Policy Brief

Building the Tech Coalition

How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense

Author
Emelia S. Probasco

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

August 2024

Introduction

There are frequent discussions about how the U.S. military should draw from the country's commercial innovation base to gain an advantage, especially when it comes to the application of artificial intelligence (AI). Too often, conversations lament missed opportunities, valleys of death, painful contracting, or other U.S. Department of Defense (DOD) processes. While these hurdles are real, there are also positive stories of instances when commercial tech companies, military leadership, and warfighters came together to create a meaningful advantage on the battlefield. One of these is the story of how the 18th Airborne Corps used the Scarlet Dragon Exercise series to develop the Maven Smart System (MSS), an instance where frontline army users and a coalition of technology companies—enabled by DOD leadership and policies—pursued and developed a new technology that is having a meaningful impact on operations.

This paper is about how MSS was developed. We examine leadership actions, commercial partnerships, and contractual approaches that enabled success, as well as the organizational and cultural hurdles that had to be overcome. The details of MSS and its application are not our focus, nor are they appropriate to publish here—this is still an operational system for the U.S. military. Rather, this examination seeks to answer the question: What did it take to build MSS for Scarlet Dragon? The goal is to collect the lessons learned that might enable future DOD innovations with software and AI.

The example of how the 18th Airborne used Scarlet Dragon as a means of developing MSS is useful to study for several reasons. As will be discussed in this report, it is a user/warfighter-driven innovation that bridges intelligence and operations functions to the benefit of joint fires.[*] It is also uniquely interesting because of how its development was managed with flexibility and speed, as well as the participation of numerous software and AI service providers in a development-security-operations (DevSecOps) cycle that relied first on commercial service providers. Moreover, the 18th Airborne case study is interesting because it is not a postmortem analysis: the DevSecOps development of the Maven Smart System (MSS) though the Scarlet Dragon exercise series continues today, though its long-term prospects are unclear. The questions that this prompts for the Pentagon are: How can the 18th Airborne's successful process for

[*] "Joint fires" is the official term encompassing the employment of all types of fires, including artillery, missiles, and weapons dropped from aircraft.

developing MSS be institutionalized, and how can this sort of innovation be established as a norm for innovation within the DOD?

For all its uniqueness, however, the story of Scarlet Dragon and MSS is also familiar. Previous studies of Project Maven and other successful quick-reaction units in the U.S. military highlight similar themes about senior leaders being willing to champion a program; flexible contracting, funding, and risk management approaches; visionary front-line leaders; direct access to the operational environment; and the implementation of mature technology.[1] The nuances of these lessons for this particular case highlight how the application of software and AI may be different from past rapid technology adoption efforts.

Background and Methodology

The military has a long history of gathering lessons learned using case studies, and these include the successes and failures of innovation during the wars in Iraq and Afghanistan. These studies range from general examinations of organizational adaptation, to studies of the role of senior leaders in innovation, to detailed looks at the successes and failures of quick-reaction units, and even specifically at lessons from army rapid acquisition efforts for command and control systems.[2] Prior lessons have identified success factors that are echoed in the development of MSS for the army's Scarlet Dragon exercises, namely: senior military and/or civilian leaders willing to champion the program; the need for flexibility in contracting, funding, and risk management; visionary front-line leaders; direct access to the operational environment with ongoing feedback; and generally relying on the implementation of mature (rather than developmental) technology.

To gather lessons learned from the 18th Airborne's experience, our research team conducted extensive interviews with current and former members of the 18th Airborne, the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), and various contractors involved with the development of MSS and Scarlet Dragon between June 2023 and February 2024. We also attended an interim development exercise held in June 2023 to observe the operators and developers working together to create the next iteration of the system. Our report includes our observations from this event and interviews, however, it does not attribute quotations to protect the privacy of our interviewees. Beyond our in-person meetings, we gathered information from media reports about Scarlet Dragon and MSS, as well as

public contracting announcements, and data from Crunchbase about the companies that have participated in developing MSS.

What is MSS, What is Scarlet Dragon, and How Did the 18th Airborne Use Them?

While this paper is focused on how the DOD successfully developed and adopted software and AI for military advantage, it helps to briefly understand what they built in this case study. Put simply, MSS is an AI-based decision-support system. The MSS system was refined over time by the 18th Airborne through the Scarlet Dragon exercise series.[*] These Scarlet Dragon exercises bring together warfighters—as well as developers, technicians, testers, and evaluators—to practice the process of finding potential targets, going through the process of identifying them, locating them, filtering down to the lawful valid targets, prioritizing them, assigning them to firing units, and firing against them. This is done in a crawl-walk-run fashion that starts with basic simulations and ends with actual units firing live rounds against practice targets. These exercises served to focus the 18th Airborne's development efforts, and as operational tests within the DevSecOps process they used for iteratively developing MSS.

The Scarlet Dragon version of MSS can access sensor data from diverse sources, apply computer vision algorithms to help soldiers identify and choose military targets, and then provide workflow support that enables a request to be approved by the chain of command in order to strike a target. It can also serve as a repository where battle damage assessments can be stored, as well as provide a map of the location of friendly forces and targets (see image 1).[3] With regard to current laws and responsible AI policies, the system organizes and integrates data, allows users to select and leverage algorithms to process that data, and gives operators the ability to more quickly make decisions under accepted army doctrine and decision workflow.[†]

---

[*] Exercises help forces train as they might operate in the face of potential conflict. They are important for preparing military forces for combat, but they also allow warfighters to test new technologies and ways of operating them.

[†] The DOD has multiple policies and memoranda guiding the responsible deployment of artificial intelligence, primary among them is DOD Directive 3000.09, "Autonomy in Weapons Systems," as well as the 2021 memorandum from the deputy secretary of defense, "Implementing Responsible Artificial Intelligence in the Department of Defense."

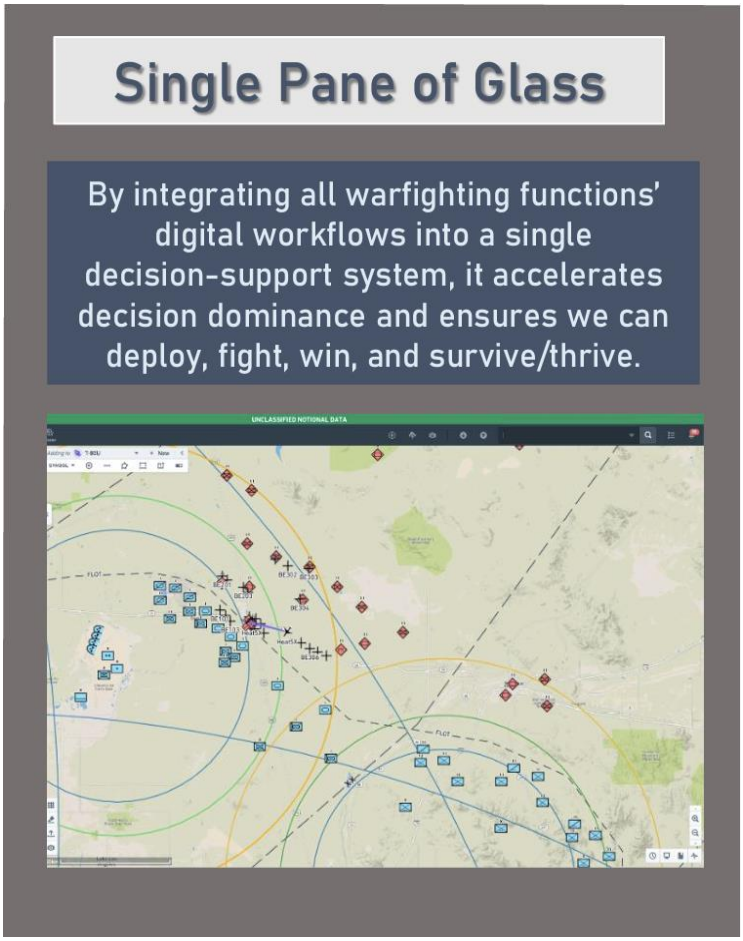


Image 1. Screenshot of Scarlet Dragon System, Source: U.S. Army Dragon Innovation Newsletter

While the description of the system may seem simple, its impact is significant. Without this software, army fire support elements (the organizations that coordinate army and joint fires) do not have easy access to sensor and image data from commercial and military satellites. To add further context, one news report called this feature of direct access to satellite data for targeting "a Holy Grail for the Army."[4] Even where the data is available, MSS offers a significant productivity gain because it automatically highlights images for intelligence analysts to review and then digitally supports the workflow from intelligence analysts, to decision-makers choosing targets, to firing units, and back to analysts examining battle damage. In the absence of MSS, the firing process is manual and riddled with inefficiencies and the potential for errors—from collecting the data to processing it, seeking permission, matching munitions, and granting permission.

Using MSS, the 18th Airborne has demonstrated an ability to match the performance of the time-critical targeting cell in Operation Iraqi Freedom, a targeting cell that is widely viewed as the most efficient in U.S. military history. What is even more impressive, however, is that the 18th Airborne achieved this milestone with roughly 20 people in its targeting cell, whereas the OIF cell benefitted from more than two thousand staff members. With these successes, army leaders hope to leverage MSS to meet a new vision for firing units to make one thousand high-quality decisions—choosing and dismissing targets—on the battlefield in one hour.

In addition to its great efficiency for joint fires, MSS has two other important features. First is the flexibility to integrate data from sensors and platforms that are not part of the software's original design. In October 2021, for example, services and combatant commands joined a Scarlet Dragon exercise and integrated their software and hardware tools into the MSS platform.[5] In February 2023, the same system integrated U.S. Space Force operations.[6] This flexibility gives the system greater longevity as both military and civilian sensors proliferate and change.

"From computer vision, full-motion video, and synthetic aperture radar algorithms identifying targets, to digital workflow tools improving speed and precision of targeting teams, to optimizing machine-to-machine communication flow, the [Scarlet Dragon] exercise marked a critical step toward digital warfighting."

– Gen. Michael "Erik" Kurilla, CENTCOM

The second notable feature is the ability of MSS to restrict access to data and shape the user interface according to the user's role or clearance level, which allows it to serve as a central command and control platform for multi-domain operations in both joint (i.e., across military services) and combined (i.e., in collaboration with allies) settings. The feature helped to enable members of the North Atlantic Treaty Organization to participate in a 2023 Scarlet Dragon exercise.[7] With this, U.S. leaders can efficiently share information with allies at the proper classification level and leverage a common operating picture.

The U.S. Navy, Army, Air Force, and Space Force, have all joined in Scarlet Dragon exercises to date, which is notable given their differing histories, operations, legacy technologies, and communications networks. A single platform that can ingest data from a diversity of sensors, as well as process it, provide it to diverse users, and then create an interface appropriate to a particular type of user, is technically and organizationally complex. But this platform is also a longstanding vision of the DOD aligned with the Combined Joint All-Domain Command and Control (CJADC2) concept. That this instantiation of CJADC2 was created at the tactical edge with operators is impressive, though the operators could not have done it without the support of the Pentagon and a uniquely productive relationship with the private sector.

What it Took to Build MSS for Scarlet Dragon

Building MSS and its Scarlet Dragon instantiation was perhaps more of an organizational feat than a technical one, and one of its most notable features was the participation of at least 21 private-sector software and AI companies (and potentially up to 70, according to interviews) in an operational DevSecOps environment.[8] Before exploring the tech coalition aspect of development, it is important to understand the preconditions for MSS, which included senior leaders championing the program and clearing a path for visionary frontline leaders; flexible contracting, funding, and risk management approaches; direct access by developers, designers, testers, and program/projector managers to the operational environment; and the implementation of mature technology. While these preconditions will be familiar to those who have studied past successes for rapid innovation, the nuances in this case are especially interesting for those studying the application and operationalization of AI for national security. Within boxes in each section that follows, we document traditional lessons learned that apply, but which have some nuances for the MSS and Scarlet Dragon case.

Senior Leaders Willing to Champion the Program and Visionary Frontline Leaders

MSS and Scarlet Dragon would not have come to fruition had it not been for a key set of individuals who could identify the opportunity, make space for experimentation, and then take ownership of delivering the solution. Those leaders happen to share three things in common: 1. significant operational experience; 2. nuanced understanding of AI, networks, and/or data science; and 3. experience and expertise with government acquisition and contracting strategies.

Among these leaders is U.S. Army Colonel Joe O'Callaghan, the AI fires officer for the 18th Airborne Corps, and the leader responsible for the development and operationalization of MSS for the artillery fires, specifically. O'Callaghan has a unique operational background, having enlisted in the navy before commissioning in the army as a field artilleryman, as well as having led fire support coordination at the battalion and the combined joint task force level. He has also attended numerous army educational courses, to include the Army Space Cadre program. In interviews, subordinates and colleagues conveyed that he is one of the nation's best artillerymen, has a broad knowledge of the capabilities and limitations of AI, and maintains a detailed understanding of army contracting and ways to partner and move quickly within the bureaucracy. Finally, his ability to communicate openly across leadership,

operators, and technical representatives visibly galvanized the Scarlet Dragon team during exercises and set a clear direction.

O'Callaghan would not have had the opportunity to participate in the Scarlet Dragon exercises had it not been for the efforts of U.S. Marine Colonel Drew Cukor in establishing MSS. Upon arriving at the Pentagon in 2016 as a member of the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), Cukor was assigned to join the "Third Offset" strategy team, a group put together and empowered by then U.S. Deputy Secretary of Defense Bob Work. Before the Pentagon, Cukor had been a marine intelligence officer and served as a foreign area officer, joint operational planner, and acquisition supervisor.[9] He had also spent time at the National Defense University and had written two draft operating concepts about the connection between intelligence and operations, as well as other technical papers, including one explaining the complementarity of human- and computer-based intelligence systems.[10]

A part of the 3rd offset strategy group, Cukor successfully argued that the deputy secretary should focus his strategy on the use of AI for warfare advantage. As a consequence, Work signed a memo establishing the Algorithmic Warfare Cross-Functional Team (AWCFT) in 2017, and put Cukor in charge of pursuing opportunities that would "integrate artificial intelligence and machine learning more effectively across operations to maintain advantages over increasingly capable adversaries and competitors."[11]

While Cukor and O'Callaghan were the essential visionaries and implementers of MSS and Scarlet Dragon, their efforts benefitted from the top cover and budget assigned by Work in his AWCFT initiative. Similar to Cukor, Work had been a marine colonel earlier in his career, and, like O'Callaghan, he had also commanded an artillery battery and a battalion. He has an extensive academic background in the sciences, as well as considerable knowledge of DOD budgetary and bureaucratic policies and politics, having previously served as the under secretary of the navy, and held a position at the Center for Strategic and Budgetary Assessments.

Lesson Learned: Trilingual Leaders

Pentagon leaders have hailed the importance of "dual-lingual" leaders who understand emerging technologies and the military to help bridge the gap between technical opportunities and operational needs. Our case study highlighted a third "language" that was critical to the successful development of Scarlet Dragon: contracting and acquisition. O'Callaghan and Cukor leveraged their knowledge of all three to cultivate workable technical solutions, rapidly experiment with them, and then implement new technologies within an army artillery unit's operation. Cukor's acquisition strategy was frequently credited in interviews for enabling rapid experimentation, which he, himself, credited to his time overseeing acquisition officers at Marine Corps Systems Command.

With Work's guidance in 2017, the AWCFT began its task by exploring AI applications within the military services. The army initially assigned a military intelligence brigade as the primary point of contact. True to his earlier research, however, Cukor was interested in the potential role for AI to more closely connect intelligence and operations. He found a similarly interested leader in O'Callaghan and U.S. Army General Michael "Erik" Kurilla, of the 18th Airborne, a unit frequently conducting deployments in rapid response to global events. Kurilla came to champion the idea, and the notion of rapid experimentation, both at the 18th Airborne and later when he led U.S. Central Command. Importantly for the success of the program, he held O'Callaghan and Cukor accountable by assessing progress in mission achievement (the efficiency of targeting) rather than platform development milestones. This gave the development team the freedom to iterate and change directions as necessary to achieve the desired goal.

The incentive provided by the deputy secretary's memo, the efforts of Kurilla and his successor, U.S. Army General Chris Donahue, and the relationships built by Cukor and O'Callaghan gave the project broad support. That support spanned the DOD, including the Office of the Under Secretary of Defense for Intelligence and Security, which was running the AWCFT; the National Geospatial-Intelligence Agency (NGA), which now runs the Maven program; the Army Research Lab (ARL), which managed the main

contracts; the Defense Innovation Unit (DIU); the 16th Air Force/Air Forces Cyber; and, the II Marine Expeditionary Force, which was the first interservice partner to the army.

Lesson Learned: Openness to Change and Partnerships

MSS and the Scarlet Dragon exercises would not have launched were it not for the openness of the army and AWCFT leadership to change directions and seek new partnerships. That openness was important at the beginning of the project but remains important as AI technologies evolve. Iterating on the system as it was developed to achieve the goal, rather than iterating to achieve a plan, enabled new applications, and correspondingly, new ways of thinking and operating.

DevSecOps with Direct Access to the Operational Environment

Senior leaders at the Pentagon deserve credit for MSS and setting the conditions to get Scarlet Dragon started, but the program's current success is due in large part to the 18th Airborne. The 18th Airborne is a special unit with the army that is often called "America's First Responders." It is designed for, and tasked with, rapid deployments in response to global events, including, for example, a deployment to Europe within 48 hours of Russia's invasion of Ukraine.[12] In a way, this made the 18th Airborne an ideal unit to experiment with MSS and apply it to the joint fires problem.

Successful quick-reaction initiatives often credit a close connection between operators and engineers, but in the case of MSS, several features appear unique to the quick application of impactful software and AI for Scarlet Dragon. First among these was the DevSecOps approach and its 90-day cycle of development, testing, feedback, and production with the 18th Airborne. This cycle allowed O'Callaghan to set goals under the Maven Broad Agency Announcement (BAA) rather than hard-and-fast requirements. Additionally, the 90-day development cycle was synchronized with regular military exercises that would leverage the technology and quickly reveal either the success or failure of developer efforts in simulated operational environments. Leaders like O'Callaghan could also use the regular cycle of development and exercises as an opportunity to evolve unit operations and technical capabilities concurrently.

"You don't buy AI like you buy ammunition."

– Col. Drew Cukor[13]

The DevSecOps approach enabled quick reactions to changes in the operational environment. For example, soldiers recounted an experience where they noticed a degradation in algorithm performance due to shifting weather conditions. While the algorithm still worked, the soldiers knew it could be improved and were able to consult and rapidly iterate with the developers to improve the algorithm's performance across different weather conditions.

Lesson Learned: Rapid Iteration and a DevSecOps Approach

MSS must continually evolve to seize new technological advantages and react to new operational challenges. That continuous evolution affects both the military unit and the developers, and requires a structured process like DevSecOps to stay in synchronization. When this process is working, it allows for the rapid coevolution of technology and processes to achieve measurable impact.

The DevSecOps approach also helped to normalize the rapid onboarding, offboarding, and updating of companies providing algorithms and software solutions. Critically, that process was managed by the defense contractor ECS Federal, which acted as a systems integrator by leveraging warfighter and program feedback to help identify and rapidly onboard the best possible developers. ECS Federal successfully onboarded (and, at various times, offboarded) a variety of companies leading in AI services and development. This included large companies such as AWS, IBM, Maxar, Microsoft, Raytheon, Sierra Nevada Corporation, and at one point Palantir (which was later elevated to a co-prime with ECS as it became the primary vendor for the user interface and workflow software), as well as smaller companies such as Black Cape, Inc., Clarifai, and CrowdAI.[14]

To help facilitate the rapid onboarding and offboarding of these new companies, ECS iterated on a network it had previously built to facilitate information sharing in

Afghanistan, Iraq, and Libya, called the Secure Unclassified Network (SUNet).[15] The network enabled the creation of virtual enclaves that allowed interagency and coalition partners to securely collaborate, as well as to share information, analytics, and software services, and "acquire, develop, and deploy mission-specific datasets and analytics that can be shared across multiple enclaves or restricted based on mission requirements."[16] Alongside companies providing the data and development services, the MORSE Corporation was hired to implement a continuous test and evaluation process that would support the DevSecOps cycle.[17] These private companies acted as amplifiers and translators for both the warfighters' needs and the developers' capabilities. It was also clear in our encounters during Scarlet Dragon exercises that O'Callaghan and his key leaders were constantly connecting industry participants with operators seeking solutions, and educating both sides on how best to collaborate.

Finally, part of the successful connection between the developers and the operators was the embedding of industry "field engineers" in 18th Airborne exercises, as well as deployments. During Scarlet Dragon exercises, for example, our team observed several field service engineers working alongside soldiers and marines, teaching them how to use the system and simultaneously collecting feedback on useful and frustrating features. We also had the opportunity to interview Palantir field service engineers who worked with the 18th Airborne at Fort Liberty, NC, and during several of its deployments abroad. These engineers shared their belief that their close connection to the operators allowed them to make more rapid and effective iterations to the system. Moreover, their direct interactions with the soldiers connected the engineers more strongly to the 18th Airborne's mission and people.

Leaders in both government and industry frequently mentioned the connection between operators and developers as a key enabler of success. The exposure of developers to operators likely led to the features often highlighted by DOD leaders, such as an intuitive user interface, a workflow that complemented the 18th Airborne's standard processes, and information-sharing features that allowed for a more efficient exchange of sensitive information with allies and international partners.

Lesson Learned: Embedded Engineering

Translating military needs and workflows to technology developers is challenging, as is explaining new technological opportunities to operators who are unfamiliar with new technologies. Embedding developers with operators in exercises as well as within real-world operations helped to close gaps and miscommunications, leading to fast and impactful technological development.

Flexible Contracting, Funding, and Risk Management Approaches

Contract reporting and interviews with members of the 18th Airborne, the DIU, and the Office of the Undersecretary of Defense for Information and Security (OUSD(I&S)), made clear that Maven and Scarlet Dragon benefited from certain contracting mechanisms, including an ARL BAA, accounting for 70% of the funding.[18] In addition to the BAA, the team used Other Transaction Authorities (OTAs) and other research and development (R&D) agreements like Cooperative Research and Development Agreements (CRADAs), Technology Investment Agreements (TIAs), and Partnership Intermediary Agreements (PIAs).[19] The team of vendors contributing to MSS was further extended through ECS Federal, which, as described above, could rapidly establish subcontracts with vendors to address specific goals in a 90-day DevSecOps spiral. Furthermore, we observed that news reports from Scarlet Dragon exercises named participating vendors that were not directly connected to MSS; we believe these vendors likely contributed on behalf of one of the military units participating in a demonstration or exercise. Altogether, the AWCFT and the 18th Airborne used several contracting tools to cultivate and maintain a team of vendors that could rapidly iterate and deliver software solutions for operational needs.

The flexibility of the BAAs, TIAs, PIAs, and CRADAs, together with the subcontracts managed by ECS, also gave the program the ability to run a competitive DevSecOps process. As described earlier, under DevSecOps, the program iteratively set development goals, and when advantageous, the program would designate multiple vendors for the same task to test different approaches. Interviews confirmed that at various times this included two UI/UX developers, two cloud service providers, as well as multiple computer vision algorithm vendors. This rapid and competitive cycle was hailed by DOD managers, vendors, and operators alike as establishing a

simultaneously collaborative and competitive environment that realized fast iterations and results.

> *"What we saw from the persistent experimentation angle is that having multiple events gives (the XVIII Airborne Corps) the opportunity to, with less stress, take on the small problems and solve them in an iterative fashion. They can also just try something out, which helps on what's functional and what can work."*
>
> *– Maj. Adam Schinder, Scarlet Dragon Observer, U.S. Army Joint Modernization Command*[20]

The contract management by the AWCFT was so notable that it received kudos from an unlikely source: the DOD inspector general. In a 2022 report, the IG reported that "the Algorithmic Warfare Cross-Functional Team successfully monitored and managed" its contracts and its only criticism was also encouragement to the AWCFT that it more thoroughly document its processes "because AI and machine learning is an emerging, complex, and rapidly moving technology that requires close monitoring and management techniques that are not captured in current procedures and best practices that are used by the DoD acquisitions community." [21] The biggest recommendation was that the program formally document its processes so that others in the acquisition and sustainment community might benefit from the AWCFT's lessons learned.

Lesson Learned: Contracting for Change

The common thread among these contracting mechanisms is their flexibility, which can allow for experimentation. This proved especially consequential in enabling the AWCFT to change direction away from an army intelligence application and toward the application of MSS for the 18th Airborne's Scarlet Dragon, but it also paid dividends in allowing for new vendors and lightweight processes as new tasks or opportunities arose.

A Motivated Commercial Market Implementing Rapidly Maturing Technologies

Leadership, flexible contracting, and access to the operational environment created essential conditions for success, but they would have been insufficient without the tech companies which efficiently translated warfighter needs into software solutions within the DevSecOps framework. Lessons learned from quick-reaction technology insertion efforts often focus on the technology itself, but a notable finding from the Scarlet Dragon case study is the uniquely important role of tech companies as not just developers but also translators and facilitators for identifying opportunities. The tech companies were needed to translate operator needs into technical capabilities, and their task was complicated by rapid changes in the field of AI during the project. How and why tech companies joined MSS and the Scarlet Dragon effort in particular is worth understanding given the critical role the companies played.

A brief analysis of the companies mentioned as contractors or subcontractors in the course of our research reveals that many were relatively new to defense contracting early in the program. Nearly a quarter of the companies mentioned were founded in the last decade, and just under half have fewer than five hundred employees. This stands in contrast to traditional prime defense contractors, which have often been working with the DOD for between fifty to one hundred years and have tens of thousands of employees. As indicated earlier, to engage some of these new vendors on the project, and create a safe space for experimentation, the army had to leverage SUNet.

Lesson Learned: Continue Lowering the Barriers to Onboarding Growing AI and Software Vendors

Public network enclaves supported faster onboarding times for new companies. Streamlined processes also made the business decision to join the effort more straightforward for vendors who are less accustomed to working with the DOD.

Joining MSS would not have been an obvious business decision for most companies, especially startups. It was funded through mostly temporary, experimental mechanisms, and there was no single point of contact or experienced program office.

Businesses likely also understood that while their efforts were funded by the Pentagon, the Scarlet Dragon version of MSS itself was not a program of record with guaranteed long-term funding. As of today, a part of the original project under the AWCFT has transitioned to the NGA as a program of record, but according to interviews, some of the funding needed to evolve MSS comes from the DOD's Chief Digital and AI Office (CDAO).

On the other hand, the 18th Airborne's operating tempo, its DevSecOps approach, flexible contracting mechanisms, and even the prospect of avoiding predictable program office processes seemed to appeal, especially since contractors mentioned these features as highlights of the program in their interviews. Furthermore, interviews with company representatives as well as Cukor and O'Callaghan indicated that the projects were not profitable for the companies in some instances, and in others, the companies invested significantly to discover and experiment with potential system improvements without a written promise of payment from the government.

> *"We are in an AI arms race frankly, and it's happening in industry. . . . I see an ecosystem of vendors . . . [where] we still have large defense industry vendors out there that are providing the mainstay of the weapon system, and a whole other ecosystem of very fast software companies . . . who can bring these algorithms to our platforms."*
>
> *– Col. Drew Cukor* [22]

Any company that joins the MSS development efforts needs to be paid if they are to survive in a market economy, but interviews with government and company representatives alike made clear that a sense of mission and an interest in challenging technical problems also drove company actions. In interviews, employees who helped to develop MSS clearly conveyed their excitement and pride about working with the 18th Airborne soldiers on Scarlet Dragon exercises, as well as their excitement about deploying overseas to support the unit on missions abroad. Similarly, employees and government observers reported that the technical difficulty of the project presented opportunities for companies to test their capabilities and to learn and improve their products.

While contracts and an interest in the mission and the technical complexity motivated companies, they also reported drawing on internal resources to work "at-risk" for the government or when they wanted to experiment with a potentially useful technical improvements for MSS and the 18th Airborne. That companies made the choice to work without certainty of payment at times, especially for a program that does not have guaranteed funding, is a difficult business decision. The need to apply internal funds is a luxury that not all companies necessarily enjoy and could deter commercial partners, like startups, who may also opt for more reliable revenue from other customers.

Lesson Learned: Tech Companies are Willing to be Flexible to Meet the Mission, but that Flexibility Comes at a Risk that not all Companies can Afford

The actions of the companies working on MSS demonstrates that they are willing to sincerely partner and take risks, or even endure temporary losses, when it comes to urgent missions or especially interesting technical problems. Presumptions that companies were "only in it for the money" were not only inaccurate but affected the enthusiasm of tech company employees. Nevertheless, most of the companies working on MSS were mid-sized and many had been operating for at least five years. Less well-established companies may not be in the same financial position as the Scarlet Dragon contractors to take business risks for the government.

Challenges

Historians have studied the challenges of military innovation since at least the interwar years and, unfortunately, many of the historical observations still apply in the case of MSS and the Scarlet Dragon exercises.[23] The challenges for MSS and Scarlet Dragon include institutional conservativism which disincentivizes innovators, organizational structures that seed parochialism, skepticism about new technologies (and, in this case, the contractors providing that technology), and, finally and perhaps most different from historical precedent, revenue risks that suppress commercial business participation.

Institutional Responses to Change and Incentivizing Innovators

Those individuals who led and executed the development of MSS and the Scarlet Dragon exercises, beyond just the individuals highlighted in this paper, challenged typical DOD processes and crossed organizational boundaries in ways that created organizational and interpersonal friction. Interviews indicated that changing directions in the MSS program from intelligence to fire-support applications put these different communities in tension. Furthermore, the quick execution of contracts with new vendors disrupted the deliberative and consultative status quo in the Pentagon in ways that provoked questions.[24] The longstanding challenges of being a person who is a "disruptor" in the military—an inherently conservative institution—are unsurprising, though it is worth considering how the Pentagon might support and protect these disruptors in times of rapid technological change.

Connecting Intelligence and Operations

Another friction apparent in interviews and reminiscent of past observations about branch or service parochialism was the challenge of integrating intelligence and operational functions.[25] While some of the frictions had to do with the differences in needs, processes, and deliverables for the two communities, some were also likely financial. Repurposing the focus of the AWCFT (technology and funding) away from intelligence analysis and toward the operations of the 18th Airborne's artillery came at a cost to the intelligence community's original plans for the funding.

Skepticism about technology and contractors

Besides the challenges internal to the DOD, MSS contractors identified frictions in some of their relationships with government personnel. These frictions were summarized by company leaders as being viewed as "just contractors" or "dirty contractors," a theme that has been echoed by companies that voluntarily contributed to the response in Ukraine.[26] This friction may have also coincided with initial skepticism about the utility of AI for artillery fires, which one soldier bluntly summarized as: "This s--- don't work."[27] Those opinions were initial obstacles that were overcome with experience, and later matured into what could be considered as justified skepticism when operators purposefully disabled algorithms when they noticed a degradation in accuracy.

Business and Financial risk

Companies acknowledged that while Scarlet Dragon gave them a chance to demonstrate capability to an important DOD customer, they also took business and financial risks to participate in the project. Several government representatives also echoed their perception that some companies performed above the funding level of their contract. On the lower end of that risk were internal R&D funds dedicated to developing new technologies or techniques for Scarlet Dragon exercises. In other instances, we heard of reports of companies working on MSS for 18th Airborne applications before a contract was finalized. In more extreme cases, we heard of instances where companies participated in the project at a financial loss, either because of the intuition that the project was important for national security or because the technical challenges posed by the project complemented the company's technical development aspirations.

Regardless of the reason, the fact that we heard in so many interviews about companies agreeing to work at risk or at a loss contradicts the notion of the "dirty contractor" sentiment noted above. Not all contractors are in a financial position where they could work at risk or at a loss, and no business can function for long without revenue in a market economy. The inability to fully contract or pay for the technical development that MSS required may have prevented some companies, particularly startups, from being in a position to contribute.

Conclusions and Recommendations

MSS and the Scarlet Dragon exercises demonstrate the potential for bottoms-up innovation to meet top-leader intent. As a partial instantiation of the DOD's CJADC2 vision, Scarlet Dragon and the 18th Airborne deserve high praise for seizing the opportunity to apply emerging technology to an important operational challenge. That praise must recognize, however, the role of strong advocacy from the highest levels of civilian leadership in the Pentagon, as well as support for flexibility and risk taking by senior leaders across the DOD and from within the tech sector.

Many of these lessons learned reenforce what the DOD should already know about leadership, flexibility, as well as the importance of the warfighter's perspective, and the value of private sector innovation. But, Scarlet Dragon also offers some unique insights for operationalizing software and AI:

- **Senior leaders are vital to clearing administrative and bureaucratic hurdles for innovators instituting change.** Developing and applying new technologies is already challenging, and institutional resistance to change is an unnecessary hurdle. Senior leaders are essential to clearing those hurdles, communicating the vision broadly, and holding innovative teams responsible for measures of effectiveness rather than measures of performance.

- **Invest in training and career pipelines that include operations, acquisition, and technical skills.** There are many advantages to "dual fluency" leaders who can speak to both technical and operational communities, but trilingual leaders—those who can communicate across operational, technical, and acquisition communities—were catalysts for success in paving a new path and developing MSS for artillery fires. Officer assignment and promotion considerations should take into account the value of all three skills for the future of innovative technology development. Leadership should also make use of personnel policy exemptions when gifted trilingual leaders are making substantial progress in developing technologies along with operational concepts.

- **Build technical and contractual systems that allow for changes of direction.** Because AI is still evolving, and new applications are emerging, the DOD must remain open to changing directions and seizing new opportunities. To do so, the DOD should be ready to establish partnerships across internal DOD boundaries, as well as through flexible contracting approaches. That openness can be supported by:
    - **Agile development processes, like DevSecOps.** No static software system is likely to be successful in modern operations. DevSecOps offers a way for the Pentagon to continuously adjust to changing circumstances. Instituting DevSecOps approaches and training operators on how to work best within a DevSecOps environment can be a long-term strategy for the DOD. Based on the experience of Scarlet Dragon, the DOD should also fund operational units to experiment and exercise with new technical solutions as they are iterated upon in the DevSecOps cycle.

- **Flexible contracting mechanisms and fast business partners.** R&D funds and BAAs gave the MSS team the flexibility they needed to make fast contracting changes, but even this was not sufficient. A prime integrator willing to seek out the best commercial partners and rapidly onboard them (rather than an integrator that distributed work tasks to only its own units and staff) proved essential to MSS' speed and flexibility. If the DOD is unable to reach the contracting speed required, as seems likely, program managers should find trusted systems integrators and hold them accountable for recruiting and rapidly facilitating external partnerships with a diverse ecosystem.
- **Software licensing or app store-like services.** The military needs a rapid and repeatable approach to agile development and deployment of software and algorithms across the force. Solutions developed for one unit should be accessible to others if the use cases are fundamentally the same. This is especially important as conditions on the ground change and as new solutions become available. Having a standardized library or store of applications that have been vetted and are available for widespread use, with appropriate risk mitigations, gives warfighters the ability to quickly access new software, data sources, and algorithms at the point of need. It also benefits commercial companies with a more efficient delivery path and a potential revenue model. The CDAO appears to be taking the lead in establishing this type of approach, starting with its new Open Data and Applications Government-owned Interoperable Repositories (Open DAGIR) multi-vendor ecosystem.[28] For MSS, this ecosystem will also be enabled by the NGA-managed Maven program.
- **Field Service Engineers**. The continuous evolution of a technical solution affects both the military unit and the developers and requires a structured process to stay in synchronization. Embedding developers with operators in exercises and real-world operations has the potential to support the co-evolution of technology and ops while also bridging gaps and miscommunications, leading to faster and more impactful development cycles.

- **Support business contributions and continuity by signposting long-term commitment to projects, faster contracting, and continuing to lower barriers to participation.** Cutting-edge companies are essential to rapidly harnessing the latest technologies and, if they have the funds, are willing to take risks to fulfill a mission or tackle a challenging problem. Prompt and fair payment for services, as well as reasonable accommodations for those without prior experience working on government networks—solutions akin to SUNet—can help ease the transition for new vendors and encourage companies by lowering the financial or operational barrier to entry. Even more, clear budget commitments that project stable funding for a program going forward can give companies confidence and the evidence they need to build a compelling business plan for investors—industry needs to see the potential for a longer-term commitment downstream and a longer-term path for [corporate] success. As one subject succinctly put it: "industry is getting experiment/proof of concept fatigue (aka innovation theater). Lots of champions have great ideas and are ready to spend money on demos, but few have a build/measure/learn plan to move forward with criteria to pivot or persevere."[29]

MSS and Scarlet Dragon are a case study in adoption and rapid iteration with software and AI for the DOD. That Scarlet Dragon achieved an efficiency comparable to the best the U.S. military has achieved in recent history—with two thousand fewer staff—should serve as a strong incentive for future responsible experimentation and development. To seize the potential, the DOD should establish the conditions for visionary leaders in technology companies and military units to build new solutions by addressing cultural, procedural, training, and contractual impediments. At the same time, both the military and the private sector will need to incentivize, develop, and retain more visionary leaders ready to create the next generation of innovations for national security.

Author

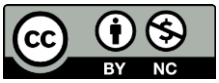
Emelia S. Probasco is a senior fellow at CSET.

Acknowledgements

This paper is the result of an ongoing collaboration and a memorandum of understanding (MOU) between CSET, the Johns Hopkins University Applied Physics Laboratory (JHU-APL), and the 18th Airborne Corps. The author wishes to acknowledge the substantial contributions of fellow project members: Christine Fox, Alan Brown, and Toni Matheny from JHU-APL, as well as Igor Mikolic-Torreria from CSET.

This project would not have been possible without the support of the 18th Airborne Corps, which shared data from the MSS system and gave the project team members access to training events. Most especially, the project is grateful to Joseph O'Callaghan, Zach Riley, and Brad Colby Jordan, who generously gave their time to multiple interviews.

Additionally, the author thanks all the individuals who shared their insights and experiences working with Project Maven, MSS, and Scarlet Dragon. Including, Akash Jain, Anna Rubinstein, Bob Hagen, C. Anthony Pfaff, Cam Stanley, Charles Stevens, Colleen Gaydos, Dan Keller, Kurt Campbell, Josh Wellner, Jared Dunnmon, Shannon Clark, Drew Cukor, and Jason Brown. Thanks also to Jon Askonas, Jason Brown, Owen Daniels, Shelton Fitch, Matt Mahoney, and Helen Toner for feedback, editorial review, and editorial support.



© 2024 by the Center for Security and Emerging Technology. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/.

Document Identifier: doi: 10.51593/20240014

Endnotes

[1] Chad Heitzenrater, Bradley Wilson, Sydne J. Newberry, Sarah W. Denton, James Ryseff, Jeff Broughton, "Lessons Learned from the Algorithmic Warfare Cross-Functional Team—Project Maven," RAND Corporation, 2023.

[2] David Barno and Nora Bensahel, *Adaptation Under Fire: How Militaries Change in Wartime,* New York: Oxford University Press, 2020; Liam S. Collins, "Military Innovation in War: The Criticality of the Senior Military Leader," Princeton University, 2014, http://arks.princeton.edu/ark:/88435/dsp01br86b3727; Jonathan Askonas, "Adapt or Die: Lessons Learned for U.S. Army Quick Reaction Capability Organizations," Author's draft. U.S. Army Asymmetric Warfare Group History & Lessons Learned Project; and Shara Williams, Jeffrey A. Drezner, Megan McKernan, Douglas Shontz, and Jerry M. Sollinger, "Rapid Acquisition of Army Command and Control Systems," RAND Arroyo Center, 2014, https://www.rand.org/pubs/research_reports/RR274.html.

[3] Osvaldo Fuentes, "Data-centric exercise showcases joint capabilities, lethality," U.S. Army, February 6, 2023, https://www.army.mil/article/263764/data_centric_exercise_showcases_joint_capabilities_lethality.

[4] Theresa Hitchens, "Army, NRO Pioneer Direct Sat Imagery Downlink In 'Scarlet Dragon,'" *Breaking Defense,* October 11, 2021, https://breakingdefense.com/2021/10/army-nro-pioneer-direct-sat-imagery-downlink-in-scarlet-dragon/.

[5] Jane Edwards, "Army Conducts AI-Enabled Target Identification Exercise Under Scarlet Dragon Program; Lt. Gen. Erik Kurilla Quoted," ExecutiveGov, October 6, 2021. https://executivegov.com/2021/10/army-conducts-ai-enabled-target-identification-exercise-under-scarlet-dragon/.

[6] Osvaldo Fuentes, "Data-centric exercise showcases joint capabilities, lethality," U.S. Army, February 6, 2023, https://www.army.mil/article/263764/data_centric_exercise_showcases_joint_capabilities_lethality.

[7] Jonathan Jay Koester, "Modernization leaders use Scarlet Dragon exercise to continue Project Convergence campaign of continuous learning," U.S. Army, Feb 13, 2023, https://www.army.mil/article/263951/modernization_leaders_use_scarlet_dragon_exercise_to_continue_project_convergence_campaign_of_continuous_learning.

[8] Reviewing the data from 2018-2023 available to the authors and validated via usaspending.gov and multiple interviews, we confirm the participation of 21 companies. However, some interviews indicated that as many as 70 companies had a role in creating MSS.

[9] "Colonel Drew Cukor, USMC," *GovExec*, https://cdn.govexec.com/media/kmc/cukor_bio1.pdf.

[10] See Drew Cukor, "Operate to Know," National Defense University thesis 2014; and John M. Graham, Kathleen M. Carley, and Drew Cukor, "Intelligence Database Creation and Analysis: Network-Based

Text Analysis versus Human Cognition," Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA, 2008, pp. 76-76, doi: 10.1109/HICSS.2008.213.

[11] Robert Work, "Establishment of the Algorithmic Warfare Cross Functional Team (Project Maven)," April 26, 2017.

[12] Rachel Riley, "18th Airborne Corps' Unit Returns to Bragg After Eight-Month Deployment," *The Fayetteville Observer*, October 19, 2022, https://www.fayobserver.com/story/news/military/2022/10/19/18th-airborne-corps-units-return-to-fort-bragg-from-europe-deployment/69569777007/.

[13] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," U.S. Department of Defense, DOD News, July 21, 2017, https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

[14] Palantir began as a subcontractor to ECS Federal and later won a direct contract for the project. The companies listed are reflected in contract W911QX21C0022 on USASpending.gov.

[15] See contracts W911QX17D0012 and W911QX17D0010 on USASpending.gov

[16] Brian Stanton, et al., "US Army Artificial Intelligence Innovation Institute (A2I2) Aiding Multi-Domain Operations (MDO)." ARL-TR-8992 DEVCOM Army Research Laboratory, July 2020, https://apps.dtic.mil/sti/citations/AD1104260.

[17] Morse Corps., "JAIC Selects MORSE for AI Test and Evaluation Effort With $250 Million Ceiling," February 10, 2022, https://www.morsecorp.com/pressrelease.html?prId=pr_02_10_2022.

[18]Government Accountability Office, "Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems," February 2022, https://www.gao.gov/products/gao-22-104765.

[19] For more information on these types of agreements, see: "R&D Agreements | Adaptive Acquisition Framework." Accessed July 29, 2024, https://aaf.dau.edu/aaf/contracting-cone/rd-agreements/.

[20] Jonathan Jay Koester, "JMC answers call for Persistent Experimentation," U.S. Army, https://www.army.mil/article/269729/jmc_answers_call_for_persistent_experimentation.

[21] U.S. Department of Defense Inspector General, Report No. DODIG-2022-049 "(U) Evaluation of Contract Monitoring and Management for Project Maven," January 6, 2022.

[22] Jon Harper, "Pentagon Struggling To Take Advantage Of Artificial Intelligence," National Defense, Vol. 102, No. 766 (September 2017), pp. 24-25.

[23] David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army, 1917–1945*. Cornell University Press, 1998.

[24] The program attracted so much attention, in fact, that it is the subject of two inspector general reports. Both largely confirm the value of the AWCFT's approach to development MSS. See U.S. Department of Defense Inspector General, Report No. DODIG-2022-049 "(U) Evaluation of Contract Monitoring and Management for Project Maven," January 6, 2022. And, U.S. Department of Defense Inspector General, Report No. DODIG-2023-044 "(U) Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network," January 12, 2023.

[25] David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army, 1917–1945*, Cornell University Press, 1998.

[26] See Christine H. Fox and Emelia S. Probasco, "Volunteer Force," Center for Security and Emerging Technology, May 2023, https://cset.georgetown.edu/publication/volunteer-force/.

[27] Katrina Manson, "AI Warfare is Already Here," *Bloomberg Businessweek*, February 28, 2024.

[28] U.S. Department of Defense, "CDAO Announces New Approach to Scaling Data, Analytics and AI Capabilities," May 30, 2024, https://www.defense.gov/News/Releases/Release/Article/3791829/cdao-announces-new-approach-to-scaling-data-analytics-and-ai-capabilities/.

[29] Jason Brown in an email message to author, June 30, 2024.