AU/SOS/2021

SQUADRON OFFICER SCHOOL

AIR UNIVERSITY

Artificial Intelligence: Air Force Unprepared for 2025 Recommendation

by

Christopher D. Klare, Capt, USAF

Advisor: Lt Col Lawrence Schutz

Contributors: Maj Kevin Beaty, Maj Jared Freeman, A1C Allen

Maxwell Air Force Base, Alabama

December 2021

ABSTRACT

The National Security Commission on Artificial Intelligence (AI) recommended the Department of Defense (DoD) be AI-ready by 2025 in their Final Report to Congress in January of 2021. This recommendation stems from an undeclared AI arms race between United States' peer adversaries and the advances taken in recent years to develop algorithms for persistent surveillance, command and control, and weaponized code. While there are strategic initiatives within the DoD aimed at leveraging AI across the services, there is a severe disconnect between tactical capability development and deployment. As the lead organization within the DoD, the Joint AI Center is charged with creating viable solutions for all DoD elements and as such, would be overwhelmed should all units attempt to be AI-ready by 2025. This paper highlights a major deficiency within the AI-development process and argues that capability development should be empowered to the Air Force Wings with funding and resources necessary to truly harness AI as a weapon. Additionally, this paper identifies successful AI concepts found through gene manipulation, smart dust nanotechnologies, and COVID-19 machine learning processes to assist tactical leaders in their understanding of how the AI-revolution could help their particular mission area and motivate them to educate themselves.

Sound the alarm. The United States Air Force is not prepared to combat peer adversaries when it comes to leveraging artificial intelligence (AI) at all levels, and with The United States in an undeclared arms race that could see adversaries take the lead in the next ten years, something needs to\ quickly to turn the tide. More troubling, this threat is not fully understood by tactical experts in the field or if they do, they likely do not realize (or are bureaucratically incapable) of delivering capabilities necessary for competition. Adversaries are gaining ground in AI research and development efforts. China has effectively proven the concept of persistent surveillance against their own people,[1] and Russia's development would include boosting information operations efforts targeting the United States democratic process and sowing division within the country.[2] While it is startling to consider, all is not lost. There is something that the community of intelligence professionals can do to combat the problem. This paper will attempt to define tactically relevant problems that squadrons can tackle and identify shortfalls for action at senior level.

In their Final Report, the National Security Commission on Artificial Intelligence recommended actions for the Department of Defense (DoD) so the services would be prepared for competition in ten years. At its heart, the commission recommended the DoD follow two lines of effort: establish the foundations for widespread AI-integration by 2025 and achieve a state of military AI readiness by 2025.[3] The most inspiring strategic efforts providing promise to this end are the developments of Project Maven, the Advanced Battle Management System, and Joint All-Domain Command and Control. These projects were in the works years before the publishing of the commission's report which shows a strategic understanding and commitment to the future reality we need in order to effectively compete. However, as stated previously, it took years to develop AI-enabled capability. In order to have widespread AI-integration, leaders at all

levels need to understand the basic complexities of AI and how to incorporate AI capabilities within their mission-space, so they can usher in the AI revolution by 2025. The three major initiatives mentioned shorten gaps between sensors and shooters from a strategic perspective, but how do elements on the edge contribute to these efforts? Furthermore, how do we empower our front lines to organize, train and equip as necessary for their mission-specific needs? The purpose of this paper is to introduce basic concepts of artificial intelligence and illuminate actions that should be taken to drive the Air Force to a state of persistent surveillance powered by artificial intelligence. The following paragraphs will discuss smart capabilities, proven analytical concepts, and showcase needs going forward.

There are a few definitions that need to be covered to provide context throughout the rest of this paper and help educate lower-level leaders on foundational concepts. First, AI requires three things: a dataset, an algorithm, and a function.[4] A dataset is a table of values, an algorithm is the process which the computer uses to parse the data, and the function is the "deterministic mapping from a set of input values to one or more output values".[5] These form the basis for AI. Overall, one can think of AI as a category of efforts which seek to employ computer algorithms and allow a human to interpret the results in a logical way. As a subset of the AI category, "Machine Learning (ML) involves the development and evaluation of algorithms that enable a computer to extract (or learn) from a dataset."[6] Nested within ML is a concept known as Deep Learning (DL). DL "focuses on creating large neural network models that are capable of making accurate data-driven decisions",[7] and DL focused initiatives are encapsulated around the idea of contributing specific functions from specific neurons of a neural network. DL understanding is vital to a commander's ability to use AI as science fiction would have imaginations believe possible.

From an intelligence, surveillance, and reconnaissance (ISR) perspective, DL is what could drive the synthesis of multiple data-sources (e.g., multi-intelligence fusion AND analysis). In lay terms, ML could help bring several intelligence functions together in a common form. However, given the appropriate dataset, algorithm, and function (or commander's intent), it is theoretically possible for DL to allow collected information to be analyzed, understood, refuted as misinformation, accepted as fact, re-tasked for additional collection, or drive new collection tasks just as a human could but autonomously in the seconds it takes for the machines to process the information and arrive at a conclusion regarding available data. While strategic and operational commanders are trying to achieve an end state which mirrors an ability similar to the aforementioned DL potential, they still must consider legal, moral, and ethical dilemmas along with security and reliability of everything that goes into developing a complete AI infrastructure.[8] If tactical leaders are not exploiting these opportunities in lock-step with senior leaders, we are doomed to fail any sort of integration with current mission sets and doomed to fail the "AI-ready military by 2025" posture as prescribed by the Nation Security Commission on AI. So, how can our force become more AI-effective? Fortunately, AI-driven capabilities, analytical techniques, and government and commercial case studies are available to explore.

Human gene editing once seemed like something unimaginable, but it is becoming more of a reality through the use of machine learning. Studies regarding clusters of regularly interspaced short palindromic repeats (CRISPR) have been going on for years. Classified as a biotechnology, one could infer that the intent for CRISPR technology is to allow scientists the ability to "alter genes or create DNA to modify plants, animals, or humans."[9] Furthermore, it is hard to argue the implications regarding gene editing as a powerful weapon of mass destruction as former Director of National Intelligence, James Clapper did in 2016.[10] With the opportunities

gene editing avails to well-equipped adversaries, it would be prudent for intelligence professionals to understand how indicators regarding gene manipulation, for purposes counter to American strategic interests, may manifest through machine learning and help commanders understand how they can combat these threats quickly. This reality is not far behind the science required to make a reality and something analysts could incorporate into their calculus if they knew how to identify the necessary factors.

If analysts do not have access to the data necessary for analysis through DL techniques, there are creative solutions to obtain the information. One such innovation on the horizon offering significant potential is the advent of tiny wireless networks known as Microelectromechanical Systems, affectionately known as Smart Dust. "Smart Dust is the size of cubic millimeter, which contains power, communications and computations."[11] For perspective, a cubic millimeter is about the size of President Lincoln's face on the penny. This is a single node of the entire sensor network. Research also suggests that smart dust particles will be able to reach microscopic levels, capable of injection as an alternative to traditional medical care approaches.[12] Even more awesome than stealth-like size is the capability this subset of devices is projected to afford. They can house cameras, environmental sensors, and communication mechanisms to transmit the data to be stored and processed further.[13] Teamed with ML efforts, a connection to a storage device or even the internet, one could conceive a collection asset with a very low probability chance of detection, a system with low need for maintenance, and if properly planned, a system that is able to reduce risk to forward deployed assets with limited placement and access to targeted collection areas.

To this point, this paper has discussed how analysts could view AI as a threat, how they could view it as a collection asset, but what about the process of analysis? Look no further than

the COVID-19 pandemic. While the pandemic of 2020 was fraught with uncertainty, this time should also be lauded for how relatively quickly the virus was analyzed, tracked, and fought within about a year's time. The world saw advancements of public health surveillance through ML techniques from local governments to a global integration of metrics.[14] The medical community teamed with DL experts to develop a COVID screening and diagnosis methodologies, drug discoveries, and eventual vaccine innovations. This required a substantial input of data from social media, text-based data, patient data, a collective of scientific data known as omics, and image and video data.[15] This system of analysis was a landmark for how humans can team with machines to create a solution out of unique datasets within a remarkably efficient window of time. Applied to standard intelligence practices of multi-source data fusion and analysis, there is no reason to believe analysts would not be able to harness the ability of DL to develop accurate assessments if given the resources.

As one can see, AI has tremendous potential regarding multiple national security issues that tactical analysts can apply to their own mission areas if they were armed with capabilities. The DoD's foremost agent regarding AI is the Joint Artificial Intelligence Center (JAIC) which was launched as an executor of the DoD's AI strategy required on February 12, 2019, by Executive Order 13859.[16] Having an organization responsible for ensuring AI needs are met is a worthwhile goal, but if the services are to be AI-ready by 2025, there is no way they would be able to handle the amount of capability development requirements for all of the DoD. There needs to be a shared commitment throughout all levels of command to avoid missed opportunities resulting from misaligned priorities. As the present AI capability development process stands, tactical solutions are unavailable.

Self-imposed bureaucracy prevents rapid, decentralized capability development. To secure an AI-powered capability, one must substantiate a significant enough need requiring the use of AI (such as sorting through millions of data points with only five analysts) and submit what is known as an Urgent Operational Need through multiple layers of bureaucracy to reach through to the Major Command. Once approved, the request is forwarded to the JAIC for adjudication. Once adjudicated and prioritized amongst the rest of the DoD requirements, it could be months before a developer is found and they start working the problem. At best, this process may see a six-month turnaround from requirement submission to development which is unsatisfactory, again, if the services are to be AI-ready by 2025. This is not the fault of the JAIC as they should be advocates of AI to DoD leaders and Congress, so the services have the funding to seek AI externally while simultaneously learning how to become deft at AI, ML, and DL capability development. This author recommends leaders seriously look at empowering the Wings with the budget necessary, training requirements, and coordination with an approved list of developers (as approved by the JAIC) to pursue AI efforts. This recommendation would not completely remove the JAIC from process and capability development as the organization would continue to assume a formal lead status, developing policy and capturing best practices to share across the DoD.

For every Airman, China is ahead of the US military in fielding and learning from operational persistent surveillance techniques. Our service needs to understand, at all levels, how we are going to compete for parity with AI or be destined to fail in many other aspects of warfighting. For better or worse, the Chinese government spies on its citizens with the use of ML and with the resulting output, uses a social credit system full of public shaming to coerce (largely in the subconscious) a citizen's submission to government demands of what is enforced as good

citizenship.[17] China has also been the subject of international condemnation stemming from accusations founded on sound evidence that they were using AI to help identify and eradicate the Uighur ethnic identity within China's own western region.[18] The bottom line here is that China has a different stance than the West regarding ethical standards, morality, and laws which provide them greater opportunity to test AI capability. The US Constitution limits the government's power to do much of anything to its citizens regarding surveillance without consent, absent a legal infraction backed by a legal proceeding and warrant. While this is one of the great things the Constitution provides, it does make it difficult to develop accurate persistent surveillance systems which account for citizen privacy restrictions. Ethical, moral, and legal dilemmas aside, China is still ahead in understanding how to conduct persistent surveillance, and leaders at levels will have to keep these things in mind as they look to maneuver with AI.

The AI-revolution is here. This paper identified a microcosm of opportunity that AI affords the force across every mission. AI, ML, and DL open the aperture to what is possible and should have ISR analysts thinking differently about problems and their solutions. From gene mutations to automated analysis to autonomous weapons, the possibilities are only limited to the data available—or how the data available is interpreted. US adversaries are already threatening and very likely increasing in the next ten years. National security requires an increase of not only AI awareness but also development and integration of AI-based weapons systems. Being reliant on contracted organizations to develop machine algorithms is not sustainable for the future. Likened to a weapons loader adjusting a loadout, we must figure out how to understand how we can adjust our mission algorithms as our mission dictates or suffer defeat across a host of capabilities.

References

Arora, Gunjan, Jayadev Joshi, Rahul Shubhra Mandal, Nitisha Shrivastava, Richa Virmani, and Tavpritesh Sethi. 2021. "Artificial Intelligence in Surveillance, Diagnosis, Drug Discovery and Vaccine Development against COVID-19." *Pathogens* 1-21.

Campbell, Charlie. 2019. *'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World* . November 21. https://time.com/5735411/china-surveillance-privacy-issues/.

Carrara, Sandro. 2021. "Body Dust: Well Beyond Wearable and Implantable Sensors." *IEEE SENSORS JOURNAL.*

Cronk, Terri. 2019. *DOD Unveils Its Artificial Intelligence Strategy* . February 12. Accessed November 30, 2021. https://www.defense.gov/News/News-Stories/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

Government Accountability Office. 2018. *National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies.* December. https://www.gao.gov/assets/gao-19-204sp.pdf.

Hitchens, Theresa. 2020. *Aging Air Force IT 'Biggest Challenge' To JADC2 Progress.* October 28. Accessed November 30, 2021. https://breakingdefense.com/2020/10/aging-air-force-it-biggest-challenge-to-jadc2-progress/.

Kanaan, Michael. 2020. *T-Minus AI.* Dallas: BenBella Books, Inc.

Kelleher, John D. 2019. *Deep Learning.* Cambridge: MIT Press.

MIT Press. 2019. *Why is Everyone Talking About Deep Learning?* August 2019. Accessed November 30, 2021. https://medium.com/@mitpress/why-is-everyone-talking-about-deep-learning-aedc247aa00f#:~:text=Deep%20learning%20is%20the%20subfield,there%20are%20large%20datasets%20available.

National Security Commission on Artificial Intelligence. 2021. *Final Report.* Final Report, Washington DC: United States Congress.

Regalado, Antonio. 2016. *Top U.S. Intelligence Official Calls Gene Editing a WMD Threat.* February 9. Accessed November 30, 2021. https://www.technologyreview.com/2016/02/09/71575/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/.

Shaik, Malik, Naseema Shaik, and Wali Ullah. 2016. "The Wireless Sensor Networks: Smart Dust." *International Research Journal of Engineering and Technology* 910-913.

Taylor, Kelsey. n.d. *5 Applications of Smart Dust*. Accessed November 30, 2021. https://www.hitechnectar.com/blogs/smart-dust-applications/#MilitaryApplications.

Zeng, Daniel, Zhidong Cao, and Daniel Neill. 2021. "Artificial Intelligence Enabled Public Health Surveillance—From Local Detection to Global Epidemic Monitoring and Control." In *Artificial Intelligence in Medicine: Technical Basis and Clinical Applications*, by Lei Xing, Maryellen Giger and James Min. Cambridge: Academic Press.

[1] Kanaan, *T-Minus AI*, 179
[2] Ibid., 201
[3] National Security Commission on Artificial Intelligence, *Final Report*, 9
[4] Kelleher, Deep Learning, 6
[5] Ibid., 7
[6] Ibid., 6
[7] MIT Press, *Why is Everyone Talking About Deep Learning?*
[8] Hitchens, *Aging Air Force IT*
[9] GAO, *National Security: Long-range Emerging Threats*, 4
[10] Regalado, *Top US Intelligence Official Calls Gene Editing a WMD Threat*
[11] Shaik et al, *The Wireless Sensor Networks,* 910
[12] Carrara, *Body Dust*, 12402
[13] Taylor, *Applications of Smart Dust*
[14] Zeng et al, *Artificial Intelligence Enabled Public Health Surveillance*, 439
[15] Arora et al, Artificial Intelligence in Surveillance, Diagnosis, and Drug Discovery, 5
[16] Cronk, *DoD Unveils Its Artificial Intelligence Strategy*
[17] Campbell, *The Entire System is Designed to Oppress Us*
[18] Kanaan, *T-Minus AI*, 188