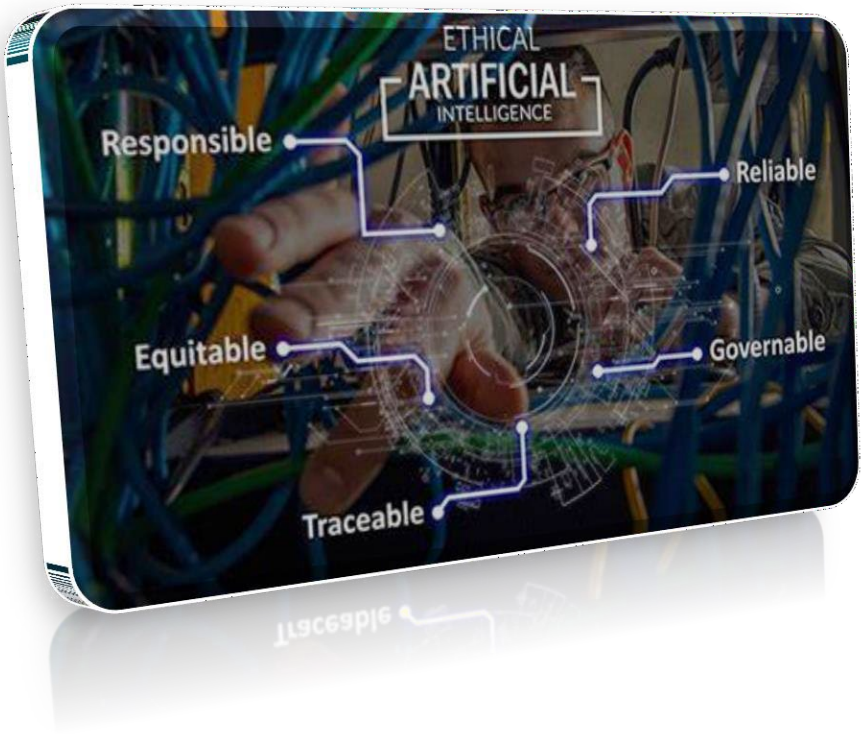


A DESIGN APPROACH FOR AI IMPLEMENTATION ACROSS DOD: PART ONE

ABSTRACT

Due to the rapidly shifting technological advances in warfare in the 21st Century, DoD needs to embark upon a comprehensive reassessment of its entire structure, practices, warfighting concepts, and doctrine to maintain critical competitive advantages in AI and Autonomy in strategic competition against near peer nations. Part One in this two-paper series explores background, definitions and doctrinal implications for AI in DoD.

Matthew Dooley and Grant Highland, Ph.D.
Fidelium, LLC

"By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it." —Eliezer Yudkowsky."

The U.S. Department of Defense stands at the precipice of yet another breakthrough in innovation. Unlike the development of stealth technology and the internet, however, the advent of autonomous robotic capabilities and the employment of Artificial Intelligence (AI) in military applications requires extensive collaboration and teaming with industry leaders who have led in the development and revolution of AI technology over the past decade. Ubiquitous in various commercial forms, AI and autonomy promise differential advantages in military applications against our potential enemies and portend important changes in the speed and even the character of war. However, it is difficult to see a path where autonomy and AI will achieve their greatest potential without commercial industry taking the lead in assisting DoD in the development of their AI programs. The internet may provide the clearest example of this need for transition.

From its embryonic beginnings in the late 1960's as a project undertaken by the Pentagon's Advanced Research Projects Agency (ARPA, now DARPA), the internet's structure, curation, communication, analysis, and explication of its data has exploded over the last 50 years.[1] But what began as a Department of Defense (DoD) led initiative has been overtaken by rapid adoption, development, and implementation across private sector enterprises. Whereas in the past, during the industrial and computational eras where DoD was on the forefront of technical innovation and advancement, the private sector in the digital and algorithmic age has taken the lead in technology innovation and application. From an economic point of view this makes sense and has evolved into the U.S. harboring some of the most advanced, industry leading, and wealthiest corporations the world has ever seen. But while the private sector has almost fully embraced the promise of digital and algorithmic benefits – adopting the networked paradigm of the internet and algorithmic age into their operating and company structures – the DoD is still struggling to fully adapt to this shift in the global paradigm.[2]

This is understandable for several reasons – the need for security, size and mass of the department, federal regulations and laws, cultural and historical biases resident within and across the services, etc. – but the department needs to radically re-think its approach toward the future if it wishes to remain preeminent in the global competition for military and economic dominance. Just as oil propelled the global economy forward while simultaneously altering the geoeconomic, geopolitical, and geostrategic structure of the world, so too has data become the *new* "oil" propelling another reorientation of the global order as well. And due to the burgeoning ubiquity of data as networks across the globe expand, connect, and grow exponentially in their complexity, the introduction of learning algorithms, machine learning, and artificial intelligence have become the tools necessary for managing and making sense of this avalanche of information.

As with the slow adoption of cyber capabilities in the late 1990's as DoD lagged behind the explosive commercial growth of internet advancements, so too has the Department belatedly recognized this

[1] Timberg, Craig, "Net of Insecurity: A Flaw in the Design," The *Washington Post,* May 30, 2015, (Accessed September 12, 2022), https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/
[2] Slaughter, Anne-Marie, *The Chessboard and the Web: Strategies of Connection in a Networked World,* Yale University Press, New Haven: CT, 2017

global paradigm shift in algorithmic and networked capabilities. Despite this lag, DoD has recently embarked on programs to discern how the department can best meet the realities of the current and coming age. That said, there remains some confusion and a general lack of understanding across the department concerning even the most basic terms and definitions for AI and autonomy. What is meant by AI, machine learning, data curation, tactical inferential reasoning, machine cognizance, and other terms of reference (TOR)? Establishing these common terms should be an essential first step in any attempts to understand the contours of what these technologies will mean for warfighting today and into the future.

This paper seeks to help define the various attributes of AI. This discussion will cover AI's components, sub-components, and interrelated dependencies and highlight current DoD language in that realm. These fundamental AI terms and definitions will serve as the foundation for exploring future processes, capabilities, and warfighting concepts where AI will augment DoD organizations. To develop common understanding between industry and DoD, the paper will be broken into four parts modelled on DoD's design methodology captured in joint doctrinal planning guidance:

1. Describe the operational environment as it exists today pertaining to AI adoption across the department to include definitional TOR as a guide to better understanding and education of the force.
2. Describe the operational environment as it pertains to the future of AI within the department utilizing national strategic guidance, DoD strategies for AI, and industry advancements as a guide.
3. Describe the challenges associated with achievement of those departmental goals, along with the opportunities to leverage in achievement of the same.
4. Describe an operational approach that may help resolve some of these issues for DoD.

If DoD is to remain dominant in the ongoing strategic competition against nations seeking to hinder U.S. influence and power across the globe, it will have to harness the power, creativity, innovation, and promise a whole-of-society approach -- including academia, the private sector, industry, DoD Centers of Excellence and offices of research and innovation – can bring. If silos were the dominant paradigm of the agricultural age, and hierarchies the dominant paradigm of the industrial age, then DoD will have to rapidly adapt a new approach. To do so, DoD must change its processes, structures, and warfighting concepts to compete in the dominant paradigm of the networked age.

What is AI and its Current State of Play in DoD?

Many within the department conceive of AI as a thing to be procured, a noun which can be bolted onto existing processes, structures, capabilities, and warfighting concepts much like cyberspace was initially conceptualized in the late 1990's and early 2000's. While AI is indeed a *thing,* it is more accurately understood as an ecosystem, or system of systems, which serves more as a verb to be actualized and synthesized across the enterprise than as a noun to be pursued and piecemealed onto existing systems and structures toward accomplishment of DoD aims. Less a linear process, the adoption of AI into the DoD needs to be conceived of in its most holistic and far-reaching terms if Joint All-Domain Operations

(JADO) are to be realized; a networked and flattened ecosystem of complementary systems and procedures. As Jeff Bezos made clear to his Amazon employees back in 2002:

- All teams will henceforth expose their data and functionality through service interfaces.
- Teams must communicate with each other through these interfaces.
- There will be no other form of interprocess communication allowed: no direct linking, no direct reads of another team's data store, no shared-memory model, no back-doors whatsoever. The only communication allowed is via service interface calls over the network.
- It doesn't matter what technology they use. HTTP, Cobra, Pubsub, custom protocols — doesn't matter.
- All service interfaces, without exception, must be designed from the ground up to be externalizable. That is to say, the team must plan and design to be able to expose the interface to developers in the outside world. No exceptions.
- Anyone who doesn't do this will be fired.[3]

Given the nature of national security and global competition, it is clear embracing a completely open architecture data interface is not likely. Modular Open Systems Architectures (MOSA) may work for software development used in autonomous behaviors, but employing the same rubric for AI capabilities expected to run trusted command and control systems is an entirely different matter. That said, Bezos' demand for a common data architecture for all company business and communications is germane, as the need to develop some commonality among systems will be necessary. DoD is currently operating off service-specific data platforms, organization-specific data platforms, a variety of contracted data platforms, and a host of other systems which do not readily lend themselves to interoperability or even sharing across platforms or organizations. The article highlighting the quote above goes on to state:

> Not surprisingly, employees took Bezos seriously. The company that had become a collection of silos (separate businesses operating fairly independently but with patched together links to the other silos) had to become a platform (a business model that facilitates interactions across a large number of participants), with a service-oriented architecture (organizing the business as well-defined services that respond to standard requests from others). Making this change would enable the company to grow in size (scale) and complexity (scope).[4]

What Bezos understood back in 2002, while the DoD was still wrestling with cyberspace and its role in warfighting functions, is that a common data architecture is essential for managing complexity and data growth into the future. DoD is in such a position now in building AI capabilities and should follow Amazon's lead. But before this paper can consider the strategic necessities required for adoption of AI within the department or qualify which commonality features should be permitted, it is necessary to define what is meant by AI, and what AI *is.*

[3] McGuire, Russell, "Amazon's Digital Infrastructure," *Clear Purpose Strategies,* June 17, 2020, (Accessed September 12, 2022), https://clearpurpose.media/amazons-digital-infrastructure-ea64be707815
[4] Ibid.

Definitions

As with any complex subject, especially pertaining to technology, there are differing opinions regarding definitional terms. That said, a useful glossary for the purposes of this paper is important to serve as a beginning for foundational understanding and further refinement of terms.

First, as mentioned above, there is no *one* AI application/capability yet in the military, but rather an ecosystem of overlapping and complementary systems of systems. AI systems incorporate data, algorithms, learning machines, neural networks, optical sensors, communications capabilities, etc. This paper will start with a broad definition of AI and then disaggregate AI into its constituent parts and intended capabilities.

Artificial Intelligence:

In the simplest terms, the most basic role for AI is as a computer system(s) that performs better over time as the AI acquires data and related experience in the performance and accomplishment of its assigned tasks. That's it. Of course, those AI systems, can aggregate data, digest data, analyze that data, and perform tasks on a scale simply impossible by human standards. This speed of data assimilation and processing as a decision making aid for leaders and staff teams offers a potentially revolutionary role AI may have across the globe.[5] For the purposes of this paper, then, two useful definitions pertain:

1. **Artificial intelligence (AI)** is a set of algorithmic techniques, tools, and technologies that provide machines with the ability to perform tasks that normally require human intelligence – to perceive the world, learn from experience, reason about information, represent knowledge, act, and adapt.[6]
2. **Artificial Intelligence for Defense Systems**: a multidisciplinary scientific field that aims to study human intelligence, and the attempt to bring rational and human behaviors into a system that can think, act, and self-manage.[7]

There are, of course, numerous other definitions of AI throughout the current literature, but the general gist of AI and its applications springs from neuroscience and our understanding of how the brain works.

Beyond specific algorithms designed by engineers for machines to perform limited and bounded tasks – what is known as *narrow* artificial intelligence (ANI), or *weak* artificial intelligence – the true power of AI is realized through learning algorithms which mimic brain processes. These artificial neural networks are modeled on the neuronal systems within the brain. Just as human neurons work in a binary fashion where they are either "on" or "off" in terms of transmitting electrical signals across the brain's neural architecture, artificial neural networks process data in a layered approach through binary language (i.e., through ones and zeros) and weigh the relative value or significance of incoming data, then transmit a measurement of the significance of that data to all the related nodes in the next layer.[8] The purpose of

[5] Kanaan, Michael, *T-Minus AI: Humanity's Countdown to Artificial Intelligence and the New Pursuit of Global Power,* BenBella Books, Dallas, TX, 2020, pg. 118

[6] Bastian, Nathaniel D., "Artificial Intelligence for Defense Applications," *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2021,* Vol. 18(3) 173–174

[7] Ehn, Eric J., "*Artificial Intelligence: The Bumpy Path Through Defense Acquisition,"* Naval Post Graduate School MBA Thesis, Monterey, CA: 2017, pg. 14

[8] Ibid., pg. 121

these networks is to distinguish characteristics of individual pieces of data, compare similarities and differences between data, and discern patterns within the data as a result.[9]

One of the concerns surrounding these middle layers of data characterization within the neural networks regards the opaque nature of the data processing that takes place in these intermediate steps before a final analysis is generated. As the machine consumes more data, as the increasing data is scrubbed, characterized, and further atomized between layers before being reaggregated into findings, the machine continues to learn and refine its knowledge. In many people's minds, those middle layers constitute a "black box" where the processes and steps are occluded and therefore inscrutable for human operators to ascertain how the final analysis is generated. While this indeed may seem problematic, it is important to note humans and our cognitive processes operate in a similar way. Much like common sense or intuition are well understood in general terms, the processes by which either is attained or applied remains a mystery to neuroscientists and behavioral psychologists. That said, this fact does not preclude us from operating off those abilities, and in fact they are often celebrated. In a defense context, if operational art is to be considered a doctrinal aspect of the art and science of war, then perhaps the "art" of how learning machines process information and deliver recommendations or actions in the physical world should be afforded equal latitude as well. One could even argue AI represents the perfect blending of the art *and* science of the warfighting domain.

Understanding AI in general terms, though, is just the beginning. From this basic understanding it is now important to determine for what purpose AI can be adopted within the Department, and what AI capabilities will be required to achieve those purposes.

Process Oriented:

As noted earlier, the size and scale of the DoD with its multivariate data streams creates analysis, management, and decision-making speed of relevance challenges. Much like humans suffer through the vagaries of language barriers due to cultural idiomatic differences, regional dialectical differences, or international language semantic and syntax differences, so too do machines suffer the same issues. Short of creating a common data architecture or business platform *a la* Amazon, AI may represent the best alternative to sort through the language, semantic, and syntax differences across those various data streams while offering the opportunity to discover new and previously unknown possibilities residing within that data. Additionally, freed from the tedious and arduous task of data assimilation and analysis, commanders and their staffs will be better able to focus on the strategic, operational, and tactical mission analyses necessary for success while simultaneously benefitting from AI-enabled course of action development in their planning processes.

Data Aggregation: Any process whereby data is gathered and expressed in a summary form. When data is aggregated, atomic data rows -- typically gathered from multiple sources -- are replaced with totals or summary statistics. Groups of observed aggregates are replaced with summary statistics based on those observations. Aggregate data is typically found in a data warehouse, as it can provide answers to analytical questions and also dramatically reduce the time to query large sets of data. Once the data is extracted, it is processed. The data aggregator will identify the atomic data that is to be aggregated. The data aggregator may apply predictive analytics, artificial intelligence (AI) or machine learning algorithms

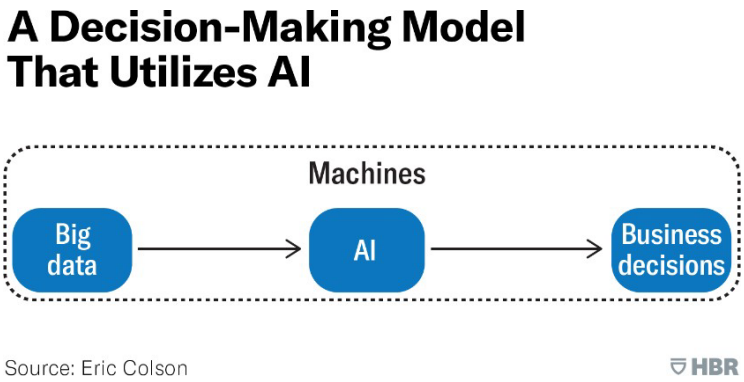
[9] Ibid., pg. 122

to the collected data for new insights. The aggregator then applies the specified statistical functions to aggregate the data.[10]

In lieu of a common department-wide data structure or business platform which would probably prove a bridge too far for a host of reasons, an AI-enabled data aggregator which could access the multiplicity of data streams resident within DoD would greatly enhance sense-making at the strategic and operational levels of command and control. By freeing the workforce to concentrate on the results of the data aggregation versus the tedious task of choosing data, merging that data, curating the data, analyzing the results of the data aggregation, and then packaging their findings, staffs will more rapidly and comprehensively be able to provide recommendations to their commanders.

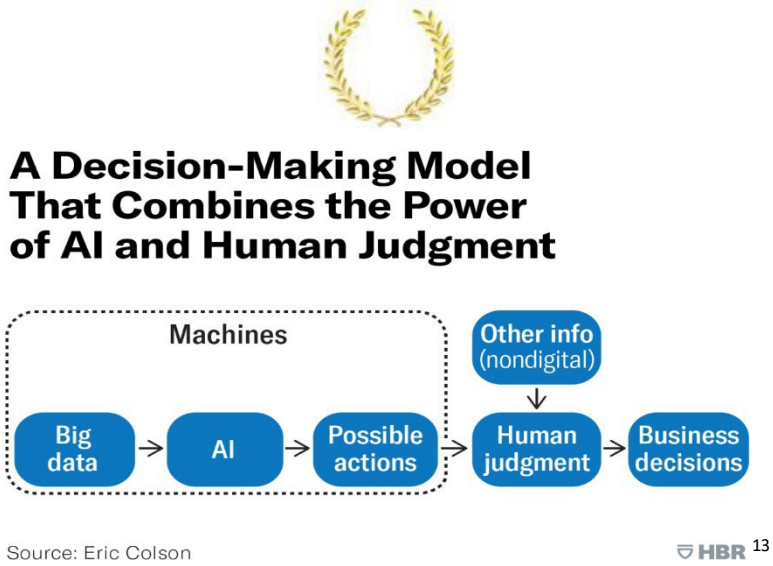
Decision Making:

1. AI can be trained to find segments in the population that best explain variance at fine-grain levels even if they are unintuitive to our human perceptions. AI has no problem dealing with thousands or even millions of groupings. And AI is more than comfortable working with nonlinear relationships, be they exponential, power laws, geometric series, binomial distributions, or otherwise.[11]



2. Removing humans from workflows that only involve the processing of structure data does not mean that humans are obsolete. AI can be used to generate possibilities from which humans can pick the best alternative given the additional information they have access to. The order of execution for such workflows is case-specific. Sometimes AI is first to reduce the workload on humans. In other cases, human judgment can be used as inputs to AI processing. In other cases still, there may be iteration between AI and human processing.[12]

[10] Mullins, Craig S., "Data Aggregation," *TechTarget,* (Accessed September 13, 2022), https://www.techtarget.com/searchdatamanagement/definition/data-aggregation
[11] Colson, Eric, "What AI-Driven Decision Making Looks Like," Harvard Business Review, July 8, 2019, (Accessed 13 September, 2022), https://hbr.org/2019/07/what-ai-driven-decision-making-looks-like
[12] Ibid.



[13]

The obvious benefit here would be for DoD intelligence agencies and organizations to provide better and more timely analysis from the multiple streams of data used in collection and analysis of intelligence information. Additionally, it would allow commanders to still apply operational art using their skill, intuition, experience, creativity, knowledge, and judgement, but at a higher tempo and with possibly unimagined alternatives based on AI interaction with the available data.[14] But, beyond enhancing the decision-making tempo, AI assisted decision-making frees commanders' staffs from the tedious tasks of information and data compilation allowing them to instead focus on strategic, operational, and tactical analysis to enable and feed AI-assisted courses of action. This would also have obvious benefits for the services and the Joint Staff in their Title X responsibilities for manning, training, and equipping the force.

Planning:

An AI equipped with a basic set of mission parameters, rules of engagement, objectives, limitations and constraints might be able to formulate base plans useful for staffs to polish and employ. An AI properly informed on Commander Critical Intelligence Requirements could monitor the execution of a plan and inform the staff and leadership when it might be time to make a planned decision. Conversely, AI that are fed poor information or out-of-date data would not build plans that were tactically sound or relevant, so marrying the data aggregation and pattern recognition described above with the planning function would enable cleaner, labelled, more timely, and more scrupulously analyzed data for use in plan development. Additionally, once concepts of operations, or COAs, are developed, AI can be used in wargaming the COAs in a more timely manner than what is currently in place using manual or computer aided methods.

<u>Warfighting Oriented:</u>

Unmanned, Automated, Semi-Autonomous, Autonomous Systems:

Various robotic, semi-autonomous, and autonomous capabilities across the services have been proposed and testing has been underway for several years. That said, there remains confusion regarding the terms for those capabilities, the application and purpose for those capabilities, what level of integration into existing formations those capabilities can achieve, the level of trust between service members and the capabilities being proposed, and the ethical considerations regarding the use of these

[13]

[14] Joint Chiefs of Staff, Joint *Publication 3-0, Joint Operations,* Washington, DC: October 22, 2018

various capabilities within the context of the Law of Armed Conflict (LOAC) and International Humanitarian Law (IHL). Since the introduction of unmanned vehicles into military operations at the end of the 1990's and into the early 2000's, the proliferation of new platforms and capabilities continues apace. And while exciting new platforms and capabilities are being developed, technology is leading the race for increased adoption across the DoD without a concomitant Department-wide systemic, conceptual, and doctrinal roadmap for how these capabilities will be integrated into warfighting concepts, how they will be integrated into procurement and acquisition processes, or how they will reshape how the DoD conducts its business and warfighting responsibilities.

Though vexing, these challenges are not insurmountable, and DoD has embarked upon initiatives to answer the lag indicated above. To assist with the Department's adoption and integration of unmanned capabilities, this glossary of definitional terms can help provide department-wide understanding and a foundational TOR for future refinement and codification into doctrine.

- **Robot**: A powered machine capable of executing a set of actions by direct human control, computer control, or both. It is composed minimally of a platform, software, and a power source.[15]
- **Autonomy:** The level of independence that humans grant a system to execute a given task. It is the condition or quality of being self-governing to achieve an assigned task based on the system's own situational awareness (integrated sensing, perceiving, analyzing), planning, and decision-making. Autonomy refers to a spectrum of automation in which independent decision-making can be tailored for a specific mission, level of risk, and degree of human-machine teaming.[16]
- **Robotic and Autonomous Systems (RAS):** RAS is an accepted term in academia and the science and technology (S&T) community and highlights the physical (robotic) and cognitive (autonomous) aspects of these systems. For the purposes of this concept, RAS is a framework to describe systems with a robotic element, an autonomous element, or more commonly, both.[17]
- **Automated Weapons System (AWS):** A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.[18]

All three of these definitions have often been accompanied by terminology referring to a human-in-the-loop, human-on-the-loop, or human-out-of-the-loop.

- Human-in-the-Loop: **Semi-autonomous operation** where the machine performs a task and then waits for the human user to take an action before continuing.

---

[15] Chairman of the Joint Chiefs of Staff, *Joint Concept for Robotics and Autonomous Systems (JCRAS),* Washington, DC: October 16, 2016, pg. 2

[16] Ibid.

[17] Ibid.

[18] Department of Defense," Autonomy in Weapons Systems," *DoD Directive 3000.09, Change 1,* Washington, DC: May 8, 2017, pp. 13-14

- Human-on-the-Loop: **Supervised autonomous operation** where the machine can sense, decide, and act on its own. The human user supervises its operation and can intervene, if desired.
- Human-out-of-the-Loop: **Fully autonomous operation** where the machine can sense, decide, and act on its own. The human cannot intervene in a timely fashion.[19]

As previously indicated, industry has been forging ahead with autonomous applications, to the point where the National Institute of Standards and Technology (NIST) had to develop its own TOR to manage and regulate industry products and advancements. Those definitional terms are captured here:

Unmanned System (UMS)- ***or more recently, 'Uncrewed System'*****:**[20]

- A powered physical system, with no human operator aboard the principal components, acts on physical world for the purpose of achieving assigned tasks. May be mobile or stationary. May include any and all associated supporting components. Examples include unmanned ground vehicles (UGV), unmanned aerial vehicles (UAV), unmanned underwater vehicles (UUV), unmanned water surface borne vehicles (USV), unattended munitions (UM), and unattended ground sensors (UGS). Missiles, rockets, and their submunitions, and artillery are not considered UMSs.
    a. The first issue regarding the definition is, what is/are the minimum requirement(s) to be a UMS. The first-tier requirement may be a robotic vehicle without a human onboard. This robotic vehicle is the main entity in the UMS that receives and acts on the defined goals.
    b. The second-tier requirement may be regarding Human-Robot Interface (HRI). If the HRI devices exist and are integral parts of the functionality of the robotic vehicles, i.e., when these entities are needed for the goals, they are parts of the UMSs. In various application domains the HRI device may be called an Operator Control Unit (OCU) or a Ground Control Station (GCS). Ultimately, the goals assigned to UMS come from the HRI.
    c. The third-tier requirement may be whether the other associated manned or unmanned subsystems are integral parts of the functionality of the robotic vehicles. In other words, when these entities are needed for achieving the goals, then they are parts of the UMS. However, they must serve the supportive roles within the context of achieving the goals.
        i. Note that the supportive, manned subsystems might dominate in sheer physical sizes or in terms of the portion of the processing that they provide. The whole integral system should still be called a UMS. Similarly, when a hybrid or dual-use vehicle operates in the unmanned manner, it is considered a UMS, but not when it operates under manned control.
        ii. These point out that, in some situations, a robotic vehicle may be developed to be solely unmanned and is always considered a UMS, whereas in some other situations, a robotic vehicle may or may not be considered a UMS depending on how it is deployed and what assignments it is performing.

[19] Scharre, Paul, *An Army of None: Autonomous Weapons and the Future of War,"* W.W. Norton and Company, New York, NY: 2018, pp. 29-30

[20] It is important to note the current terminology recently proposed and in use utilizes the more gender-neutral descriptor of uncrewed versus unmanned. This is a direct quote from the NIST paper, so unmanned remains, but in all other Fidelium created products, the term uncrewed will be applied.

- Autonomy
    a. A UMS's own ability of integrated sensing, perceiving, analyzing, communicating, planning, decision-making, and acting/executing, to achieve its goals as assigned.
    b. We further define the stated, integrated "sensing, perceiving, analyzing, communicating, planning, decision-making, and acting/executing" as Root Autonomous Capabilities (RACs). Note that the essence of "UMS's own ability" is independent of human interactions.
    c. There are also discussions on whether the aspects of learning and world modeling should also be parts of the RACs. They should be resolved in the future workshops and may result in updates to the definition.
- Contextual Autonomous Capability (CAC) Model for Unmanned Systems
    a. A UMS's CAC is characterized by the missions that the system is capable of performing, the environments within which the missions are performed, and human independence that can be allowed in the performance of the missions.
    b. Each of the aspects, or axes, namely, mission complexity (MC), environmental complexity (EC), and human independence (HI) is further attributed with a set of metrics to facilitate the specification, analysis, evaluation, and measurement of the CAC of particular UMSs.
    c. This CAC model facilitates the characterization of UMSs from the perspectives of requirements, capability, and levels of difficulty, complexity, or sophistication. The model also provides ways to characterize UMS's autonomous operating modes. The three axes can also be applied independently to assess the levels of MC, EC, and HI for a UMS.
    d. The CAC encompasses the following layers of abstraction:
        i. At the low layers, a UMS is characterized by the metric scores, including the percentage of a mission that is planned and executed by the UMS onboard processors, the levels of task decomposition, how easy it is to find a solution in the operating environment, etc.
        ii. Above the metric layer, a UMS is characterized by the three scores for the aspects or axes, namely, MC, EC, and HI. These axis scores are weighted averages of the individual metric scores.[21] 'Autonomy,' as a distinctly separate topic from 'AI,' is discussed in separate Whitepaper entitled "Autonomy on the Battlefield: Defining Operational Expectations for Robotic Combat Vehicles'

So What? How does DoD visualize the future of AI within the Joint Force?

There are numerous strategies, concepts, and papers within the DoD family of strategy and planning, force design, and force development processes which highlight the importance of AI in future operational contexts. While the strategic guidance documents – NSS, NDS, CPG, NMS, JSCP, etc., -- within the department make some mention of AI, the general nature and paucity of detail associated

[21] Huang, Hui-Min, Elena Messina, James Albus, et.al., "Autonomy Levels for Unmanned Systems (ALFUS) Framework, "*NIST Special Publication 1011-II-1.0, National Institute for Standards and Technology,* Washington, DC: December, 2007

with those documents does not bear on the purpose of this paper. Instead, some analysis of the AI-specific strategies from the SECDEF, Joint Staff, and service levels will instead be the focus of this paper's analysis.

Department of Defense Artificial Intelligence Strategy:

DoD published its AI strategy in 2018. As the document notes in the preface, "The 2018 DoD AI Strategy will drive the urgency, scale, and unity of effort needed to navigate this transformation. The Joint Artificial Intelligence Center (JAIC)[22] is the focal point for carrying it out. As we systematically explore AI's full potential, study its implications, and begin the process of learning about its impact on defense, we will remain thoughtful and adaptive in our execution."[23] Within the strategy, the Department describes its strategic approach toward implementation.

1. **Delivering AI-enabled capabilities that address key missions:** We will launch a set of initiatives to incorporate AI rapidly, iteratively, and responsibly to enhance military decision-making and operations across key mission areas. Examples include improving situational awareness and decision-making, increasing the safety of operating equipment, implementing predictive maintenance and supply, and streamlining business processes. We will prioritize the fielding of AI systems that augment the capabilities of our personnel by offloading tedious cognitive or physical tasks and introducing new ways of working.

2. **Scaling AI's impact across DoD through a common foundation that enables decentralized development and experimentation:** One of the U.S. military's greatest strengths is the innovative character of our forces. It is likely that the most transformative AI-enabled capabilities will arise from experiments at the "forward edge," that is, discovered by the users themselves in contexts far removed from centralized offices and laboratories. Taking advantage of this concept of decentralized development and experimentation will require the Department to put in place key building blocks and platforms to scale and democratize access to AI. This includes creating a common foundation of shared data, reusable tools, frameworks and standards, and cloud and edge services. In parallel, we will take steps to ready existing processes for AI application through digitization and smart automation. Taken together, these enterprise-wide changes promote the spread of adaptable problem-solving using AI, increase the rate of experimentation and speed of delivery, and streamline the scaling of successful AI prototypes.

3. **Cultivating a leading AI workforce:** The transformative and rapidly advancing nature of AI requires that the Department adapt its culture, skills, and approaches. To succeed, we will encourage rapid experimentation, and an iterative, risk-informed approach to AI implementation. We will cultivate the talent of our existing workforce by investing in providing comprehensive AI training, while simultaneously bringing critical AI skills into service by recruiting and partnering with world-class AI talent.

[22] Now the Chief Digital and Artificial Intelligence Office (CDAO) led by Dr. Craig Martell.
[23] Department of Defense, *Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity,* Washington, DC: 2018, pg. 4

4. **Engaging with commercial, academic, and international allies and partners:** Strong partnerships are essential at every stage in the AI technology pipeline, from research to deployment and sustainment. We will work with academia and industry to help address global challenges of significant societal importance and make funding available to entice our best academics to invest in long-term research relevant to defense and remain in the business of educating the next generation of AI talent. We will enhance partnerships with U.S. industry to align civilian AI leadership with defense challenges while evolving our crucial international alliances and partnerships abroad. Further, we will engage with and contribute to the global open-source community to identify and advance emerging technologies and applications.

5. **Leading in military ethics and AI safety:** The Department will articulate its vision and guiding principles for using AI in a lawful and ethical manner to promote our values. We will consult with leaders from across academia, private industry, and the international community to advance AI ethics and safety in the military context. We will invest in the research and development of AI systems that are resilient, robust, reliable, and secure; we will continue to fund research into techniques that produce more explainable AI; and we will pioneer approaches for AI test, evaluation, verification, and validation. We will also seek opportunities to use AI to reduce unintentional harm and collateral damage via increased situational awareness and enhanced decision support. As we improve the technology and our use of it, we will continue to share our aims, ethical guidelines, and safety procedures to encourage responsible AI development and use by other nations.

In addition to the strategic approach, the 2018 DoD AI Strategy also outlines the strategic focus areas for AI implementation.

Delivering AI-enabled capabilities that address key missions

- **Improving situational awareness and decision-making** – AI applied to perception tasks such as imagery analysis can extract useful information from raw data and equip leaders with increased situational awareness. AI can generate and help commanders explore new options so that they can select courses of action that best achieve mission outcomes, minimizing risks to both deployed forces and civilians
- **Increasing safety of operating equipment** – AI also has the potential to enhance the safety of operating aircraft, ships, and vehicles in complex, rapidly changing situations by alerting operators to hidden dangers
- **Implementing predictive maintenance and supply** – We will use AI to predict the failure of critical parts, automate diagnostics, and plan maintenance based on data and equipment condition. Similar technology will be used to guide provisioning of spare parts and optimize inventory levels. These advances will ensure appropriate inventory levels, assist in troubleshooting, and enable more rapidly deployable and adaptable forces at reduced cost
- **Streamlining business practices** – AI will be used with the objective of reducing the time spent on highly manual, repetitive, and frequent tasks. By enabling humans to supervise automated tasks, AI has the potential to reduce the number and costs of mistakes, increase throughput and agility, and promote the allocation of DoD resources to higher-value activities and emerging mission priorities

Partnering with leading private sector technology companies, academia, and global allies and partners

- **Forming open mission initiatives focused on global challenges –** We will form open AI missions with academia and industry that will contribute to addressing global challenges of significant societal importance, such as operationalizing AI for humanitarian assistance and disaster relief for wildfires, hurricanes, and earthquakes. We will bring our data, domain expertise, and real-world problems to these public private partnerships, and combine efforts with a wide range of actors to produce inspiring AI technology that benefits society beyond the benefit of fulfilling our core defense mission. These open missions will challenge a broad community to advance the state of AI and learn how to operationalize the technologies on an integrated basis across domestic and international organizations. They will contribute to the development of thousands of new AI experts needed for public service over the next decade and spur future AI progress across multiple sectors.
- **Strengthening academic partnerships and seeding new AI innovation districts –** For academia, we will make longer-term, stable funding available to entice our best academics to invest in long-term research relevant to critical DoD areas and remain in the business of educating the next generation of AI talent. This entails increasing investment through existing channels, such as DARPA/IARPA and the Military Service Research Laboratories and sponsoring long-term discoveries relevant to the Department. It also involves stimulating the development of geographic concentrations of interconnected companies and institutions in AI. Strong and stable academic partnerships clustered in this manner will provide benefits to the Department, industry, and national competitiveness.
- **Enhancing partnership with U.S. industry –** Engaging with and strengthening the AI technology ecosystem requires us to experiment with a range of partnership models. These include bold new AI initiatives with large industrial partners, small start-ups, and venture capital firms. In addition, we will take steps to make it easier for members of the AI community to engage with the Department, for example, by working to accelerate critical partnership processes and lower administrative barriers. We will also establish a centralized AI portal for potential partners that details key processes, topics of interest, and contacts in order to streamline contracting, acquisition, and on-boarding processes.
- **Evolving international alliances and partnerships –** An extended network of mutually beneficial alliances and partnerships provides a durable means of overcoming global AI challenges, deterring aggression, and supporting stability through cooperation. Foreign allies and partners offer critical perspectives and talent that can be leveraged through personnel exchanges, combined portfolio planning, and the deepened interoperability and trust that comes from collaborative AI development and deployment. Engaging with the open-source community. The open-source community is a vibrant global incubator of talented individuals and transformative ideas. We will contribute our data, challenges, research, and technologies to this community and engage with the open-source ecosystem as a vehicle for attracting talent, identifying and advancing new AI technologies that can transform defense, and broadening our accessible technology base.

Cultivating a leading AI workforce

- **Offering the chance to make an impact –** DoD offers opportunities to develop cutting-edge AI applications to meet some of the Nation's most difficult and most consequential challenges, leveraging the latest technology to create positive real-world impact for U.S. forces and the society and freedoms that we defend**.**
- **Providing comprehensive AI training and cultivating workforce talent –** We will invest in developing the skills of our existing workforce and ensuring their career progression. The DoD workforce will have access to curated AI training programs designed to help them keep pace with AI developments in the private sector, accelerate the achievement of expertise, and give personnel the knowledge they need to adapt to new roles in the future. These AI training programs will be made widely available, from junior personnel to AI engineers to senior leaders, and will leverage digital content combined with tailored instruction from leading experts.
- **Bringing critical AI skills into service –** We will use streamlined, non-traditional pathways to bring world-class AI talent into service and expand access to outside expertise. This will complement our existing workforce with roles such as machine learning engineers, data engineers, data scientists, and AI product managers, in order to form a modern, agile, AI-advantaged workforce with a deep passion for addressing the world's most pressing challenges.
- **Building a culture that embraces experimentation –** We are building a culture that welcomes and rewards appropriate risk-taking to push the art of the possible: rapid learning by failing quickly, early, and on a small scale. Although embracing disruptive approaches will not be easy, doing so is imperative for implementing and adopting AI – which requires running experiments daily, iterating based on user feedback, measuring results, and continuously adapting.

Leading in military ethics and AI safety

- **Developing AI principles for defense –** The Department will articulate its vision and guiding principles for AI ethics and safety in defense matters. We will consult with a wide range of experts and advisors from across academia, the private sector, and the international community to learn as much as possible from past insights and existing approaches to AI ethics and safety. We will also continue to undertake research and adopt policies as necessary to ensure that AI systems are used responsibly and ethically.
- **Investing in research and development for resilient, robust, reliable, and secure AI –** In order to ensure DoD AI systems are safe, secure, and robust, we will fund research into AI systems that have a lower risk of accidents; are more resilient, including to hacking and adversarial spoofing; demonstrate less unexpected behavior; and minimize bias. We will consider "emergent effects" that arise when two or more systems interact, as will often be the case when introducing AI to military contexts. To foster these characteristics in deployed systems in both military and civilian contexts, we will pioneer and share novel approaches to testing, evaluation, verification, and validation, and we will increase our focus on defensive cybersecurity of hardware and software platforms as a precondition for secure uses of AI.
- **Continuing to fund research to understand and explain AI-driven decisions and actions –** We will continue funding research and development for "explainable AI" so users can understand the basis of AI outputs. This will help users understand, appropriately trust, and effectively manage AI systems.

- **Promoting transparency in AI research –** We will actively and continuously engage in an open dialogue and internationally collaborative research agenda concerning AI ethics, resilience, robustness, reliability, and security to reduce the chance of misperception, miscalculation, or accidents. This will promote responsible behavior.
- **Advocating for a global set of military AI guidelines –** We will engage in dialogue and articulate our vision for ethical and safe military AI use to the broadest-possible audience. To do this, we will build strong channels for military-to-military dialogue as well as exchanges among DoD, the private sector, academia, allies and partners, and the global AI community. Within the Department, we will continue operating in accordance with the law of war, and we will demonstrate responsible use of AI in accordance with our nation's values.
- **Using AI to reduce the risk of civilian casualties and other collateral damage –** We will seek opportunities to use AI to enhance our implementation of the Law of War. AI systems can provide commanders more tools to protect non-combatants via increased situational awareness and enhanced decision support.

Parsing this strategy document in addition to the Defense Responsible AI Strategy and Implementation Pathway discussed below will help inform industry and DoD components with development and implementation of AI strategies.

The Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway:

The DoD released its Responsible Artificial Intelligence Strategy and Implementation Pathway in June 2022. The resulting DoD RAI S&I Pathway is organized around six tenets: RAI Governance; Warfighter Trust; AI Product and Acquisition Lifecycle; Requirements Validation; Responsible AI Ecosystem; and AI Workforce. Organized around these tenets, the Pathway identifies lines of effort to:

1. Modernize governance structures and processes that allow for continuous oversight of DoD use of AI, taking into account the context in which the technology will be used;
2. Achieve a standard level of technological familiarity and proficiency for system operators to achieve justified confidence in AI and AI-enabled systems;
3. Exercise appropriate care in the AI product and acquisition lifecycle to ensure potential AI risks are considered from the outset of an AI project, and efforts are taken to mitigate or ameliorate such risks and reduce unintended consequences, while enabling AI development at the pace the Department needs to meet the National Defense Strategy;
4. Use the requirements validation process to ensure that capabilities that leverage AI are aligned with operational needs while addressing relevant AI risks;
5. Promote a shared understanding of RAI design, development, deployment, and use through domestic and international engagements; and
6. Ensure that all DoD AI workforce members possess an appropriate understanding of the technology, its development process, and the operational methods applicable to implementing

RAI commensurate with their duties within the archetype roles outlined in the 2020 DoD AI Education Strategy.[24]

As part of the implementation pathway, DoD will adhere to five enumerated ethical principles:

1. **Responsible**: DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
2. **Equitable**: The Department will take deliberate steps to minimize unintended bias in AI capabilities.
3. **Traceable**: The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedures and documentation.
4. **Reliable**: The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life cycles.
5. **Governable:** The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.[25]

A key quote from the document is, "Ultimately, DoD cannot maintain its competitive advantage without transforming itself into an AI-ready and data-centric organization, with RAI as a prominent feature."[26]

The remainder of the document outlines roles and responsibilities across the DoD, chief among them the Chief Digital and Artificial Intelligence Office (CDAO), an organization that supersedes the previous Joint Artificial Intelligence Center (JAIC). Within DoD, the CDAO will centrally coordinate all AI policies while allowing for decentralized execution across the various components and organizations. Of note, though, is how lean the DoD AI strategy and RAI pathway is on details regarding the exact purpose for AI within the department. For what will AI be used, and for what purpose? What is the overarching 'Why' of AI beyond outpacing our global competitors in this critical arena? What is the Department's overarching vision for AI in national security? The definitional terms captured above can give a hint toward what that 'Why' ought to be and the contours of how implementation might coherently proceed. This will be explored in the Challenges and Opportunities discussion in the next section.

Joint Chiefs of Staff Joint Concept for Robotics and Autonomous Systems (JCRAS):

The Joint Staff released its JCRAS in 2016 to provide broad concepts in directing DoD focus on RAS adoption and implementation by 2035. DoD has since recognized that timeframe is too long and has subsequently pushed for a 2025 timeframe for several RAS capabilities to be fielded. That said, the

[24] Hicks, Kathleen, *Responsible Artificial Intelligence Strategy and Implementation,* Department of Defense, Office of the Deputy Secretary of Defense, Washington, DC: June 2022, pg. 2
[25] Ibid., pg. 5
[26] Ibid., pg. 8

JCRAS nevertheless provides a window into DoD thinking and outlines several key precepts and concept informed capabilities. The central idea articulated in the JCRAS is:

> By 2035, the Joint Force will employ integrated Human-RAS teams in a wide variety of combinations to expand the Joint Force commander's options. This concept envisions a future Joint Force that capitalizes on technological advances to embed highly capable and interconnected RAS into every echelon and formation. RAS evolve from tools for basic tasks into team members capable of coordinating and collaborating across domains and Services. RAS play a central role in performing and supporting an extensive array of complex mission sets across the range of military operations.

Precepts:

1. **Employ Human-RAS Teams**: Humans and RAS will work together as complementary team members. Humans and RAS together will create new types of teams. Advances in human-machine collaboration, interoperability, and survivability will enable mutual support and seamless interaction between humans and RAS. The relationship will range from RAS performing tasks in support of humans, to RAS teaming with humans, to humans launching autonomous RAS capable of cooperative behavior.
2. **Leverage Autonomy as a Key Enabler and Match Autonomy to the Mission**: Greater autonomy has implications for both RAS and humans. Autonomy makes it possible to reduce unnecessary manual labor, increase the range of operations, reduce the time to conduct time-critical operations, and provide increased levels of operational reliability, persistence, and resilience.[27]
3. **Integrate RAS Capabilities to Develop Innovative Concepts of Operation:** As RAS perform more tasks, the sequence of actions and the risk calculus to the Joint Force and the mission will change. Joint Force commanders and planners must understand the unique capabilities, limitations, and advantages of RAS to develop innovative concepts of operations (CONOPS).

Concept Required Capabilities (greater detail for each can be found in the JCRAS document)**:**

1. **Human-RAS Teams Operating in the Future Environment:**
    a. Interoperability
    b. Survivability and Resilience
    c. Autonomy
    d. Teaming
    e. Functional Modularity
    f. Policy
2. **Leveraging Technology Development**
    a. Articulate Joint Force Requirements
    b. Leverage Commercial and non-DoD Development
    c. Joint Force Development of Military-Specific Capabilities
    d. Rapidly Field and Incorporate Technology

[27] United States Air Force Office of the Chief Scientist, *Autonomous Horizons: System Autonomy in the Air Force – A Path to the Future, Volume I, Human-Autonomy Teaming*, AF/ST TR 15-0, Washington D.C.: June 2015, pg. 1

Risk of Adopting the JCRAS:

1. Human operators and policymakers may not trust or understand RAS employment.
2. Policy, ethics, and law
3. Unmitigated Network/Cyberspace vulnerabilities pose a risk of failure
4. Risk of escalation and unintended consequences
5. Global proliferation of technology may limit operational advantages
6. Risk to integration with Allies and Partners
7. Risk of diminishing Joint Force capability and capacity

U.S. Army Robotics and Autonomous Systems Strategy (RAS):

The Army published its RAS strategy in March, 2017. It outlines five capability objectives, three temporally based priorities for the near-term, mid-term, and far-term horizons, a recommended process for implementation, and the Army Warfighting Challenges (AWfC) which application of RAS capabilities can help mitigate.

Capability Objectives:

1. Increase Situational Awareness
2. Lighten the Soldiers' physical and cognitive workloads
3. Sustain the force with increased distribution, throughput, and efficiency
4. Facilitate movement and maneuver
5. Protect the force

Priorities:

1. **Near-Term (2017-2020)**:
    a. Increase situational awareness for dismounted forces at lower echelons
    b. Lighten the physical load for dismounted forces
    c. Improve sustainment with automated ground resupply
    d. Facilitate movement with improved route clearance
    e. Protect the Force with EOD RAS platform and payload improvements
2. **Mid-Term (2021-2030):**
    a. Increase situational awareness with advanced, smaller RAS and swarming
    b. Lighten the load with exoskeleton capabilities
    c. Improve sustainment with fully automated convoy operations
    d. Improve maneuver with unmanned combat vehicles and advanced payloads
3. **Far-Term (2031-2040)**
    a. Increase situational awareness with persistent reconnaissance from swarming systems
    b. Improve sustainment with autonomous aerial cargo delivery
    c. Facilitate maneuver with advancements to unmanned combat vehicles

Development Process for RAS:

1. **Sustain current systems**
    a. Maintain current fleet of tele-operated UGSs and remotely piloted UAS
    b. Recapitalize older robots
2. **Improve existing systems**
    a. Field a universal controller for legacy and new programs
    b. Field autonomous technologies within UGS and UAS where possible
    c. Refine automated ground resupply operations as the Army's first semi-autonomous vehicle
3. **Develop new capabilities**
    a. Develop off-road autonomy for unmanned combat vehicles
    b. Develop swarming for advanced reconnaissance
    c. Develop artificially intelligent augmented networks and systems
4. **Replace obsolete systems**
    a. Replace non-standard equipment systems with new programs of record
    b. Replace manned systems with unmanned systems to allow Soldiers to perform other tasks
5. **Assess new technologies and systems**
    a. Continue assessments on the state of UGS and UAS autonomy to ensure systems progress with available technology
    b. Determine where technologies can serve cross-domain solutions, especially with new payloads

Army Warfighting Challenges for RAS Applications:

1. **AWfC 1 - Develop Situational Understanding**
    a. RAS improve reconnaissance and security operations by focusing on terrain and enemy forces, by developing the situation, and by protecting the force through early and accurate warning. RAS also increase situational awareness in complex environments through reconnaissance and mapping of sub- and supersurface environments. RAS collects and processes raw data (e.g., full motion video) to produce intelligence such as visualization of a potential adversary with a location identifier. Such information helps shape and identify hazards, providing leaders with better situational awareness and improved understanding
2. **AWfC 7 - Conduct Space and Cyber Electromagnetic Operations and Maintain Communications:**
    a. RAS will provide unmanned air and ground communications relays and support uninterrupted access to critical data links. Potential enemies are developing cyber-electromagnetic and space capabilities (such as disruptive and destructive malware, and electronic warfare systems and anti-satellite weapons) to disrupt, jam, spoof, and hack communications and precision navigation and timing systems.
3. **AWfC 11 - Conduct Air-Ground Reconnaissance and Security Operations:**
    a. RAS provide persistent surveillance and reconnaissance with unmanned systems allowing units to conduct security operations across a wider area for longer durations while enabling Soldiers to focus on other missions. Future systems employ advanced technologies to extend endurance and standoff.

4. **AWfC 12 - Conduct Joint Expeditionary Maneuver and Entry Operations:**
    a. UGS and UAS equipped with mission payloads and armaments will conduct reconnaissance based on tasks given by the operator. High-definition sensors will integrate threat detection, queuing, and imagery over an integrated network in degraded visual environments for extended duration in areas inaccessible by Soldiers. Use of unmanned systems in mounted and dismounted maneuver formations leads to smaller platforms that are more mobile and transportable, enabling greater expeditionary maneuver capability.
5. **AWfC 13 - Conduct Wide Area Security:**
    a. See AWfC 15 below
6. **AWfC 15 - Conduct Joint Combined Arms Maneuver:**
    a. RAS contribute to AWfC 13 and 15 by conducting persistent surveillance of enemy avenues of approach, terrain denial with anti-armor robotic platforms, and targeting data collection to support indirect and direct fires. RAS provide units and teams with protection and standoff from IEDs and other explosives through detection, diagnostics, identification, neutralization, and render safe capabilities. RAS support operations to enhance friendly force freedom of action, shape terrain, and control enemy movement.
7. **AWfC 16 - Set the Theater, Sustain Operations and Maintain Freedom of Movement:**
    a. RAS augment sustainment operations with autonomous ground and aircraft systems. Associated sensors, computers and decision support tools aid navigation, route selection, vehicle control, and vehicle management such as speed, intervals, and obstacle avoidance. They also conduct triage and evacuate casualties under fire. Autonomous aircraft systems provide increased resupply capabilities while reducing manning requirements.
8. **AWfC 17/18 - Employ Cross-Domain Fires:**
    a. RAS contribute to both AWfC 17/18. UAS have demonstrated the potential to generate accurate targeting locations for precision fires and the ability to report battle damage assessments. By employing next generation sensors and shooters, RAS achieve real-time integration and optimization of targeting data for a range of fires applications. RAS fuse data from all joint, national, and multinational sensors from space to subterranean to achieve real time integration and optimization of targeting data. RAS enable forces to move accurately and quickly track and defeat targets, match targets with effects, and coordinate capabilities.
9. **AWfC 19 - Execute Mission Command:**
    a. RAS will facilitate mission command by collecting, organizing, and prioritizing immense amounts of data to aid decisions making. RAS will also improve command post tactical mobility while reducing the cyber, electronic, and physical signature.

Apart from the Army's well-articulated strategy, the Air Force, Navy, and Marine Corps have each developed their own strategies for AI implementation and are largely in line with the strategies listed above. The Space Force is currently in development of its AI strategy at the time of this writing. In the follow-on Part 2 of this Whitepaper series, we will explore the challenges and opportunities of adopting AI in DoD applications.