BIG DATA AT WAR: SPECIAL OPERATIONS FORCES, PROJECT MAVEN, AND TWENTY-FIRST-CENTURY WARFARE

Richard H. Shultz and Gen. Richard D. Clarke | 08.25.20

During the Iraq war America's special operations forces (SOF) demonstrated a remarkable capacity to innovate to accomplish a mission for which they were not prepared—finding and dismantling al-Qaeda in Iraq's (AQI) network of secret cells, which served as the backbone of the insurgency. It did so by developing new operational methods to uncover and eradicate a critical mass of AQI's mid-level commanders and managers, the linchpins of those secret networks.

In Iraq, SOF Task Force 714 was able to adapt to this unexpected mission through organizational transformation, interagency collaboration, and the adoption of cutting-edge software applications. This turned Task Force 714 into an intelligence-driven organization capable of analyzing and exploiting "big data" through state-of-the-art data integration tools.

Since the United States withdrew from Iraq in 2011, the US Special Operations Command (USSOCOM) has continued to innovate, adapting to an ever-changing war zone in the second decade of this century. And, most recently, USSOCOM and its subordinate commands have played important roles in the Department of Defense pathfinder effort to employ artificial intelligence (AI) and machine learning (ML) in the fight against ISIS, al-Qaeda, and their geographically dispersed proxies.

Designated Project Maven, this effort's initial objective is to automate the processing, exploitation, and dissemination of massive amounts of full-motion video collected by intelligence, surveillance, and reconnaissance (ISR) assets in operational areas around the globe. With a yawning scarcity of human analysts to sort through burgeoning amounts of imagery intelligence, a combination of AI and ML presented an ideal solution. Specially trained algorithms could search for, identify, and categorize objects of interest in massive volumes of data and flag items of interest.

From its initial efforts in Iraq to exploit "big data" to operationalizing AI/ML with Project Maven and beyond, SOF have been key stakeholders in the DoD struggle to

SEARCH ...

FOLLOW US

FACEBOOK

YOUTUBE

TWITTER

DISCLAIMER

The articles and other content which appear on the Modern War Institute website are unofficial expressions of opinion. The views expressed are those of the authors, and do not reflect the official position of the United States Military Academy, Department of the Army, or Department of Defense.

The Modern War Institute does not screen articles to fit a particular editorial agenda, nor endorse or advocate material that is published. Rather, the Modern War Institute provides a forum for professionals to share opinions and cultivate ideas. Comments will be moderated before posting to ensure logical, professional, and courteous application to article content.

MOST POPULAR POSTS

The Motivations and Methods Behind Russian Hybrid Warfare

How to Avoid Tripping Over Russia's

transition from a hardware-centric organization to one that must be software empowered and data driven. Only by doing so will the Pentagon be able to harness artificial intelligence to equip future commanders to understand, coordinate, and orchestrate operations to deter or defeat twenty-first-century adversaries.

The essay that follows highlights early SOF transformation in Iraq, its continuing adaptation after 2011 to the fight against al-Qaeda, ISIS, and its affiliates, and USSOCOM's partnership with Project Maven as a first step toward a data-enabled force.

Ugly Surprise in Iraq

As President George W. Bush pronounced on May 1, 2003 that major combat operations in Iraq "have ended," no one in his administration expected an armed resistance to materialize. Consequently, Task Force 714 joined in DoD's effort to mop up key officials from Saddam Hussein's scattered inner circle. This was the kind of mission for which they were prepared. For two decades, USSOCOM had cultivated specialized units that had honed surgical direct-action operations for very occasional use. This force was a strategic scalpel, not intended for day-to-day wartime operations.

But as insurgent violence burgeoned, Task Force 714 played a key role in the coalition effort to find and dismantle AQI's secret underground apparatus, which was unlike that found in previous insurgencies. AQI was a web of complex networks that did not resemble any insurgent pattern that had been seen before. For this mission, Task Force 714 was not prepared, said its commander, then Maj. Gen. Stanley McChrystal. He explained that as constituted, the task force could not keep pace with, let alone reduce, AQI's operational tempo. The unit was "losing to an enemy that . . . we should have dominated," he subsequently reflected. By early 2004, McChrystal decided Task Force 714 had to "adapt to new, more ominous threats."

Over the next two years the task force reinvented itself. Consider the acceleration in its operational tempo. In August 2004, it was able to execute eighteen raids across Iraq, which "couldn't make a dent in the exploding insurgency," McChrystal lamented. But in August 2006, Task Force 714 executed three hundred raids against AQI. And those raids began dismantling its networks, killing or capturing a large number of mid-level operational commanders and managers. By 2009, in the words of McChrystal, the task force had "clawed the guts out of AQI."*

Task Force 714 transformed from a strategic scalpel to a wartime organization that could "capture or kill on an industrial scale, which was not something it had ever been built to do," explained Adm. William McRaven, who in 2004 was the task force's deputy commander and later served as its commander. To do so meant the task force "fundamentally had to change . . . the way we were organizationally structured, manned, trained, equipped, and everything else."*

Organizational Transformation and Interagency Collaboration

To dismantle AQI's networks, his chief intelligence officer, then Col. Michael Flynn, told McChrystal the task force had to become an intelligence-driven organization. "Your intelligence operations . . . need to be 80 percent of what you do," Flynn recalls telling McChrystal. The task force "did not have the intelligence it needed."* It had to be restructured. McChrystal put it this way: "We brought an industrial-age force to an information-age war." McRaven convinced him to adopt a little-known concept—a joint interagency task force (JIATF)—which is a "model for whole-of-government problem-solving." By fostering "organizational collaboration," it seeks to overcome the "tendencies [of agencies] to seek autonomy rather than interagency collaboration."

The JIATF construct had to be adapted to SOF's missions. What that meant, McRaven told McChrystal, was forming partnerships with members of the intelligence

Ransomware Threat

Call for Submissions: Cyber Policy Challenge Essay Contest

UPCOMING EVENTS

There are no upcoming events at this time.

ANNOUNCEMENTS

Call for Submissions: "The Army in 2040" Essay Contest

Announcing the Modern War Institute's 2021–22 Nonreside...

Call for Applications: MWI's 2021–22 Fellow and Adjunct...

Call for Submissions: Polar SOF Essay Contest

community.* McChrystal was persuaded. But operationalizing a JIATF proved vexing. Deeply rooted cultures of secrecy infused those intelligence agencies McRaven proposed as partners. The key, explained McChrystal, was "we shared things they would not have otherwise had access to. . . . Suddenly, [they learned] we weren't just consumers of their intelligence; we were providers of our intelligence," which was a treasure trove of information.*

As the JIATF took shape, and raids increased to three hundred a month, intelligence became unmanageable with massive amounts of captured enemy material—documents, hard drives, thumb drives, cell phones—flowing into the system. The team also had access to imagery intelligence collected by unmanned aerial vehicles (UAVs), a capability that grew rapidly grow across DoD. All of this intelligence empowered the task force's interrogation program. That information was vital, Flynn explained, because detainees came to think the interrogator "knows more about him than he knows about himself."* McRaven affirmed "detainees would tell you literally everything they knew."*

When considered en masse, all the intelligence collected is illustrative of what today is called "big data." But to exploit it necessitated state-of-the-art data integration applications. To make discoveries in the intelligence, analysts needed new tools to decipher AQI's complex networks. The task force also needed a redesigned targeting cycle.

Exploiting Big Data through a Redesigned Targeting Cycle

As analysts encountered mammoth flows of "big data," they took two approaches to exploit it. First, Task Force 714 brought many more analysts to Iraq to comb through the data, an unsustainable solution in the long run. Second, they began building massive, organized databases that would allow them to amalgamate disparate forms of information to query. Now called "multi-INT data fusion," at the time it was revolutionary. It permitted analysts to penetrate AQI's physical and virtual hideouts. The goal was to identify targets of interest (e.g., an AQI financier) and, once located, monitor their activities and learn more about the network. But to do so, analysts needed new automated tools.

Initial software was rudimentary but powerful, drawing connections across vast arrays of data. Once the system was up and running, analysts could search fused data to uncover previously unknown activities that would then receive closer scrutiny. To exploit this intelligence bonanza, a new targeting cycle—F3EAD (find, fix, finish, exploit, analyze, disseminate)—was adopted to foster ops-intel collaboration. At two points in this cycle—exploit and analyze—analysts played key roles.

In the exploit phase, documents, electronic devices, and interrogations from a night raid were immediately made use of by analysts with operators, to identify a new target that was hit immediately. Intelligence derived from raids, explained McChrystal, could also be "studied to better know our enemy and identify opportunities to further attack its networks."* This was the goal of the analyze phase of the cycle. Here analysts became sleuths, finding needles in haystacks, all enabled by data integration, algorithmic computations, and spreadsheets.

Beyond Iraq: Evolution of Counterterrorism Operations

While Iraq dominated the attention of USSOCOM's counterterrorism forces during the 2000s, they were also expanding into other areas of operations across Africa and the Middle East to counter emerging extremist nodes. This expansion was driven by al-Qaeda's adaptations in the wake of losing the group's Afghan sanctuary in 2001. Bin Laden and several hundred al-Qaeda members retreated to a new safe haven in Pakistan and from there the organization slowly began reconstituting itself.

By the early 2010s, different al-Qaeda affiliates were located in several areas described by DoD as anti-access environments and ungoverned territories. This context was unlike Iraq, where the United States had a large-scale force on the ground. In places with growing al-Qaeda affiliates, the United States had a comparatively much smaller physical presence, if it had any at all.

To manage this complicated situation the Obama administration precluded the deployment of regular ground forces. Instead, SOF teams became increasingly engaged in multiple geographic locations in the 2010s. According to Gen. Joseph Votel, these units were small and operated from remote bases located in areas adjacent to al-Qaeda affiliates. And, he added, they required persistent intelligence collected by UAVs.*

In summary, as a result of these developments, US counterterrorism operations geographically expanded. And SOF elements continued to play a key role. But to do so in this greater area of operations, they needed an exponential increase in ISR imagery collected by UAVs.

Burgeoning UAV Platforms

As al-Qaeda's affiliates grew in the late 2000s, a new approach in how to execute counterterrorism operations gained traction. In 2008, Defense Secretary Robert Gates established an ISR task force to expand the role of UAVs in the fight against extremism. This resulted in considerable growth in UAV platforms, and they became crucial counterterrorism tools. They had the potential to collect massive amounts of actionable intelligence over a wide span of territory. Intelligence collected by UAVs could be employed to find al-Qaeda affiliates hidden in that territory. UAVs became even more essential with the emergence of ISIS.

With few boots on the ground, sensors became a key capability for waging that fight. The expanded UAV fleet provided a potentially exceptional alternative to troops. These platforms carried an array of sophisticated sensors that could collect massive amounts of imagery and other geospatial data to expose physical features and activities taking place in specific areas of the globe on a 24/7 basis. And those platforms and sensors became increasingly sophisticated in reconnaissance and surveillance operations in the 2010s.

Full-motion video (FMV) collected by UAV platforms grew exponentially in the early 2010s. Understanding what this encompassed can be stupefying. For example, one estimate noted that in 2011, UAVs "sent back over 327,000 hours (or 37 years) of FMV footage." By 2017, it was estimated for that year that the video US Central Command collected could amount to "325,000 feature films [approximately 700,000 hours or eighty years]."

To analyze FMV from all these data feeds required considerable exploitation capabilities to extract meaning from pictures. The procedure for doing so is referred to as PED—processing, exploitation, and dissemination. To this day, it remains labor intensive, carried out by analysts attempting to sort through mountains of data at processing centers largely located in the United States. A considerable number of analysts were tasked to watch video screens, interpret what they saw, extract meaning from it, and provide their findings to operators deployed forward in the area of operations. This labor-intensive approach could not scale to meet the PED needs of warfighters.

In effect, while the UAV platforms and sensor systems experienced one technological transformation after another, no technical solutions were adopted to automate the processing of the data being collected. By the mid-2010s, if not earlier, PED had become an issue of scale. There was just too much data for the analyst workforce to manage. And expanding the size of it was prohibitive. As FMV sensor collection burgeoned, analysts assigned to process, exploit, and disseminate all that intelligence simply became snowed under by data. And this became a serious problem for USCENTCOM in the fight against ISIS, explained Votel, who in 2016 was its commanding officer.*

In the midst of these developments and overwhelmed by the amount of FMV and an expanding area of operations, complaints began emanating from deployed SOF personnel. Warfighters were frustrated by the inability to exploit the intelligence being collected by UAVs. This was what Under Secretary of Defense for Acquisition, Technology, and Logistics Frank Kendall heard during a 2016 visit to Baghdad. He watched video from tactical UAVs. "Upon asking who was performing PED, the answer was no one was," according to a description of the visit. Kendall "was not too happy [when he heard] that."

The same unhappiness was expressed at USCENTCOM headquarters in Tampa, Florida. Too much real-time intelligence was not being exploited because there was no capacity to process, exploit, and disseminate the tactical and medium-altitude FMV collected by UAVs. It was at that point that the Warfighter Support division of the Under Secretary of Defense for Intelligence (USDI) was tasked to find an automated solution for the FMV-PED conundrum.

USDI's Automation Working Group

Eric Schmidt, former Google CEO, commenting in 2020 on his collaboration with DoD, observed that "the way to understand the military is that soldiers spend a great deal of time looking at screens." He argued that this was not the best use of a soldier's time, and advances in computer vision were beginning to show the potential to relieve soldiers from these mundane tasks. This same appraisal underpinned recommendations made by a team working inside the Warfighter Support division of USDI three years earlier.

In October 2016, on the heels of complaints coming out of the warzone and from USCENTCOM headquarters about the failure to exploit FMV, an Automation Working Group was established in USDI. Its mission was to scrutinize all possible options for automating PED practices and recommend the one best able to exploit geospatial intelligence. What they found was a tech world experiencing a revolution in AI and ML, with computer vision, image recognition, and scene understanding all in the forefront. The Automation Working Group concluded the solution to DoD's problem was to be found in Silicon Valley, and not in the existing network of defense laboratories and the defense industries that had long supported DoD.

The working group visited the world's best AI companies and discovered a revolution taking place in the application of computer vision technologies to autonomous driving and other industries. The group saw an opportunity to apply commercial technology, trained on DoD data, to help solve DoD's PED problem.

Following two months considering all possible options, the working group reported its findings. Its bottom line was unequivocal—AI and ML solutions could revolutionize PED methods so that vast amounts of FMV collected by UAVs could be exploited to support warfighters. To make this point, the group's presentation began with a slide of AI billboard advertisements that festooned the Highway 101 corridor linking San Francisco and Silicon Valley. The takeaway from these software sales pitches was that readily available AI solutions were on the shelf and could be adapted to address the FMV-PED challenge. Indeed, cutting-edge computer vision was available and adaptable with massive potential to change the way DoD fights.

When briefed on the Automation Working Group's recommendation and shown a demo of how computer vision could be used to put dots on vehicles and store them for use later, Deputy Secretary Work requested they prepare a formal proposal. He wanted it titled *Modernizing PED for 21st Century Warfare: Go Big with Automation.* It was ready by mid-February 2017. From the perspective of the working group, *Go Big with Automation* was judged so overpowering that all other options were rejected as non-starters.*

Project Maven, USSOCOM, and the Transition to an AI-Enabled Mission Command

Go Big with Automation became the mission statement Deputy Secretary Work assigned to the Algorithmic Warfare Cross-Functional Team (AWCFT), the element established to execute Project Maven on May 20, 2017. The immediate objective was to "automate Processing, Exploitation, and Dissemination (PED) of tactical . . . and Mid-Altitude Full-Motion Video" in support of operations to defeat ISIS. Through "computer vision algorithms for object detection, classification, and alerts," real-time actionable intelligence could be delivered to warfighters. The AWCFT's mantra became "AI for intelligence." It would be achieved by bringing industry-best software in AI and computer vision to FMV, fielding it to warfighters, gathering feedback, and rapidly using that feedback to upgrade the tools' performance.

The algorithmic warfare team planned to bring that AI software to those parts of the military engaged in combat operations. Consequently, the immediate consumers were USSOCOM units who were at the forefront of the fight against ISIS and al-Qaeda. SOF were receptive to the initiative given past experiences learning how to exploit big data through data integration systems. Moreover, they faced the challenge of managing an area of operations that had expanded considerably, as noted above. If AI could be trained to watch all the FMV collected across a wide stretch of territory to identify those entities that warranted human scrutiny then, suddenly, that area of operations could become more manageable.

The guidance communicated from USSOCOM's commander at the time, Gen. Tony Thomas, to those units was his keen interest in Project Maven. He directed his deployed SOF units to experiment relentlessly with these new technologies. And that guidance still stands for the command today. As a result, deployed SOF units came to embrace the potential Maven could offer. And they worked closely with Maven specialists assigned to their units.

Project Maven aimed to operationalize AI in the hands of warfighters within six months. To get there, they had to build everything from scratch, from a data pipeline to algorithm development to computer power to integration on live FMV feeds to user interfaces that could display the object detections from the computer vision algorithms. This had never been done before in DoD. Project Maven started with nothing more than a vision and a willing partner in USSOCOM.

DoD had a traditional, lockstep approach to acquisition that was incongruous with how commercial technology companies did business. New approaches were required to think like a tech company. There was no playbook for this since AI, broadly, and computer vision algorithms deployed on live FMV, in particular, were so new to DoD. Good software development requires quick, iterative experimentation by users. Embracing this model, the team sent software engineers to the field to learn from users and rapidly turn software improvements on the spot. They called the approach "field to learn."

The full story of the deployment of algorithms that could exploit FMV data by recognizing and singling out different objects in the battlespace such as vehicles, people, buildings, and weapons remains to be told. Maven is still a work in progress. What is known about those early days is that software tools were first sent to units from one of USSOCOM's service components engaged on forward operating bases. Teams from a naval special warfare group were the first out of the gate. They were not immediately impressed with the algorithms' performance but said they could see their potential. Later, the tools were also sent to USSOCOM's counterterrorism teams conducting operations forward in other parts of the warzone. They had analogous reactions.

While the AI could place a boundary box around vehicles, buildings, and people, and display them on a map, the algorithms were rudimentary with many false detections. In this process, called geo-referencing, analysts hoped to add location information to otherwise untagged data, so they could watch and track it. But that was not possible in the startup phase. Indeed, accuracy of detections was only around 50 percent. Determining the difference between men, women, and children was challenging.

Initial fielding of the algorithms generated varied feedback from the SOF warfighters. They were interested in the potential of what they saw, but critical of the algorithms' performance, bluntly pointing out mistakes and limitations. They told the Maven representatives what they hoped AI could do for them. For example, they discussed the ability to identify potential targets through geo-referencing, and then allow users to click on a dot AI placed on those objects to create a target ID for possible exploitation. That was intriguing to SOF operators. So was receiving alerts about activity in areas adjacent to those being watched on a screen by an analyst. And they wanted to be able to track an object identified by the AI.

Early attempts by Maven representatives at remote bases to retrain algorithms based on inputs from users was also fraught with shortcomings. The representatives found that integrating algorithms into existing or legacy systems did not work well. It created many technical problems. The Maven team started out thinking they only had to focus on adopting the best algorithms, but they realized the need for a new interface system to better integrate algorithms with the users. They successfully turned to a leading commercial vendor who supplied an improved platform for human-machine teaming.

It was a cumbersome start. SOF teams reported seeing potential in Maven and quickly offered suggestions for improvement. For example, if they were focused on a targeted individual, could the appearance of dots on other individuals signal the presence of enemy personnel or noncombatants? Or if they were building a pattern of life for a location, could the AI be trained to help them do so? And for the territory surrounding a target site, could AI provide alerts in the form of indications and warning?* This type of user feedback was exactly what the data scientists needed. While the hands-on systems could quickly evolve in the daily back-and-forth between user and engineer, Project Maven had uncovered a much larger obstacle within the defense data infrastructure itself.

Years of US military operations had left exquisite data repositories—fuel for developing quality AI/ML capabilities. However, the data was fragmented across many silos. If a system had access to one repository, it could not access the others. Data classification—both in terms of archival organization and security compartmentalization—had become a monumental roadblock. Early in Project Maven, data engineers would buy multi-terabyte hard drives, mail them to operational units, and request that the units download their richest data sets for transport to USSOCOM's headquarters in Tampa, Florida.

Once returned to Tampa, the data passed through a laborious process. Handlers would transfer the data from hard drives to a dedicated repository platform. Reviewers would curate the contents to create suitable data sets. Handlers would again transfer the data to a separate platform. Labelers would clean and catalogue the data to feed algorithm design and development. Handlers would transfer the data back to transportable media. The data would move to a lab for algorithm development. At any given point, the team had fifty or more hard drives slinging around the globe, coming and going, being downloaded and uploaded, and being painstakingly transferred between silos. Every step of the process required direct human interaction. While the process has gained some increased automation over time, the lack of a dedicated cloud-based data management infrastructure capable of quickly cutting across classification levels is the greatest roadblock to advancing AI capabilities for the warfighter.

Not only did AI development require a cross-domain data platform, it quickly became clear that the explosion of data made available by such a platform would require AI to make sense of it. The ability to access publicly available data, find connections within classified archives, and rapidly alert a strategic commander to a threat, update the situational awareness of a unit in the field, or enable quick and precise information operations became a very real possibility and an invaluable opportunity. Effectively, operationalized AI and cloud computing were inseparable. Recognizing the potential, USSOCOM extended the partnership with Project Maven and US Air Force research and development offices to build an algorithmic capability that will blend publicly available data with classified information across the intelligence, planning, and operational portfolios. This vision has expanded beyond Project Maven and USSOCOM, and now features prominently in DoD's Digital Modernization Strategy.

Since the spring of 2018, the AWCFT and its SOF partners have endeavored to move Project Maven beyond these initial challenges to solve the PED problem and further realize the potential of AI-enabled mission command. They have made tremendous progress. Recent assessments by SOF leaders report a near-transformative effect of the human-machine interface in producing a functional common operating picture. Under the hood, the algorithms are improving as well, exhibiting greater utility and accuracy.

Project Maven has not replaced the analyst, but it has already demonstrated the ability to reduce the transaction cost of information as it flows from sensor, to analyst, to commander, to the special operator in the field. Reinvesting the analyst's expertise and energy away from screen-watching and onto more exquisite tasks is not just economical, it is a combat multiplier. AI tools—like Maven and its successors—provide a solution to make sense of and exploit the sheer volume of data that inundate military leaders at all levels. These efforts will increasingly provide commanders with a dynamic, shared view of a multi-domain battlespace and enable them to fluidly make decisions with speed and confidence.

Readying the Force for the Future—Beyond Maven

Make no mistake, Project Maven is not the endgame—it is a start point. The PED problem with FMV was a single point of entry. The intelligence warfighting function alone has many other data-rich nodes, such as digital media and other forms of captured enemy material, that are ripe for AI/ML application. Nor has USSOCOM been a lone champion in DoD's efforts to develop and adapt data-driven technologies. Each of the military services understands the value. The US Air Force invested earlier and heavily in a number of applications during the post-9/11 wars, and the US Army Futures Command has made growing investments in this space as the Army modernizes to support the emerging Joint Warfighting Concept.

However, USSOCOM is uniquely suited to serve as pathfinder for DoD capability development and integration across a wide range of technologies—AI/ML among them. SOF units are actively engaged around the globe in a wide range of activities. Their force structure and processes are inherently flexible, and they are both willing and able to assume risk in experimenting with new tools and techniques. The type of innovation and flexibility exhibited by SOF units in Iraq and Afghanistan was exceptional, but it is not exclusive. That willingness and drive to adapt is a crucial part of the SOF identity, and it is still alive and well with SOF's partnership with the AWCFT and other efforts.

Both DoD and USSOCOM see broad application for data-enabled technologies. USSOCOM has taken steps to begin transforming to an AI-ready workforce—a team that is literate in data-driven technologies, is able to spot potential applications, and owns sufficient expertise to maintain those technologies in house. This began in August 2018 with the creation of USSOCOM's Command Data Office to oversee this workforce transformation, as well as provide a node for industry outreach, data governance, and application of a data-focused perspective to capability development decision-making processes. DoD has now followed suit.

USSOCOM is investing in a range of AI/ML applications. Project Maven and the AI-enabled mission command initiative is only the beginning. In partnership with DoD's Joint Artificial Intelligence Center, USSOCOM ran a study to apply predictive maintenance algorithms to select aircraft systems of the Army's 160th Special Operations Aviation Regiment. The results were so powerful that USSOCOM is accelerating integration of these tools across the command's full rotary-wing and fixed-wing aviation fleets.

Ongoing studies and capability development initiatives among various SOF units seek to apply the power of these analytical tools to drive increased efficiency, cost savings, and lethality. These range from detection tools (offshoots of Maven) and autonomous system operation to cyber security and monitoring the brain health of special operators. USSOCOM's SOF Acquisition, Technology, and Logistics (AT&L) directorate has also restructured to better advance these goals. Not only is SOF AT&L taking steps to seek out potential applications of AI/ML in all existing programming lines, in March 2020, the directorate formally created a Program Executive Officer for SOF Digital Applications to improve enterprise-wide acquisition of software solutions.

The extent to which Project Maven has advanced toward the goals set out in 2017, and the role the AWCFT and USSOCOM played in achieving those ends is a story that is still unfolding. But when that story is told, it will not only be about automating FMV-PED to empower SOF teams to more effectively degrade and debilitate al-Qaeda and ISIS. It will also be the story of whether Project Maven served as the springboard to prepare DoD as an institution for future wars—a transformation from a hardware-centric organization to one in which AI and ML software provides timely, relevant mission-oriented data to enable intelligence-driven decisions at speed and scale. When that happens, US commanders will be able to gain decisive advantage over current and future enemies.

* Quoted material is from interviews with various individuals.

Richard H. Shultz, Jr., is Lee E. Dirks Professor of International Politics and Director of the International Security Studies Program at Tufts University's Fletcher School of Law and Diplomacy.

Gen. Richard D. Clarke is Commander of US Special Operations Command.

The views expressed are those of the authors and do not reflect the official position of the United States Military Academy, Department of the Army, or Department of Defense.

Image credit: Technical Sgt. Luke R Sturm, US Air National Guard

10 COMMENTS

Chris on 08.26.20 at 10:25 am

The article makes a number of astute observations about the growing importance of AI/ML to operational forces. One of the observations I found that resonated was about data.

“Project Maven had uncovered a much larger obstacle within the defense data infrastructure itself.

Years of US military operations had left exquisite data repositories—fuel for developing quality AI/ML capabilities. However, the data was fragmented across many silos. If a system had access to one repository, it could not access the others. Data classification—both in terms of archival organization and security compartmentalization—had become a monumental roadblock. Early in Project Maven, data engineers would buy multi-terabyte hard drives, mail them to operational units, and request that the units download their richest data sets for transport to USSOCOM’s headquarters in Tampa, Florida.

Once returned to Tampa, the data passed through a laborious process. Handlers would transfer the data from hard drives to a dedicated repository platform. Reviewers would curate the contents to create suitable data sets. Handlers would again transfer the data to a separate platform. Labelers would clean and catalogue the data to feed algorithm design and development. Handlers would transfer the data back to transportable media. The data would move to a lab for algorithm development. At any given point, the team had fifty or more hard drives slinging around the globe, coming and going, being downloaded and uploaded, and being painstakingly transferred between silos. Every step of the process required direct human interaction. While the process has gained some increased automation over time, the lack of a dedicated cloud-based data management infrastructure capable of quickly cutting across classification levels is the greatest roadblock to advancing AI capabilities for the warfighter.”

It is often said that 80% of Data Science deals with identifying and preparing data while the remaining 20% deals with analytics. Data and AI/ML are like the Chicken and Egg problem. Before you can develop and deploy effective AI/ML algorithms you need to have the data in place, aggregated, cleaned, tagged, discoverable, etc. This means that if AI/ML is a high priority for DoD, then evolving the DoD data ecosystem is also a high priority activity.

REPLY

Zoe on 09.29.21 at 9:27 am

Based off this article and what the public knows about successful missions in the past, intelligence networks and capabilities are the main way forward for both the DoD and USSOCOM. I agree with the author that Project Maven is a reliable first step toward a data-enabled force and that SOF units need to seek to apply the power of these analytical tools (AI/ML applications) to drive increased efficiency, cost savings, and lethality.

REPLY

Zoe on 09.29.21 at 9:30 am

***main way forward for USSOCOM under the DOD

REPLY

Brock on 10.01.21 at 11:14 am

I appreciate how this article shows the evolution of military/strategic intelligence through America's operations opposing AQI, among other groups. It is interesting to see how new technological capabilities have led to the development of new strategies and TTPs (e.g. F3EAD) to incorporate this tech and exploit its advantages. However, the authors' note that Project Maven is just the beginning is a very important one. While this piece highlights the bright and advantageous future for our newly-honed AI/tech capabilities, it would also be wise to consider dangers to blind use of the technology as well. First it the danger of overuse. We mustn't let 'big data' control the senses of our commanders: especially in the field, this massive data set is something that is potentially blinding. Second is the danger of misuse. For good reason, bureaucrats on the civilian side and officers on the military side are highly focused on tradition and best practices that have worked before. Technological development has been tumultuous and we are in an ongoing state of technological revolution, in which the most efficient uses of technology mustn't be prescribed, per say, but rather continuously scrutinized and evolved. This is a job, as the authors say, that is perfect for SOF, but it is a practice that must be sustained and embraced in the larger operational forces as well.

REPLY

Arush on 10.01.21 at 1:29 pm

I agree. I think that this technology has a role to play, and the US military will benefit from AI enhanced capabilities, but we should be careful to not become dependent on the technology. There will be situations where Project Maven is unable to work effectively or is compromised, and we should not let our unenhanced capabilities suffer so we are not caught off guard.

REPLY

Carson L. on 10.01.21 at 1:22 pm

The use of AI is a huge analytical and electronic marvel. Using AI to derive information and necessary intelligence is a huge step in cyberspace. Simple application of an AI to find relevant info can reshape how analysts look at information for missions and military-oriented records. This isn't just limited to the military. Civilian organizations could reshape their analysis of economic and judicial documents and records. This new capability is a huge step toward the automation of just more than military analysis, but also automated systems. The idea of a reconnaissance drone running itself is a huge leap toward just one aspect of automation. In the military realm, special forces members can be given information relevant to their missions efficiently. Analysts also no longer need to spend weeks collecting and deriving information, putting manpower in more crucial roles. In the civilian realm, there's almost no end to the possibilities of an AI system that can collect, derive, and exploit information on a national scale. Seeing where these developments go in the future will be a huge step toward global automation of menial and critical tasks and work across the world.

REPLY

Aristotle Colarossi on 10.01.21 at 1:41 pm

I completely agree. Now more than ever due to technological advances will military intelligence play a crucial role in the way in which we conduct war. It

will be interesting to see how the U.S. military develops these technologies and just how effective and efficient they end up being.

REPLY

Jillian on 10.01.21 at 1:49 pm

I see this as a huge advancement towards protecting human lives, all while being even more effective and collecting more information. More accurate intelligence will make it more plausible to successfully complete our strategic goals. Something interesting to think about is that we are only getting more advanced from here. In the near future, we may have different AI/machine learning technologies that are only a figment of our imagination right now.

REPLY

Nathaniel Frederickson on 10.01.21 at 1:53 pm

Personally, I wonder how development of these systems of intelligence collection and analysis could become a target for cyber attacks. Clearly, systems like this are present to help make sense of the mass amount of data that we are receiving, which in the information age, is a lot. However, given the sheer number of recent hacks on US infrastructure, and government agencies, I wonder if a repository of data of this size could potentially just be a huge target for cyber "hacktivists" of Cyber terrorists, or ever adversary states. On some level, getting into a repository like though would be a golden goose. It's be a trove of data the activist didnt have to spend near as many resources collecting.

REPLY

CONNOR on 10.01.21 at 1:59 pm

The development of the AI and intelligence intersection in regards to the battlefield is interesting. The most interesting aspect of this is the disconnect between the UAV footage and ability to analyze. My uneducated assumption was that the UAV intelligence collecting capabilities were developed simultaneously with the analysis capabilities. The future of capabilities, kickstarted by project Maven, resemble video game-like battlefield capabilities.

REPLY

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

COMMENT

NAME * EMAIL * WEBSITE

□ Save my name, email, and website in this browser for the next time I comment.

POST COMMENT