user. The program created a World Class Alignment Metrics (WAM) framework,[23] an industry best practice for better evaluating information technology (IT) investment and performance by connecting data to mission outcomes. The WAM framework translates technical and business metrics into outcomes important to the mission, enabling decision-makers at every level to make better-informed IT investment decisions that enhance customer experience and operational resilience, ultimately improving overall warfighting readiness. WAM also previews an alternative oversight mechanism. Instead of leaning only on milestone delivery status, metrics like WAM's can shape investments and make sure that appropriated funds are delivering the mission outcomes we need.

The Navy's PEO for Integrated Warfare Systems (PEO IWS) is similarly leading the way. The office has already stood up a software factory,[24] and it is working on a cATO process, opening up systems interfaces, implementing Modular Open

Systems Architecture (MOSA) acquisition models,[25] using digital twins to enable federated software development, and pioneering a portfolio management approach across its more than 140 constituent programs. PEO IWS is the poster child for resourcing flexibility. As the PPBE commission's recommendations around appropriation categories and portfolio management highlight, such flexibility is essential to create adaptability in combat capability.[26] Bit by bit, the Navy is moving closer to something like an app store model for deployment. For example, Project Overmatch and the Naval Command and Control Systems Program Office (PMW 150) oversaw the first ever over-the-air installation of a software element of a major acquisition program to a US Navy ship in FY2023, followed weeks later by the first over-the-air update.[27] While PMW 150's progress looks humble to begin with, there is reason to believe these developments can be scaled significantly.

In the Air Force, the original Advanced Battle Management System (ABMS) got off to a rough start, focusing more on demonstrations than solving the underlying problems associated with building and evolving modern battle networks.[28] But in recent years, the ABMS Cross-Functional Team has demonstrated a modern approach to requirements for adaptable capability. The program has well-vetted top-level needs and continuous measurements for assessing progress, but is careful not to over-specify solutions.

On the execution side, the PEO for Command, Control, Communications, and Battle Management (PEO C3BM) is pioneering a more adaptable way to build out complex battle networks and decision aids.[29] It has invested in accredited digital infrastructure and takes a modular approach. For example, it is deploying Tactical Operation Center-Light (TOC-L) kits as a basic building block for C2 infrastructure. The program's goal is to deploy simple, proven technologies first, starting from a foundational level, then iterate and scale up to more complex capabilities over time, allowing systems to adapt more quickly to operational needs.[30] PEO C3BM's approach takes inspiration from a systems theory principle called Gall's Law.[31] This principle suggests that complex systems that work invariably evolve from simpler systems that worked.

It is important for oversight bodies in Congress, the services, and the Office of the Secretary of Defense (OSD) to not simply hold programs accountable for fulfilling initial predictions, but to assess whether programs demonstrate effective learning and adaptation. The Air Force's Kessel Run, with its software factory, was an early pioneer that delivered remarkable accomplishments.[32] But it also fell victim to marketing hype, including with an early choice of development platform. To its credit, Kessel Run recognized this architectural misstep and course corrected. In another instance, the insights of highly talented technical personnel that Kessel Run brought in on a rotational tour of duty helped save the effort millions of dollars by identifying and averting a key architectural error. As Kessel Run shows, the path to success for software programs rarely follows an initial plan, but rather requires continuous learning, identification of issues, and adaptation as needed. Overseers should look for this type of demonstrated learning and responsiveness and hold it up as a positive example. Such a mindset mirrors the safety culture found in Air Force flight debriefings or civil aviation, where the focus is on honestly surfacing problems and learning from them rather than assigning blame.[33]

The Army, whose reform efforts are led by its deputy assistant secretary for strategy and acquisition reform, has just marked a significant shift in how it approaches software development and deployment. This is indicated by the force's sweeping new policy, Enabling Modern Software Development and Acquisition Practices.[34] The policy's most important aspect may be that—like the Air Force's ABMS effort— it seeks to change how requirements are written. The policy shifts software acquisitions to broad Capability Needs Statements (CNSs) and Software-Initial Capabilities Documents (SW-ICDs),

which allow for iterative refinement as software development progresses. It also shifts more resource allocation authority to individual program managers and recognizes the need for continuous improvement and development throughout a system's lifecycle, including during sustainment. Finally, the policy seeks to broadly scale these practices and set new norms across a wide range of software development efforts, as it is applicable to "all [software development] efforts executed across the Army."

Inside the OSD, the deputy assistant secretary of defense for acquisition integration and interoperability (AI2) in the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) is leading by example, demonstrating how to quickly implement the software acquisition pathway for joint programs, using the AAF for evolving requirements alongside development, and facilitating faster delivery of capabilities to warfighters.[35] This effort broke records by completing a draft SW-ICD in weeks and securing Joint Capabilities Board validation just a few weeks later. This is not only a model for software development, but for joint capability acquisition in general.

The Department of Defense is taking the data and data access problem increasingly seriously. It recently stood up the new role of chief digital and artificial intelligence officer (CDAO) as a principal staff assistant. This office is new but has the potential to break down data silos, ensure that system interfaces are exposed and made broadly available across program offices, and enable a broad community of government and industry partners to integrate data and build powerful applications—including those using artificial intelligence—on these robust assets. By building on Advana's success in exposing data broadly, [36] The CDAO can develop data repositories or libraries with the right safeguards to substantially increase the speed with which companies can develop data analysis software and improve such products' abilities to produce accurate, meaningful analysis to inform mission decisions.[37]

Congress directed the CDAO to "develop and report on an actionable plan for the deputy secretary to reform the technologies, policies, and processes used to support accreditation and authority to operate decisions to enable rapid deployment into operational environments of newly developed government, contractor, and commercial data management, artificial intelligence, and digital solutions software."[38] This direction is well placed, as the office of the CDAO is home to the most prolific authorizing official (AO) in the Department of Defense. The CDAO's AO has already completed more than 2,000 authorizations, with a typical timeline of 6 weeks instead of a typical 12-month cycle.[39] By contrast, some AOs at the Defense Information Systems Agency (DISA) are limited to approving only 12 systems a year. The department already has innovative, effective personnel driving positive changes. The DoD needs to figure out how to amplify their efforts, hold them up as models, and train others to follow their path.

These successful leaders and teams demonstrate that, even within the constraints of the current system, the DoD can achieve significant improvements in capability adaptability by keeping software fluid and allowing software developers to refine capability based on operational feedback. By embracing modern development practices, fostering close collaboration with industry, managing risk continuously, and empowering software teams to iterate rapidly, these organizations have been able to deliver real value to the warfighter at a pace that would have been unthinkable just a few years ago.

Looking ahead, it will be important for the DoD to build on these successes and scale them across the defense enterprise. This will require continued leadership and investment in software innovation and a willingness to experiment with new models and approaches. It will also require a concerted effort to capture and share best practices across the DoD so that more organizations can replicate and adapt successful models to meet the unique needs of their mission areas.

By learning from these promising developments and best practices, the DoD can begin to chart a path toward a more adaptable, software-driven future. While the challenges are significant, the potential benefits—increased agility, responsiveness, and operational effectiveness—are too great to ignore.

Key Recommendations

To overcome software adaptability's challenges and build on its promising developments, the Department of Defense needs to take bold action across several key areas. The following recommendations are designed to accelerate the DoD's progress and address the most pressing needs and opportunities for reform.

a. Enable personnel to rapidly deploy and update software.

The DoD should prioritize efforts to streamline the software deployment process and enable more rapid updating of software capabilities in the field. A key part of this effort will be to reform the ATO process. The DoD should move ATOs from a static, compliance-based model to a continuous, risk-based approach. This will require close collaboration between software development teams, cybersecurity experts, and operational commanders to ensure that software is deployed quickly and securely while also meeting mission needs. In particular, the department should make the following changes, which are within existing law:

Encourage accountability for authorizing officials around ATO approvals. The DoD's chief information officer (CIO) can and should collect data cataloging all active AOs across the department, their approval throughput rates and timelines, and the portions of their ATOs that are continuous by design and have modern risk management features.

Establish a DoD-wide cATO framework. The DoD should broadly implement cATO frameworks and guidance to continuously manage risk. The department should leverage automation, standardize security controls and practices, and—combined with the training below—reduce deployment timelines significantly for new and updated software capabilities.

Establish an ATO accelerator program. The DoD should fund a project wherein the most prolific AOs in the department develop a curriculum to educate other AOs on high-throughput, risk-centric, agile best practices in the authorization ecosystem.

Champion ATO reciprocity within and between DoD programs, services, and agencies. This would enable the sharing and reuse of software platforms, components, and infrastructure across systems and networks. This would facilitate rapid integration of capabilities across platforms and military services. The department should move to a *default yes* posture for reciprocity and fund the development of a reciprocity playbook that establishes norms and standards.

b. Attract and empower top technical talent and foster a culture of *doers*.

To drive software innovation and adaptability, the DoD needs to attract and retain top technical talent from across industry and academia. While the DoD can outsource coding, it cannot outsource all the thinking or technical competence needed to structure a successful acquisition and development process. This will require a multifaceted approach that includes reforming the hiring process, ensuring that talented hires have autonomy in their roles, creating more flexible career paths, and providing employees with opportunities for continuous learning and development.

The Department of Defense has demonstrated that it can compete to hire great talent. In particular, the tour of duty approach, which the Defense Advanced Research Projects Agency (DARPA) and Kessel Run have used to bring in industry

talent on a temporary basis, has proven highly effective for sourcing personnel to contribute to specific projects. The limited term of the appointment motivates these temporary hires to make an impact before the clock runs out and pushes them toward action and accountability. Additionally, the fluidity between private and public sectors brings in fresh perspectives and cutting-edge familiarity with commercial trends.

The DoD needs to foster a culture of *doers* by encouraging accountability and pride in outcomes at the individual level. Below are three strategies to help do so:

Expand existing authorities that enable a tour of duty program. The DoD should widely adopt term appointments like highly qualified expert (HQE) positions and hold human resources (HR) organizations accountable for quick hiring. Organizations should be empowered to temporarily convert some permanent billets to term positions using tools like DARPA's 10 U.S.C. § 1109 "direct hire authority" to encourage personnel rotation.[40]

Overhaul performance evaluation. HR departments across the DoD should reform evaluation and promotion criteria for digital and technical roles to reward rapid delivery, user impact, experimentation, and continuous improvement rather than solely compliance with bureaucratic processes. The department should also create fast-track promotion opportunities for high performers.[41] Moreover, the DoD should explore ways to streamline its hiring processes and reduce time-to-hire from months to weeks. This may require the department to comprehensively review the current process, eliminating unnecessary steps and leveraging automation where possible. But by creating a more agile and responsive hiring system, the DoD can better compete with the private sector for top talent.

Invest in training and development for acquisition professionals. Training innovation needs to keep pace with software innovation. The DoD should ensure its officers have the skills to implement the full spectrum of acquisition approaches and rapidly acquire software. The Defense Acquisition University (DAU) and other training organizations should expand their programs to emphasize procuring nontraditional and emerging technologies. Training programs should also utilize case studies and experiential learning to demonstrate how procuring software differs from procuring hardware and how working with small businesses differs from contracting with large defense primes.

c. Prioritize APIs and data accessibility.

The DoD should prioritize exposing the APIs and interfaces of its existing systems and, in accordance with the law, require that developers of new systems publish their APIs and interfaces as well. This would facilitate greater software adaptability, enable the composition of new tactics and operational concepts, unlock the power of data, and accelerate the development of AI capabilities. The DoD can no longer treat software like a hardware deliverable; it needs to embrace the fact that each component is part of a larger ecosystem of interacting elements. Greater accessibility would unleash a new industrial base to create the foundation for innovation in AI and machine learning applications. Specifically, the DoD should:

Establish clear guidance and best practices for API development and management. This effort should focus on exposing interfaces in machine-readable form and widely distributing them. The department should then propagate this guidance to PEOs, PMs, and contracting officers.

Publish comprehensive data catalogs that document key DoD data sources, data types, schemas, and APIs. The department should make these catalogs available to qualified users across the DoD, industry, and research community via platforms like Advana.

Broadly educate the acquisition and contracting workforce on MOSA.[42] MOSA sets standards for interface definition and API delivery, and many acquisitions professionals and contracting officers would benefit from a greater understanding

of it. The DoD should also update contract deliverables to move away from the *boxed software* model of delivery.

Stand up one or more centralized repositories for key interfaces, associated documentation, and reference implementations. Section 804 of the FY2021 NDAA explicitly called for the creation of these "interface repositories." Yet they still have not been implemented.

Work with industry partners to ensure that critical interfaces are well-documented, secure, and scalable to enable continuous evolution and integration. The single best method for doing this is to create and share reference applications that use interfaces and link them together with other data, creating clear and unambiguous linkage between data types.

d. Embrace a diverse, software-centric industrial base.

The DoD needs to work to foster a more diverse, software-centric industrial base that can support its needs for adaptable, innovative software capabilities. America's future industrial base needs will not be met by adding one more prime contractor. Washington needs to tap into a diverse base of hundreds or thousands of companies that have specialized capabilities that can be brought to bear.

There are cases where the DoD can and should meet its needs directly with commercial software solutions. When the department can clearly frame a need with a service level agreement (SLA), it should leverage readily available commercial offerings using the software as a service (SaaS) model. An SLA is a contract between a service provider and a customer that specifies the level of service expected, usually in terms of quality, availability, and responsiveness.[43] For example, a contract for a weather data feed could stipulate 99.9 percent uptime of 90 percent global temperature coverage, among other things.

Where needs are still too uncertain to accommodate such a framing, the DoD should not over-specify a requirement. The department should instead work with its industrial partners to gradually understand the intersection between technical feasibility and mission needs and develop high-value solutions. While some use cases may merit special consideration, the DoD should generally prioritize maintaining access to interfaces (to ensure interoperability) and avoiding vendor lock-in over seeking to own all software source code. This approach allows for a more collaborative relationship with industry partners, where requirements can be iteratively refined based on feedback and technological advancements.

These changes are already within the scope of existing law, but they require that the department commits to a sustained effort to drive change and position itself to harness the full potential of software for adaptive military advantage.

e. Adopt recommended resourcing reforms.

Finally, the DoD needs to strengthen available tools and establish new acquisition and budgetary tools that shorten the cycle time to develop and approve software projects, with automated reporting and review to enhance oversight.

The final report from the PPBE commission makes multiple recommendations that would support faster software fielding. These recommendations, if implemented, will have a broader impact than just software. The commission's report recognizes the need for resourcing speed and agility given the reality of ever-increasing geopolitical threats and the acceleration of emerging technologies.

These PPBE recommendations acknowledge that PEOs and PMs need the agility to insert new technology and move modest amounts of funds in the year of a program's execution. In addition, they recognize that PEOs and PMs would benefit from the ability to roll over small budget excesses into the following year. The recommendations also acknowledge that the misalignment of funding to appropriation category often delays program execution. Specifically, the commission recommends

allowing procurement, RDT&E, or O&M funding to be used for the full cycle of software development, acquisition, and sustainment. Currently, costs and schedules are preset to hardware-centered regulations and processes that are mismatched to the speed of delivery needed for relevant software.

Conclusion

The United States stands at a critical juncture in its pursuit of military superiority in an era of strategic competition. While America still possesses the world's most formidable military, Washington's current approach to software development and acquisition threatens to undermine that advantage.

Policymakers hold the map to a better way forward. The Department of Defense already has a handful of forward-leaning trailblazers who have succeeded amid organizations and processes built for a bygone era. But the US military need not be the victim of an industrial-age approach to digital-age capabilities. DoD leaders can learn from these trailblazers' successes, amplify their efforts, and scale their models across the department.

The stakes could not be higher. If Washington fails to transform its approach to software, it risks ceding the advantage to its adversaries and losing the ability to compete effectively in the long-term strategic competition ahead. But if the DoD embraces the power and fluidity of software, empowers its workforce, and builds the technical and institutional foundations for adaptability, the US has the opportunity to out-innovate, out-adopt, out-scale, and out-compete would-be aggressors for decades to come.

Appendix: Abbreviation List

AAF: Adaptive Acquisition Framework

ABMS: Advanced Battle Management System

AI: Artificial intelligence

AI2: Acquisition integration and interoperability

AO: Authorizing official

API: Application programming interface

ATO: Authority to Operate

BA-8: Budget Activity 8

C2: Command and control

cATO: Continuous Authority to Operate

CDAO: Chief digital and artificial intelligence officer

CI/CD: Continuous integration and continuous delivery

CIO: Chief information officer

CNS: Capability Needs Statement

DARPA: Defense Advanced Research Projects Agency

DAU: Defense Acquisition University

DEAMS: Defense Enterprise Accounting and Management System

DIB: Defense Innovation Board

DISA: Defense Information Systems Agency

DoD: Department of Defense

FY: Fiscal year

HQE: Highly qualified expert

HR: Human resources

IT: Information technology

MOSA: Modular Open Systems Architecture

NDAA: National Defense Authorization Act

O&M: Operations and maintenance

OSD: Office of the Secretary of Defense

OUSD (A&S): Office of the Under Secretary of Defense for Acquisition and Sustainment

PEO: Program Executive Office

PM: Program manager

PPBE: Planning, Programming, Budgeting, and Execution

RDT&E: Research, development, test, and evaluation

SaaS: Software as a service

SLA: Service level agreement

SWAP: Software acquisition and practices

SW-ICD: Software-Initial Capabilities Documents

TOC-L: Tactical Operation Center-Light

UAV: Unmanned aerial vehicle

US: United States

WAM: World Class Alignment Metrics

Endnotes

1 *CITI Hearing: Too Critical to Fail: Getting Software Right in an Age of Rapid Innovation before the House Armed Services Committee*, 118th Cong. (2024), https://armedservices.house.gov/hearings/citi-hearing-too-critical-fail-getting-software-right-age-rapid-innovation.

2 See, for example, "Software in Defense Coalition," LinkedIn, https://www.linkedin.com/company/software-in-defense-coalition/; "Our Partners," Software Factory Ecosystem Coalition, https://coalition.dso.mil/partners/; "Commission on Software-Defined Warfare," Atlantic Council, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/forward-defense/commission-on-software-defined-warfare/.

3 A "waterfall" system of development is one wherein aspects of software cannot be amended after a certain stage of development. See Ben Lutkevich and Sarah Lewis, "Waterfall Model," TechTarget, November 2022, https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model.

4 Consider the delays in Technology Refresh 3 (TR-3), the crucial enabler for Block 4 modernization that provided the F-35 with the necessary computational power. However, its delivery faced delays due to challenges in hardware and software development and the testing of the Integrated Core Processor (ICP), documented in: *F-35 Lightning II Joint Strike Fighter Program: December 2022 Selected Acquisition Report (SAR)* (Arlington, VA: Department of the Navy, December 2022), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/FY_2022_SARS/F-35_SAR_Dec_2022_25_July_2023.pdf.

5 This and other examples from the conflict in Ukraine are sourced from Dr. Jack Watling of the Royal United Services Institute, who is a leading scholar on technological trends in land warfare. See "Russia Is Starting to Make Its Superiority in Electronic Warfare Count," *The Economist*, November 23, 2023, https://www.economist.com/europe/2023/11/23/russia-is-starting-to-make-its-superiority-in-electronic-warfare-count.

6 J. Michael McQuade et al., *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Alexandria, Virginia: Defense Innovation Board, May 2019), https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF; *Software Acquisition: Additional Actions Needed to Help DOD Implement Future Modernization Efforts* (Washington, DC: Government Accountability Office [GAO], April 2023), GAO-23-105611, https://www.gao.gov/products/gao-23-105611.

7 *Defense Software Acquisitions: Changes to Requirements, Oversight, and Tools Needed for Weapon Programs* (Washington, DC: GAO, July 2023), GAO-23-105867, table 4, https://www.gao.gov/products/gao-23-105867.

8 For example, ATOs focus on obtaining system authorizations but fall short in implementing continuous monitoring of risk once authorization is reached. See David W. McKeown, "DoD Memorandum for Senior Pentagon Leadership: Continuous Authorization to Operate (cATO)," Office of the Secretary of Defense, February 3 , 2022, https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF.

9 McQuade et al., *Software Is Never Done; Software Acquisition,* GAO-23-105611.

10 These are usually based on NIST SP 800-160 and practices of systems/systems security engineering, which are cybersecurity and resiliency enablers, throughout the system development lifecycle (SDLC). See Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (Gaithersburg, MD: National Institute of Standards and Technology, December 2021), https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final.

11 See William Greenwalt and Dan Patt, *Competing in Time: Ensuring Capability Advantage and Mission Success through Adaptable Resource Allocation* (Washington, DC: Hudson Institute, February 2021), https://www.hudson.org/national-security-defense/competing-in-time-ensuring-capability-advantage-and-mission-success-through-adaptable-resource-allocation.

12 This example is from Ellen Lord and Robert Hale, *Defense Resourcing for the Future* (Alexandria, VA: Commission on Planning, Programming, Budgeting and Execution Reform, March 2024), section V, https://ppbereform.senate.gov/wp-content/uploads/2024/03/Commission-on-PPBE-Reform_Full-Report_6-March-2024_FINAL.pdf.

13 Lord and Hale, *Defense Resourcing*. It is also notable that legislators in the Fiscal Year 2024 defense appropriation bill included "FA 281A" which permits combining RDT&E dollars with procurement dollars on certain projects.

14 *Software Acquisition*, GAO-23-105611, 32.

15 See William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2020), section 804, https://www.congress.gov/bill/116th-congress/house-bill/6395; this section mandates exposed system interfaces and extends the preexisting Modular Open Systems Architecture (MOSA) law: Requirement for Modular Open System Approach in Major Defense Acquisition Programs, 10 U.S.C. § 4401 (2024), https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section4401&num=0&edition=prelim.

16 See, for example, the famous treatise on software *The Mythical Man-Month*, which states that estimation techniques "reflect an unvoiced assumption that is quite untrue; i.e.: that all will go well." The author also notes issues of effort being confused for

progress (the assumption that months and man-months are interchangeable), that progress is difficult to monitor, and that managers are impatient. Frederick P. Brooks Jr., *The Mythical Man-Month: Essays on Software Engineering* (Boston, MA: Addison-Wesley, 1975),15–36.

17 See an excellent overview of this progress: Gergely Orosz, "What Changed in 50 Years of Computing: Part 1," The Pragmatic Engineer (blog), March 12, 2024, https://newsletter.pragmaticengineer.com/p/what-changed-in-50-years-of-computing.

18 See extended discussion on the diversity of needs of different kinds of national security software in Jason Weiss and Dan Patt, *Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era* (Washington, DC: Hudson Institute, December 2022), https://www.hudson.org/national-security-defense/software-defines-tactics-structuring-military-software-acquisitions.

19 For an overview of the various pathways in the AAF and its history, see "Adaptive Acquisition Framework Pathways," DAU, https://aaf.dau.edu/aaf/aaf-pathways/.

20 For an excellent overview of the software acquisition pathway, including statute, policies, guidance, and other resources, see "Software Acquisition," DAU, https://aaf.dau.edu/aaf/software/; Ellen Lord, "DoD Instruction 5000.87: Operation of the Software Acquisition Pathway," Department of Defense, October 2, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF; Section 800 of the FY2020 NDAA mandated that the Department of Defense develop a software acquisition pathway following recommendations. National Defense Authorization Act for Fiscal Year 2022, S. 1605, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1605.

21 DevSecOps is the integration of security, software development, and software operations into a continuous cycle, with security baked in as a forethought, and feedback from operations informing development priorities.

22 "As of February 2023, DOD was tracking 49 programs using the software acquisition pathway." From *Weapon Systems Annual Assessment: Programs Are Not Consistently Implementing Practices That Can Help Accelerate Acquisitions* (Washington, DC: GAO, Jun 2023), GAO-23-106059, 20, https://www.gao.gov/products/gao-23-106059.

23 "Memorandum: Leveraging World Class Alignment Metrics," Department of the Navy Chief Information Officer, March 7, 2024, https://www.doncio.navy.mil/ContentView.aspx?id=16683.

24 See Kirsten Errick, "Several Navy PEOs Put Personnel First in Modernization Efforts," Federal News Network, October 27, 2023, https://federalnewsnetwork.com/navy/2023/10/several-navy-peos-put-personnel-first-in-modernization-efforts/.

25 See "MOSA: DAU Glossary Definition," DAU, https://www.dau.edu/acquipedia-article/modular-open-systems-approach-mosa.

26 See Lord and Hale, *Defense Resourcing*, 83, section V, recommendation 11, "Address Challenges with Colors of Money": "It is very difficult to predict the exact ratio of RDT&E and O&M funding that will be required when building the budget, due to the unforeseen challenges that arise in the development and sustainment of a business system. In FY 2023, a software patch was needed to address technical issues on the program. Financial managers and fiscal attorneys spent considerable time assessing and determining which parts of the patch represented a true upgrade in capability (RDT&E funded) vice basic sustainment (O&M funded), even though there is no such distinction to the software developer. A realignment of funding was required to fully fund the software patch, creating execution delays and further pressure on the program since O&M funds would soon be expiring."

27 "Tear Sheet," Naval Command and Control Systems Program Office (PMW 150), May 1, 2023, https://www.peoc4i.navy.mil/Portals/98/Documents/Tear-Sheets/2023_PMW%20150_Tear%20Sheet.pdf?ver=VTpy7S0zRS6ePS1wblcdJw%3D%3D.

28 See, Valerie Insinna, "New US Air Force Secretary to Shake Up Advanced Battle Management Program," *Defense News*, August 19, 2021, https://www.defensenews.com/air/2021/08/19/new-us-air-force-secretary-to-shake-up-advanced-battle-management-program/; and *Defense Acquisitions: Action Is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System* (Washington, DC: GAO, April 2020), https://www.gao.gov/products/gao-20-389.

29 Kimberly Underwood, "Special C3BM Air Force Team Takes on JADC2," *Signal*, May 22, 2023, https://www.afcea.org/signal-media/defense-operations/special-c3bm-air-force-team-takes-jadc2.

30 Mikayla Easley, "Cropsey: Air Force C2 Modernization 'Hamstrung' by Lack of Fiscal 2024 Budget," *DefenseScoop*, February 14, 2024, https://defensescoop.com/2024/02/14/air-force-cropsey-c3bm-c2-budget/; Greg Hadley, "DAF Outlines a New 'Battle Network' as Its Contribution to JADC2," *Air and Space Forces*, March 23, 2023, https://www.airandspaceforces.com/daf-battle-network-contribution-jadc2/; and Kimberly Underwood, "Illuminating the Department of the Air Force Battle Network," *Signal*, June 1, 2023, https://www.afcea.org/signal-media/technology/illuminating-department-air-force-battle-network.

31 John Gall, *Systemantics: How Systems Work and Especially How They Fail* (New York, NY: Quadrangle, 1977).

32 "Product Lines," Kessel Run, https://kesselrun.af.mil/product-lines/OpsC2.html; Brian Beachkofski and Dan Patt, "Kessel Run Shows How to Bridge the Gap between Development and Operations," *War on the Rocks*, July 28, 2022, https://warontherocks.com/2022/07/kessel-run-shows-how-to-bridge-the-gap-between-development-and-operations/.

33 Sidney Dekker, *The Field Guide to Understanding "Human Error"* (Boca Raton, FL: CRC Press, 2014) delves into the principles

and practices behind civil aviation's safety culture, including its emphasis on open reporting, learning from mistakes, and focusing on systemic issues rather than individual blame.

34 "Army Announces New Policy to Drive Adoption of Agile Software Development Practices," press release, US Army, March 9, 2024, https://www.army.mil/article/274356/army_announces_new_policy_to_drive_adoption_of_agile_software_development_practices.

35 See "Joint Integration and Interoperability Symposium: Technical Innovation for the Future of Joint Warfighting," Hudson Institute, video, 3:25:24, https://www.hudson.org/events/joint-integration-interoperability-symposium-technical-innovation-future-joint-warfighting.

36 "Data Analytics," Office of the Assistant Secretary of Defense, https://www.acq.osd.mil/asda/ae/ada/data-analytics.html.

37 National Defense Authorization Act for Fiscal Year 2022, §229; National Defense Authorization Act for Fiscal Year 2023, H.R. 7900, 117th Cong. (2022), https://www.congress.gov/bill/118th-congress/senate-bill/2226.

38 National Defense Authorization Act for Fiscal Year 2023, §1513.

39 See "Operation Vulcan Logic (OVL) Onboarding Training Registration," Arlo Solutions, https://arlo-solutions.com/ovl/.

40 Requirement for Modular Open System Approach.

41 Consider the recommendations in Jennifer Pahlka, *Recoding America: Why Government Is Failing in the Digital Age and How We Can Do Better* (New York, NY: Metropolitan Books, 2023).

42 See DoD description of MOSA efforts in "Systems Engineering and Architecture: Modular Open Systems Approach," Office of the Under Secretary of Defense, Research and Engineering, https://www.cto.mil/sea/mosa/.

43 Weiss and Patt, *Software Defines Tactics*.

About the Authors

Ellen Lord, Former Under Secretary of Defense for Acquisition and Sustainment

The Honorable Ellen Lord is a distinguished figure in the defense industry and government sectors, with a career that spans over three decades. She served as president and CEO of Textron Systems Corporation, and later as the first US under secretary of defense for acquisition and sustainment. Lord's tenure in the Department of Defense is marked by her significant contributions to acquisition policy reform, emphasizing simplicity, speed, and cybersecurity within the acquisition process. She is credited with recognizing the importance of integrating software into hardware platforms and weapon systems, addressing cyber vulnerabilities, and fostering strong bipartisan and bicameral relationships. She now holds positions on various industry and advisory boards, including as a commissioner for the Senate's Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform, the Atlantic Council Commission on Software-Defined Warfare, and as a Member of the Center for New American Security (CNAS) Board of Advisors.

Dan Patt, Senior Fellow, Center for Defense Concepts and Technology, Hudson Institute

Dr. Dan Patt is a technologist and strategist with a career focused on the intersection of emerging technologies, innovation, and national security, innovation. He is senior fellow at Hudson Institute's Center for Defense Concepts and Technology. Previously, Patt held leadership positions at the Defense Advanced Research Projects Agency (DARPA), including deputy director of the strategic technology office, where he launched the groundbreaking Mosaic Warfare initiative. His tenure at DARPA was marked by significant investments in human-machine teaming, robotic systems, electronic warfare, and the development of widely adopted situational awareness technologies. As an entrepreneur, Patt cofounded and served as CEO of Vecna Robotics, guiding the company through its early growth in the warehouse robotics and workflow orchestration space. He now holds executive and advisory roles with various organizations, including Thomas H. Lee Partners, STR, the University of Michigan College of Engineering, and Worcester Polytechnic Institute.

About Hudson Institute

Hudson Institute is a research organization promoting American leadership for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, energy, technology, culture, and law.

Hudson seeks to guide policymakers and global leaders in government and business through a robust program of publications, conferences, policy briefings, and recommendations.

Visit www.hudson.org for more information.

Hudson Institute
1201 Pennsylvania Avenue, NW
Fourth Floor
Washington, DC 20004

+1.202.974.2400
info@hudson.org
www.hudson.org