Artificial Judgement: A Case for Rethinking the Future Vector of Military Technological Innovation

By Col Brian J. Gross, USAF; Col Douglas D. DeMaio, USAF; and COL Matthew F. Ketchum, USA

Article Originally Published in Air Land Sea Bulletin 2018-1, June 2018

Introduction

The United States (US) military is falling behind in the global race for military technological superiority. This lag is due to a number of factors, which include: a cumbersome acquisition system, budget constraints and uncertainty, a focus on the counterinsurgency fight, a culture that is adverse to failure, and a pervasive lack of focus on innovation and invention. The Service secretaries and chiefs, among others in the Department of Defense (DOD) and defense industrial base, have made a marked push to reverse course. Now that the counterinsurgency fight has subsided, the DOD budget forecast is more robust, and a concentrated effort to devise a rapid acquisition process has begun, the Services have signaled full speed ahead for innovation and risk tolerance. In a future faced with contested domains across the spectrum of warfare (particularly air, space, and cyber), the US must not only catch up with technology, but leap ahead to regain a competitive advantage.

Many of the latest Service initiatives center on two ideas: gaining better networks and exploiting machine learning. There are incentives to improve the US military's command and control (C2) networks and reap the benefits of big data synthesis and artificial intelligence (AI). However, when it comes to pulling the trigger on the front lines in battle, networks cannot be guaranteed and AI will continue to fall short of human capabilities. Neither the unaided human nor unmanned machine will win a future conflict. Exploring the benefits of AI at the tactical level requires a new strategy for innovation and invention.

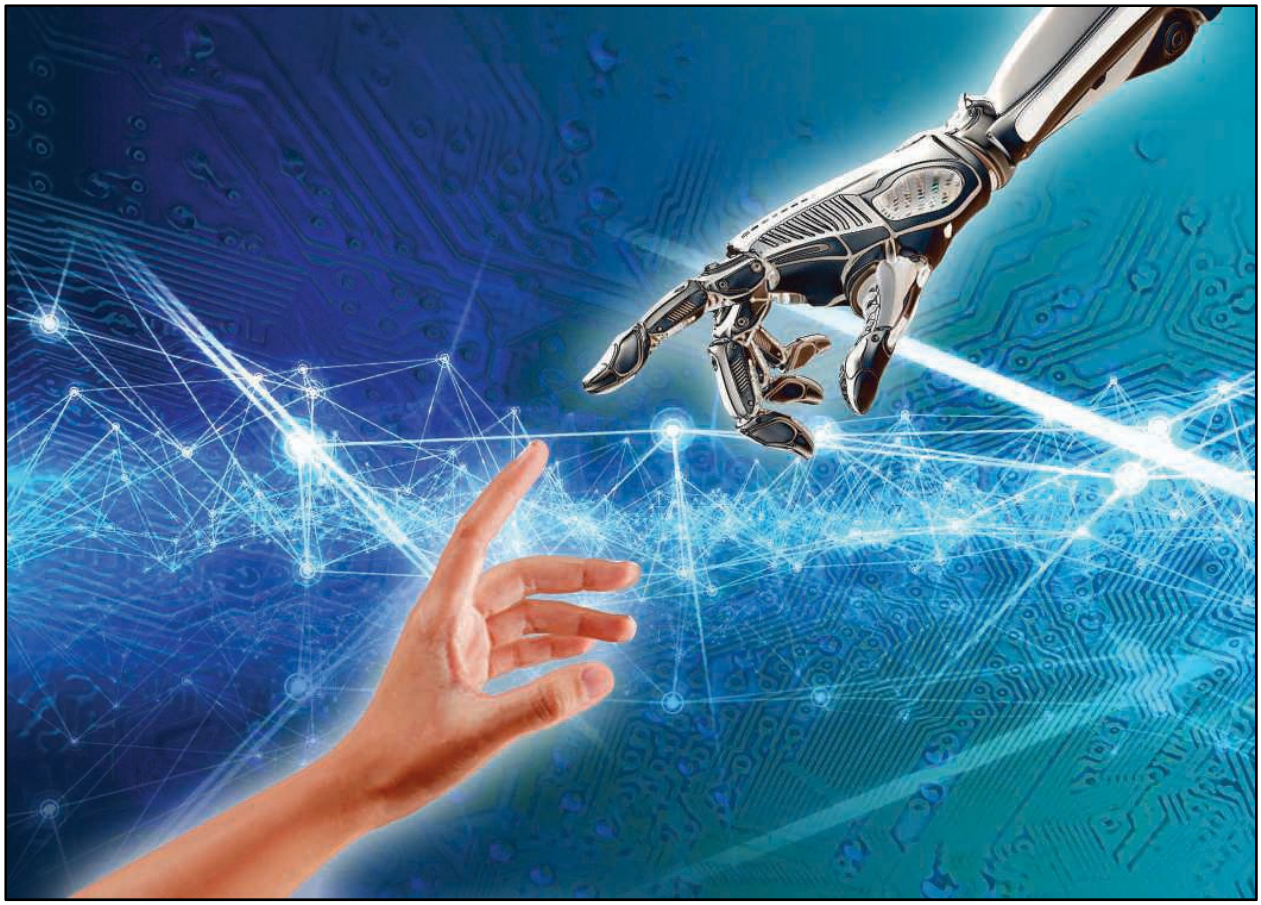

Illustration by Daniel Armstrong, LeMay Center, USAF

A Need for Innovation

"…our technological overmatch is decreasing as near-peer adversaries increase their capability and capacity," said General Joseph F. Dunford Jr., during his nomination for reconfirmation as Chairman of the Joint Chiefs of Staff in September 2017. He later went on to add, "While we have identified areas in which we have limited capacity, the larger issues are that our technological overmatch is eroding and our adversaries' speed in narrowing capability gaps is accelerating; increasing capacity alone will not reverse these issues."[1] Adversaries who were once labeled as near-peer have leveled the battlefield by possessing technological capabilities that are on par with, and in some instances have exceeded the capabilities of, the armed forces of the US. It is clear from his comments, and those of other Service leaders, the US is lagging behind in a global race for military technological superiority. For the last 16 years, the Services have focused their attention on battling the counterinsurgency fight while failing to recapitalize or modernize legacy weapons systems and C2 capabilities.

The Service chiefs are endeavoring to reverse course and enter a new era of technological advancement with an increased or renewed focus on innovation. They are seeking advanced, integrated communications technologies to support the future operations in multiple domains. American military leadership acknowledges the benefits

of coordinated air, land, sea, space, electromagnetic spectrum, and cyber operations but lack the compatible technology, acquisition strategy, and doctrine to guide it.[2]

Though it is not a new concept, when one considers future conflict with a sophisticated adversary or competitor, advancement of the multidomain battle concept is almost certain. Adversaries, potential adversaries, and competitors have learned to exploit US military vulnerabilities and contest US superiority in warfighting domains, particularly in the cyber domain. In the last 50 years, the US was contested in the air, ground, and maritime domains. Now, US capabilities and access are contested in space, cyberspace, the electromagnetic spectrum, and across C2 networks.[3]

The Service chiefs, among others in the DOD and defense industry, have advocated for a technological revolution to unite warfighting domains and functions, and the Services to counter advancing adversary capabilities. During the 2017 Air, Space, and Cyber Symposium in Washington DC, General David L. Goldfein, Air Force Chief of Staff, emphasized an imperative for Air Force advancement of technology, and what he called the future "wars of cognition." General Goldfein posed the question, what does the Air Force need to be in the year 2030? He went on to consider that question, partially answering it with two additional questions and answers: "Can it connect? Good. Can it share? Even better."[4]

Soon after, General Mark A. Milley spoke at the AUSA Eisenhower Luncheon in 2016, relaying much of the same sentiment, but went a bit further in depth discussing the role of AI and potential, profound changes in the future character of war.[5]

General Goldfein's point on a connectivity and data sharing imperative serves to highlight the military's current lack of innovation and a dynamic acquisition strategy. The problem with the connectivity and data sharing argument with a 2030 target, however, is that the timeframe is off by about 30 years. Technology in 2030 will, or should, surpass the proposed benchmark. The world is already connected and can share. US weapons systems cannot; and potential adversaries know it. If leaders want to shape an acquisition strategy which targets the year 2030, they must ask different questions and try to understand what is beyond connectivity.

During the February Air Force Association Symposium, General Goldfein updated his position by pushing out the timeframe to the year 2045 and adding an important question to his two earlier ones. In addition to the ability to connect and share, he added the following question: "Can it learn? Perfect." This addition is important because he took the Air Force effort from current technology to emerging technology. While this was an important step forward, it continues to miss the mark in some regard. If the Air Force is to "push the boundaries of Moore's Law" and "kickstart the technological edge," it should not equate machine-learning technology with perfection.[6] Machine learning and AI represent immense opportunities, not necessarily the pinnacle. While defining future technology, perfection is difficult. It is reasonable to suggest including the human nexus as well.

Future Landscape

Big data, machine learning, and other forms of AI will inform the future joint warfighter, with access to, and rapid synthesis of, information being key asymmetric factors to

winning the next fight. Leveraging information to build perfect situational awareness has been the dream of warfighters since the dawn of warfare; a quest that can never be fully achieved. However, coordinated, multidomain operations are achievable but will require instantly and reliably integrating all domains and warfighting functions, with a common understanding of the battlespace[7]. Integration begins with common, reliable communications. Commanders at the strategic and operational levels who already have access to enormous amounts of information will soon have access to much, much more. They will have so much data that computers will have to learn to do the heavy lifting. This represents an area in which the military is falling behind; it is, effectively, throwing away enormous amounts of usable data due to a lack of capacity, for machine learning and other forms of AI[8] to help lighten and, exponentially, speed up the traditionally human burden of information synthesis.

Current efforts for redundancy and hardening the network are needed but do not, necessarily, equate to ensured network reliability. At all levels of warfare (particularly, the tactical level), redundant, multi-node, layered networks will not be enough to ensure US weapons systems remain connected. The legacy networks, like the Army's Warfighter Information Network-Tactical, are insufficient to counter emerging threats, therefore, new systems are needed. As the US military builds new capabilities (where every tactical vehicle, aircraft, and ship are nodes in the network) the US becomes more dependent on a system which can never be guaranteed. This is an era where America's adversaries have a proven ability to deny network access, target and exploit electromagnetic signatures, and shoot down communications satellites. The US' competitors have modernized their forces and have learned to exploit America's vulnerabilities.[9] Therefore, tomorrow's warfighter cannot expect unlimited network access.

Tactical-level Approach and Artificial Judgement

With a future of contested domains and increased effort toward simultaneously enabling operations on multiple domains, the joint community must not focus on a catch-up strategy but step up efforts in developing innovative strategies designed to leap forward. Current efforts to bolster C2 systems and jump-start innovation initiatives take a top-down approach, tackling the enterprise perspective first. A bottom-up approach is warranted also.

Looking from the tactical warfighter's perspective, the ability for all warfighters (from Air Force fighter pilots to infantry Marines) to win will be determined by their ability to fight in a denied or degraded operational environment against a peer competitor. The challenge is not to figure out how to capture big data and advance machine learning (both of which US forces must do) but how the trigger pullers can leverage information when access is intermittent or denied. This, of course, presumes trigger pullers are human, which is not necessarily what some developers are working toward.

As technology evolves and traditional human tasks become more automated, a compulsion emerges where autonomous tactical weapons systems are almost a foregone conclusion. The defense industry appears intent to write humans out of the equation, replacing them with the superior speed and accuracy promised from AI. However, important questions remain. What about the paradox which exists where data

and algorithms are continually informed by a network which cannot be guaranteed due to outage or exploitation? What is the failure rate of a computer versus the failure rate of a human? While it is difficult to determine the consequences of connectivity that is not guaranteed or is exploited upon implementation of AI on live targets, it is reasonable to assert, at a minimum, mistakes will occur and innocent lives could be lost. Left to themselves, brilliantly-fast machines likely will decide counter to what military leadership and politicians want, and they will fail.

The benefits of automation to the warfighter, on the other hand, are great. Automated systems designed for threat detection and response (for physical and cyber threats) offer superior response times and accuracy over those requiring human input. For example, when it comes to physical threats, such as inbound surface-to-air missiles, the success of automated detection and countermeasure systems is immediate and has proven successful. Likely, future systems will be even better, such as closed-loop infrared countermeasures, which promise to identify specific missiles and jam threats before they are launched and without human input[10]. For cyberattacks, detection is becoming increasingly difficult as capabilities of adversaries grow in sophistication and using advanced automation. Future threat detection and countermeasure employment will rely on cyber teams with their own automated, adaptive AI tools.[11]

Automation has bested human capacity and capability in many areas, yet, it is more difficult to determine which traditional human activities are better suited for AI and machine learning. While automation follows predefined and predictable actions based on human authorization, an autonomous system would identify its own course of action without human interaction.[12] What is required for a machine to continue a mission with imperfect, compromised, or missing information? Given, it is impossible to program a machine with every possible scenario it could encounter in combat, a machine would have to analyze all information, discount erroneous or otherwise useless information, extract relevant information, and learn from it.[13] It is easy to envision the risks involved. The ability of a machine to learn to drive a car from San Francisco to Los Angeles, California; which movie a person from Des Moines, Iowa may enjoy on a Saturday; or to pick potential terrorists from a live video feed can be accomplished with relatively little risk. As the US debates who is accountable when AI fails, the stakes increase immensely when considering inserting machine learning into the kill chain.

Can AI replace having a human in the loop? Even if we accept that the world is open to a future where AI takes over part, or all of, large data synthesis functions, the risks associated with AI-driven kill or live decisions are unacceptable. At a time the US is risk adverse, considering collateral damage, civilian casualties, fratricide, or a laser-guided bomb drop without a combined force component commander's approval, it is unlikely the US will allow a machine to make the life or death decision.

To abide by the principles of international law, autonomous systems would be required to distinguish between civilians and combatants, and adhere to the principles of proportionality and precaution.[14] Autonomous systems would have to make informed, considered decisions and come to a sensible conclusion—in other words, they must use their own judgement. [15] Furthermore, should a mistake occur where a machine directed or caused the death of a noncombatant, officials involved would want to know how the

machine came to make its judgement. With machine learning, there is no guarantee the decision points can be explained clearly and lessons learned.

As the world becomes more comfortable with the prospects and potential benefits of AI, the idea of becoming comfortable relying on “artificial judgement” seems unpalatable. If intelligence is the ability to acquire and apply knowledge, and judgement as the ability to make considered decisions and arrive at sensible conclusions, it is clear which role is more suited to machine learning. When it comes to life or death decisions, the world is not ready for artificial judgement.

It is reasonable to predict that a future foe, whether a state or non-state actor, will opt to wage war with rules of engagement lacking moral value by international standards. The adversary will trade what the US considers moral conduct for the speed and accuracy of AI and the promise of a quick and complete victory. It can be argued that the US and allies will not have the same calculus, and will have to figure out a way to retain its morals while defeating a moral-less enemy. That avenue to victory will need man-machine teaming.

A Vector for Innovation

Getting the warfighting trigger pullers to their targets in a contested environment, armed with the best AI-informed data to make sensible decisions is a challenge. America’s next generation weapons systems require near-continuous connectivity for everything from navigation and identifying friendly systems to data sharing and voice communications for weapons release clearance. To remain ahead of competitors and continue to enjoy freedom to maneuver and relative freedom from attack, the US must innovate.

The great effort afforded to hardening networks and redundancy are important but the US should not rely on that which cannot be guaranteed. Thus, a similar effort should be placed on ways to leverage large amounts of synthesized information without fully relying on it. While America’s best and brightest throughout the defense industrial base advance AI and bolster C2 systems, the military should consider focusing some of that intellect on dumbing down weapons and weapons systems. This involves refraining from the current momentum in distributing capability and capacity across large communications environments to concentrate it in time and space, while eliminating much of the connectivity requirement.

Consider this: humans are the smartest, “dumb” weapons system available. No computer can replicate the ability to assess a situation with limited information like a human. Also, consider computers with AI and machine learning can synthesize, exponentially, more information at a much faster rate than humans. Military leaders must marry human cognition with machine learning and automation; i.e., team man with machine. This imperative becomes clear when looking from the tactical perspective as opposed to the theater-wide/operational perspective.

“Dumbing down” our weapons systems is a bit of a misnomer, but is meant to paint a picture that intelligence does not require constant connectivity. To survive in a future contested electronic environment, weapons and weapons systems must be AI informed, and human and machine applied. Humans for cognition, situational awareness, and

judgement; machines for synthesis and automation. These systems should be nearly autonomous, informed before deployment, self-navigating, able to run without (or with little) outgoing electronic emission, and be able to receive updates via data burst or a similar direct means. They should leverage information, never fully relying on it, while capable of distilling limited, available information to make the weapons systems or man-machine team smarter.

For the Services, “dumbing down” appears to go against a tradition of continual cutting edge invention. It does not. The next revolution (or offset) in American military capability may be the ability to merge AI and human cognition to stop envisioning the two capabilities as independent, and begin building complementary systems from the ground up. The next generation bomber, submarine, or combat vehicle should be able to transit theaters and travel to their targets without electronic transmission of any kind. For example, the US Army’s Next Generation Combat Vehicle is being envisioned with some remarkable technology, including an unmanned turret and autonomous driving capability with a flexible architecture designed to allow for future innovation. [16] That technology could be built with the flexibility to travel and employ weapons without being connected to a network.

The same applies to all future capabilities the US must continue to fund and research, including hypersonic weapons.[17] Having the capability to disconnect and work autonomously eliminates an adversary’s opportunities for electronic spectrum denial, spoofing, or using emissions to find and target a friendly weapons system. Integrating a human with AI at the tip of the spear helps ensure future leaders make the right judgment call.

Endnotes

---

1 General Joseph F. Dunford, Jr., For reappointment to the grade of general and reappointment to be Chairman of the Joint Chiefs of Staff, United States Committee on Armed Services, September 26, 2017. https://www.armed-services.senate.gov/hearings/17-09-26-nomination_--dunford

2 David G. Perkins and James M. Holmes, Multidomain Battle: Converging Concepts Toward a Joint Solution, JFQ 88, 1st Quarter 2018. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_54-57_Perkins-Holmes.pdf?ver=2018-01-09-102340-943

3 See Multidomain Battle: Combined Arms for the 21st Century, 24 February 2017 http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf

4 See 2017 Air, Space & Cyber Symposium Remarks by General David L. Goldfein, US Air Force Chief of Staff, 19 September 2017.

http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf

5 General Mark A. Milley, AUSA Eisenhower Luncheon, October 4, 2016. http://wpswps.org/wp-content/uploads/2016/11/20161004_CSA_AUSA_Eisenhower_Transcripts.pdf

6 https://www.dvidshub.net/video/586175/2018-air-warfare-symposium-gen-david-goldfein-csaf

7 Multi-Domain Battle: Evolution of Combined Arms for the 21st Century (December 2017). http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_Evolutionfor21st.pdf

8 Gideon Grudo (February 22, 2018). Alphabet Executive: USAF Wasting Opportunities for Future Innovation.

www.airforcemag.com/Features/Pages/2018/February%202018/Alphabet-Executive-USAF-Wasting-Opportunities-for-Future-Innovation.aspx

9 Corey Dickstein (2017). Army Rolls Out Field Manual Focused on Fighting Near-peer Adversaries, Stars and Stripes. https://www.military.com/daily-news/2017/10/11/army-rolls-field-manual-focused-fighting-near-peer-adversaries.html

10 Knowles, J. (2003). Infrared Countermeasures. PC Magazine, 22(12), 87.

11 Gale, S. F. (2017). AI vs. Hackers. PM Network, 31(4), 14-15.

12 Future Unmanned System Technology: Legal and Ethical Implications of Increasing Automation, Joint Air Power Competence Centre (November 2016), 12. www.japcc.org

13 Reema Bhatia (August 7, 2017). What is Machine Learning? Forbes.com. https://www.forbes.com/sites/forbestechcouncil/2017/08/07/what-is-machine-learning/#7e3e2f4979a7

14 Future Unmanned System Technology, 20-27.

15 Definition adapted from https://en.oxforddictionaries.com/definition/judgement

16 Sean Kimmons (January 29, 2018). Army Secretary Directs New Team to Speed Up Next-Gen Combat Vehicle Program, Aerotechnews. http://www.aerotechnews.com/blog/2018/01/29/army-secretary-directs-new-team-to-speed-up-next-gen-combat-vehicle-program/

17 Sharon Weinburger (March 1, 2018). The Pentagon Official Says US Hypersonic Weapons research Underfunded, Foreign policy. http://foreignpolicy.com/2018/03/01/pentagon-official-says-u-s-hypersonic-weapons-research-underfunded/

Disclaimer. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.

Originally released 1 June 2018 in Air Land Sea Bulletin 2018-1