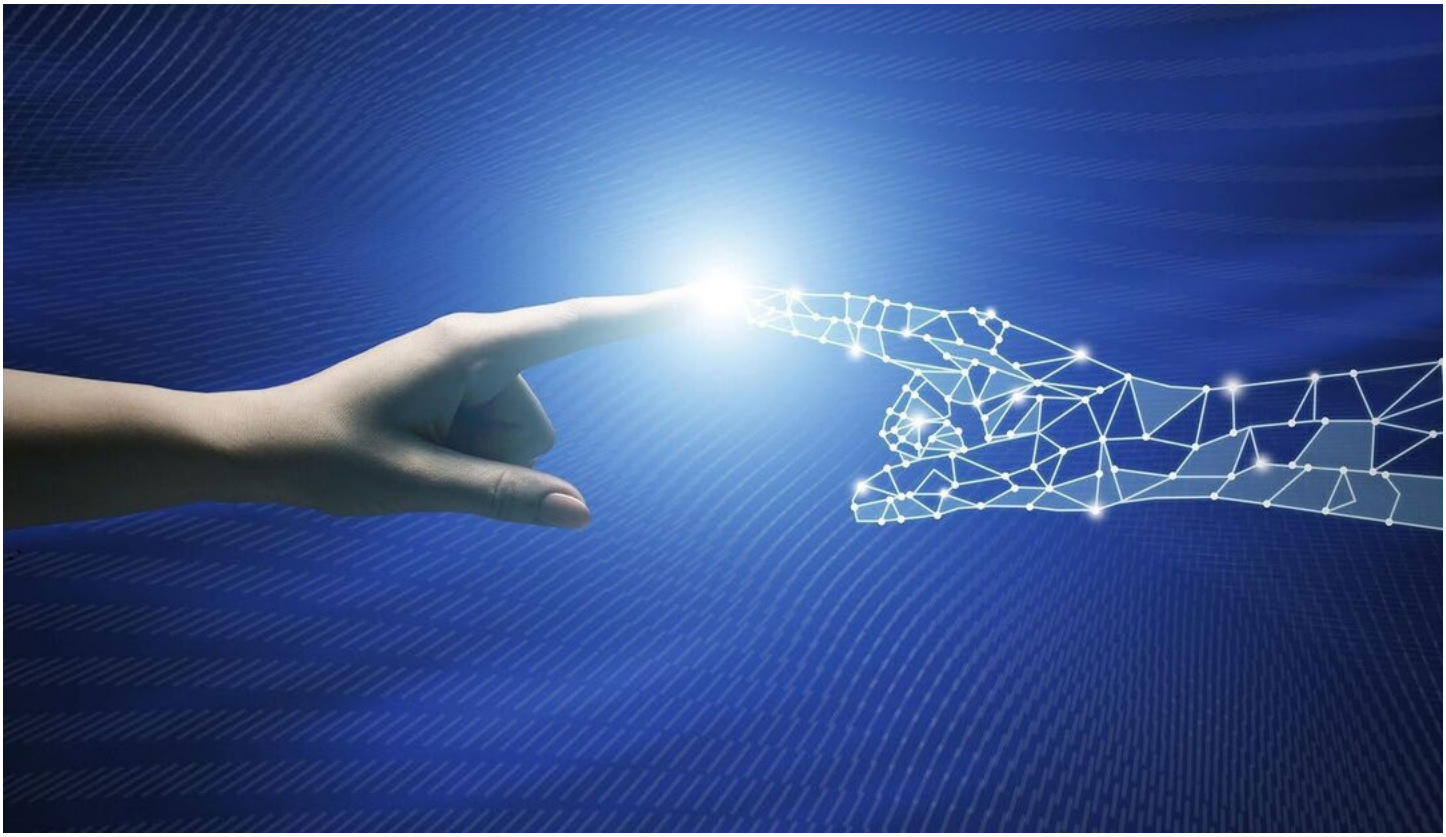
Leadership: Artificial Intelligence in Decision-Making

By Lt. Col. Joseph L. Huitt



AI generated illustration

Despite the recent announcement from the Department of Defense (DoD), I posit that Artificial Intelligence (AI) cannot replace the critical *human* factor in leadership decision-making. The Hill recently published an article outlining the formation of a new cell, Artificial Intelligence Rapid Capabilities Cell (AI RCC), whose namesake unsurprisingly gives insight into its purpose.[1] The AI RCC is charged with improving the speed at which the military implements AI technology, focusing on generative AI. What I found alarming was how this new office was going to utilize AI: "command and control, autonomous drones, intelligence, weapons testing, and even for enterprise management like financial systems and human resources."

To frame my argument, it's important to ensure that some terms are defined and put into context. My former boss, Lt. Gen. Stanton, routinely and with much fervor repeated, "you cannot, as a professional in this field (Cyber Corps), use the terms AI or machine learning (ML) without putting them into context." So, what is AI? When thinking of AI, many people conjure up ideas brought to them from the Hollywood big screen, such as robots taking over the world or the AI "Skynet" deciding that humanity is a threat and must be eradicated. However, AI is loosely defined as the ability of machines (computers) to perform tasks that humans do with their brains.[2]

There is also a subset of AI known as Artificial General Intelligence (AGI), which has been slow in development as it seeks to provide machines with comparable human intelligence, able to perform any intellectual task that humans can.[3] Machine learning is a subset of AI and if set up properly, helps make predictions and reduces mistakes that arise from merely guessing.[4] Generative AI is a sub-field of machine learning, capable of developing content such as text, visual depictions, audio, code, and synthetic datasets.[5] Since this is a military-focused article, I would be

remiss not to mention *CamoGPT*, which incorporates data from joint and Army doctrine, lessons learned, best practices [and] Training and Doctrine Command content, among other sources.[6] To understand better, it must be noted that machine learning is made possible by using large language models.

So, what is a large language model (LLM)? LLMs are a category of foundation models trained through data input/output sets using immense amounts of data. This data could have billions of parameters, enabling the LLM to understand and generate content to perform a wide range of tasks. While many are familiar with OpenAI's GPT-3 and 4 LLM, popular LLMs include open models such as Google's LaMDA and PaLM LLM (the basis for Bard), Hugging Face's BLOOM and XLM-RoBERTa, Nvidia's NeMO LLM, XLNet, Co:here, and GLM-130B.

Further scoping my position, this article focuses on two aspects of the AI RCC priorities of implementing AI technology within the Warfighting Functions of Intelligence and Command and Control. Army Doctrine Publication 3-0, Operations, defines a warfighting function as "a group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives."[7] Human factors are prevalent in every element of operational planning. From the intelligence officer assessing enemy COAs to the operations officer creating the friendly COAs, and the leader selecting the best course of action, the human element cannot be overlooked.

An example of how the DoD is using AI was an endeavor started in 2017, Project Maven, transitioned to the National Geospatial Intelligence Agency in 2022.[8] Specifically, the project established the "Algorithmic Warfare Cross-Functional Team (AWCFT) to accelerate DoD's integration of [AI]…to turn the enormous volume of data available to DoD into actionable intelligence and insights at speed."[9] This project successfully analyzed massive amounts of data collected from unmanned aerial systems (UAS). The DoD used UAS to capture video feed of the battlefields in Iraq and Syria against the Islamic State; however, it lacked the capacity to process, exploit, and disseminate (PED) the feed in a timely manner, rendering the data useless. The AWCFT created algorithms to review the full motion video (FMV) in near-real time, classifying objects and alerting analysts if there were irregularities.

As a former intelligence officer, the term *intelligence drives operations* (and operations drives intelligence) was repeated often at professional military education and at my assigned units. The Intelligence Warfighting Function is defined in ADP 2-0, Intelligence, as the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment.[10] Intelligence enables *command and control*, facilitates initiative, and allows commanders to develop situational understanding and take decisive action to overcome complex issues that leaders are faced with in today's multidomain battlefield. While intelligence can help lift "the fog of war", what Clausewitz aptly described as unknown factors, it is the leader who is charged with shaping the situation and making decisions to seize the initiative over the adversary.[11]

ADP 3-0 defines the Command-and-Control Warfighting Function as the related tasks and a system that enables commanders to synchronize and converge all elements of combat power. Its main purpose is to assist commanders in integrating the other elements of combat power (leadership, information, movement and maneuver, intelligence, fires, sustainment, and protection) to achieve objectives and accomplish missions.[12] It's easy to grasp why this warfighting function is so critical as it establishes the process to drive operations across all elements of military functions.

If intelligence enables Command and Control, what if the data that drives the intelligence or the data that feeds all warfighting functions becomes corrupted? I agree with Deputy Defense Secretary Hicks that the main reason for integrating AI into military operations is straightforward, it improves decision advantage.[13] However, only one year has passed since the Pentagon unveiled the Data, Analytics and Artificial Intelligence Strategy, and the development of AI in the United States has not advanced to the point where is should transition from improving decision making for

military leaders to *allowing* AI technology to *make* decisions—especially in the war fighting functions tasked to the AI RCC charter. In my opinion, these are the most critical among all six warfighting functions, and while technology should be used to assist military commanders, it should not supplant their decision making. There should always be a human-in-the-loop element when it comes to these types of decisions; if not in-the-loop, minimally, humans-on-the-loop should be maintained within the decision-making process where AI is concerned.

The reason that a human must remain in the decision-making cycle is simple: AI can produce false and misleading information and just like any other technology, it can be "hacked." No matter how good the program purportedly is, technology is riddled with security issues—hence the need for routine updates (e.g. patches, protocols, etc.). Recall earlier in the article, LLMs require billions of parameters to be used for the data sets to generate useful information. Not only can these data sets be biased, they can also be unreliable, incomplete, or otherwise undesirable, producing bizarre outputs called hallucinations. Some of these hallucinations can produce false information. Furthermore, humans build the software that drives these AI technologies, and humans are imperfect-they make mistakes. These mistakes create attack surfaces, or opportunities for hackers to take advantage of the mistakes for their benefit.[14]

While there are different motivations that drive hackers, this article will focus on nation states whose cyber operations are ultimately to assist their country in dominating and winning its wars. The adversarial cyber operator could take advantage of the programming mistakes and enable them to purposefully change parameters that the AI technology uses. Recall earlier the great work done by Project Maven: what if an adversary changed the parameters set by the DoD, replacing them with their own? An example could be that the UAS data no longer identifies structures, buildings, personnel, weapons or equipment as intended when using the corrupted AI technology.

Research has already been successful in highlighting ML models are vulnerable to malicious inputs to produce erroneous outputs, which appear unmodified to human observers. Researchers successfully attacked a deep neural network (DNN) hosted by MetaMind and found it misclassified 84.24% of the adversarial examples crafted with its substitute. In their study, the researchers conducted the same attack against models hosted by Amazon and Google, yielding adversarial examples misclassified at rates of 96.19% and 88.94%. Their study also highlighted their approach was capable of evading defense strategies previously found to make adversarial example crafting harder.[15]

Although humans are imperfect beings, the imperfection is why humans remain superior to robots, as they are not constrained by programming and can adapt to unforeseen changes. This is also true for our military, despite being transparent and publishing our tactics, techniques, and procedures (TTPs), our enemies have been baffled when we don't always follow those TTPs on the battlefield. That's because TTPs are merely guidelines, and commanders utilize mission command delegate authority to subordinate leaders, empowering them to accomplish tasks with the given resources and determine the best course of action to meet mission requirements. U.S. history is rich in countless battles where the initiative was seized due to creative leaders at all echelons.

What makes a good leader? Since football terms are often used to understand cyber operations (i.e. offense and defense) the author highlights a quote by the National Football League (NFL) Hall of Fame coach, Vince Lombardi, "Leaders aren't born, they are made and they are made just like anything else, through hard work."[16] Prior to the NFL, Lombardi was an offensive line coach at West Point where he likely learned the foundation of good leadership. ADP 6-22, Army Leadership and the Profession, highlights the characteristics of a good leader. While one can read about leadership, it is through experiences, both successful and failures, that develop leaders, just as Lombardi stated. It takes effort to learn TTPs, conduct battle drills, care for your people, disagree with superiors, and even admit when you're wrong. But these are the qualities that leaders have obtained and sharpened through experiences that enabled them to make

decisions.

While AI/ML technologies will certainly continue to ***assist*** our military, there will always be a human factor that cannot be overlooked. Experience, gut feeling, and leadership are all influenced by human factors. Lastly, DoD leaders have routinely stated that the secret to its success, time and time again, boils down to leadership, the ingenuity of our NCO corps, and the ability for leaders at echelon to make decisions.

Even our adversary, Russia, has a U.S. movie based on a true story about a military officer who prevented World War Three during the Cold War; the officer refused to trust their radars that falsely indicated that the U.S. had launched numerous ballistic missiles aimed to destroy them.[17] To continue our military prowess, Artificial Intelligence should never replace the critical *human* element in leadership decision-making. There must always be a human-in-the-loop.

BIO

Lt. Col. Joseph Huitt is a Cyber Warfare Officer, currently serving as Deputy Director, Office Chief of Cyber, U.S. Army Cyber School. He is a graduate of the College of Naval Command and Staff, U.S. Naval War College, and a Distinguished Military Graduate of Augusta University. Lt. Col. Huitt holds master's degrees in Defense and Strategic Studies, and Intelligence Studies. Lt. Col. Huitt has served in leadership positions from the tactical to strategic levels, over his 26-plus years of service. He has gained invaluable experience serving as the Executive Officer to the Cyber Center of Excellence Commanding General; managing Talent at U.S. Army Cyber Command; senior fellow at West Point's Center for Junior Officers; serving as a Team Lead and Battalion Executive Officer within the Cyber Protection Brigade; serving with Special Operations Command in West Africa; serving as Officer-in-Charge within USAFRICOM J2 in England; commanding a Regional Operations Company in the 513th Military Intelligence Brigade; leading first-ever multi-function team in NATO-ISAF in Afghanistan; leading a ground SIGINT platoon in the 66th Military Intelligence Brigade in Germany; deploying in support of USARCENT in Saudi Arabia enabling U.S. invasion into Iraq; serving as a Noncommissioned Officer in Charge at Camp Casey, 2nd Infantry Division in South Korea; and various other stateside units.

References

1. Dress, Brad. "Pentagon Announces New AI Office as It Looks to Deploy Autonomous Weapons." The Hill. December 11, 2024. https://thehill.com/policy/defense/5034805.

2. Potember, Richard. "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD." Federation of American Scientists. January 1, 2017. https://irp.fas.org/agency/dod/jason/ai-dod.pdf.

3. Ibid.

4. IBM Data and AI Team. "AI Vs. Machine Learning Vs. Deep Learning Vs. Neural Networks: What's the Difference?" IBM. July 6, 2023. https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks.

5. "What Is Generative AI?" Innodata. December 14, 2024. https://innodata.com/what-is-generative-ai/.

6. South, Todd. “From CamoGPT to Life Skills, the Army Is Changing How It Trains Troops.” Defense News. October 16, 2024. https://www.defensenews.com/land/2024/10/16/from-camogpt-to-life-skills-the-army-is-changing-how-it-trains-troops/.

7. U.S. Department of Defense. “ADP 3-0 Operations.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf.

8. Hitchens, Theresa. “Pentagon’s Flagship AI Effort, Project Maven, Moves to NGA.” Breaking Defense. April 27, 2022. https://breakingdefense.com/2022/04/pentagons-flagship-ai-effort-project-maven-moves-to-nga/.

9. U.S. Department of Defense. “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven).” National Security Archive. The George Washington University, April 26, 2017. https://nsarchive.gwu.edu/document/18583-national-security-archive-department-defense.

10. U.S. Department of Defense. “ADP 2-0 Intelligence.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18009-ADP_2-0-000-WEB-2.pdf.

11. Clausewitz, Carl V. 1976. *On War*. Translated by Michael Howard and Peter Paret. Princeton: Princeton Press. https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf.

12. U.S. Department of Defense. “ADP 3-0 Operations.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf.

13. Clark, Joseph. “DOD Releases AI Adoption Strategy.” Defense. U.S. Department of Defense, November 2, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/.

14. Metz, Cade. “How To Fool AI Into Seeing Something That Isn’t There.” Wired. July 29, 2016. https://www.wired.com/2016/07/fool-ai-seeing-something-isnt/.

15. Papernot, Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. “Practical Black-Box Attacks against Machine Learning.” Arxiv. March 19, 2017. https://arxiv.org/pdf/1602.02697.

16. “Vince Lombardi.” The Official Website of Vince Lombardi. Accessed December 15, 2024. https://vincelombardi.com/.

17. Harvey, Ian. “The Man Who Saved the World – The Russian Who Avoided WWIII.” War History Online. October 1, 2015. https://www.warhistoryonline.com/featured/real-life-man-saved-world-russian.html.