2021

Major General Harold J. "Harry" Greene Awards *for* Acquisition Writing

Honoring a Legacy of Service and Sacrifice

by Lt. Gen. Robert L. Marion

It is through the Maj. Gen. Harold J. "Harry" Greene Awards for Acquisition Writing that we remember a leader, mentor and friend who left a legacy that endures today. When Harry served as the deputy for acquisition and systems management (DASM) in the Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology) at the Pentagon, I was his deputy, so I know firsthand of his passion for delivering capability to our Joint Force, mentoring junior leaders and taking care of Soldiers.

Harry left the DASM position and was assigned as the deputy commanding general, combined security transition command-Afghanistan on Jan. 14, 2014. His service, sacrifice and tragic death there on Aug. 5, 2014, reminds us of the dedication, commitment and risk our men and women in uniform take to ensure our nation's security.

We honor his legacy of service and sacrifice annually through the Maj. Gen. Harold J. "Harry" Greene Awards for Acquisition Writing. Now in its eighth year, the competition is open to everyone and designed to advance the dialogue on the way forward for the acquisition community in these challenging times. Entrants are invited to share their experiences and ideas, and communicate about ways to improve acquisition outcomes in four categories—acquisition reform, future operations, innovation and lessons learned.

This special supplement of Army AL&T magazine showcases the 2021 winners and honorable mentions. My sincere thanks to all who participated and to their families and teammates who supported them. I also want to thank our panel of judges for their time and expertise in reviewing and assessing the submissions.

My congratulations to all on another successful year.

2021 Major General Harold J. "Harry" Greene Awards for Acquisition Writing

The winners and honorable mentions are:

Category: Acquisition Reform

Winner: The Authority to Compete

Authors: **Maj. David J. Delassus** is a Defense Acquisition Workforce Improvement Act (DAWIA) Level III (Contracting) acquisitions officer. He is serving as the plans and operations branch chief for the Operational Contract Support Division Joint Staff J45.

Abstract: Joint doctrine has recognized the competition continuum. Lawmakers and the military need to realign the acquisition continuum to support global competition below armed conflict.

Honorable Mention: Acquiring Innovation in the 21st Century: Accelerating Procurement as a Weapon of War

Author: **Robert E. Finley** is AFLCMC, Materiel Leader Qualified, a DAWIA Level III certified program manager, part of the Acquisition Professional Corps, graduate of The Eisenhower School for National Security and Resource Strategy Senior Acquisition Course with an international security cooperation concentration, and won the Maj. Gen. Antonelli Award - Best Industry Study Group Paper - Strategic Materials.

Abstract: Looking to the past, I.B. Holley advised that "the procurement process itself is a weapon of war." The hypothesis offered here is that acquisition policy and law are not the underlying root cause of confusion and delay. The obstacles to capturing novel warfighting capabilities lie inside the acquisition community with clumsy processes and arcane tools. The acquisition community must automate the management of the program manager's trinity of cost, schedule and performance (C/S/P). Mobilizing for the Great Power Competition requires leveraging the power of information technology and high-powered big data analytics.

Notoriously slow, opaque and prone to error, DOD contract development is stuck in the 1990s, at best. The contract is where an acquisition strategy truly becomes manifest. The contract binds principals to agent, incentives to outcomes, requirements to funding, and solidifies the choice among potential alternatives into concrete decisions. Digitally connecting the tools of contractor assessment, program estimating, source selections, and contract management multiplies their power by creating a digital feedback acquisition loop that more actively controls C/S/P. Each step inherits value from the previous step and feeds decision-making benefits forward to the next. The battle is uphill. Up to 85 percent of big data projects fail and the primary difficulties stem from the challenges of management resistance, internal politics, skill development, security and governance.

Accelerating the acquisition process with high-powered big data analytics modernizes Holley's procurement process as a digital weapon of war and is a more compelling method to challenge China's strategic authoritarian decision-making advantage.

Category: Future Operations

Winner: Change the Contingency Contracting Support Model to a Centralized, CONUS-Based Contingency Contracting Support Center

Author: **Maj. Joseph D. Levin**

Abstract: The Army has relied heavily upon regional contracting centers (RCCs) co-located with forward-deployed units to support contingency contracting missions. Focusing on RCCs in the U.S. Central Command (CENTCOM) area of responsibility (AOR), this paper identified numerous weaknesses of this contracting support model including high costs, difficulty training and recruiting qualified personnel, and high turnover rates of both civilian and military personnel creating continuity gaps. These weaknesses contributed to multiple Department of Defense Inspector General audits identifying fraud, waste and abuse as recurring material weaknesses in the contracts managed by these RCCs.

This paper proposes a new contingency contracting support model. Specifically, this paper proposes using the technological innovations and the remote work model adopted by many government offices in response to the Coronavirus pandemic to create one centralized Contingency Contracting Support Center permanently located in the continental United States (CONUS) that provides remote contracting support to contingency missions anywhere in the world. This paper considers how a centralized, CONUS-based Contingency Contracting Support Center could provide superior contracting support to contingency operations while addressing the weaknesses identified in the current model. This paper next addresses foreseeable concerns with the proposal and discusses how to resolve or mitigate these concerns. Finally, this paper concludes that adopting the proposed model would resolve the problems identified while creating a technology-leveraged, modern contracting center that reduces costs and is capable of supporting future operations worldwide.

Honorable Mention: Protecting the Future Force in Multi-Domain Operations

Authors: **Lt. Col. Curtis Brooker** is the Product Manager Force Protection Systems within Program Executive Office Intelligence, Electronic Warfare and Sensors (PEO IEW&S) at Fort Belvoir, Virginia. He holds a B.S. in business administration from The Citadel and an MBA from the Naval Postgraduate School.

Dr. Christina Bates provides contract support as a strategic advisor, planner and strategic communications expert to various organizations within the Army acquisition and research, development, and engineering communities, including the Project Manager Terrestrial Sensors. Bates holds a Ph.D. in communications with an emphasis on organizational communication and behavior from Arizona State University; an M.S., with distinction from Boston University; a JD from Boston University; and a B.A., cum laude from Boston College.

Abstract: Throughout the 20-year war in Afghanistan and Iraq, the United States Army's notions of force protection evolved and matured. In turn, the capabilities required to provide robust force protection evolved to pace threats. In light of the Afghanistan withdrawal, the Army's focus on modernization, and the advent of the multi-domain operations (MDO) construct, the Army now must re-examine notions of force protection as it relates to MDO. In other words, the Army must determine and predict its force protection posture and needs, and in turn the associated capabilities required to preserve combat power and minimize casualties within a MDO battle. This article represents an initial step in this critical thought process. Its primary aim is to set forth enduring force protection tenets and to discuss potential paths for extrapolating from these tenets to plot the likely, main enablers of force protection within MDO.

Category: Innovation

Winner (Tie): Creative Acquisition and the Cyber Battlefield: Using Rapid Prototyping to Address Pressing Cyberspace Challenges

Author: **Fianna Litvok** is the communications lead for Applied Cyber Technologies, within the Program Executive Office for Enterprise Information Systems (PEO EIS). She also serves part time as a military intelligence chief warrant officer in the U.S. Army National Guard's 91st Cyber Brigade. She holds an M.A. in English from Stony Brook University, and is certified in Scalable Agile Frameworks for Program Owners/Program Managers and Information Technology Infrastructure Library.

Abstract: The cyber domain is a fast-paced, constantly evolving battlefield. Threats, tactics and even threat actors themselves, change rapidly. The only way to fight—and defeat—these threats is to provide the U.S. Army's world-class cyber defenders with the best technology as quickly as possible. Applied Cyber Technologies (ACT)—a product office within Defensive Cyber Operations (DCO), in U.S. Army's Program Executive Office Enterprise Information Systems (PEO EIS)—aims to continually adapt, develop and update defensive cyber capabilities to ensure cyber-Soldiers' operational readiness. To that end ACT created Labyrinth, a nimble mechanism designed to resolve the most acute challenges facing cyber warriors. Capitalizing on the power of the COBRA OTA, Labyrinth creatively leverages industry partners and academia to quickly secure or refine existing cyber tools within weeks or months. Labyrinth prioritizes prototypes over long-term material solutions and cultivates collaboration over competition. With its Labyrinth framework, ACT is changing the paradigm not only for defensive cyber solutions acquisition, but for technology innovation throughout the military.

Winner (Tie): Scaling Innovation at the Department of Defense: An Actionable Framework and Practical Steps for the Joint Force

Author: **Dr. Marina Theodotou** is an organizational change expert at the Defense Acquisition University, at the United States Department of Defense and the curator and host of the "Think Differently" webcast series, one of the 13 series of the award-winning DAU Webcasts Program, which inspires and empowers the workforce to think differently, learn deliberately and lead boldly. She recently completed a rotation as the director for learning experiences at NavalX at the United States Department of the Navy.

Theodotou is an assistant professor at the Jack Welch Management Institute, a mentor in the Executive Women in Government Program and Chief Learning Officer Learning in Practice Awards. She holds a digital transformation certification from Management Science and Engineering at Standford University, a Lean Six Sigma Black Belt from Bank of America and is certified in design thinking by IDEO University.

In 2021, Theodotou was recognized as winning author at the Pentagon in the category of innovation in the Maj. Gen. Harold J. "Harry" Greene Awards in Acquisition Writing competition. She holds a Ph.D. in education, organizational change and leadership from the University of Southern California an M.S. and B.A. degrees in economics from the University of South Carolina.

Abstract: One of the biggest challenges facing the Department of Defense today is how to scale innovation. While over 100 innovation cells and initiatives are active within the Department, they are not effectively resourced to fully scale their learnings and outcomes across the DOD. This paper defines "scaling" as the adaptation, uptake and synergistic use of innovations, including practices, outcomes, technologies and market arrangements across communities, stakeholders, and broader domains to achieve performance outcomes. The DOD's inability to scale innovation achieved from ideas, pilots, processes, approaches, technologies and acquisition contracting vehicles prevents the Joint Force from optimizing innovation scaling in warfighter capabilities and therefore winning the Great Power Competition. This paper presents an innovation scaling framework and outlines practical implementation steps that can be applied by the Joint Force.

Honorable Mention: Animated Data: How Healthcare Data Lives Alongside Patients

Author: **Holly S. Joers** is the program executive officer-for the Program Executive Office, Defense Healthcare Management Systems (PEO DHMS). The mission of PEO DHMS is to transform the delivery of healthcare and advance data sharing through a modernized electronic health record for service members, veterans and their families.

Abstract: The United States Army, and more broadly, the DOD, Department of Veterans Affairs and the United States Coast Guard will benefit from living and evolving health data sets that improve the wellbeing of over 9.6 million beneficiaries in the coming years. The revolutionary advantages of the single, common federal electronic health record, MHS GENESIS, will progress patient-centered care for decades to come; however, its development also challenges us to shift how we fundamentally relate to data. In short, the development of MHS GENESIS lends itself to understanding data as not a foreign and insipid series of numerals, divorced from the health experiences of men and women. Like an organism itself, PEO DHMS creates the mechanisms for data to live alongside patients, changing, growing and evolving while enhancing health outcomes along the way.

Category: Lessons Learned

Winner: Building Trust: A Cyber Story

Author: **Lt. Col. (Promotable) Rachael M. Hoagland** is the former product manager for Mission Equipment at the Technology Application Office and currently serving as the director of operations for the assistant secretary of the Army for acquisition logistics and technology (ASA(ALT)). She holds an M.A. in strategic studies from the U.S. Army War College and an M.S. in global leadership from the University of San Diego. She is Level III certified in program management and is a member of the Army Acquisition Corps.

Abstract: Cyber assessments take many of us out of our comfort zone. A phased approach can provide time needed to educate yourself and the team. Breaking the assessment into phases can also bring quick wins and credibility to the effort. However, highlighting vulnerabilities often breaks trust, and an assessment will not succeed without trust. Developing a common language and a shared mental model help build the trust needed to conduct a meaningful cyber assessment. The article walks you through a three-phased approach, detailing how building and keeping trust throughout the phases lead the team to success.

Honorable Mention: Onboarding New Employees as Remote Working is Here to Stay

Author: **Maj. Jared J. Ryan** is an assistant product manager and supports the Product Manager Army Watercraft Services, Program Manager Transportation Systems, Program Executive Office Combat Support and Combat Service Support. He is currently working on the development of the Maneuver Support Vessel (Light). Ryan has an BBA and an MBA from the University of Oklahoma as well as an M.S. from Missouri University of Science and Technology.

Abstract: The COVID-19 pandemic has changed how the Army Acquisition Corps operates on a daily basis. As a result, how new hires are onboarded needs to change. Organic conversations that happen in an office environment can provide valuable opportunities for a new hire to better understand their job. With these conversations vanishing, or happening one-on-one in a MS Teams call, as people work from home, it is important to get an office together regularly. This allows the new hire to not only get to know their coworkers, but also to listen to how they talk about their projects. Likewise, the new hire should understand the importance of being proactive in a virtual environment and reaching out early and often.

Major General Harold J. "Harry" Greene Awards for Acquisition Writing Distinguished Judges

Vincent E. Boles, Maj. Gen. USA (Ret.), Defense Acquisition University (DAU) professor of life cycle logistics

Charles A. Cartwright, Maj. Gen. USA (Ret.), DAU faculty member and former program manager, Future Combat Systems

Professor John T. Dillard, former senior lecturer, Graduate School of Engineering and Applied Sciences, Naval Postgraduate School

Professor Raymond D. Jones, professor of practice and academic associate, Defense Acquisition and Program Management Curriculum, Naval Postgraduate School

Roger A. Nadeau, Maj. Gen. USA (Ret.), senior vice president, American Business Development Group and former commanding general, U.S. Army Test and Evaluation Command

Gary Martin, president of GPM Consulting LLC and former program executive officer for Command, Control and Communications – Tactical

Kris Osborn, president and editor-in-chief, Warrior Maven - Center for Military Modernization and Defense Editor, The Center for the National Interest

Dana J.H. Pittard, Maj. Gen. USA (Ret.), vice president, defense programs, Allison Transmission

Ken Rodgers, Col. USA (Ret.), director, Strategic Defense Systems and C4I, Cypress International

Chérie Smith, managing director of Chérie Smith, Consulting LLC and former program executive officer for Enterprise Information Systems

Rickey E. Smith, former deputy chief of staff, G-9, U.S. Army Training and Doctrine Command

Michael A. Zecca, chief futures officer, U.S. Army DEVCOM Armaments Center

Category: Acquisition Reform

WINNER

The Authority to Compete

By the following author:

Maj. David J. Delassus

Introduction – Modern Warfare

The strategic rivals of the United States compete without U.S.-based laws or rules and are gaining a strategic advantage. The U.S. is a nation of laws and rules and is organized to function as a state at peace or at war. Modern military doctrine including Joint Doctrine Note 1-19 the "competition continuum" has begun to recognize the competition continuum. The competition continuum describes: "a world enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict."[1] In order to compete within the competition continuum especially below armed conflict, our government needs to make changes to existing laws and acquisition regulations.

Within acquisition law, including the Federal Acquisition Regulation (FAR) there exists a similar binary state of peace and war. The black and white nature of the FAR is being exploited by our adversaries and lacks the flexibility required to effectively complete below armed conflict. Modern military doctrine has recognized the competition continuum, perhaps a change in acquisition regulations wouldn't be a bridge too far.

The Acquisition Continuum

While generally black and white, an acquisition continuum of sorts exists within the FAR and acquisition laws. This continuum exists as a sliding scale of restrictions depending on geography (OCONUS/CONUS) and declaration (humanitarian assistance, natural disaster, national emergency, contingency, war, etc.).

During peacetime within the 50 states and territories, the DOD encounters the most restricted acquisition conditions. Mandatory sources, domestic restrictions, and protectionist laws including the Buy American Act, and the Berry Amendment are enforced. These laws are in place to insulate the American economy from the global free market, while providing support to the Defense Industrial Base (DIB). While at peace, contracting and acquisition can be a bureaucratic and litigious business with long procurement administrative lead times (PALT). The longest official PALT goals published by the DOD in 2019 can reach 270 days for certain items.[2] Such lengthy lead times are not effective for combatant commands competing below armed conflict.

When the president, secretary of defense or state declare contingencies, the sliding scale of increased acquisition authorities appear. Contingency declaration results in expanded procurement authorities and relief from protectionist laws. FAR part 18 special emergency procurement authorities allow for streamlined procedures and reduced contracting lead times. Contracting moves faster with less bureaucracy.

If the U.S. encounters national level emergencies and large scale war, then the U.S. Government has the ultimate authority of the Defense Production Act (DPA). "The DPA is the primary source of presidential authority to expedite and expand the supply of materials and services from the U.S. industrial base needed to promote the national defense."[3] Employment of the broad reaching powers and full capability of the DPA represent the most extreme end in the acquisition continuum. The DPA is nearly a limitless economic tool for control of the civilian economy for national defense. The DPA was most recently used during the COVID-19 pandemic response and helped to increase availability of personal protective equipment, produce vaccines, and keep mission critical aspects of the U.S. economy functioning during the pandemic.

The Competition Continuum

The competition continuum includes the following conditions: Armed conflict, competition below armed conflict and cooperation. Competition below armed conflict is the condition which U.S. rivals are exploiting in order to achieve strategic aims. "Competition below armed conflict is defined as "situations in which joint forces take actions outside of armed conflict against a strategic actor in pursuit of policy objectives."[1]
Joint Doctrine describes the new state of the world. "Rather than a world either at peace or at war, the

competition continuum describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict and armed conflict."[1] It is important for modern military doctrine to view the world as our adversaries do. This concept was described by the previous Chairman of the Joint Chiefs of Staff (CJCS) in 2016: "Our traditional way that we differentiate between peace and war is insufficient to [the dynamic of competition below armed conflict]." "We think of being at peace or war…our adversaries don't think that way."[1] Furthermore, Joint doctrine describes how rivals play in the competition continuum, "The current operational environment requires a more nuanced model. Geopolitical rivals such as Russia and China employ a mixture of instruments of national power to achieve significant strategic advantages in a manner calculated not to trigger our legal or institutional thresholds for armed conflict."[1]

When rivals compete below the threshold for armed conflict they achieve political ends without triggering U.S. thresholds. When thresholds are not met, contingency declaration, expanded authorities, protectionist law waivers, and the DPA are not used. The procurement hands of the military are tied and the full capability to react at the speed of war cannot be realized.

A Call for Change

In order to successfully compete below armed conflict, combatant commanders need the equivalent wartime acquisition authorities to maneuver at the speed of relevance.

During the summer of 2020, the secretary of defense directed EUCOM to execute a flexible deterrent option (FDO) in the form of a dynamic force employment (DFE). This DFE called for the reposition of a Combined Arms Battalion to Eastern Europe. This movement required a $1 million commercial line haul contract in order to reposition the force as soon as possible. The peacetime contracting lead time for this action was 90 days. This timeline failed to meet the commander's intent preventing timely power projection. Expanded wartime acquisition authorities could have reduced the acquisition timeline to 10 days. Delegation of wartime acquisition authorities to combatant commanders will enable effective competition below armed conflict.

The speed of operational requirements in the modern world occur faster than Congress can pass an appropriation or the president declare a contingency. In order to compete today, contracting requires planning and global integration. Lawmakers should consider changes that allow for wartime FAR authorities at the discretion of the combatant commander's competition requirements. Certain domestic restrictions such as the Berry Amendment and Buy American Act could receive blanket waivers for acquisitions needed for competition. The DPA could be leveraged offensively by the president to compete against our rivals. The DPA could be used to deny or degrade strategic rivals access to U.S. resources and our economy.

Conclusion

Joint doctrine has recognized the competition continuum. Lawmakers and the military need to realign the acquisition continuum to support global competition below armed conflict. Wartime FAR authorities should be allowed for use by combatant commanders and domestic restrictions waived for acquisitions supporting competition. The DPA could be weaponized for competition against our rivals. In order to compete, our government needs to make changes to laws and acquisition regulations.

Disclaimer: the opinions or assertions contained herein are the private views of the author, and are not to be construed as official, or reflecting true views of the Department of the Army or the Department of Defense (DOD).

Notes:

[1] Joint Doctrine note 1-9 competition continuum

[2] ASA (ALT) Fiscal year 2019 Procurement Administrative Lead Times Goal memorandum

[3] https://www.fema.gov/disaster/defense-production-act/dpa-authorities

HONORABLE MENTION

Acquiring Innovation in the 21st Century: Accelerating Procurement as a Weapon of War

By the following author:

Robert E. Finley

Introduction

"Speak softly and carry a big stick."

—Teddy Roosevelt

To retain its position as the dominant superpower, the U.S. must "speak softly," that is, engage its allies and adversaries in productive economic and diplomatic dialogue, and "carry a big stick," meaning sustain a highly proficient, well equipped, and ready military. A non-nuclear conflict with China or Russia will escalate too quickly to mobilize the U.S. industrial base. The Great Power Competition is upon us. Unlike WWII, the U.S. must be ready at a moment's notice to fight and win in any domain, Air, Sea, Land, Space or Cyber.

However, there are accusations that the acquisition system is "at an inflection point in terms of its competitiveness and technological advancement against global competitors, friends, and foes."[1] Fears prevail that China's autocracy expedites strategic decisions in acquiring innovative weapons. Former Secretary of the Air Force for Acquisition Dr. Will Roper critically points out that "we do not own the Acquisition OODA loop[2]. If this remains status quo, we lose the competition with China."[3] Popular "reform initiatives" commonly suggest competing head-to-head with China by streamlining policy or relaxing legislative oversight, yet with minimal success.[4] Instead, evidence suggests that most "political reforms have the effect of promoting selective private interest at the larger sacrifice of the public interest."[5]

Looking to the past, I.B. Holley advised that "the procurement process itself is a weapon of war."[6] The hypothesis offered here is that acquisition policy and law are not the underlying root cause of confusion and delay. The obstacles to capturing novel warfighting capabilities lie inside the acquisition community with clumsy processes and arcane tools. This theory aligns with General Hyten's observation that "the interesting thing I found when I went through all of [the acquisition policies] is that actually, if you want to go fast, all the authorities are right there. They're written down and they're allowed."[7] Roper proselytized his acquisition reformation by proclaiming the gospel of "The Digital Trinity."[8] While his transfiguration of digital engineering is a crucial initiative, his plan alone is insufficient. The acquisition OODA loop must also automate the "Program Manager's Trinity" of cost, schedule and performance (C/S/P).

eBay© democratizes commerce[9] by transforming a Saturday rummaging through boxes at the neighborhood yard sale into a late-night impulse purchase powered with a global digital query. Likewise, mobilizing for the Great Power Competition requires leveraging the power of information technology and high-powered Big Data[10] analytics to modernize Holley's procurement process into a digital weapon of war.

The Root Dilemmas

"If you choose not to decide, you still have made a choice."

—Neil Peart

Reimagining Acquisition as a computerized arsenal of information, two critical dilemmas emerge. Program managers face a planning dilemma of balancing "the need for speed and efficiency in acquisition against the need to provide proper oversight of how DOD spends taxpayer dollars."[11] During execution, the program managers' dilemma becomes balancing "the need to push the technological edge in developing weapons systems against the imperative to deliver programs on-time and on-budget."[12] Rooted in the challenges of the principal-agent problem, failure to address these dilemmas sprouts the weeds of distracting delay, stunts acquisition growth and chokes the fruit of innovation.

Notoriously slow, opaque, and prone to error, DOD contract development is stuck in the 1990s, at best. Sponsors spend extensive political capital getting projects approved only to wait 12-36 months for a contract award. Furthermore, once a program starts, a post-award validation that the contract implements the strategy intended seldom occurs. The contract is where the acquisition strategy truly becomes manifest. It is the contract that binds principal to agent,[13] incentives to outcomes, requirements to funding, and solidifies the choice among potential alternatives into a single concrete decision.

Therefore, first and foremost, the principal's mission to capture an innovation's value lies in creating a high-quality contract.

Quickening the acquisition OODA loop is imperative. The "paralysis by analysis" of "getting it right" during the Orient step "means that there are no decisions and thus no actions. In reality, a decision has been made to do nothing. Time keeps moving, and resources are used."[14] Meanwhile, the decisiveness of authoritarianism moves forward.

Improving Acquisition – A Basic Remedy

"Real strategies render choices about what not to do as important as choices about what to do." [15]

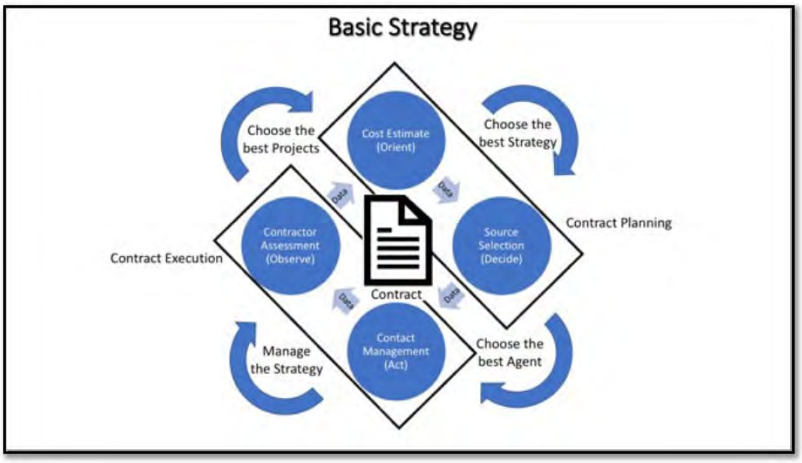
—Michael Porter

Currently, "acquisition strategies" are not strategies in the way generals think about a military strategy. The name acquisition strategy conjures an image of comprehensive battle plans that clearly outline the ends, ways and means for delivering the exotic gadgets warfighters desperately deserve. However, once leaders approve funding, the process chews and casts aside the compulsory checklist like bureaucratic crumbs in the Pentagon's multi-billion-dollar game of Hungry Hungry Hippos.[16] To make decisive trade-offs, for example, the purchase of expensive intellectual property rights,[17] principals controlling a major defense acquisition program (MDAP) require real-time, integrated and continuous situational awareness of both current and life cycle C/S/P.

Previous generations accepted the premise that the "relevant information for evaluating performance is imperfect, costly to obtain and unequally distributed between the agent and his principals."[18] However, over the past 20 years, companies like eBay©, Amazon©, and Google© show the value created by the power of information technology and cheap, ubiquitous data. Large datasets are now inexpensive to collect relative to their size and update in real-time. The data exhaust of life "can be recorded and quantified in a way that would have been hard to imagine just a decade ago"[19] and reveals insights that lead to better decisions and strategic business moves.[20] Big data holds the promise to lubricate the frictional delays of the acquisition OODA loop.

Following the pattern prescribed by John Boyd, future program managers need improved capabilities to:

- Observe. Choose the best projects.
- Orient. Choose the best strategy.
- Decide. Choose the best agent.
- Act. Manage the strategy.



CONTRACTOR ASSESSMENT

When considering a new project, principals should first observe agents' productivity across multiple existing projects more objectively. Today's Contractor Performance Assessment Reporting System (CPARS) is similar to the Personal Credit Rating systems of the 1840s that used subjective reputation reports to establish an individual's creditworthiness.[21] Principals require an objective "Equifax©- like" system, leveraging C/S/P data collected from hundreds of projects, which institutes an accurate "credit rating" system for all agents. A persistent industry analysis of relevant business units arms principals with information to temper ambitious warfighter desires with credible feasibility assessments. Principals must choose the best projects before financing.

Program Estimating

Losing early advantage in contract planning, principals do not orient themselves with high-quality, independent estimates. A lesson from French procurement reform found "poor ex ante analysis means that projects are given low cost estimates, which then naturally rise once the contracts are let."[22] More focused on keeping the program alive, the principal's motivations to avoid a failed award often outweigh the primary duty to award a high-quality contract. Developing more realistic and informative program estimates will enable multi-scenario comparisons and inform budgeting decisions before poor decisions become commitments. Like using Zillow© to scour the housing market for real estate investment opportunities, high-fidelity life cycle cost models highlight the value and risks of choosing the best strategy.

Source Selection

Just as using Turbo-Tax© lessens the trepidation of an audit, improving the consistency, workflow, transparency and integrity of source selections and contract awards clarifies the principal's ability to decide. Wanting to avoid disaster, principals rush, sometimes without due diligence, into flawed contracts, and do not choose the best agent. As noted earlier, the contract award is the critical juncture, and here motivations are most misaligned. Agents prefer contracts with loopholes and use the threat of protest as pressure. By reducing the anxiety of protest and increasing the confidence of conducting a transparent and open competition, there is an enormous opportunity to accelerate the acquisition OODA loop by automating the creation and release of substantial proposals. Maximizing speed and assurance in proposal evaluation and negotiation reduces audit fear and allows principals to focus on crucial value choices.

Contract Management

While principals often get earned value management (EVM) data from agents, the lack of real-time impact assessment obfuscates its usefulness to manage the strategy. Like a version of Google Maps© that only provides a current location and no directions, cost overruns and schedule slips surface after the opportunity to act is passed. The agent's incentive is embellishing progress and obscuring alterations in performance. The predictive power of EVM is typically possible only with a labor-intensive and agent-driven cost and schedule risk assessment (CSRA). Extracting EVM source data directly from the agent and automating a principal-led CSRA more clearly illuminates future risks with helpful schedule and cost predictions. With improved "turn-by-turn driving directions," principals make timely course corrections before they "get lost or stuck in traffic."

Connecting these tools of contractor assessment, program estimating, source selections and contract management multiplies their power by creating a digital feedback acquisition OODA loop that more actively controls C/S/P. Reformed contractor assessments enhance future program estimates, which improve source selections and contract awards, which lead to more predictive contract management, which returns accuracy to contractor assessments. Each step inheriting value from the previous step and feeding decision-making benefits forward to the next. "Gaining an advantage comes from quickness over the entire OODA loop. With each iteration, the changes are smaller and can be more easily managed, therefore staying ahead of the competition"[23] with China.

Risks

"Governments never learn. Only people learn."

—Milton Friedman

The transition to high-powered data analytics is an uphill battle. According to David Spiegelhalter, Winton Professor of the Public Understanding of Risk at Cambridge University, "There are a lot of small data problems that occur in big data. They don't disappear because you [have a large dataset]. They get worse."[24] Up to 85 percent of projects fail, and evidence suggests that management understanding, organizational alignment and general organizational resistance are the more common culprits. The primary causes of failure are the difficulties of integrating new tools with existing business processes and applications and overcoming the challenges of management resistance, internal politics, skill development, security and governance.[25]

Conclusion

"Let us not seek to fix the blame for the past. Let us accept our own responsibility for the future."

—John F. Kennedy

The initiative for innovation lies in the Armed Services' hands, and acquisition policy and law are not the only impediments. Though challenging, the opportunity for introspective acquisition reform is readily accessible to the principals. Using rapid, competitive and intelligent

business decision-making to improve cost estimating, source selections, contract management and contractor assessment will secure more value from innovations. Accelerating the acquisition OODA loop is a more compelling method to challenge China's strategic authoritarian decision-making advantage. High-powered big data analytics modernizes Holley's procurement process as a digital weapon of war.

The views expressed in this paper are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense or the U.S. Government.

Notes:

[1] "Emerging Technology And National Security," 2018 Analytic Exchange Program, July 26, 2018, https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf

[2] "Developed by Col. John Boyd, U.S. Air Force, the Observe, Orient, Decide, and Act Loop (OODA) describes the decision-making processes needed to win at war or gain strategic advantage in any situation. Recently, the OODA Loop has been applied to business and product development as a way to describe decision-making cycles."- Ullman. David G., "'OO-OO-OO!' The Sound of a Broken OODA Loop," CROSSTALK The Journal of Defense Software Engineering, April 2007, https://docs.wixstatic.com/ugd/20f020_65b20dec99cb45d0bd-1456ed526c09b8.pdf

[3] Roper, Will, "There is No Spoon: The New Digital Acquisition Reality," September 18, 2020

[4] Sapolsky, Harvey, "Let's Skip Acquisition Reform This Time," DefenseNews, February 9, 2009, p. 29

[5] Lee, Dwight R., "Public Goods, Politics, and Two Cheers for the Military. Industrial Complex"

[6] Holley Jr., Irving B., "Buying Aircraft : Matériel Procurement for the Army Air Forces," United States Army in World War II, Special Studies, Office of the Chief of Military History, Dept. of the Army, 1964, pg. 569, https://history.army.mil/html/books/011/11-2/CMH_Pub_11-2.pdf

[7] Hyten, General John E., "A Conversation with General John Hyten, Vice Chairman of the Joint Chiefs of Staff," Transcript, Center for Strategic and International Studies, January 17, 2020, https://www.csis.org/analysis/conversation-general-john-hyten-vice-chairman-joint-chiefs-staff

[8] The "Digital Trinity" is the control of engineering and technology information through 1) Digital Engineering and Management, 2) Agile Software Development, and 3) Open [Hardware] Architectures. - Ibid. Roper

[9] Kawasaki, Guy "The art of innovation | Guy Kawasaki | TEDxBerkeley," TEDx Talks, February 22, 2014, accessed October 26, 2020, https://m.youtube.com/watch?v=Mtjatz9r-Vc

[10] "Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis." - "Big Data What it is and why it matters," - SAS Institute Inc., 2021, accessed February 27, 2021, https://www.sas.com/en_us/insights/big-data/what-is-big- data.html

[11] Blume, Susanna V., Parrish, Molly, "Make Good Choices, DoD Optimizing Core Decision-making Processes for Great-Power Competition," Center for a New American Security, November 2019. https://www.jstor.org/stable/pdf/resrep20433.7.pdf

[12] Ibid. Blume & Parrish

[13] In this review, the term Principal will refer to Department of Defense Acquisition officials that are typically the authors or approvers of Acquisition Strategies for MDAPs. From here, the term Agent refers to the producers or suppliers of the acquired product or service via the Acquisition Strategy, that is, defense contractors.

[14] Ibid. Ullman

[15] Porter, Michael, "What is Strategy?" Harvard Business Review, November-December 1996, https://hbr.org/1996/11/what-is-strategy

[16] [Satire] "Pentagon admits defense budgeting modeled on Hungry Hungry Hippos," Duffleblog, October 1, 2019, https://www.duffelblog.com/p/pentagon-admits-defense-budgeting-modeled-on-hungry-hungry- hippos

[17] Erwin, Sandra I., "Intellectual Property Fights Par for the Course in F-35 Program," National Defense Magazine, September 8, 2016, accessed October 26, 2020, https://www.nationaldefensemagazine.org/articles/2016/9/8/intellectual-property-fights-par-for-the-course- in-f-35-program

[18] Ibid. Johnson.

[19] Harford, Tim, "Big Data: are we making a big mistake?" FT.com, March 28, 2014, Accessed September 1, 2021, https://www.proquest.com/trade-journals/big-data-are-we-making- mistake/docview/1519224530/se-2?accountid=40390

[20] Ibid. SAS Institute.

[21] Trainor, Sean, "The Long, Twisted History of Your Credit Score," Time, July 22, 2015, accessed February 28, 2021, https://time.com/3961676/history-credit-scores/

[22] Ibid. Kia-Stein.

[23] Ibid. Ullman.

[24] Ibid. Harford.

[25] Asay, Matt, "85% of big data projects fail, but your developers can help yours succeed," Tech Republic, November 10, 2017, accessed October 27, 2021, https://www.techrepublic.com/article/85-of-big-data- projects-fail-but-your-developers-can-help-yours-succeed/

Category: Future Operations

WINNER

Change the Contingency Contracting Support Model to a Centralized, CONUS-Based Contingency Contracting Support Center

By the following author:

Maj. Joseph D. Levin

Throughout the War on Terror, contracting personnel have supported the warfighter in different countries, through surges and drawdowns, and towards many different mission priorities. Through it all the contracting mission has fluctuated and adjusted to provide continuous support to the warfighter. The challenges of sustaining the contingency contracting mission have exposed weaknesses in the outside the continental United States (OCONUS) contracting center model specifically as it applies to contingency operations. In particular, reliance upon regional contracting centers (RCCs) located inside combat zones has increased costs and created substantial logistical challenges while reducing the effectiveness of the government civilian workforce assigned to the RCCs.

To address these issues, the Army should change how it provides contingency contracting support by leveraging the lessons learned and technological advancements of the remote working model relied upon in response to the Coronavirus pandemic. The Army should establish a continental United States (CONUS)-based contingency contracting support center which is dedicated to providing OCONUS contingency contracting support, including supporting the missions in the U.S. Central Command (CENTCOM) area of responsibility (AOR) and other future operations. Applying the lessons learned about the use of remote working capabilities to contingency contracting missions would allow the Army to fully utilize the strengths and benefits of the government civilian workforce, reduce costs and the logistical burden of supporting numerous overseas contracting offices mostly staffed by civilian employees, and increase the agility and flexibility of the contracting command to support future operations.

In the current contingency contracting model, using the CENTCOM AOR as an example, RCCs are located throughout the CENTCOM AOR supporting regional contingency operations. Similar to their CONUS counterparts, the RCCs are primarily staffed with military and government civilian employees, with civilian employees being the majority of the workforce. The civilian employees staffing these centers deploy from permanent CONUS home stations with tour lengths ranging from 6–24 months. While deployed, civilian employees receive temporary pay increases up to 70 percent more than their normal hourly pay, generous overtime opportunities, and some even take positions that include temporary General Schedule (GS) grade promotions.

Despite these generous incentives, RCCs have experienced persistent civilian staffing challenges. To

deploy, civilian employees must meet stringent medical eligibility standards and accept the challenges of deploying to a contingency environment. This includes separation from family, austere living conditions and residing in hostile fire areas. The deployed positions are stressful; employees are expected to maintain a high operational tempo and often work the maximum permitted overtime hours, while facing many of the same safety risks as the warfighters they are supporting. Unsurprisingly, the RCCs experience high turnover rates of civilian employees (based on normal rotation schedules as well as those who elect to voluntarily end their tours early) and difficulty filling the overseas positions. In this environment, both military and civilian employees often find themselves preparing to end their rotation just as they were getting settled into the position.

The result of the high turnover rate of the civilian workforce in the RCCs is a loss of continuity—normally one of the bedrock benefits of the Army's civilian workforce. This lack of continuity of either civilian or military personnel creates persistent gaps in institutional knowledge, where lessons learned are lost and contract actions are constantly being handed off to newly incoming personnel, who themselves inherit contract actions knowing they will not be there through the end of the requirement. These knowledge gaps are exacerbated because the newly incoming civilian employees frequently receive inadequate training on contingency contracting before deploying.

In addition to these staffing and training issues, the logistical and cost burdens of maintaining RCCs in the CENTCOM AOR is substantial. Every individual mobilization and re-deployment costs the Army thousands of dollars, in addition to the increased employee compensation costs due to the pay differential, while the deployed civilian leaves a gap in their home station's ranks while they are away. As the mission shifts, RCCs also relocate or get consolidated, creating confusion when old contracts require follow-on actions.

The justification for these high costs is more in doubt considering that placing RCCs in combat zones has not increased their effectiveness for contract oversight—audits have repeatedly identified fraud, waste and abuse as a material weakness in contingency contracting that goes uncorrected. Furthermore, logistical challenges such as unreliable networks cause RCC personnel to frequently lose access to systems and recordkeeping databases necessary to perform their tasks. These high costs, decreased effectiveness and the unresolved material problems directly resulting from the current contingency contracting program indicate the need for a new model.

The Coronavirus pandemic forced the Army to change how it performs many of its day-to-day functions. One of the most significant changes is reducing the number of personnel co-located in buildings through increased use of remote work stations. The necessity of remote work has caused a rapid increase in the utilization of technology such as Zoom and Microsoft Teams to accomplish tasks that previously required in-person interaction. The technology has rapidly advanced including increased reliability, improved security and new capabilities in response to the demands of its user base. Remote work technology is now a fixture of the contracting support workplace and basic technological literacy in its use is already required across the civilian workforce.

While many are understandably eager to return to a pre-pandemic workplace, we should not abandon these new capabilities. The past 18 months have shown that remote workplace technology works and it can be leveraged to allow contracting support centers to function with more agility and flexibility by providing contingency contracting support from one centralized location to multiple missions in remote locations. A CONUS-based contingency contracting support center could use the same technology to provide continuous support to multiple contingency contracting missions from one centralized location while removing the logistical and institutional challenges the RCCs currently face when placed in forward deployed locations.

A CONUS-based contingency contracting support center would permanently employ government civilians who are not on deployment rotation schedules, while applying the same medical hiring standards as other CONUS offices. These civilian employees of the contingency contracting support center would restore the tremendously important value-added features of continuity and institutional knowledge at a fraction of the current personnel costs of OCONUS RCCs. Because the CONUS-based contingency contracting support center would be centrally and permanently located in one place, it would be able to provide support to multiple contingency operations without needing to uproot and relocate itself as the mission shifts. Whereas a change in mission requirements in the CENTCOM AOR could currently

require physically relocating an entire office as well as adding or subtracting personnel through the arduous mobilization and deployment process, a CONUS-based office would never need to relocate, and could surge personnel through a faster hiring process or by accessing CONUS-based borrowed manpower.

Along with providing better, more consistent contingency contracting support, a CONUS-based center would reduce the contracting command's footprint in the deployed environment, thus reducing costs and freeing up space for use by the warfighter. If the RCC commander still wished to be physically present in the combat zone to integrate with their requiring activity, and to perform their role as advisor to the senior mission commander, they could still maintain a deployed posture. This forward deployed posture of the RCC commander and their core support staff would be in a significantly reduced footprint and could utilize technology to maintain command and control of the CONUS-based contracting station. Alternatively, the RCC commander could remain primarily at the CONUS-based station, and assign a liaison officer to the forward deployed OCONUS locations, utilizing technology and temporary duty (TDY) travel as necessary to interface with the requiring activity.

This is not an entirely new concept. The RCCs have historically relied upon reach back support from CONUS contracting offices as well as using liaison officers at bases in the CENTCOM AOR, even when the RCC commander was also forward deployed. Several larger contracting requirements have been procured by CONUS-based offices such as Army Contracting Command (ACC)-Rock Island and then assigned to administrative contracting officers stationed at the OCONUS RCCs. Whereas current reach back support is provided by personnel from various contracting offices, or the rear detachment of whichever unit provided the forward-deployed RCC command team, the proposed contracting center would provide consistent, co-located support and consolidate reach back resources in one dedicated location.

Understandably, there would be some concerns with this model. The contracting center would be in a different time zone and not co-located with its requiring activities. For the first concern, there is precedent for CONUS reach back support elements maintaining a duty day schedule aligned with their forward-deployed elements, when necessary. Whereas an office such as ACC-Rock Island, which only provides occasional contingency procurement support, would typically not alter their duty day, a CONUS-based contingency contracting center could manage larger overseas procurements, reducing their reliance upon other contracting offices and allowing them to better align their schedule and their focus exclusively on the contingency missions they are supporting.

The second concern, that the RCC commander is not co-located with their requiring activities, is readily addressed by the same remote work technology already discussed. Personnel could travel in a TDY status when necessary, or could rely upon forward deployed liaison officers from the contracting command to provide in-person interface as needed. Finally, individually forward-deployed personnel could also be utilized for positions that absolutely require it, such as some personnel involved in contract administration and quality assurance.

In conclusion, the Army should utilize the lessons learned from the Coronavirus pandemic by leveraging the advances in remote work technology to create a CONUS-based contingency contracting center. This CONUS-based contingency contracting center would be the permanent duty station of the civilian contracting employees supporting overseas contingency operations. It would handle the functions currently performed by OCONUS RCCs located in combat zones as well as those already being done by various CONUS reach back support elements. Forward deployed contracting personnel would be reduced to a smaller element comprised of the senior mission commander's business advisor and his core staff, or a contracting command liaison officer. This contingency contracting center would support the CENTCOM AOR as well as any future contingency or expeditionary contracting missions. This solution would resolve the problems described in this paper that exist in the current contingency contracting model while creating a technology-leveraged, modern contracting center that is flexible, agile, and ready to support the warfighter in whatever missions may come.

Disclaimer: The opinions, summaries and views presented are personal in nature and do not represent the official opinions or views of the Department of Defense or its components.

Notes:

Department of Defense Office of the Inspector General, Audit of Army Contracting Command-Afghanistan's Award and Administration of Contracts, DODIG-2020-094, at 2 (June 18, 2020) [hereinafter "ACC-A AUDIT"]

Id. At 3.

For further discussion, see, e.g. Defense Finance and Accounting Service, Theater Entitlements, November 16, 2015, retrieved from: https://www.dfas.mil/civilianemployees/understandingyourcivilianpay/theaterentitlements/

ACC-A AUDIT, supra note 1, at 57.

Id. At 23.

See Modification Fifteen to USCENTCOM Individual Protection and Individual-Unit Deployment Policy, para. 15.C (August 29, 2020).

ACC-A AUDIT, supra note 1 at 57.

See, e.g., id. at 20 (finding that ACC-A employees "were unfamiliar with key contingency contracting procedures.").

Id. at 18-20.

Discussed supra note 3.

ACC-A AUDIT, supra note 1 at 4-5.

Id. at 27-28.

See Zoom for Government, https://www.zoomgov.com/.

See Microsoft Teams, https://www.microsoft.com/en-us/microsoft-teams/group-chat-software For further discussion, see, e.g., Zoom Platform Updates: Empower Hybrid Teams, Connect Workstreams, and Engage Communities, ZOOM BLOG, September 13, 2021, https://blog.zoom.us/zoom-platform-enhancements-zoomtopia-2021/.

Under the current model, it takes six months to fill a vacancy, including approximately 90 days from date of selection to deploy someone to an OCONUS RCC. ACC-A AUDIT, supra note 1, at 23.

HONORABLE MENTION

Protecting the Future Force in Multi-Domain Operations

By the following authors:

Lt. Col. Curtis Brooker

Dr. Christina Bates

Throughout the 20-year war in Afghanistan and Iraq, the United States Army's notions of force protection evolved and matured. In turn, the capabilities required to provide robust force protection evolved to pace threats. For example, in the early days of the war, the threat from improvised explosive devices (IEDs) ultimately led to the deployment of up-armored Humvees, the development of the Mine Resistant Ambush Protected (MRAP) family of fighting vehicles, and the deployment of sensors to detect IEDs at standoff ranges (force protection) during route clearance missions. Similarly, the proliferation of forward operating bases (FOBs), as well as expeditionary combat outposts led to the need for sophisticated, integrated surveillance and reconnaissance capabilities to both detect and deter potential threats to the force, thereby preserving combat power, minimizing casualties and protecting critical assets.

In light of the Afghanistan withdrawal, the Army's focus on modernization, and the advent of the multi-domain operations (MDO) construct, the Army now must re-examine notions of force protection as it relates to MDO. In other words, the Army must determine and predict its force protection posture and needs, and in turn the associated capabilities required to preserve combat power and minimize casualties within a MDO battle.

This article represents an initial step in this critical thought process. Its primary aim is to set forth enduring force protection tenets and to discuss potential paths for extrapolating from these tenets to plot the likely,

main enablers of force protection within MDO. It is the authors' hope that others will take up the principles discussed in this piece and continue their development with a drive toward eventual application and execution.

Force Protection: Then

Long-standing Army notions of force protection point to a two-fold purpose: Preserving the force's combat potential; and minimizing casualties and damage to resources. One may decompose these two broad purposes into more specific tenets, as follows: detection of any and all threats; integration of intelligence information to ensure informed decisions; destruction of enemy threats (including long-range counter-measures) before they may be employed; defending against enemy systems; and measures taken to survive successful enemy attacks.

If we trace force protection efforts throughout the Afghanistan and Iraq wars, we quickly recognize that all of the tenets played an integral role in protecting the force (and its enablers—resources) and preserving combat potential. While the threats to the force certainly evolved throughout the 20-year span (and some did so exponentially), the need to address the force protection tenets remained not only steady, but urgent.

Across these two decades, the Army Acquisition Corps and specifically Project Manager Terrestrial Sensors (PM TS) were heavily engaged in developing, deploying and sustaining numerous force protection capabilities to pace and combat threats to the force, even as these threats continued to evolve and morph. Many of these capabilities were developed and deployed to combat very specific threats, including tunneling, IEDs, vehicle borne IEDs and numerous other asymmetric threats.

Now, the Army is modernizing to fight the future war. It is theorized that this future war will largely comprise various threats originating from, and operating across multiple domains (hence, the MDO construct). While threats to the force may "look and feel" different than in the previous war, and may originate from unexpected domains that were rarely, if ever encountered, the tenets of force protection remain. In other words, as long as we have a force (whether comprising man and/or machine), that force will require protection to preserve combat potential and resources, and ultimately save lives. Additionally, as future wars will likely involve a significant coalition effort, notions of force protection must span the coalition, since, at minimum, coalition preservation is in essence, combat preservation.

Force Protection: Now

If we assume the force protection tenets previously discussed endure in an MDO environment, then the question for the Army becomes, "what capabilities are needed to effectively address these tenets and in turn, protect an MDO force?"

To begin to think through how the Army may answer this question, we must first examine MDO. MDO is formally defined as "a description of how the U.S. Army, as part of the Joint Force (Army, Navy, Air Force, and Marines) can counter and defeat a near-peer adversary capable of contesting the U.S. in all domains (air, land, maritime, space and cyberspace) in both competition and armed conflict. The concept describes how U.S. ground forces, as part of the joint and multinational team, deter adversaries and defeat highly capable near-peer enemies in the 2025-2050 timeframe." Army leadership has indicated "MDO will not only have an impact on Army organizations and operations; it will drive Army modernization efforts as well, in terms of development and acquisition of supporting capabilities and systems." Thus, it is clear that MDO must drive the evolution of force protection capabilities, as they are clearly "supporting capabilities and systems."

The caliber, accuracy, access to and sharing of data will be absolutely consequential in future wars. As evidenced by the increased emphasis on the cyberspace domain, and recent examples of the impact of cyber-attacks, including attacks on the U.S. gas pipelines in 2021, the ability to keep the force informed with accurate, uncompromised and rapid data will prove pivotal. Data will be a main factor in the force's ability to develop and maintain a timely understanding of the battlespace, for defensive and offensive purposes. Hence, force protection systems must have the ability to rapidly access, interpret, secure, and share data that informs decisive action.

At PM TS, we are exploring how artificial intelligence (AI) and machine learning (ML) can assist with force protection, and particularly with the processing of data that ultimately eases the burden on the commander by organizing and prioritizing information. For example, the faster and more accurately information can be prioritized for further evaluation and interpretation, the faster decisions can be made to improve force protection posture.

In years prior, PM TS began looking at these principles as part of its Sensor Computing Environment initiative.

(Sensor CE) The aim of the initiative was to develop standards and formats for sensors to achieve a "plug-and-play" type of environment in which they could "see" and share data with each other, thereby acting as a kind of data "force multiplier." Sensor CE also endeavored to break down existing, singular "stove-piped" sensors and, in turn stove-piped data and integrate the "pipes" to enable rapid data-accessing and sharing.

In a very real manner, Sensor CE was moving down the path to AI and ML. Before a system can leverage all the benefits of algorithms, data of a particular caliber must exist to effectively develop and inform the algorithms. Thus, the data that early force protection sensor systems gathered was a necessary prerequisite to ultimately realizing the early potential of AI and ML for force protection systems.

In rough parallel with the Sensor CE initiative, PM TS also began pursuing, and ultimately implemented data fusion (a predecessor of what we now think of today in the Army as AI and ML). Data fusion served to further exploit the data being gathered by surveillance and reconnaissance sensors, resulting in a "whole is greater than the sum of its parts" effect.

Bringing this thinking to the current day, it stands to reason that a key enabler of force protection in MDO will be data that informs AI, and AI in turn enables rapid decision making and associated action. As such, PM TS is examining and assessing capabilities that not only "stare" (i.e., survey) and to a degree "fuse" data, but also store and process data and present that data in ways that are immediately meaningful to, and actionable by the commander. These systems will incorporate sophisticated algorithms that are capable of conducting a degree of "thinking" and "evaluating" for the commander, thereby easing the burden on him/her, reducing the time from sensor-to-shooter and enabling more robust force protection.

Moving Forward

In this article, the authors suggest that force protection will continue to be a critical component as we transition from current ways of conducting war to the future fight, such as MDO. Therefore, the manner in which we execute force protection must advance in a way that both satisfies the existing tenets of force protection, and simultaneously exploits advancements in technology, including AI and ML to unlock the full potential of data. Unlocking the full potential of data will inform better and faster decision-making and action in the MDO space. As long as we have a force, it needs protection. The Army must continue to wrestle with the questions posed in this article to determine how to provide robust force protection in the future and to continue to evolve critical capabilities to do so.

Category: Innovation

WINNERS

Creative Acquisition and the Cyber Battlefield: Using Rapid Prototyping to Address Pressing Cyberspace Challenges Acquisition

By the following author:
Fianna Litvok

The U.S. faces significant cyber threats every day. In recent months, cyberattacks have intensified in scale, frequency and scope, putting us on heightened alert and threatening our national security. The cyberspace battlefield is constantly evolving as threats and tactics continue to shift. In response, the U.S. Army's defensive cyber enterprise is fielding cutting-edge capabilities to cyber warriors as rapidly as possible. Defensive Cyber Operations (DCO)—part of the U.S. Army Program Executive Office Enterprise Information Systems (PEO EIS)—aims to continually adapt, develop and update those capabilities to ensure cyber defenders' operational readiness and their ability to outpace U.S. adversaries' cyber arsenals.

Time is of the essence in the defensive cyber domain. In January 2020, the Department of Defense (DOD) rewrote its DOD 5000 series acquisition policies, introducing the Adaptive Acquisition Framework (AAF) to shorten prototype, development and acquisition timelines. According to the AAF, the "urgent capability" pathway aims to "fulfill urgent operational needs (UONs) or other quick reaction capabilities (QRCs) in less than two years."[1] This revision was a huge step in the right direction, but the cyber enterprise needs something even faster.

The cyber battlefield necessitates an innovation paradigm that empowers us to work at the "speed of relevance,"[2] or, what we like to call, the "speed of cyber." Cyber challenges demand creative solution delivery methods and novel ways of thinking. But novelty and innovation do not always come easily to military organizations. As scholar Andrew Hill stated, "For modern militaries, innovation is not a scientific or technical problem; it is an organizational challenge."[3]

In 2018, Applied Cyber Technologies (ACT), a product office within PEO EIS's DCO, was charged with rapidly assessing, acquiring, integrating and deploying advanced defensive cyber solutions for cyber forces. Many questions had to be answered, including: How do we secure cyber solutions faster than traditional acquisition methods allow? How do we solve pressing cyber challenges in an iterative way? How do we continually improve defensive cyber tools to meet cyber warriors' evolving needs?

Shortly after ACT's inception, the team developed a rapid acquisition framework by strategically using the other transaction authority (OTA), an acquisition vehicle that offers a truncated, flexible way to develop prototype solutions. Prototypes often adequately address cyber defenders' immediate needs and lay a solid foundation for material solution acquisition. To this end, ACT created its own OTA—the Cyberspace Operations Broad Responsive Agreement (COBRA)—to meet the specific needs of the defensive cyber enterprise.

In 2019, ACT introduced the "Labyrinth," a nimble mechanism designed to resolve the most acute challenges facing cyber warriors. Labyrinth capitalizes on the power of the COBRA OTA and creatively leverages industry partners and academia to quickly secure or refine existing cyber tools within weeks or months.

The Labyrinth Process

Labyrinth is a surprisingly simple process: ACT works with various entities within the defensive cyber enterprise to identify a critical issue. Once an issue is identified and defined, ACT informs its partner ecosystem about it. In response, the partners submit white papers detailing how they propose to address the problem. The ACT team reviews the submissions and down-selects to those partners that can best resolve the issue.

ACT uses industry-leading project management practices such as development, security and operations (DevSecOps) and Agile methodologies. Within this construct, work is performed in segmented blocks, the smallest of which is called a "sprint." Labyrinth partners are required to perform work in sprints and demonstrate completed work at the end of each performance block. If a task is performed satisfactorily, the government pays the partner. Once a partner receives payment, also known as the "bounty," the government takes ownership of the intellectual property and data rights. If a partner does not complete a task on time, the government can grant the partner additional time. Alternatively, the government may choose not to pay for the task and instead, close it. Notably, Labyrinth partners are paid for a successfully completed task, not for their time. This enables the Army to better manage costs and provides greater control over end product delivery.

Labyrinth requires a common platform where partners can communicate, manage projects and collaborate. ACT decided to use JIRA, a tool in the Defense Intelligence Information Enterprise (DI2E), the DOD's robust project management platform. Labyrinth partners secure DI2E accounts during the onboarding process. By heavily leveraging existing platforms, ACT is able to maximize productivity, efficiency and innovation, while keeping costs down.

The Labyrinth 1.0: Breaking Ground and Shifting Cultures

When ACT embarked on Labyrinth 1.0, the team had to accept a fundamental truth: Labyrinth wasn't just a new process; it was a jolt to a deeply-entrenched ethos. It was unlike anything the DOD and industrial base had seen before. Labyrinth required partners to step outside their comfort zone of using the Federal Acquisition Regulation (FAR)—and even AAF—and into an OTA world unfamiliar to many. ACT knew that Labyrinth was an acquisition oddity but had faith it would work … it needed to work. Cyber defenders are on the front lines of the cyber battle every day, and they need the best tools right now. The stakes for them and our country are high.

The technical goal of Labyrinth 1.0 was to update virtual machine images for the Army's defensive cyber tools. Virtual images provide cyber defenders with significant operational advantages, including the ability to deploy cyber capabilities and troubleshoot technical issues more rapidly than ever before. Five partners collaborated in the project. Thirty-three sprints and 14 months later, the

Graphic by Applied Cyber Technologies

Army now has updated virtual machine images for four of its most complex defensive cyber tools.

Labyrinth 1.0 proved successful in several key ways, but it also enabled us to identify areas for improvement. The ACT team learned that it needed to better manage workflows, simplify administrative tasks and streamline the onboarding process. But the most salient takeaways related to the cultural shift that Labyrinth inspires.

One of Labyrinth's most valuable features is the fact that it doesn't just enable teamwork—it inherently requires it. Labyrinth is not a competition; it's a collaboration. Unlike FAR, which often pits one "vendor" against another, Labyrinth asks partners to join forces. We ask partners to unite to provide the greatest value for the DOD and, ultimately, our Soldiers. With Labyrinth, partners have the freedom—or rather the "permission"—to work together for the greater good.

Moreover, instead of competing against each other, teams can complement and learn from each other. In order to understand, accept and work within this new dynamic, partners have to fundamentally adjust their long-held beliefs.

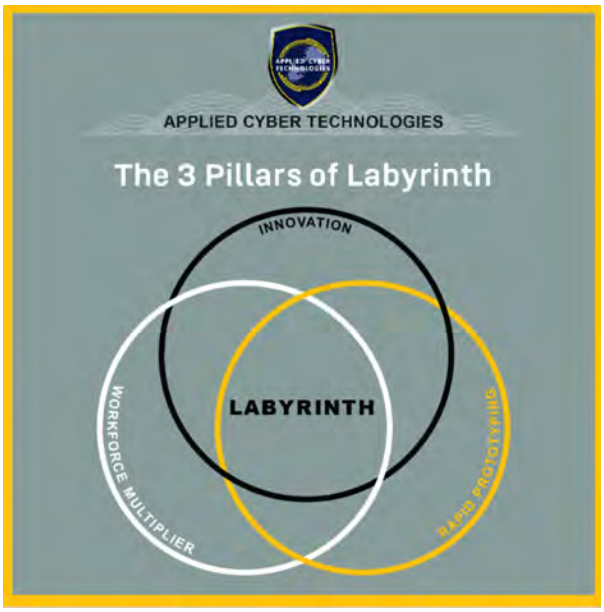
Additionally, Labyrinth changes the game with regard to deliverables. In FAR-based contracting, companies get paid when they deliver a finished product—regardless of whether it works as intended. Labyrinth gives the government the opportunity to flip the script; partners only get paid if the technology they deliver does exactly what they said it would. This is a vastly different dynamic for partners, but it immeasurably improves cyber Soldier readiness.

Lastly, we learned that—like much of the Army and the DOD—partners are at different levels of maturity with respect to DevSecOps. At times, one partner takes the lead in a particular area; at other times, partners learn collectively. The team is most effective when we recognize that we are better together. Furthermore, pooling talent resources in Labyrinth enables augmentation of the workforce. In this way, Labyrinth serves as a powerful force multiplier.

Labyrinth 2.0: Refining the Process

Labyrinth 2.0 was announced in May 2020. Its technical goal was to automate defensive cyber tool deployment and improve tool interoperability. These enhanced features pay dividends for cyber defenders by greatly minimizing operational issues and enabling cyber Soldiers to work much more rapidly, seamlessly and effectively.

At the time, there was a solution within the cyber enterprise that automated tool deployment. However, it was sole-sourced to one vendor and constantly increased in cost. ACT could not continue on this path, and there were no other solutions on the market. The only option was to develop a new solution.



Graphic by Applied Cyber Technologies

Fortunately, the team identified a commercial off-the-shelf (COTS) product with an encouraging solution. The COTS product would not satisfy the immediate requirement but contained basic code which, once enhanced within Labyrinth, could potentially solve our problem.

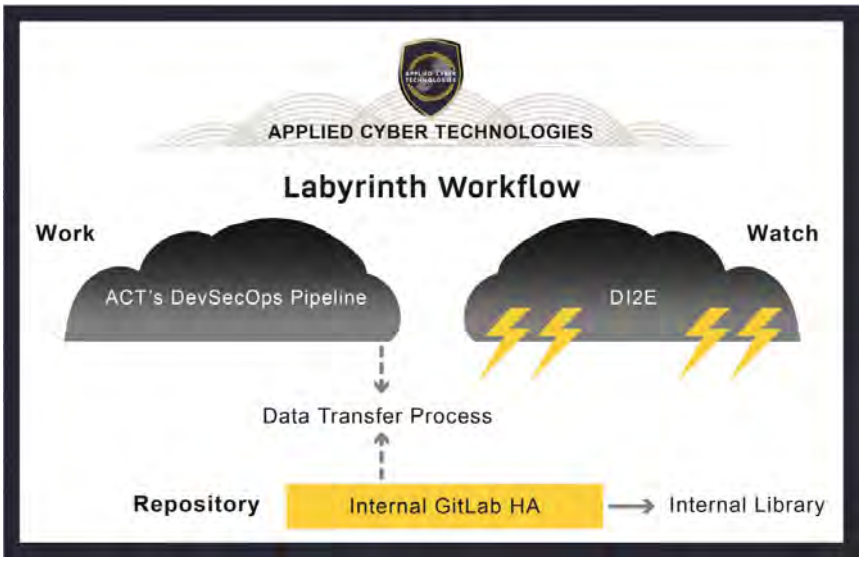
ACT issued an announcement stating the government's intent to repurpose the COTS solution and subsequently received 33 white papers—30 from industry and three from universities—in response. After evaluating the papers, ACT down-selected to six companies and two universities. Sprints began in June 2020. By April 2021, the team had successfully conducted nine sprints and reached a minimum viable solution (MVS). The MVS successfully resolved the stated problem. Moreover, it was delivered a month ahead of schedule and came in at 18 percent under projected costs.

Labyrinth 3.0 and Beyond: Facing Today's Challenges and the Way Ahead

Acquisition practices must intrinsically respond to operational speed. The cyber domain requires it. In the current cyberspace environment, winning comes down to speed. To solve acute issues in real time, teams must rapidly and continually update capabilities. Cyber defenders must maintain readiness in an ever-changing threat landscape, and we must create solutions to support their missions. These are not options for our nation's cyber defenders; these are absolutes. In a uniquely profound way, Labyrinth answers the need for speed.

Labyrinth respectfully rejects the idea that operations should stop when acquisition needs time to catch up. By creatively using OTAs, prioritizing prototypes over long-term material solutions and cultivating collaboration over competition, ACT is changing the paradigm not only for acquisition, but for technology innovation throughout the military.

The Army's focus on multi-domain operations makes it more critical than ever for organizations to think outside the box with respect to solutions procurement. It is incumbent upon every technology-driven Army



Graphic by Applied Cyber Technologies

organization to explore and identify solutions delivery practices that best serve our warriors. If those practices aren't readily available, the government should encourage teams to be resourceful. OTAs provide an avenue for organizations to craft processes that may well produce results previously thought impossible.

ACT will continue to refine Labyrinth, and we look forward to seeing what future iterations bring. Perhaps what is most exciting is knowing that any Army or DOD organization can adopt this model. Implementing novel prototyping mechanisms is not difficult, but changing organizational culture is. To make great strides, organizations must first believe that it is possible to do things better, faster and—most importantly—differently. Once that belief takes hold, organizations may find that the only true limitation to progress is simply their imagination.

Notes:

[1] DOD 5000 Series, Acquisition Policy Transformation Handbook, Multiple Pathways for Tailored Solutions, January 15, 2020, at 10 https://www.acq.osd.mil/ae/assets/docs/DoDDOD%205000%20Series%20Handbook%20%2815Jan2020%29.pdf

[2] DOD 5000 Series, Acquisition Policy Transformation Handbook, Multiple Pathways for Tailored Solutions, January 15, 2020, at 3. https://www.acq.osd.mil/ae/assets/docs/DoDDoD%205000%20Series%20Handbook%20%2815Jan2020%29.pdf

[3] Andrew Hill, Military Innovation and Military Culture (Parameters Carlisle Barracks Vol. 45, Iss. 1, Spring 2015: 85-98)

Category: Innovation

WINNER

Scaling Innovation at the Department of Defense: An Actionable Framework and Practical Steps for the Joint Force

By the following author:
Dr. Marina Theodotou

Adversarial advances, as well as the complexity, volume and velocity of change, and the digital disruption brought by emerging technologies such as AI and 5G, are only a few of the key drivers making the need to scale innovation at the Department of Defense (DOD) an imperative during this era of Great Power Competition (CRS Report, 2021). The 2018 National Defense Strategy prompts us to out-smart, out-think and out-innovate adversaries (NDS, 2018), and yet, one of the biggest challenges facing the DOD is the inability to scale innovation. In 2018, Dr. Eric Schmidt, Chairman of the Defense Innovation Board (DIB), during his testimony to the House Armed Services Committee, famously asserted: "The DOD does not have an innovation problem; it has an innovation adoption problem" (Schmidt, 2018).

Today, this paper posits that the DOD now has an innovation scaling problem. Today, there are numerous successful DOD innovation cells, initiatives, and programs, including the Army Software Factory, Kessell Run, AFWERX, NSIN and NavalX, among others, that are achieving substantial outcomes within their domain and to some degree across the Joint Force. However, while these successful initiatives focus on the learning, training, partnering, funding and application of innovative technologies and outcomes at the DOD, they are not effectively resourced to fully scale their learnings and outcomes across the DOD. This paper defines "scaling" as the adaptation, uptake and synergistic use of innovations including practices, outcomes, technologies and market arrangements across communities, stakeholders and broader domains to achieve performance outcomes (Eastwood et al., 2017; Wigboldus, 2018). The DOD's inability to scale innovation achieved from ideas, pilots, processes, approaches, technologies and acquisition contracting vehicles prevents the Joint Force from opti-

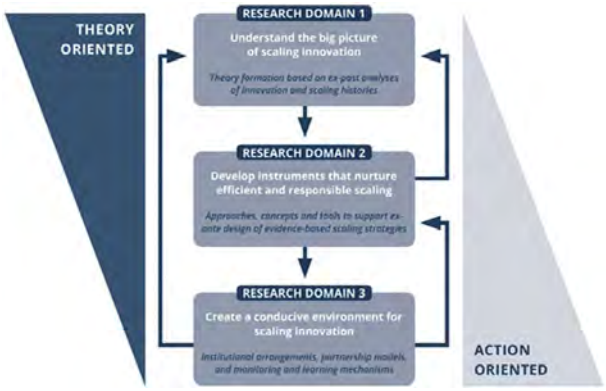


FIGURE 1 Three domains in innovation scaling (Schut, Leeuwis and Thiele, 2020)

mizing innovation in warfighter capabilities (Barnett, 2020; Green, 2020; Jasper, 2021).

Scaling innovation at the DOD is complex and complicated. The complexity of the undertaking, which would require research, analysis and synthesis across numerous moving parts including multiple innovation cells, adaptive acquisition initiatives and programs, stakeholders, policies, procedures, processes, technologies and data across the Joint Force, mandates the consideration of an innovation scaling framework to drive the research and its applications within the DOD. According to Schut, Leeuwis and Thiele (2020), as seen in Figure 1, a practical innovation scaling research framework straddles both theory and action and focuses on three interconnected and interrelated domains.

These three research application domains are: 1) understanding the big picture of innovation scaling innovation, 2) developing approaches and tools to facilitate innovation scaling and 3) creating and fostering a conducive environment for scaling innovation.

This paper studies this innovation scaling framework by examining each of the three domains, framing each domain into a DOD context, and outlining a feasible solution for consideration by the Joint Force. This proposal carves a path forward in addressing the DOD's innovation scaling challenge to ensure the warfighter perpetuates their decisive edge in the extraordinary power competition.

Domain 1: Understand the Big Picture of Scaling Innovation

This first domain focuses on understanding the various innovation scaling theories and models across industry, academia and the federal government and forming a model that best fits the needs and context of the DOD. Here, it is essential to highlight that scaling innovation is different from adopting an innovative technology or diffusing innovation. Adopting an innovative technology would be one of the steps in scaling innovation efforts. According to de Roo et al. (2019), scaling innovation varies greatly from diffusing innovation, which centers on the premise that spreading innovation depends on the individual decisions of the early adopters. In contrast, scaling innovation consists of holistic approaches that include adopting innovative technologies and diffusing innovations and broader strategies and interactions that cut across numerous institutions, agencies, leaders, stakeholders, processes, technologies and users (Low and Thiele, 2020).

It is evident that scaling innovation is complex and requires collaboration and connecting nodes across several innovation programs, agencies, initiatives and stakeholders at the DOD to support and foster both "push" and "pull" innovation scaling across the Joint Force. Presently, the DOD lacks an organization or initiative at the Joint level which studies the various scaling innovation models, examining their strengths and weaknesses to adopt and adapt them and formulate the scaling innovation model of the DOD. The DOD has funded 11 FFRDCs (Federally Funded Research and Development Centers) and 14 UARCs (University-Affiliated Research Center Laboratories). While all are doing important work, none is focusing specifically on building a framework to enable the DOD to scale innovation, as defined herein, across the Joint Force (Defense Innovation Marketplace, 2021).

A key research question for this domain includes: "How might the DOD examine the various research models on scaling innovation to formulate a DOD-specific innovation scaling framework that will guide and facilitate the flow of successful practices, lessons learned, approaches, and technologies from across the numerous DOD innovation cells and initiatives to adopt and adapt them into a

DOD innovation ecosystem to deliver business outcomes faster and at scale for the warfighter?" To address this challenge, this paper recommends that the DOD funds a UARC to focus specifically on scaling innovation. Such a UARC will collaborate with existing UARCs FFRDCs, leading universities adept in researching innovation scaling with DOD innovation cells to build such framework and rapidly study, experiment and optimize the scaling of innovation holistically across the DOD.

Domain 2: Develop Skills, Approaches and Tools for Scaling Innovation

While an innovation scaling framework will help the DOD holistically study and understand the critical elements needed for successful innovation scaling efforts, scaling innovation requires specific skills, tools and capacities.

First, in terms of innovation scaling skills, innovators across the DOD will need to develop growth mindsets, become adept at connecting the dots and recognizing patterns across innovation programs and initiatives and also sharpen their networking and storytelling skills. Such skills will enable DOD innovators to develop into scaling champions who are critical force multipliers for innovation scaling efforts. According to Klerkx and Aarts (2013), innovation champions understand scaling partners' needs and goals, and have the capacity and stamina to convince others, pursue and capture windows of opportunity. Innovation champions also often create the context and momentum for tipping points (Gladwell, 2006). Today, the DOD lacks a department-wide strategy of teaching innovation skills. A lack of strategy leads to multiple, often overlapping, uncoordinated, under-resourced initiatives that struggle to scale. While today at least two courses are teaching innovation leadership and the skills needed to scale innovation, including the Sense21 course at the Naval Post Graduate School, and the "Project Mercury" at Air University, which provides an innovation certification from the University of Michigan, they have only been able to graduate 150 students each mainly due to lack of departmental commitment and resources. To address this challenge, we recommend that the DOD chief learning officers collaborate and set an innovation skills learning strategy for the Joint Force leveraging successful initiatives and multiple learning modalities.

Second, in terms of approaches, networking is critical to scaling innovation in large organizations. It is critical to network across silos. Innovation champions have strong networking skills, which include cultivating a diverse, broad and "high brokerage" network (Uzzi and Dunlap, 2005). Today, the DOD lacks a department-wide network mechanism for DOD innovators to connect, engage, share learnings and problem solve. While the DOD has many innovation champions, most operate in minor and often unrelated networks due to the lack of an innovation scaling framework at the Joint Force level. Three examples of innovation champion initiatives include TEDxDAU, NavalX and the Army Software Factory. Alas, none of these programs knew of each other's efforts until innovation champions from these programs, which serendipitously happened to network across the siloed agencies, connected them. To address this challenge, this paper recommends that the DOD examine best practices from successful DOD innovation initiatives and industry in creating dynamic networks and communities that scale innovation through exchanging ideas and best practices.

Third, the DOD lacks a tool to evaluate program innovation scaling readiness. This mechanism, coupled with an innovation scaling framework and a network, can facilitate evaluating and scaling successful insulated initiatives to share their learnings with others across the Joint Force. To address this challenge, as a first step, we recommend that each innovation program or initiative will need to assess their innovation scaling readiness using tools such as the "Scaling Scan" developed by Jacobs et al. (2021) and the Management Systems International (Cooley et al. 2020). Such tools provide teams a rigorous approach to evaluate innovation scaling readiness across ten criteria and offer guidance on steps to scale.

Domain 3: Foster a Conducive Environment for Scaling Innovation

To foster a conducive environment for scaling innovation, the DOD needs to focus on the people, ideas, process, technology, governance and data of its innovation ecosystem (Theodotou, 2021). An innovation ecosystem enables leaders, innovators, stakeholders, partners and the workforce at large to interact and engage using digital tools, platforms and communities that facilitate crowdsourcing and leveraging data to make data-driven decisions (Greenhalgh and Papoutsi, 2019). The National Security Innovation Network (NSIN) is an excellent example of this effort. Initiatives such as Propel, Starts and Vector focus on the innovation development of dual-use ventures (NSIN, 2021).

However, more work is needed to scale these efforts from pilots to department-wide baked-in efforts. According to Prain et al. (2020), two essential requirements in the people component of scaling innovation are first: hiring fluidity which allows innovation champions to shift across organizations with relative ease; and second: staff stability which enables the organization to reap the return of the investment made in people and innovation scaling initiatives. As previously highlighted by the DIB and other organizations, the current DOD human resources system is rigid, inflexible and limited to creating a culture of innovation, let alone fostering the scaling of innovation (DIB, 2017).

To address this challenge, this paper recommends that the DOD moves forward with the appointment of a chief innovation officer as initially recommended by the DIB (2017), not to centralize innovation efforts which would be detrimental, but to focus on enhancing workforce capacity, human capital, professional training programs and fostering the scaling of innovation across the numerous, successful innovation efforts across the DOD.

Conclusion

Scaling innovation is a complex, yet essential undertaking that would enable the DOD to tackle change and adversarial advances faster to provide the warfighter the decisive edge (Seelos and Mair, 2020). To begin the innovation scaling journey, it is recommended that the DOD formulates a UARC that centers on scaling innovation, creates an innovation scaling framework, provides the workforce the innovation scaling skills and tools they need, and fosters a conducive environment that shifts from innovation adoption to innovation scaling.

The views expressed in this article are those of the author and not necessarily those of the Department of Defense or any of its components. This paper has been approved for public release.

References:

Barnett, J. (2020). The Pentagon is failing to scale emerging technology, senior leaders say. Retrieved from: https://www.fedscoop.com/dod-innovation-emerging-technology-acquisition-aspen-security-sumit/

Cooley, L., & Kohl, R. (2020). Scaling up—from vision to large-scale change: a management framework for practitioners. Washington, DC: Management Systems International.

CRS Report (2021). Retrieved from https://fas.org/sgp/crs/natsec/R43838.pdf

Defense Innovation Marketplace (2020). Retrieved from https://defenseinnovationmarketplace.dtic.mil/ffrdcs-uarcs/

Defense Innovation Board (2017). People and Culture – Recommendation 1: Appoint a Chief Innovation Officer and Build Innovation Capacity in the workforce. Retrieved from: https://innovation.defense.gov/Portals/63/documents/Recommendations/People%20and%20Culture%20%20Recommendation%201%20Appoint%20a%20Chief%20Innovation%20Officer.pdf?ver=2020-09-08-121955-900

Eastwood, C., Klerkx, L., & Nettle, R. (2017). Dynamics and distribution of public and private research and extension roles for technological innovation and diffusion: Case studies of the implementation and adaptation of precision farming technologies. Journal of Rural Studies, 49, 1-12.

Gladwell, M. (2006). The tipping point: How little things can make a big difference. Little, Brown.

Green, J. (2020). United Space: United Space: Military and Commercial Sectors Working Together to Harness Innovation in Space Research and Development Retrieved from: https://apps.dtic.mil/sti/citations/AD1112337

Greenhalgh, T., & Papoutsi, C. (2019). Spreading and scaling up innovation and improvement. Bmj, 365.

Jacobs, F., Ubels, J., Woltering, L., & Boa, M. (2021). The scaling scan: A practical tool to determine the strengths and weaknesses of your scaling ambition. Retrieved from: https://repository.cimmyt.org/bitstream/handle/10883/21507/63710.pdf

Jasper, M. (2021). Lawmakers Want DOD to Explore Tech's Valley of Death Problem https://www.nextgov.com/emerging-tech/2021/07/lawmakers-want-dod-explore-techs-valley-death-problem/184079/

Klerkx, L., & Aarts, N. (2013). The interaction of

multiple champions in orchestrating innovation networks: Conflicts and complementarities. Technovation, 33(6-7), 193-210.

National Security Innovation Network (2021). Retrieved from: https://www.nsin.us/portfolios/acceleration/

Prain, G., Wheatley, C., Odsey, C., Verzola, L., Bertuso, A., Roa, J., & Naziri, D. (2020). Development partnerships for scaling complex innovation: Lessons from the Farmer Business School in IFAD-supported loan-grant collaborations in Asia. Agricultural Systems, 182, 102834.

Seelos, C. & Mair, J. (2020). Innovation and Scaling for Impact. Redwood City: Stanford University Press. https://doi.org/10.1515/9781503600997

Schmidt, E. (2018). Congressional Testimony. Retrieved from: https://es.ndu.edu/Portals/75/Documents/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf

Schut, M., Leeuwis, C., & Thiele, G. (2020). Science of Scaling: Understanding and guiding the scaling of innovation for societal outcomes. Agricultural Systems, 184, 102908.

Theodotou, M. (2021). The five building blocks of a learning ecosystem. In T. Elkeles (Ed.) Forward-focused Learning: Inside Award-winning Organizations (pp. 41-52). Association for Talent Development.

Uzzi, B., & Dunlap, S. (2005). How to build your network. Harvard Business Review, 83(12), 53.

Wigboldus, S. (2018). To scale, or not to scale–that is not the only question: rethinking the idea and practice of scaling innovations for development and progress (Doctoral dissertation, Wageningen University).

HONORABLE MENTION

Animated Data: How Healthcare Data Lives Alongside Patients

By the following author:
Holly S. Joers

For those of us who work with data on a regular basis, we may understand many of the key functions and uses of ones and zeros; however, what we do with data and how we organize it determines its potential and influences how we relate to information. The Program Executive Office, Defense Healthcare Management Systems (PEO DHMS) leads acquisition activities designed to transform the Defense Department's (DOD) management and use of health data to maintain readiness and drive patient-centered care.

The United States Army, and more broadly, the DOD as well as the Department of Veterans Affairs (VA) and the United States Coast Guard (USCG) will benefit from living and evolving health data sets that will improve the wellbeing of over 9.6 million beneficiaries in the coming years. The following will examine not only the revolutionary advantages of the single, common federal electronic health record, known as MHS GENESIS, but it also will interpret this new endeavor as a catalyst for a shift in how we fundamentally relate to data. In short, data is not a foreign and insipid series of numerals divorced from the health experiences of men and women. Like an evolving organism itself, PEO DHMS creates the mechanisms for data to live alongside patients, changing, growing and enhancing health outcomes along the way.

A common notion, particularly with those who live outside of the information technology (IT) world, is that data can be somewhat dull, stagnant or stale. Like an old dusty toolbox sitting in your garage, data can be there when you need it; however, the toolbox remains rarely reorganized or creatively utilized, making the metaphorical hammer, drill or wrench siloed in its function. These tools are not malleable and do not grow or communicate with one another to solve tasks. In this view, data seems to patiently wait to be picked up as a tool, but, when it comes to health data, optimization of that toolbox ought to evolve with the life of the individual. Focused on

patient-centered care, MHS GENESIS sets the program office on the path to throw out this antiquated notion that data represents digital dormancy. The work of each PEO DHMS program office exemplifies how data lives along with the patient, evolving in an agile and accessible manner that will benefit service members for decades to come.

In order for data to manifest itself as a living entity alongside the patient, like any biological organism, it must have certain protections as well as organizational structures that allow for levels of self-sustainment. To achieve these goals, PEO DHMS' Enterprise Intelligence and Data Solutions (EIDS) program office created an extraordinary migration of vital population health data and applications from traditional digital storage facilities to the cloud in record time, not only making the data more secure but revolutionizing data access and analytic capabilities across the Military Health System (MHS). In just 93 calendar days, the team exceeded expectations via the Accelerated Migration Project (AMP), partnering with 20 vendors, restructuring 14 native cloud services, transferring over 60 applications and consolidating 1.7 petabytes of data employed daily by more than 200,000 MHS users. AMP will save DOD $26.9 million over the next five years.

Through AMP, EIDS successfully completed one of the most challenging cloud migrations in history, and this migration to the cloud ensures secure and accessible health information. To relate this back to data as a metaphorical living entity, the security features and teams involved in the AMP cloud transfer liken to the body's immune system, effectively warding off external threats. The EIDS cybersecurity team represents the immune system for the program, and AMP functions as the immune booster, capable of confronting any potential future digital disease.

Certain data systems and projects such as AMP work to consolidate and secure health data; however, like a biological organism, data becomes more agile when it employs a mechanism of communicating not only within its own system but with the outside environment. To achieve this, PEO DHMS' teams apply application programming interface (API) solutions and continuously optimize them to allow for interconnectivity and communication between data sources, e.g., DOD and private sector healthcare providers. Serving as the intermediary, APIs transfer information between data systems or applications and translate this information into a 'common language' in which two potentially disparate systems can send and receive patient information. When one relates this to living organisms, the nervous system comes to mind. Your brain and muscle fibers, in essence, are very different systems and physically separated by the space between them; however, our biology utilizes neural connectivity to serve as the intermediary between these systems.

When touching a hot stove, the pain receptors in your fingers rapidly send information through millions of neurons, reaching your brain in a chemical language it can understand, which then provides a response back to the point of pain. This likely appears in the form of an impulsive muscle activation in your fingers and wrist to get away from the heat. This intermediary, like APIs, serves to form a connected and communicative system.

With regard to health data, a certain type of API called a Fast Healthcare Interoperability Resource (FHIR) API allows for faster communication between health data sources as well as for the ability of providers to select which data integrates into a system such as MHS GENESIS. This capability aids collaboration with the private sector. Expanding the reach of MHS GENESIS, PEO DHMS partners with private treatment facilities so that whether treated at a military hospital or Massachusetts General, patient data can be selectively and rapidly transferred. Like touching a hot stove, your nervous system prioritizes the pain instead of an itch on your leg as the more pressing matter. Through FHIR APIs, certain providers access prioritized MHS GENESIS data in the service of their patients. MHS GENESIS then provides the means for clinicians to view this data in real time and at the patient's side.

Today, MHS GENESIS lives alongside patients in Army and other military treatment facilities (MTFs) around the country. The DOD Healthcare Management System Modernization (DHMSM) program office deploys and implements MHS GENESIS. As part of its mission, this team acquires, tests, delivers, integrates and transitions to the revolutionary MHS GENESIS EHR. With deployments across 47 commands and 16 military hospitals, affecting as many as 2.7 million beneficiaries, DHMSM is implementing this single common record that will stay with each beneficiary throughout their lives. When it comes to the Army, following the September 25 deployment of MHS GENESIS to Tripler Army

Medical Hospital and the Desmond Doss Health Clinic, 10 Army commands and over 11,000 users now benefit from the MHS GENESIS EHR. These deployments allow Army clinicians and patients to receive the consolidated, patient-centered care that PEO DHMS finds essential throughout the MHS.

The combined efforts of EIDS and DHMSM allow for the right data to be in the right hands as quickly as possible. When it comes to patient-centered care, this is not only presciently compassionate but, in some cases, urgently needed to save lives and improve a patient's overall wellbeing. The work conducted by EIDS and DHMSM lends itself to a more holistic approach to medical care as MHS GENESIS demonstrates scalability to other health factors, including the social determinants of health. This foundation of data aggregation, consolidation and utilization enables a truly expansive application of MHS GENESIS.

Just as we look to our futures and progress throughout our lives, through MHS GENESIS, PEO DHMS creates health optimization measures that allow data utilization to develop alongside service members, continuously finding new opportunities to promote health and wellness, even in the field. PEO DHMS' Joint Operational Medicine Information Systems (JOMIS) program office works with the services to ensure EHR access through various OpMed environments to include point-of-injury aboard ships, planes, en-route care, etc. These systems interface to MHS GENESIS so providers maintain access to patients' complete medical records when needed. Capability expansion will progress only through the work of JOMIS leadership and engineers.

Patient-centered care serves as a major component of the innovation of MHS GENESIS. If IT takes attention away from the primary function of a care provider, then innovation must take place to maximize patient-centered care. If patient data is not collected, maintained and accessed effectively, then risk to the patient increases. The DOD finds this scenario unacceptable; hence, our EIDS team conducted the most challenging data migration in history, our DHMSM team implements a single, common federal record in MTFs around the world and our JOMIS team pursues capability delivery at the speed of relevance. Data saves lives and lives alongside the patient. As the patient's health and circumstances evolve, so does their data due to the innovative work of these teams.

PEO DHMS ensures data functions similarly to a growing and evolving organism that resides literally at a patient's side when in need. PEO DHMS will continue to make data animated and agile, arriving in the right hands, at the right time and in the right place. This includes after one concludes their service. PEO DHMS works with the VA to implement this consolidated health record so veterans progress throughout the next chapters of their lives with a living data set that accrues along with them. Not only can data be compared to physiological processes, but it also has a more subjective experiential connection to our lives, living and growing with us as we do so ourselves.

Through stakeholder engagement and outreach, PEO DHMS aims to make data exciting, lively and engaging through relating it to our very selves. When we take care of health data, we take care of people through a patient-centered approach that will positively affect beneficiaries through each point of care and at each point in their lives.

Category: Lessons Learned

WINNER

Building Trust: A Cyber Story

By the following author:
Lt. Col. (Promotable) Rachael Hoagland

Cyber assessments are stressful and unforgiving. They show flaws in your program and often produce more questions than answers. I had recently taken over a new team in a program I was completely unfamiliar with and been tasked with doing a cyber assessment. To add more pressure, I had to soon brief the commands in charge of special operations aviation on the plan that did not yet exist. I was overwhelmed. Where to even begin? My team had no experience conducting a cyber assessment, no insights into the process, no idea what to focus on, and no money to complete the evaluation. To compound the problem, my team had found vulnerabilities.

Rumors about cyber vulnerabilities can cripple a program. The fear of rumors stopping my teams great

work and potentially delaying critical capabilities from reaching the battlefield kept me up at night. I eventually overcame my initial concerns about being the first project manager to possibly ground Special Operations Aviation Regiment (SOAR) aircraft for a cyber weakness. Instead, we shifted focus to the more significant concern of how to ensure the organization's reputation was not damaged while exposing cyber flaws. We persevered, and out of the chaos, hatched a three-phased approach: no cost, low cost and cost.

Phase one focused on what the program office and the user could do at little to no expenditure. Phase two involved the cyber assessment. Finally, phase three, would address and correct any vulnerabilities the assessment discovered.

We used phase one to buy time until I could figure out how and when to conduct a comprehensive cyber evaluation. Surprisingly, it turned out to be the best thing we did. The program office examined all our existing contracts to assess the language each contained regarding cyber security and its applicability to the aircraft. Simultaneously, the user group would look at the SOAR's tactics, techniques and procedures, and their training. I would then be able to brief the results and recommend fixes at the next quarterly meeting. This would show progress and buy time.

This stalling tactic gave the team time to build our narrative on how important conducting a cyber assessment was. We constructed a problem statement, but in every briefing where it was included, I only saw blank stares. The audience thoroughly understood the problem statement, but no one comprehended what we were attempting to do with the assessment. Finally, a warrant officer from the regiment turned to me and said: "Ma'am, we can tell the regimental commander the risk to every flight down to the littlest detail, but we can't explain to him what the cybersecurity risk to that same flight is." This statement changed everything; weaving cyber risk into a current process provided a shared operational picture amongst stakeholders.

The contracts review turned out to be more than a stalling technique, it revealed some significant issues. For example, not all vendors were not compliant with acquisition regulations; this meant that the vendors building our systems did not follow simple standards, such as having computers used for coding with proper login procedures. Without proper login procedures, an unauthorized person could get on the system and make changes to the aircraft software, potentially leaving the aircraft vulnerable to cyber-attacks in the future.

During phase one, cybersecurity discussions became a planned part of every meeting. My primary goals for this were twofold. I wanted to first assess the different companies' understanding of software cybersecurity, and second, ensure that my team, the user and the vendors all shared my concerns about cybersecurity. The cybersecurity discussions worked as planned. I quickly realized that our software developers were highly ignorant about potential cyber-attacks from our adversaries.

The discussions also helped the teams to understand what cybersecurity was and to develop a common language. Two major cybersecurity issues became clear. The aircraft had software developed in foreign countries and we had an unsecured file transfer site to share software between organizations.

When I first heard that we had multiple companies outsourcing software development to foreign businesses, I felt as if I had been hit in the stomach with a cannon. The Department of Defense has rules mandating domestic sources for things as innocuous as textiles. Other components such as microchips also must be made in the U.S. But several countries were working on SOAR software? Feeling uneasy about foreign companies developing critical code, I met with the vendors to discuss concerns. What we learned ended up being more alarming than I initially anticipated and a serious of progressively concerning meetings ensued.

In our first meeting, a particular vendor assured me that no foreign company was developing SOAR code. This did not make sense since historical documents showed that we saved six million dollars by agreeing to let them outsource it, so I scheduled a second engagement. At our second meeting, the vendor assured us that the foreign company was only conducting low-level testing in isolation and did not have access to the consolidated code. Their explanations were incomplete at times, however, and we felt we did not have a complete understanding. A third meeting was scheduled. That meeting revealed that foreign companies were building the test plan for SOAR software, which meant they had our requirements, even if they did not know who the customer was. Knowing our requirements meant the foreign company knew

what our aircraft were and were not capable of, exposing potential operational weaknesses.

Significant concerns prompted us to give the vendor an intelligence brief on cybersecurity threats to our systems. The intelligence briefing was another pivotal event as it created a sense of urgency and understanding with a group of key stakeholders that historically did not get information on the cybersecurity threat. The vendor asked to schedule a fourth meeting and volunteered to provide our cybersecurity assessment support at no cost to the government. The fourth meeting revealed even more about the system's exposure and vulnerabilities. A foreign company had access to the consolidated code, they were manipulating the consolidated code, they knew who the customer was, and they had at least one person who flew to the U.S. a couple of times a year to work on software at the vendor's laboratory.

We realized through our discussions, however, the problem was not that the vendor was trying to hide the foreign involvement, but that they had a poor understanding of their own complex processes. We identified three main issues: We had no process to track and control what the foreign engineers manipulated; the program office had a minimal understanding that foreign companies were working software; and the vendor did not understand the threat. Fighting urges to immediately pull all software development out of the foreign country, we conducted a thorough risk assessment. We determined that managing the risk instead of eliminating it would satisfy the security issues while keeping the program on schedule and within cost.

The file transfer site intended to share software between the vendor, the program office and the customer also proved to be critical vulnerability. The problem was that literally anyone could request a username and password and gain access to it. The computer produced usernames and passwords to the site without any check to confirm an individual should have access. We removed the site immediately.

Establishing a common language, creating a shared operational picture, quickly removing the file transfer site, and developing an off-ramp of foreign software development built understanding and swift trust among the organizations. Stakeholders at all levels now understood the positive impact a cyber assessment could have, paving the way for phase two.

Phase two, began with establishing the cyber assessment team. We built a small core team including the program office, the pilots, the vendor and the intelligence community. What we needed to find next was a cyber team that was not only certified to hack DOD equipment, but also one with enough discipline and discretion to enable us to be the ones to tell our bosses about problems, enabling us to maintain the trust we had built to that point.
The team read several cybersecurity reports previously

conducted on similar helicopters and associated equipment. We witnessed a cyber assessment of a Coast Guard helicopter and attended an executive out brief of a cyber assessment to a Navy Admiral. Attending these events helped the team understand the technical capabilities of each group and also helped us build a shared mental model of how our cyber assessment should look.

The success of phase one and the common picture developed at the beginning of phase two provided the credibility we needed to get funding from SOCOM for the assessment. With money in hand, it was now time to build the assessment team, which was undoubtedly the most critical step. I needed the right experts from each organization and needed to turn the swift trust built in phase one into conventional trust that would last well beyond the assessment. Egos would be damaged. The assessment would expose failures by the program office, a large corporation with millions of dollars in current and future contracts at risk and operational and training flaws within the prestigious 160th SOAR. Preserving the trust we had worked so hard to build required each organization to be vulnerable during the assessment. Stonewalling the process or placing blame by any group would destroy that confidence.

Phase two ended with a series of executive and technical briefings to stakeholders, which guided priorities on making fixes and allocating funding in phase three. Sadly, I left the team before phase three was underway. However, I was able to see the effect our efforts in this project left on the various organizations. The program office restructured to better address cybersecurity on all projects. The pilots were now building requirements with cybersecurity as part of the key system attributes and key performance parameters. The contracting office implemented a template of cybersecurity language into contracts. The vendor focused on the cyber hardening of their systems. Finally, a community of practice developed from our shared interest in making the SOAR more resilient against cyber-attacks. Team members originally opposed to an assessment were now asking what the next cyber event was and if they could be part of it.

If presented with conducting a cyber assessment do not fear. Take time upfront to educate yourself and your stakeholders before jumping in. Taking the time upfront to build a common language and a common operating picture will help with the overall understanding and aid in communicating your findings. The key to a successful assessment is the people. Spend the majority of your time developing them and the rest will fall into place—you will be successful.

HONORABLE MENTION

Onboarding New Employees as Remote Working is Here to Stay

By the following author:
Maj. Jared J. Ryan

In March 2020, the COVID-19 pandemic changed how we as the Army Acquisition Corps function. What started as a two- or three-week telework experiment has morphed into the reality that the virtual environment is here to stay. Gone are the days of everyone at the office during working hours—and likewise, gone are the days of a new employee showing up to the office on his or her first day of work to meet his or her new team. This face-to-face interaction had a lot of ancillary benefits that have all but disappeared over the past year and a half.

As someone who started his first acquisition assignment in September 2020, I did not realize what I was missing until the first couple of in-person interactions I had with my Product Manager (PdM) team. As we are coming out of the pandemic, and leaders are making decisions about how to strike the correct balance of force protection and workplace interaction, I want to share what I learned throughout my onboarding process. Specifically, I want to share why it is important for leaders at the PdM level to bring in their workforce once a month, how my PdM onboarded me and why it was effective, as well as the importance of new employees being proactive.

For acquisition professionals, transitioning between jobs is a way of life while working for the Army, and onboarding requirements differ greatly: from something as simple as changing positions within the same PdM to as complicated as moving across the country to a new Program Executive Office (PEO). Starting a new job can be as quick as changing a signature block, to as long as meeting all the new stakeholders and learning the interactions between sections. Each onboarding process is

unique and varies greatly depending almost entirely on the people involved.

Before the pandemic started, onboarding and the first days and months on a new job generally happened in person. There are two major benefits that new employees started missing out on when everyone began working from home. The first is they are no longer able to listen to others in their section speak casually about what they are working on. Conversations between people who have been working together for months, or even years, used to happen in the office, and the new employee would just naturally learn by hearing things. Now those conversations are one-on-one in a virtual environment and generally, have to be pre-planned. The new employee does not know what they do not know yet, and hearing other conversations organically in the office leads to questions they would otherwise not have thought of. These impromptu in-office conversations benefited acquisition programs by allowing the new employee to bring multiple options to his or her supervisor when he or she encountered challenges.

The other major benefit of these in-person interactions is the new employee is able to start building relationships with all the other people that they sit in on regular meetings with, but not necessarily work with, on a day-to-day basis. People from finance, contracting, engineering, testing, program management and every other section have both formal and informal discussions when together. The new employee not only gets all the same benefits when in person with his or her section, but also, they are able to gain a better understanding of where they fit into the acquisition process as a whole. This better understanding bears fruit, as the new employee is now able to either provide more accurate responses, or ask more detailed questions, when exchanging information with each section.

While there is no one way to onboard a new employee, PdM Army Watercraft Systems (AWS) brought me on to the team in an efficient manner that allowed me to start contributing almost immediately. A month before I started, different sections started to carbon copy me on emails related to the product I was taking over. This allowed me to start gaining situational awareness. Second, the product officer set aside two hours the day before I started to brief me not only on my project, but the PdM as a whole, and where AWS was headed. This gave me a better understanding of my role and where I fit into the big picture. Quarterly, PEO Combat Support and Combat Service Support holds a new employee orientation. This four-and-a-half hour block shows the organization's commitment to new employees. Among other topics, the program executive officer briefs for an hour to go over the PEO's mission, vision, priorities, expectation and culture. This is a great way to set the standard early and ensure everyone is moving in the same direction. Finally, I had daily meetings with an experienced APM. This gave me a person to direct all my questions to, and if he did not know the answer, he knew who I should contact to get it. Having scheduled time with a single point of contact was invaluable—if I could not reach him for any reason, there was always a set time for us to talk, and it allowed me to course correct quickly as issues came up … keeping the program on track for cost, schedule and performance.

Lastly, it's important to also discuss the increased pressure on the new acquisition professional on being proactive in a virtual environment. The opportunities to learn and ask questions organically has decreased dramatically. To learn faster and become a functioning member of the team, the new employee must reach out to people he or she has never talked to before. For some, this is easy, however, a lot of people have trouble initiating that conversation. It is important to understand this new reality, and ensure not only that the new employee knows they must reach out to be successful, but also that established people in the organization can quicken the learning curve by reaching out first. Something as simple as a chat in Microsoft Teams welcoming the new employee can have immediate impact with onboarding.

In conclusion, the pandemic has proven that the acquisition community can be productive while working virtually. Countless businesses and organizations have seen the benefits of remote work, and some form of remote work should be permanent. However, when onboarding new acquisition professionals, there are too many benefits of in-person interaction to be completely ignored. I believe meeting once a month in person at the PdM level, either through a normal day at the office, or an afternoon of team building, is the right balance of force protection and work place interaction. This regular in-person contact will result in getting higher-quality capabilities into the hands of Soldiers faster.