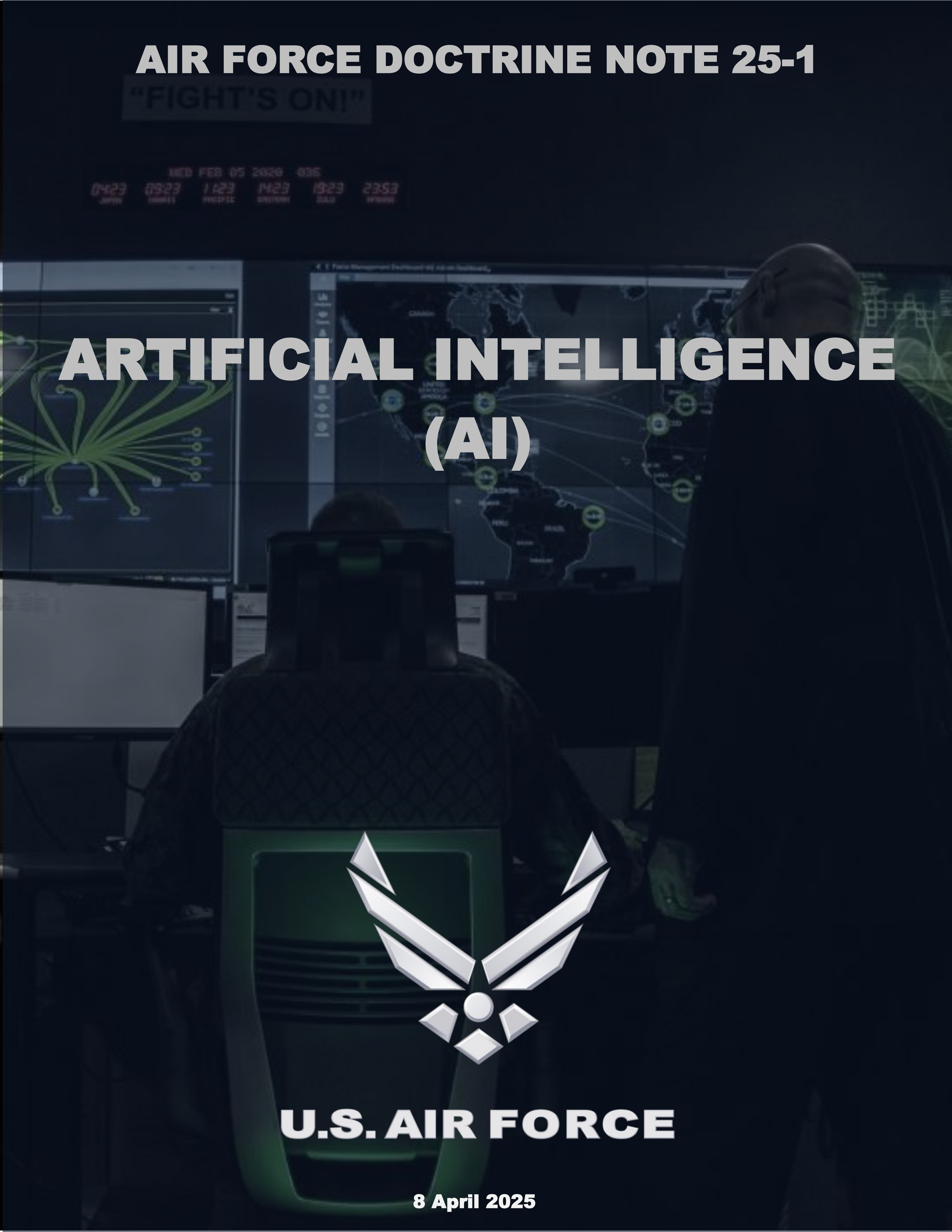
AIR FORCE DOCTRINE NOTE 25-1



ARTIFICIAL INTELLIGENCE (AI)

U.S. AIR FORCE

8 April 2025

Air Force Doctrine Note 25-1, *Artificial Intelligence (AI)*

Table of Contents

FOREWORD

This Air Force Doctrine Note (AFDN) describes Artificial Intelligence (AI) and anticipates its role in air operations across the competition continuum. It references various sources, including pertinent joint and service policy and strategies, public law, academic and industry writings, and subject matter expert consultations. This AFDN supplements existing AI policy and strategies of the Department of Defense (DoD). It is intended to be authoritative and informational, but not directive.

This AFDN examines problems and potential solutions to support Air Force doctrine development at the operational level. It informs forecasted doctrinal gaps regarding operational topics that will have Service-wide impacts in the near term. The AFDN socializes emerging lessons learned and best practices that commanders and staffs can use in strategy development and air operations planning.

Finally, this AFDN acknowledges that opinions differ amongst AI experts regarding the exact definitions of AI-related terms and concepts. Therefore, this AFDN provides descriptions of AI-related terms to facilitate Airmen's understanding and to align future Service and Joint AI policy.

If there are any conflicts between this AFDN and a joint or service policy publication, the respective policy takes precedence for the United States Air Force (USAF) activities.

CHAPTER 1: INTRODUCTION

THE PROMISE OF AI

Computers transformed how wars were fought. The British “Bombe,” an early computer, cracked the German Enigma cipher in World War II. This produced exquisite intelligence for the Allies and turned the tide in the Battle of the Atlantic.

The development of early electronic supercomputers, powered by vacuum tubes, enabled massive calculations supporting the space and missile programs. In addition, the introduction of silicon-based semiconductors revolutionized computing by enabling miniaturization. In turn, the advancement of transistors played a key role in driving innovation in both Cold War-era defensive systems and advanced weaponry. These advancements in armed platforms with onboard computing power transitioned the USAF from its reliance on mass to unprecedented precision attacks in Operation DESERT STORM.

A new data-driven era has emerged. Academic and commercial innovations are creating cutting-edge capabilities at increasingly affordable prices. Our environment is saturated with "smart" devices that connect us through a digital domain of unprecedented information. High-speed data processing, the availability of large data sets, and big data analytics from machine learning (ML) are all contributing to the emergence of new AI technologies with seemingly unlimited possibilities.

AI will supercharge Intelligence, Surveillance, and Reconnaissance (ISR) by providing networked sensors capable of identifying hidden “needles in a haystack” without prior threat knowledge. AI will fuel robotics advancements and enable intelligent swarms of autonomous agents to perform tasks once thought to exist solely under human control. AI is anticipated to accelerate training, create information advantage, strengthen readiness, and generate synthetic experiences that ultimately drive both machine and human learning.

AI will assist planners with advanced tools to plan for highly complicated tasks, such as sustainment, and then wargame solutions informed by real time analysis of the environment and our adversaries’ potential actions. It will assist in the testing and evaluation of various strategies and operational concepts in a virtual sandbox. In international affairs, AI will support the design and implementation of cooperation and assistance programs to strengthen strategic partnerships. It may even recommend new partnership scenarios for strategic advantage.

AI has great promise. There are significant national security implications for United States leadership in developing safe, secure, and trustworthy AI while fostering a stable and responsible international governance framework to manage risks and promote global benefits. AI will help commanders make more informed decisions across the strategic, operational, and tactical levels of warfare.

THE RISK OF AI

Despite its novelty, AI is ubiquitous and already proving its value as a force multiplier in competition and conflict. AI technology could prove to be a cost-effective way that limited-resourced countries enhance their capabilities to erode U.S. strategic advantage. In the realm of Great Power Competition, our competitors and potential adversaries, such as China and Russia, invest heavily in AI. The People's Republic of China publicly stated its goal is to lead the world in AI development by 2030. Today, China is using AI to monitor and repress its people at scale. Its access to US citizens' data, particularly Airmen, creates new pathways for AI-enabled attacks against the US and targets in the Homeland.

Both China and Russia are wagering on the potential of AI for military applications. China is accelerating efforts to become an "intelligentized" force that is optimized by human machine teaming. In addition to investing in autonomous vehicles and intelligent robotic systems, China is focused on applying AI to command decision-making, logistics, cyber operations, swarms, missile guidance, and the cognitive domain. Similarly, Russia is integrating AI into its doctrine and strategies. Russia is making great strides in Unmanned Aerial Vehicles (UAV), autonomous ground vehicles, and underwater systems. Both China and Russia are focused on integrating AI for more effective command and control, targeting and reconnaissance, and electronic warfare systems.

We anticipate AI will strengthen many warfighting capabilities, but warfighters must be aware of its potential pitfalls. Specifically, decision-making delegated to AI may lower the threshold for conflict by accelerating actions and responses beyond the capability of traditional "human firewalls." Also, given the collaborative nature of AI system development, which often involves commercial, academic, and military organizations with varied information security standards, it is crucial to carefully determine both the data that AI systems can access, and the individuals authorized to access that data. Further, adversary efforts and inaccurate data sets can "poison" AI systems with bad data, leading to erroneous decisions and pathways for deception and surprise. This will challenge our trust in AI and inhibit its adoption. Therefore, we must embrace responsible AI through understanding and experimentation. As Airmen, we must employ AI to enhance kinetic and non-kinetic capabilities while defeating adversary disinformation campaigns.

Since our service's inception, Airmen have harnessed new technologies to strengthen our nation's strategic advantage. AI is no different. We must accelerate ethical enterprise adoption, experimentation, and fielding of AI-enabled capabilities to rapidly develop the required infrastructure and Governance required to successfully employ AI.

CHAPTER 2: AI OVERVIEW

WHAT IS AI?

Recent technological breakthroughs and application development within the field of AI have uncovered opportunities and possibilities once considered impossible. In many ways, these exponential developments out-paced our ability to deliberately develop a shared understanding and consensus on AI-related topics. Across academia and industry, there are nuanced distinctions among AI definitions and terminology. Currently, DoD has not established a doctrinal definition for AI but has deferred to, and directed the Services to utilize, U.S. Code and Executive Orders to establish AI-related definitions and guide policy development.[1] This AFDN does not establish official Department of the Air Force (DAF) definitions for AI or its associated terms**.** Rather, this AFDN provides descriptions of AI terminology and concepts, which are intended to provide a better understanding of AI's potential in USAF operations. Generally speaking, AI uses technology systems, in combination with rule-based and ML approaches, to approximate aspects of human cognition. However, unlike humans, AI is limited in that it does not critically examine the validity of its system's inputs or the broader consequences of its outputs.

DESCRIPTION OF AI TERMINOLOGY

To integrate AI into military operations, it is essential to understand AI terminology. The examples in this Doctrine Note are not exhaustive but illustrate true distinctions between related and complementary AI disciplines and aspects.

The terms **"Narrow AI"** and **"Weak AI"** have slight nuanced differences but are used interchangeably in this document. These terms refer to AI systems that are limited to performing a specific task or function <u>and</u> do not have the ability to learn new tasks.

In contrast to Narrow or Weak AI, **Artificial General Intelligence (AGI)** aims for AI with human-like understanding, learning, and adaptation across tasks. AGI does not currently exist, and some experts argue it may never exist. However, there is consensus that AGI is not possible with today's capabilities. AGI is a long-term goal facing technical, ethical, and philosophical challenges. Despite this, there is progress towards AGI with new algorithms and hardware. While AGI systems are not ready for airpower employment, Airmen must consider ethical and practical challenges in operations and planning if AGI becomes a reality.

Expert Systems, meant to complement and not replace human experts**,** use human expert knowledge combined with rule-based and/or advanced mathematical

---

[1] 15 U.S.C. 9401(3) define artificial intelligence as: a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."

representations to solve narrowly defined problems. A common application in decision support applications is a medical diagnosis consultant system.

Machine Learning (ML) is a field of AI concerned with the development and study of statistical algorithms that can learn from data and generalize to unseen data and thus perform tasks without explicit instructions. ML-based AI systems do not follow traditional programming rules. Instead, they draw from various disciplines such as computer science, statistics, psychology, neuroscience, economics, and control theory to analyze data and extract patterns from the data. However, ML does not possess the ability to understand or utilize these disciplines independently. Rather, it finds patterns in the data based on how it was programmed. The ML behind AI systems that defeated human champions in cognitive games such as chess or Go still required significant human knowledge to be encoded into its design before the ML process started.

Training Data is the information used to teach AI models to make predictions and classify data by identifying patterns from input-output pairs. The quality, quantity, and diversity of the training data impacts AI system performance and accuracy, with any unintended biases or inconsistencies leading to incomplete or erratic results. **Test Data** is data not used during training and is reserved to evaluate the performance of the model after training. After a system is trained and tested, additional training and testing may be required if the input data begins to differ substantially from the original training data.

Neural Networks (NN) are inspired by the human brain. NNs are composed of interconnected units called neurons arranged in multiple layers. At a minimum, an NN will have three layers (an input layer, at least one hidden layer, and an output layer). In the past, NNs were not often used due to the computational burden of training and operating them. However, with advances in computational power and access to more data, NN have become more complex and layered.

Deep Learning (DL) is merely a multi-layered neural network that employs more than one hidden NN layer to learn from complex datasets and create more accurate associations between inputs and outputs. DL models are powerful tools in AI applications because they learn complex features or patterns that are not recognizable by people.

Natural Language Processing (NLP) uses DL as a core technique to allow computers to comprehend, interpret, and generate human language using multi-layered NNs, which analyze and understand the structure and meaning of text. NLP is used for a wide range of tasks, such as machine translation and speech recognition, and is the core technology behind virtual assistants like Siri, Alexa, and translation devices.

Generative AI analyzes vast amounts of data to find patterns and connections between words, audio, images, and video to generate content. AI systems that can process multiple modalities (or types) of inputs (e.g. images, text, video, etc.) at once are called **Multimodal AI.** Unlike large language models (LLMs) that focus on language-based data, Generative AI trains algorithms on vast datasets to learn inherent patterns and structures. Post-training, these algorithms replicate data styles, characteristics, and distribution of the data to produce new content.

Large Language Model (LLM) is a type of AI model that uses probabilistic models to analyze patterns and connections between words and phrases to understand and generate human language. LLMs are trained on large amounts of text data, such as books, articles, and web pages, and use this data to learn the statistical relationships between words and phrases. LLMs are used in a wide range of applications, including virtual assistants, chatbots, language translation, and text summarization. One of the most popular LLMs is Chat Generative Pretrained Transformer (ChatGPT), which is a model developed by OpenAI. ChatGPT can generate answers to user prompts and summarize topics by using its understanding of language patterns and connections to generate coherent and relevant responses.

Computer Vision (CV) is a field of AI that extracts meaningful information from digital images, videos, and other visual inputs. It involves using techniques such as image processing, pattern recognition, and DL to analyze and interpret visual data. CV algorithms process images at the pixel level, which means they analyze the individual pixels in an image to extract features and patterns. CV's applications are wide-ranging, including areas such as surveillance, target recognition, autonomous navigation, and medical imaging.

AUTOMATION VS AUTONOMY

"Automation" and **"autonomy"** are critical terms regarding the military's employment of AI. **Automation** is a system's ability to undertake a narrow and constrained task with low levels of complexity, where that task is highly repetitive and independent of choice. **Autonomy** is a system's ability to utilize rules-based processing to undertake a variety of tasks, of varying levels of complexity, and to complete those tasks while achieving multiple goals. Both systems are constrained by the goals (and authorities) delegated to them. Stated another way, automation tasks are more comparable to the auto factory line while autonomous tasks are more like self-driving vehicles, which must dynamically react to unknown variables.

The USAF uses a mix of automated and semi-autonomous systems that augment an Airman's performance. With a holistic AI understanding, the USAF can apply the same developmental mindset to AI systems as it does to aviation, every achievement is an innovation stepping-stone. Just as pilots gain confidence and competence with each sortie, each automated or autonomous system's process repetition builds a system's competence. This competence increases an Airmen's confidence in their ability to leverage a system for decision-making.

CHAPTER 3: AI APPLICATION

HUMAN-MACHINE TEAMING

The USAF approach to AI employment will be Human-Machine Teaming (HMT). AI systems will augment the performance of Airmen and the execution of USAF operations. Ideally, HMT will function as an amplifier for Airmen capabilities. Military discretion lies with Airmen, but AI can enable faster and superior operational decisions. Though AI quickly processes large datasets, it lacks context sensitivity and reasoning. In HMT, human strengths (e.g. intuition and reasoning) and machines (e.g. fast data processing) combine to maximize capability. For AI-enabled processes, the exercise of appropriate human judgment is an important consideration, especially in strategically high-risk operations. The human-machine relationship is dynamic and situation-dependent in complex AI systems. Airpower leaders must acknowledge this conditions-based construct to make critical decisions on the input Airmen will provide the AI system. Leaders' risk tolerance decisions should inform the appropriate level of human judgment required. In situations where an occasional false prediction or misclassification is tolerable, the appropriate level of human judgment may be lower, and the machine may be granted more autonomy. Conversely, in situations where machine miscalculations would create significantly detrimental effects, the appropriate level of human judgment may be higher, resulting in closer supervision.

Common Human-Machine Teaming Constructs*

Human-in-the-Loop–The machine makes recommendations and, the person makes the decision (e.g. proximity alerts in your car).

Human-on-the-Loop–The machine makes recommendations, and the machine recommendation will be implemented unless the person vetoes the machine action (e.g. lane keeping).

Human-off/out-of-the-Loop–The machine makes the decision, and the person cannot override the machine's action (e.g. engine compression ratio, antilock braking action).

* These common constructs have been used colloquially within industry and academia to discuss the human-machine relationship within AI. This inset is included for information only and does not constitute USAF endorsement or policy for executing appropriate human judgment.

Tactics that optimize the balance between decision speed and risk tolerance will evolve to integrate HMT into Air Force AI systems. As the relationship between Airmen and AI strengthens, HMT optimization will improve through communication, coordination, cooperation, social intelligence, language exchange, and shared situational awareness. In addition, trust evaluation methods between humans and machines must consider factors like distrust, trust evolution, and team goal changes. Transparency and explainability in AI systems are crucial for understanding system behavior and building confidence in the HMT. Training HMT as a unit helps build accurate mental models, while key design decisions impact human workload, situational awareness, and overall success. Ultimately, AI system responsivity, predictability, and “directability” enhance trust.

AI APPLICATION: AIR FORCE CORE FUNCTIONS

Future warfighting requires Airmen to understand the relationship between AI development and Air Force Functions. In coordination with the Science and Technology community, Airmen must identify operational gaps that are well-suited for AI and autonomous systems applications. HMT must capitalize on the best of human intuition and reasoning, combined with AI’s extremely fast data processing capability, to strengthen kinetic and non-kinetic effects across all missions.

AIR SUPERIORITY

The USAF is called to conduct offensive and defensive operations to achieve air superiority as part of joint operations. AI will advance our efforts in contested environments by facilitating improved and timely execution of various air missions designed to achieve air superiority and information advantage. AI-enabled early warning and detection systems, as part of our integrated air and missile defense systems, will provide data to airpower C2 systems to alert Defensive Counterair (DCA) assets to threats. For Offensive Counterair (OCA) to gain or retain air superiority it is imperative that AI-powered ISR systems, targeting mechanisms, and aircraft support all aspects of air operations ranging from Combat Air Patrol (CAP) missions over adversary terrain to Suppression of Enemy Air Defenses (SEAD), and to Air Interdiction operations designed to destroy adversary aircraft on the ground.

As an example, aircraft such as autonomous swarms and semi-autonomous Collaborative Combat Aircraft (CCA) may be used in multiple air superiority-associated missions. In a demonstration of the growing confidence and trust between humans and AI-enabled aircraft, the Secretary of the Air Force was the passenger in a modified F-16 with an AI-controlled dogfighting module in May 2024. The CCA program, and related experiments as part of the Autonomous Collaborative Platform (ACP) program, demonstrate the ability of semi-autonomous aircraft to support manned fighter aircraft. CCA’s potential capability to act as weapons platforms or ISR platforms also serves as a sign of the possibilities of HMT and human-directed engagement. The success of these initial developmental efforts represents a solid foundation for further advancement.

GLOBAL PRECISION ATTACK

In Global Precision Attack, the USAF strives to achieve technological advances to attack anywhere, anytime, more quickly, and with greater precision than ever before. AI improvements to aircraft and munition targeting are making great strides in this arena. As an example, AI CV, combined with improved target recognition and tracking algorithms, will further minimize civilian risk caused by high precision, low collateral damage munitions. Additionally, continued use of AI-enabled modeling will improve U.S. stealth capabilities and continue to offer options for striking targets in denied areas. In the realm of targeting and "sensor-2-shooter" integration, AI empowers an automated C2 capability to accelerate the decision cycle, rationalize risk, and enable effects faster. Advancements in CCA and preventative maintenance are just two examples of AI-enabled airpower tools to achieve and improve Global Precision Attack.

RAPID GLOBAL MOBILITY

The Agile Combat Employment scheme of maneuver requires adaptive basing and rapid, responsive logistics in contested environments. AI will prioritize operating location selection by analyzing the criteria of potential locations for survivability, efficiency, resiliency, and sustainment capacities. AI systems use predicative analysis to detect failure and usage trends at scale to improve predictive maintenance processes while optimizing the inventory and transportation procedures to strengthen adaptive logistics planning and execution. To these ends, there have been many breakthroughs in how we execute logistics for dispersed operations. One example is AFWERX collaboration with an industry partner to develop a semi-autonomous airlift capability. During the Bamboo Eagle/Agile Flag exercises in August 2024, an Air Expeditionary Wing's A4 successfully leveraged the semi-autonomous airlift asset to deliver over 20 urgently needed Mission Capable Parts orders to multiple geographically separated locations. These just-in-time airlift operations, controlled at the tactical level, relieved pressure on traditional airlift assets. Further, it provided flexibility for the A4 and maintenance personnel while accelerating an aircraft's return time to a mission capable status. These experiments show the promise AI and ML-enabled systems represent for future USAF operations.

GLOBAL INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

The operational capability for multi-intelligence, cross domain data fusion shows promise with multi-modal AI (i.e. systems that can translate and process data sets that are in different formats and of different types). These AI systems can assist with real-time pop-up threat detection and identification along with multi-domain situational awareness synchronization. AI-enabled programs can be leveraged to eliminate disconnects between Service-unique intelligence platforms and processing programs. In addition, autonomous ISR platforms offer the potential for persistent audio, visual, signals, or electromagnetic collections in previously denied areas.

COMMAND AND CONTROL

AI will assist the processes of targeting, resource allocation, planning, and scheduling in support of multi-domain C2 and battle management. AI-enabled communications networks will provide resiliency and survivability for C2 in contested, degraded, and operationally limited environments. For example, if communication between two operation centers is severed, AI-driven communications networks could re-direct communication pathways to instantaneously restore a connection. In addition, if a higher echelon's C2 capability is degraded, an AI-enabled communications system could re-vector data feeds to subordinate C2 elements to maintain C2.

Autonomous Collaborative Platforms

The Air Force is developing ACP, variants of semi-autonomous aircraft, which work in concert with more expensive crewed, platforms, to provide the ability to operate runway flexible aircraft capable of expeditionary launch and recovery operations to complement major weapons systems already in acquisition. The ACP Ecosystem of Capabilities includes CCA and collaborative mobility, surveillance, bomber, and training aircraft.

CCA use semi-autonomous software to enable seamless and effective collaboration with and augmentation of the performance of manned combat aircraft by providing enhanced situational awareness, greater lethality, and improved survivability in highly contested environments.

CCA development will leverage the existing crewed-uncrewed teaming efforts from previous generations of ACP development such as the XQ-58A and XQ-67A. These generations of ACP have proven the ability to build relevant combat capability fast while treating low cost as the primary objective. More modern CCA, such as the YFQ-42A and the YFQ-44A will build on success of previous ACP development.

Concepts of the uncrewed fighter aircraft YFQ-42A (bottom) and the YFQ-44A are pictured in artwork. The aircraft are designed to leverage autonomous capabilities and crewed-uncrewed teaming to defeat enemy threats in contested environments. (U.S. Air Force artwork courtesy of General Atomics Aeronautical Systems, Inc. and Anduril Industries)

CHAPTER 4: CONSIDERATIONS FOR EMPLOYMENT

The USAF must be positioned to capitalize on the commercial sector's AI advancements. Current and forthcoming DoD and USAF policy and governance structures for AI will shape the manner AI is employed across the USAF. This section highlights several considerations planners and commanders should understand when harnessing AI for their mission.

AI-READY FORCE

USAF personnel must be AI fluent to integrate its capabilities into operations. In the context of this doctrine note, AI fluent implies proficiency beyond simple literacy. Airmen should not just possess a basic AI understanding, but they should comprehend the application, interpretation, and effective navigation of AI systems. Airmen must seek to utilize AI-powered tools and experiment with available tools to find areas for improvement, how to provide feedback, and apply corrective actions. AI capability awareness and understanding underpins effective collaboration with automated systems, informed decision-making, and risk mitigation. AI fluency keeps personnel competitive, enables a strategic edge for the integration of more technologies and lays the foundation for our AI ecosystem.

DATA

Data must be treated as a valuable enterprise-level asset. Everyone in the enterprise must understand the importance of data management and collection efforts, including the curation of records and information made available for AI development and implementation. The collection and management of high-quality data is a critical challenge in the development and implementation of AI tools. The accuracy and reliability of AI models are heavily dependent on the quality of the data used for training and testing. Therefore, proper data management and collection efforts are essential to gather properly conditioned data across datasets. These efforts lead to better performance and practical utility of AI models. As partnerships between the USAF and industry produce excellent AI tools, data ownership, storage, and processing will present risks and opportunities for USAF decision-makers. Airmen must consider these factors when developing AI tools and implementing them within the enterprise.

COMPUTE

Currently, training and running AI models requires a massive amount of compute power, which will drive a recurring demand signal for increased computer and technology acquisitions for host platforms. This reality can be a critical deciding factor in Air Force AI integration. AI-use plans should outline computing, data collection and storage, mission assurance, communications, authorization to operate, and energy requirements for development, testing, and deployment at the enterprise level. At the same time, leaders should balance the risk associated with fielding open source and commercial AI tools with the speed and increased computing power often resident in commercial sources.

TALENT

The USAF's AI subject matter experts are sparsely scattered across staffs and in centers such as the Air Force Research Laboratory. However, to build an AI-fluent force, we must find, recruit, develop, and incentivize individuals who can build, operate, and lead an AI enterprise. This goal requires collaboration across various specialties, including partnerships between developers and operators, scientists and ethicists, coders and system architects, planners and programmers, and military personnel. Outreach to strategic partners, academia, labs, and industry underpins a future AI-fluent force.

PROBLEMS AI CAN SOLVE

AI is best suited for military applications with consistent patterns. Practical AI usage requires substantial high-quality data and computational power. In addition, understanding the problem structure is critical. While simple problems may not need advanced techniques, AI can address **complicated** and some portions of **complex** problems.

COMPLICATED PROBLEMS

Complicated problems and systems, like designing and running intricate machinery or aircraft components, involve multiple aspects and challenges that possess consistent structures and activity patterns over time. Since the problem-solving approaches are mostly the same every time, they can be adequately modeled with mathematical formulas. Specifically, AI excels in solving these problems with probabilistic mathematics to detect patterns at scale and speed. The logistics industry demonstrates AI's effectiveness in dealing with complicated problems, optimizing inventory management, transportation, and enabling predictive maintenance through accurate demand forecasting and part failure predictions.

COMPLEX PROBLEMS

Complex problems (often called "wicked") are unpredictable, with frequently changing rulesets and patterns of interaction that make it difficult or impossible to adequately or reliably model the kinds of mathematics currently used by AI. For instance, social issues are inherently complex. They typically require balancing between tightly coupled competing interests that cannot be accommodated simultaneously. They require managing human intuition and perception, including working out compromises. Current AI models struggle with complex problems. They are better suited for solving the individual, complicated tasks that make up components of the larger complex issue. For example, some complex problems, such as nuclear deterrence, fundamentally require human characteristics like an understanding of context, judgment, wisdom, and ethical considerations.

The Air Force Rapid Sustainment Office partnered with Defense Industrial Base (DIB) command, control, and communications (C3) AI to develop the Predictive Analytics and Decision Assistant (PANDA), a System of Record for achieving Condition Based Maintenance. PANDA uses AI to optimize fleet maintenance, increasing aircraft availability, and minimizing downtime. PANDA utilizes Enhanced Reliability Centered Maintenance (eRCM) and Sensor Based Algorithms (SBA) to achieve these goals. eRCM uses AI to analyze historical component failure data to predict component failures. SBA uses AI to analyze sensor data to detect degrading performance or impending component failure. PANDA synthesizes aircraft-specific performance data with airframe-wide historical failure data to preempt component failures.

GOOD DATA AND BIAS AWARENESS

AI systems need good training data. Obtaining accurate, properly labeled, and conditioned data without introducing unintended or harmful biases is a challenge. Quality results from AI depend on good data management, which includes the gathering, contextualization, extraction, and dissemination of properly curated data that sufficiently represents the problem or phenomenon to which AI is applied. This requires finding, accessing, reformatting, and restructuring data, eliminating unintentional biases, and ensuring accuracy. Unintentionally biased data or algorithms may cause discriminatory outcomes, leading to a lack of trust in AI systems. To mitigate certain unintentional biases, developers and decision-makers must address potential sources of bias throughout the AI development process using diverse datasets, transparent and explainable algorithms, and regular audits and evaluations. Only when data is accessible, understandable, and filtered can military applications be built. The accessibility of data should also be a planning consideration when deciding the classification level and network requirements for AI systems.

CYBER DEFENSE OF BLUE AI

Robust cyber defense is required for implementing AI within the USAF. The success of AI systems and AI-enabled operations relies on quality data and uncompromised processes. Cyber defense for AI systems is crucial due to their sensitivity and the criticality of processed data. Malicious cyber activity often focuses on data poisoning to target ML models with manipulated data. Data poisoning alters the fundamental behavior of AI systems and results in false or misleading outcomes. In addition to poisoning input data, an adversary gaining access to an AI model itself could reverse engineer a system to reveal sensitive input data or manipulate control of the data output. For example, with access to an ISR model trained to detect military equipment in satellite imagery, an adversary could develop a digital camouflage to prevent detection. To prevent such threats, the cyber defense of AI systems must include multi-layer protection like access controls, encryption, network security, intrusion detection, and data verification processes. Failure to secure AI systems will lead to grave consequences.

AI AND ETHICS

The ethical use of AI tools is a significant concern. AI applications must be consistent with law, policy, and used responsibly. In line with the Deputy Secretary of Defense Memorandum on Implementing Responsible AI, all DoD AI capabilities must be responsible, equitable, traceable, reliable, and governable. The DoD Chief Digital and Artificial Intelligence Office (DoD CDAO) and the DAF Chief Data and Artificial Intelligence Office (DAF CDAO) lead the ethical development and adoption of AI-powered tools.

However, it is worth noting that our adversaries are not always beholden to the same ethical guidelines, and the DoD may encounter significant challenges when faced with systems employed with fewer ethical considerations.

CHAPTER 5: A VISION FOR THE FUTURE

True technological innovation is unlocked not by the technology itself, but how we are able to conceptualize and apply it. Our competitive advantage will be amplified by our ability to gauge and shape implications of that technology faster and more completely than our adversaries.

Recent AI developments are no exception. They require interdisciplinary efforts to achieve benefits while avoiding pitfalls. Airmen must anticipate and embrace AI's changes while navigating potential vulnerabilities and internal challenges. The USAF must invest in data collection, computing, energy, communications, human capital, and multidisciplinary knowledge to maintain a secure and ethical AI enterprise. Airmen must be ready, innovatively minded, and willing to push that technology to its limits. Our task will be to constantly demand the best of our AI tools for employment integration.

DAF Battle Network

The Advanced Battle Management System (ABMS) is a "system of systems" designed to share data seamlessly and securely across multiple weapons systems. ABMS, and overarching DAF architectures such as the DAF Battle Network, will be critical enablers to the Defense Department's Joint All Domain Command and Control (JADC2) effort to connect sensors and shooters around the globe.

This doctrine note's Appendix will help Airman prepare for the employment of new AI tools and pursue the right opportunities to employ AI today for victory tomorrow. For Airmen to continue their individual journey in AI knowledge, reference products and webpages of Air Force AI leaders such as AFRL, the DAF AI Accelerator at Massachusetts Institute of Technology (MIT), and DAF Bot Operations Team (DAFBOT) at the USAF Lifecycle Management Center (LCMC).

APPENDIX: QUESTIONS TO ASK BEFORE DEVELOPING AN AI SOLUTION

The questions below are meant to assist an Airman's assessment of how and if AI systems can provide a solution to their problems. Airmen should also reference DAF CDAO site (ai.af.mil) for information materials, tools, and products to guide their AI journey.

- ✪ Is the problem, question, or phenomenon sufficiently well-structured to apply the desired AI tools, given the inherent limitations of the mathematical tools being used?
  - ✪✪ The more well-structured the problem is, and the more the same rules apply to multiple instances of the phenomenon, the better suited the AI application.
- ✪ Have operators who will be using the AI tool been involved in the design of the tool, and is there a plan to ensure that the AI results will be externally valid?
  - ✪✪ This is important to ensure developers ask questions and design AI tools relevant to the field, and useable by the Airmen. It is also important that operators are part of the data collection effort, to ensure data is collected and categorized correctly.
- ✪ Are there adequate edge cases to test safety and reliability of AI, and how will they be tested?
  - ✪✪ Edge cases are situations in which the AI will fail or be insufficient to deal with the external realities of a situation. Ideally, testing should deliberately seek to identify and expose those edge cases to either improve the AI model or limit what the AI is asked to do. More complex situations potentially present an infinite number of edge cases, which makes reliability testing increasingly difficult, and failure in the field more likely.
- ✪ Is there sufficient high quality labeled/curated/documented data for the AI system to use? Is data conditioning sufficient and congruent across aggregated datasets?
  - ✪✪ A lesson learned from an early AI defense project named Project Maven was that data conditioning was an even bigger challenge than creating algorithms, especially when trying to aggregate data across many separately designed systems. Data often requires annotation/labeling to indicate how and why it was collected, and that context may determine if data collected to answer one question is suitable to answer a different question in a different context. Data labeling can also create problems if the system of labeling is not consistent between different systems.
- ✪ Are there protection measures for the entire system from either accidental or deliberate data poisoning, model inversion attacks, or algorithmic manipulation?
  - ✪✪ In addition to the internal challenges of protecting the systems and data needed to apply AI, consider how vulnerable AI applications will be to external adversarial

actions or manipulation, and if sufficient safeguards can overcome these countermeasures.

- ✪ Are there sufficient, consistent, and mission assured data storage, power supply, and processing power for the AI task?

  - ✪✪ Many advanced AI applications require massive computing power, hence lots of data storage and energy. Even edge computing on the frontlines requires adequate power supplies and storage capability.

- ✪ Is pursuing automation in this area justified given the amount of natural learning and experience my personnel are likely to lose by trusting the machine to perform this task versus performing them with more traditional techniques?

  - ✪✪ One of the potential downsides of automation or applying AI to tasks (normally accomplished by humans) is humans lose the "deep knowledge" and experience in the subsumed function, and therefore are unable to handle the "handover challenge" when the automated system encounters a different situation than it was designed for. People accustomed to accepting AI generated answers will lose the benefits of research, which is slower when it comes to finding answers to known problems, but also facilitates the serendipitous learning and discovery that prepares them to handle new future problems.

- ✪ What are the opportunity costs of trying to use AI for a problem versus using more traditional means or classical computing, and why is the tradeoff potentially worth it?

  - ✪✪ Given a simple problem, traditional computing methods may be more than adequate to assist. Above all, consider the new resources, human capital, hours of labor, and potential new sources for potential failure across the entire ecosystem if sophisticated AI tools are applied to problems that could be adequately addressed by less sophisticated but also less vulnerable traditional methods.