Enhancing Situational Understanding through Integration of Artificial Intelligence in Tactical Headquarters

Maj. Benjamin Scott, U.S. Army

Capt. André Michell, U.S. Army

We cannot be an Industrial Age Army in the Information Age. We must transform all linear industrial age processes to be more effective, protect our resources, and make better decisions.

—Gen. James C. McConville,
40th Chief of Staff of the U.S. Army

To meet the demands of modern battlefields, the Army must enhance tactical command posts by integrating artificial intelligence (AI) into its systems. AI presents tremendous opportunities to provide corps, division, brigade, and even battalion command posts with quantitative and qualitative advantages in situational understanding relative to potential threat formations and commanders. Properly developed, tested, and fielded AI capabilities will better consolidate, prioritize, and relate information to enhance situational understanding and enable more effective decision-making. Multi-domain operations (MDO) on modern battlefields require commanders and their staffs to fight in a multidimensional battlespace. This will challenge even the most adept staff officers, and already units are dealing with an overwhelming amount of information. Well-designed AI algorithms and AI-enabled applications will help U.S. maneuver units better understand their operating environment and will enable a more robust common operating picture.

"Enable decision-making" is a core task within information advantage activities, and execution of this core task will enable commanders, staffs, and formations to gain and maintain information advantages. Enhanced situational understanding is a necessary but insufficient condition for commanders to achieve decision advantages; enhancing situational understanding is both imperative and achievable in the short term with currently achievable technology. AI integration into this core task will indirectly contribute in varying degrees to Army capabilities within all core tasks of information advantage activities. This article details specific current needs and recommendations for integration of AI into extant systems and networks over the next three years. The article does not and is not intended to provide detailed proposals for further development or fielding of nascent capabilities with longer-term timelines. Instead,

Capt. Sarah Miller and Tech. Sgt. Carrol Brewster, 834th Cyber Operations Squadron, discuss options in response to a staged cyberattack during filming of a scene for an Air Force Reserve Command mission video at Joint Base San Antonio-Lackland, Texas, on 1 June 2019. (Photo by Maj. Christopher Vasquez, U.S. Air Force)

the authors' feet are firmly planted in the realities of the present, immediate needs and available technology.

In the future, AI-enabled sensors, fire-control systems, delivery assets, and algorithms may create battlefields of incredible velocity and lethality where humans on the loop struggle to keep pace with machines meant to do commanders' bidding. Swarms of collection and delivery assets may someday autonomously execute missions and dynamically act to accomplish collection, delivery, and assessment while making continuous adjustments to react as events unfold. These systems and events in physical domains will be accompanied by similarly advanced employment of AI-enabled capabilities in the cyberspace domain as friendly, neutral, and threat systems interact. Such capabilities are currently not available for widespread fielding and employment, and the underlying AI technologies are not robust enough for us to seriously consider their introduction in the immediate future. In the meantime, the Army must begin integration of AI in a manner that is feasible, timely, and effective.

As *The U.S. Army in Multi-Domain Operations 2028* asserts, "The key to converging capabilities across all domains, the EMS [electromagnetic spectrum], and the information environment is high-volume analytical capability and sensor-to-shooter links enabled by artificial intelligence, which complicates enemy deception and obscuration through automatic cross-cueing and target recognition. The intelligence refinement required for disintegration depends on five interrelated systems."[1] The five systems are as follows: wide-area surveillance, penetrating reconnaissance, standoff surveillance and reconnaissance, expendable surveillance and reconnaissance, and human networks. Each of these five systems could benefit from immediate development, experimentation, and employment of AI-enabled systems in tactical headquarters through improvement of situational understanding. Such integration would not automate decision-making but instead would enable better decision-making by human commanders and staffs. As stated in *The U.S. Army in Multi-Domain Operations 2028*, "Man-machine interfaces, enabled by artificial intelligence and high-speed data processing, improve human decision making in both speed and accuracy."[2]

The authors reaffirm integrating AI into the tactical headquarters and more broadly into systems within maneuver units at large to improve human decision-making. As the Army moves to achieve this vision of warfighting by 2028—or, depending on the referenced publication, years earlier—the authors identify two key gaps in the doctrine and leadership guidance offered to set conditions for this upcoming revolution in military affairs. First, the Army lacks a means to evaluate its progress in achieving AI-enabled MDO. Second, no practical guidance has been issued to maneuver units in how to prepare for the integration of AI-enabled systems. After addressing these two gaps, the authors also propose a system the Army could build with currently available technology to enhance situational understanding in tactical command posts.

If the Army is to integrate AI into MDO, and if we are to provide a way to evaluate AI readiness, we first need to understand what AI is. In this article, the authors use the National Security Commission on Artificial Intelligence's (NSCAI) definition referenced in its final report and originally published by senior Carnegie Mellon University current and former faculty members. Moore et al. define artificial intelligence as a "stack" or collection of technology layers requiring "talent, data, hardware, algorithms, applications, and integration."[3] The NSCAI's final report places greater importance on the talent who will drive adoption and implementation of AI-enabled systems and the data that will enable its included algorithms and models.[4] This article encourages early adoption of recommendations in the same areas because they align with current Army capabilities.

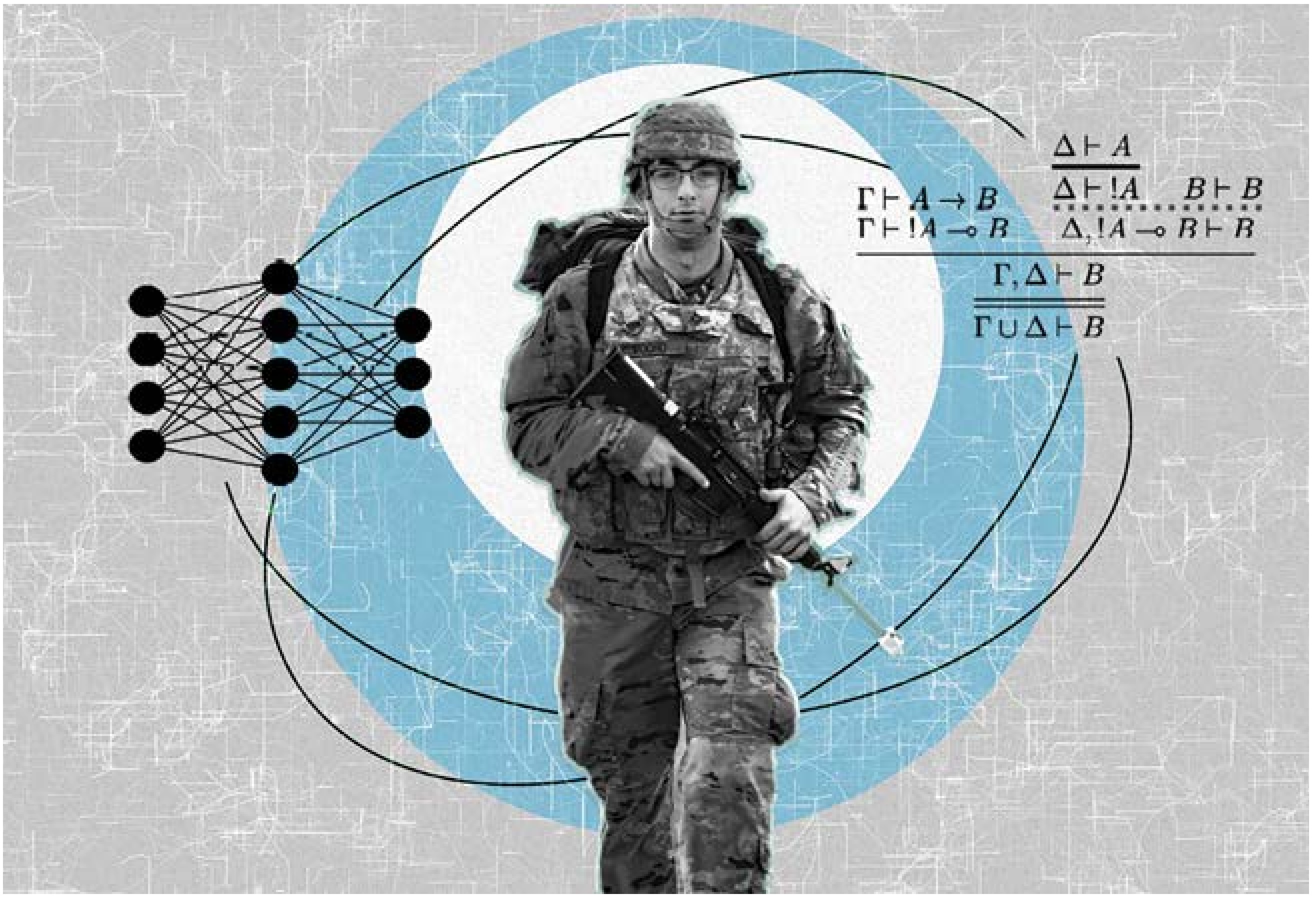
Maj. Benjamin Scott, U.S. Army, serves as Security Cooperation Division chief at U.S. Army Cyber Command after completing assignments as operations officer for the 1st Battalion, 27th Infantry Regiment, executive officer for 2nd Squadron, 14th Cavalry Regiment, and as a future operations planner for the 25th Infantry Division. Scott is an infantry officer and received his commission after graduating from the University of Tennessee. He holds an MA in military operations from the U.S. Army Command and General Staff College. His operational assignments include multiple tours in Iraq and Afghanistan as well as a humanitarian assistance mission to Liberia.

Capt. André Michell, U.S. Army, serves as a data engineer at the Artificial Intelligence Integration Center, Army Futures Command, after completing an assignment as an artificial intelligence scholar at Carnegie Mellon University. His previous assignments include serving as a platoon leader and plans officer in 1st Battalion, 27th Infantry Regiment, on Schofield Barracks, Hawaii. Michell is an infantry officer who received his commission from the U.S. Military Academy at West Point and holds an MS in computational data science from Carnegie Mellon University.

Beyond AI's components, it is important to understand what an AI-enabled system offers a user. Using algorithms designed specifically to train AI, the AI component of an application is "taught" to identify patterns within vast amounts of data such that it can categorize or predict additional information about new data. This is intentionally broad and ambiguous; it is an abstract process that can be applied to many situations. It is limited by the need for vast amounts of *labeled data* and the need to continuously collect more. Labeled data is data enriched with identifying information about the category or value an AI component can learn to predict. Labels must be related to the desired predictive capability. For example, building an AI that can identify a tank within satellite imagery would require a dataset of satellite images labeled to identify if they contain a tank or not. A more detailed prediction will require more detailed labels, meaning if we want to predict the model of tank, labels would need to include the type of tank in the image. The quality of any artificial form of intelligence is directly related to the quantity of high-quality data available to that system.

Fielding and developing an AI-enabled system is a process, and the authors propose evaluating AI readiness in the Army similarly with four phases. These are adapted from the four phases proposed by Eric Nyberg of Carnegie Mellon University for how an organization can evaluate its readiness for and use of AI.[5] They focus heavily on data management and organizational processes that are the foundation for creating and implementing an effective AI-enabled system. While these steps insinuate a progression, changes in circumstances beyond a unit's control can cause it to move backward or forward in the process of AI-enabling.

The process begins with being *data science ready*. An organization is data science ready when relevant data sources are identified, accessible, and consistently



According to the U.S. Army Development Command, "Army researchers develop[ed] an artificial intelligence architecture that can learn and understand complex events, enhancing the trust and coordination between human and machine." (Photo illustration by Rudi Petry, courtesy of the U.S. Army)

managed. Leaders in an Army unit at this stage will be able to access relevant personnel, logistics, training, intelligence, and tactical data in a reliable, timely, and contextually relevant manner. Critically, a maneuver unit must consider how to do this in a combat environment. Units will need to establish processes for organizing, normalizing, and storing information in training and combat. Furthermore, data must be integrated between systems and warfighting functions. In this phase, data is complete and soldiers with skills in statistical analysis can use this data to better describe their environment, actions, and subsequent outcomes. Army units that are data science ready will have engaged leadership who understand how data is collected, maintained, and shared within their organization.

A data science ready organization will strive to become *data science enabled*, the second phase. An organization is data science enabled when correlations between multiple data sources are identified and predictive models created from organizational data are employed to improve workflows and decision-making. Army units that are data science enabled will use data they collect, maintain, and access to enhance situational understanding, contextualize enemy and friendly actions, and predict future behaviors. Data science enabled maneuver units will collect, clean, and organize data in tactical command posts during field training exercises, command post exercises, and combat training center rotations. Soldiers will employ predictive analytics developed during preparatory training to identify enemy behaviors and react more quickly to highly dynamic, complex battlefields. Army units that are data science enabled will have invested leadership who integrate large volumes of data into the military decision-making process and rapidly adjust to changing conditions.

After using data science to enable better performance, units will pursue becoming *AI ready*, phase three. In this phase, organizations use data science as a part of operational processes and have integrated software applications that modernize their workflows to integrate computing techniques. Leaders who will employ AI understand what processes and requirements will be used to enhance, and they are able to communicate directly with AI engineers to design and implement relevant solutions. Army units will have a practical understanding of the capabilities and limitations of AI as a weapons system. Maneuver units will collaborate with units in Army Futures Command such as the Software Factory or the Artificial Intelligence Integration Center (AI2C) to develop AI solutions that enhance their mission readiness and capabilities. Data will be shared with sister organizations and made accessible in both tactical and garrison environments, and software updates created in the rear can be pushed over Army networks to applications at the tactical edge. Army units that are AI ready will have informed leadership who command their data presence and drive the requirements process for future AI-enabled software and applications.

Finally, an organization will become *AI-enabled* when it deploys AI systems and is able to directly measure their impact on mission success. These units can employ AI in tactical environments to automate processes and deliver mission success. These systems work on mission, and in critical environments and conditions. For Army units, these are resilient applications that can adapt to dynamic network conditions and provide value when enemies disrupt or deny communications networks. Organizations at this phase are characterized by highly resilient processes and systems that adapt to changing situations quickly to achieve decision dominance on a multi-domain battlefield. These systems display critical multidimensional data and insights in a timely manner. Data collection will grow in scale and velocity as modern systems both generate and consume immense volumes of information. AI-enabled Army units will have empowered leadership who use AI to lead complex missions with innovative solutions derived from interactions with man-machine interfaces.

It is intimidating to realize maneuver units are not even data science ready today, and the process of becoming AI-enabled will require a massive transformation. This is the nature of technological advancement as revolutionary as AI and represents an incredible opportunity for small units to embrace and influence the future of AI in the Army. Maneuver units should begin a practical response today to match the policy and doctrinal emphasis provided by Army and Department of Defense leaders. AI is an asymmetric capability wherein a relatively small investment can have outsized impacts. While this can harm large, slow-moving organizations, it can also provide opportunities for individuals and small units to have an outsized, positive influence on the entire organization. By encouraging and supporting innovative solutions from small units and their leaders, the Army can react nimbly to the disruptive impacts of AI in military affairs. An early step in encouraging this innovation is preparing the data environment for AI.

The Army also has a unique opportunity to learn from the mistakes of the larger AI community, specifically when it comes to data. As a team of AI engineers at Google wrote last year, the lack of focus on "data work" has been a significant detriment to large companies and AI pioneers who have suffered notable gaffs and missteps in deploying AI-enabled systems.[6] By focusing organizational and cultural change first in modernizing data management processes, the Army will naturally immunize itself against some of these concerns. The nature of the Army's mission and the dangers associated with AI-enabled systems' mistakes exacerbate the impact of undervaluing data quality in the Army.

Similar to how the Army directs maintenance activities through exercises such as a maintenance terrain walk, units can prepare the data environment through a data health evaluation. This is an appropriate evaluation for a theater command to perform in subordinate divisions. It may also be appropriate for corps headquarters to perform a similar evaluation in its subordinate brigade combat teams. These evaluations consider how well units steward the data they generate and to which they have access. Evaluating data health is, next to talent development, the best place to begin preparation for AI-enabled systems in maneuver units.

While evaluations should be unique and planned with special knowledge of the units to be evaluated, the general concepts would be similar across units. The data health evaluation asks the following question: How well does this unit collect, clean, and manage data about everyday operations in garrison and tactical

"Tomorrow's operating environment will be filled with smart autonomous devices and platforms that create diverse and complex information signatures," according to the U.S. Army Development Command. (Image courtesy of the U.S. Army/Shutterstock)

environments? Data collection should be complete in that it describes the context, environment, action, and result of unit activities. Units will collect data well when collection is automated and integrated into all processes. Data is clean when it is consistent in its architecture, types, format, and storage location. Clean data is ready for descriptive analytics and can be understood readily through well-adhered-to documentation. Data is well managed when it is accessible, persistent, and reliable. Units that do this well will have considered how to apply the data they gather into systems and processes. Part of a thorough data health evaluation will also consider how much information is visible across staff sections and working groups. Broadly shared data encourages collaboration and builds shared understanding. Some specific behaviors this evaluation could consider follow.

Performing a data health evaluation requires, above all other priorities, an honest assessment of unit readiness in this area. As Leonard Wong and Stephen Gerras of the Strategic Studies Institute share in their report and the authors of this article can anecdotally ratify, the Army struggles with competing requirements and incentive structures that lead to units sometimes knowingly reporting inaccurate information to meet readiness requirements.[7] AI-enabled systems will be particularly sensitive to these challenges and as such, the Army's data health evaluation must include a mechanism to evaluate the veracity of the data it has collected. One mechanism for this can be removing some elements of human intervention. For instance, a vehicle, aircraft, or cannon can be instrumented with sensors that identify if it is functioning properly or has faults in components of its system. This has the significant challenge of adding to the complexity of these systems. Another mechanism that is in line with industry best practices would be to randomly subsample data points to reevaluate. Examples include selecting units to perform simple actions that validate their equipment's condition such as executing crew drills on a 155 mm Howitzer, conducting a

The U.S. Army is seeking intelligent vehicles to ease soldier burdens in multi-domain operations. (Image courtesy of the U.S. Army/Shutterstock)

convoy with all functioning vehicles to a rally point in the training area, or executing a no-notice record qualification on individual weapons. Requiring these alert activities to validate the accuracy of the data a unit has stored are excellent ways to ensure our AI-enabled systems are outfitted with high-quality data. Army leaders must create the space for units to report this information truthfully without fear of retribution. The Army's ability to effectively fight in an AI-enabled multi-domain battlefield depends on changing this element of Army culture.

Beyond setting conditions for and evaluating accurate data collection, there are steps units can take today to prepare for the integration of AI-enabled systems. The following recommendations apply to units at all echelons. They are firmly grounded in capabilities available today and represent the initial steps in preparing the data environment for AI-enabled systems. These recommendations will help units become data science ready.

Maneuver units must appreciate the value of the data they interact with each day by immediately stopping deletion of data from shared file systems. These "shared drive" or SharePoint systems enable collaborative efforts within and across units but also hold within them a treasure trove of unit behaviors, training exercises, and reports. Files on these systems are often deleted when units run out of space to maintain the records from previous years. To create effective intelligence, Army data scientists and AI engineers will require access to many tens of thousands of labeled data points for each AI-enabled technology they develop. This represents a relatively small dataset in the AI community, and the Army cannot afford to lose more data by thoughtlessly deleting old files. Units should direct discretionary spending funds to purchase external hard drives and perform intermittent backups of their shared file systems; to do this, units must be enabled with specific additional funding and requirements. Additionally, all officers should have the ability to read nonsensitive files from all units at least two echelons above and adjacent to them. This will encourage collaboration and introduce immediate efficiencies while transforming our data culture to a sharing culture. When receiving support from a data scientist or AI engineer in the future, these devices should be offered as context to help create effective intelligence for the unit.

Organizations should restructure how they collect information from their subordinate units to increase the use of tabular formats like Excel. These formats are already standard for many status, logistics, and maintenance reports as well as inspection documents. Collecting this data in a tabular format will provide immediate benefits to units by enforcing data completeness in the near term. Doing so will also enable future computer-based methods to process and train AI more readily. In a tactical environment, the structure of a tabular format will help standardize documents such as intelligence collection, fires support coordination, and operations synchronization matrices. It will also create more useful and reproducible products for Army staffs while providing future computer-based systems with rich, comprehensible data about Army operations. When practical and effective, any documents or tools units use—like those described above but that currently reside in a document- (Microsoft Word) or slide- (Microsoft PowerPoint) based format—should be immediately replaced with a tabular document (Microsoft Excel). When collecting data in Excel, units should specify consistent column header names and consistent data types (numerical, time series, or text) within the documents. This transition will directly result in more robust and accurate AI systems and is a critical step to making decisions quickly. This transition is enabled when standard Army forms and documents are better structured, easier to use, and provide more useful information to users and consumers of data.

To guide AI development and requirements generation, units should collect and document how time is spent in garrison and in field training exercises. This can be a challenging, onerous task and the authors recommend two different ways units could do this. The first is to collect anecdotal information about areas or processes where data is manually copied between systems or humans are relied upon for coordination between data sources. This might be particularly useful in the tactical command post to identify areas where we rely on soldiers to coordinate between disparate systems. The second option is for commanders to direct the chief information officer/G-6 to install and collect data via keystroke loggers and application monitoring devices on Army computers. Data scientists and AI engineers can use this information to identify inefficiencies and time-consuming computing activities to develop systems against. The raw usage data and anecdotal examples of data inefficiencies can be shared with organizations in Army Futures Command such as the Software Factory or AI2C that can then work with units to rapidly develop and field solutions.

All Army systems in the future and many of the recent past generate immense amounts of data which must be made accessible immediately. First, for any program of record that the Army considers acquiring that will generate data, the authors recommend instituting a data accessibility and storage review. The purpose of this review would be to evaluate the ability for Army personnel to access data collected and stored by this system. It is unacceptable that all but a few Army systems lack a commonly available application programming interface and the ability to support programmatic system access. Further, historical data stored by these systems is the property of the U.S. Army and as such must be made available to its soldiers and officers through industry-standard methods without requiring any civilian intermediaries. The current data environment of these systems is prohibitively difficult to develop AI-enabled systems within.

Second, the Army should initiate a review of current systems that fail to meet this standard and reconsider the requirements specified for these programs. By revising acquisition processes and reviewing currently awarded contracts, the Army will establish itself as a leader in government and private sector organizations for its standards of data quality and accessibility.

At professional military education courses, the U.S. Army Training and Doctrine Command should immediately introduce appropriate instruction in data management and usage strategies. As part of the Basic Officer Leader Course, data education should include such topics as general data collection strategies, organization of unit- and branch-specific information, and modern data visualization tools. These tools will enable logisticians to better organize unit maintenance data, intelligence officers to better synthesize diverse intelligence sources, and maneuver officers to better report and collect data. The core principle of such education must be relevant; teach students about how this directly applies to their next job. In the Captains Career Course, this can be built on by including instruction in how to manage multiple data sources and establishing a culture of data collection. The Command and General Staff College ought to introduce a data collection elective course to educate field-grade officers in integrating authoritative data sources, managing a common operating picture, and the infrastructure required to support data collection and management. The Army War College should educate senior field grade officers to identify strategic gaps in data collection strategies and prepare them to lead with computer augmented situational awareness. Additionally, brigade, division, and corps commanders and chiefs of staff should be provided the opportunity to complete the AI2C's senior leader education program to understand and appreciate how to lead organizations with AI-enabled systems. The Army needs to adapt officer education in data collection and management techniques to prepare for the changing requirements of combat in MDO.

Combat training centers provide an excellent place to develop and implement AI-enabled systems for tactical applications. By storing labeled data on unit rotations and providing the opposing force with early versions of AI systems created for tactical command posts, combat training centers can be at the heart of AI development in the Army while also providing rapid feedback for complex systems that will be challenging to fully test and implement until the Army faces a near-peer adversary in combat. Similar opportunities exist within training conducted by the mission command training program for command post exercises.

While there is value in synergy and common lines of effort across large organizations, the Army will benefit from different units independently considering and adopting these recommendations. Over time, these independent ideas will form a stronger foundation for AI-enabled systems from the natural sharing and mixing of ideas as people move and change positions. The Army can model its creation of an environment for AI in MDO after the open-source software community sharing ideas and learning rapidly from one another's unique approaches. By developing unique solutions locally and then collaborating over time, units will identify common challenges while also reducing the likelihood of overlooking specific characteristics or mission-specific unique elements.

Concurrent to efforts detailed above, the Army should develop, experiment with, and employ state-of-the-art technologies to enable tactical headquarters' operations. To accomplish this, the Army could begin integration of AI in training during command post exercises conducted by the Mission Command Training Program and training rotations at combat training centers. This would begin by recording data from computers used in control systems, voice from participants, and location data from combat systems. Such data would then be available to data scientists with access to operational data from a controlled environment. Using AI and natural language processing combined with details and timings of events and opposing-force actions, this data could then be analyzed to identify trends where current processes fail to meet the demands of combat. Anomalies from these trends with optimal or better performance could then be further studied to identify successful tactics, techniques, and procedures. This would fuel development of improvements to existing systems and development of additional tools to enable warfighting. An example would be analysis of a brigade combat team's reaction to activation of an opposing force's air-defense radar system. By capturing all data associated with the event and knowing precise details about the opposing-force actions, after-action analysis could be more robust to understand the technical method and details of friendly detection, communication within the staff and friendly units (both content and methods of transmission), actions taken, and effectiveness in targeting including assessment. Done iteratively with numerous units, this would enable accurate understanding of capabilities, gaps, and effectiveness of Army units. With the quantity and variety of events inherent in command post exercises and training rotations, there is a tremendous and underused mountain of available data to enhance Army warfighting capabilities.

The goal for near-term AI integration into tactical headquarters would be production of an enhanced common operational picture (COP) for echelons from brigade through corps. This will reduce friendly cycle time in operations and targeting processes while increasing decision quality for commanders. An enhanced COP would provide more accurate and detailed friendly-force information, provide enhanced situational understanding of operational and mission variables, and enhance commanders' ability to see through the fog of war. This would be accomplished through integration of various and currently disparate systems within tactical operations centers including the Command Post Computing Environment, the Advanced Field Artillery Tactical Data System, the Air and Missile Defense Workstation, Electronic Warfare Planning and Management Tool, Distributed Common Ground System-Army, and Global Combat Support System-Army. Currently, these systems do not provide a sufficiently integrated COP on a single human-machine interface. Additionally, priority must be assigned to development, experimentation, and fielding of software and hardware that ingests data on mission and operational variables to analyze data and prioritize time-sensitive data for analysis and action by staffs and commanders.

This system, and others like it, will synchronize and integrate Army data to enable faster decision-making in complex, dynamic environments. It is a necessary advancement to fight in a modern war; however, it will also introduce more risk. In terms of system complexity, AI components are significantly more complex than software components and bring additional challenges.[8] No AI can explain why it made the prediction it did, and the best performing forms of intelligence unfortunately are also the least understandable. State-of-the-art AI systems can provide only measures of effectiveness and accuracy to justify their use. Furthermore, the real world cannot be wholly modeled by the data an AI engineer uses when training on intelligence and there is no clean, labeled dataset for combat. This data bias must be accounted for with ethical software engineering and intimate knowledge of both the Army and AI. Current efforts to bring this technology to the Army are staggeringly small in comparison to similarly ambitious products from private sector companies. In 2022, the Army graduated and began to employ twenty AI professionals. By comparison, Google in 2016 employed approximately a full-strength corps, 41,456 people, of just software engineers.[9] Of that number, two divisions worth, 27,169 people, are dedicated just to research and development.[10] Since 2016, Google's overall number of full-time employees has more than doubled.[11] If the Army is to modernize its workforce by developing and fielding the AI-enabled systems it needs to fight in MDO, then it must start preparing the data environment today. ■

Notes

Epigraph. "40th Chief of Staff of the Army Initial Message to the Army Team," Army.mil, 12 August 2019, accessed 8 July 2022, https://www.army.mil/article/225605/40th_chief_of_staff_of_the_army_initial_message_to_the_army_team.

1. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 38, accessed 8 July 2022, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.
2. Ibid., 20.
3. Andrew W. Moore, Martial Hebert, and Shane Shaneman, "The AI Stack: A Blueprint for Developing and Deploying Artificial Intelligence" (Paper presentation, SPIE Defense and Security, Orlando, FL, 4 May 2018),https://doi.org/10.1117/12.2309483.
4. National Security Commission on Artificial Intelligence (NSCAI), *2021 Final Report* (Arlington, VA: NSCAI, 2021), accessed 8 July 2022, https://www.nscai.gov/2021-final-report/.
5. Eric Nyberg, "Foundations of Computational Data Science" (lecture, Carnegie Mellon University, Pittsburgh, PA, Fall 2020), accessed 8 July 2022, https://mcds.cs.cmu.edu/11-637-foundations-computational-data-science.
6. Nithya Sambasivan et al., "Everyone Wants to Do the Model Work, Not the Data Work: Data Cascades in High-Stakes AI," *CHI '21*: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, no. 39 (2021): 1–15, https://doi.org/10.1145/3411764.3445518.
7. Leonard Wong and Stephen J. Gerras, "Lying to Ourselves: Dishonesty in the Army Profession" (Carlisle, PA: US Army War College Press, 2015), accessed 8 July 2022, https://press.armywarcollege.edu/monographs/466.
8. D. Sculley et al., "Hidden Technical Debt in Machine Learning Systems," *NIPS'15: Proceedings of the 28th International Conference on Neural Information Processing Systems 2* (2015): 2503–11, accessed 8 July 2022, http://papers.nips.cc/paper/5656-hidden-technical-debt-in-machine-learning-systems.pdf.
9. "Alphabet Inc.: Form 10-K, for the Fiscal Year Ended December 31, 2016," U.S. Securities and Exchange Commission, accessed 8 July 2022, https://www.sec.gov/Archives/edgar/data/1652044/000165204417000008/goog10-kq42016.htm.
10. Ibid.
11. "Alphabet Inc.: Form 10-K, for the Fiscal Year Ended December 31, 2021," U.S. Securities and Exchange Commission, accessed 8 July 2022, https://www.sec.gov/Archives/edgar/data/1652044/000165204422000019/goog-20211231.htm.