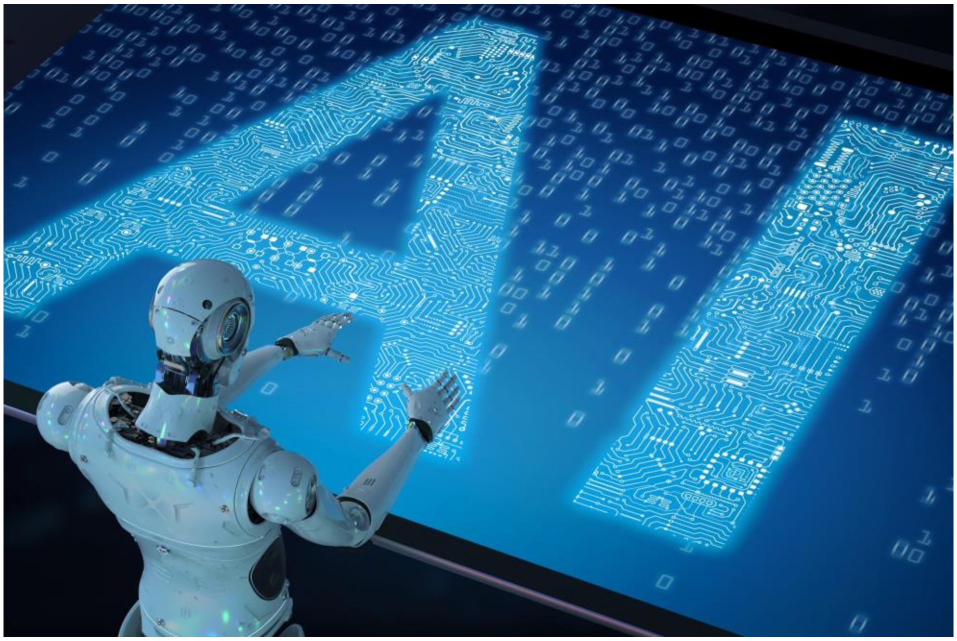

A DESIGN APPROACH FOR AI IMPLEMENTATION ACROSS DOD: Challenges and Opportunities

ABSTRACT

Due to the rapidly shifting technological advances in warfare in the 21st Century, DoD needs to embark upon a comprehensive reassessment of its objectives, structure, practices, warfighting concepts, and doctrine to maintain critical competitive advantages in AI and Autonomy in strategic competition against near peer nations. This second chapter in this two-part Whitepaper series explores challenges, opportunities, and conclusions on the importance of inserting AI capabilities into DoD. The time to act now.

Matthew Dooley and Grant Highland, Ph.D.

Fidelium, LLC

Challenges and Opportunities Associated with DoD AI Adoption

In Part One of this two-paper series, the authors explored the background, definitions and doctrinal implications for inserting AI in DoD. As with any complex topic, words have meaning, and coming to a common understanding and lexicon for what we mean when we say “artificial intelligence” is critical first step before crossing into the much harder task of defining operational requirements for AI on the battlefield. This second paper in this series dives deeper into the challenges and opportunities, once we have successfully settled on proper definitions and dogma. Ultimately, the most important element in this ongoing discussion of integrating AI in DoD is in selection of performance capabilities and objects. What precisely is it that we want AI to do for us on the battlefield? The elements of Operational Design may provide us the logical analytical framework we need to answer that question.

Defining Challenges

The DoD faces six primary challenges in meeting its vision for AI implementation department wide. These challenges encompass technology and testing, personnel, computing infrastructure, data, policy, and budgeting processes. Beyond these, the DoD also suffers from bureaucratic inertia, cultural biases, incentives based on past performance versus future innovation, as well as the management complexity inherent in an organization the size and scope of the DoD enterprise. While the latter issues mentioned are beyond the scope of this paper, it is encouraging to note the tide is slowly beginning to turn in those domains.

1. Technological Innovation and Reliable Testing

The DoD currently lacks a trusted system for testing and evaluating AI and ML security. The lack of a common trusted testing system leaves many AI and autonomy products open to spoofing and exploitation. For example, researchers have discovered that computer vision systems for autonomous vehicles can be easily deceived by placing a sticker over a stop sign, causing the car to mistake stop signs for speed limit signs. Without its own system for testing for these issues, the DoD is leaving itself vulnerable to potentially catastrophic accidents. At minimum, it will be impossible for it to accurately evaluate the quality and safety of AI products that it procures from vendors.

Moreover, the DoD acquisitions process is not designed for the high level of experimentation and modification necessitated by AI. Instead, it assumes that products are ready for use once procured. However, as the stop sign example above demonstrates, this does not hold true for AI, which needs to be constantly improved upon as new data becomes available and new vulnerabilities are uncovered.[28] Another interesting dynamic in this realm is the responsible and moral application of the use of force. Whereas in the past commanders assumed responsibility for the ethical use of newly fielded weapons systems -- the burden of adherence to the LOAC and IHL resting in their judgment on how, when, and where to use military force – with AI this relationship may be transferred to the engineers and developers responsible for the algorithms used in their systems. Should a system or capability be fully autonomous, then this is an ethical and moral dimension which will have to be clearly delineated and enforced with industry and systems developers.

2. Personnel- *AI Literacy/Competency/Accountability*

The DoD lacks a larger enough workforce with foundational AI literacy, which hinders its ability to successfully acquire and deploy AI. There is a growing body of subject matter experts, but it is not yet enough to reach the critical mass necessary for rapid development. Despite recognizing this deficiency, DoD efforts to recruit new talent knowledgeable about AI face challenges. First, where these employees will work within the components—the agencies,organizations, and military services included under the DoD umbrella—is unclear. Second, managers tasked with recruiting qualified technical talent often do not possess the foundational knowledge necessary to assess candidates' qualifications. Third, some in the defense community are resistant to cultural changes that could be necessary to build a technical workforce, and their arguments against incorporating new skillsets into the workforce are often hyperbolic and rely on stereotypes of STEM professionals. The most prominent of these stereotypes is that the cyber community dislikes hierarchy, which would make it incompatible with the famously bureaucratic DoD. Fourth, the DoD is not competing for technical talent in a vacuum or solely against U.S. firms, which usually pay more and offer greater flexibility.[29]

3. Computing Infrastructure and Data

The DoD struggles to implement up-to-date software because DoD processes do not incentivize leaders to update and modernize IT equipment, operating systems, computing power, and software packages at the pace necessitated by the current rate of technological evolution. System permissions are also not readily available to DoD employees. For example, Python is a computer language widely used in machine learning, yet DoD computers do not come with Python installed nor do employees have administrative permissions to download it. The DoD also struggles to integrate AI with legacy systems that are not readily compatible with modern computing capabilities. Legacy systems include antiquated hardware, such as floppy disks (which the DoD used to control the U.S. nuclear arsenal until June 2019), and old pieces of software that have not been updated for possibly decades. The legacy systems that the department chooses to keep will not be modernized overnight and are not going away any time soon.

The data-scarce environment of the DoD is another hurdle to successful AI adoption. Often, the data required for AI systems is simply not gathered. The data that does exist is frequently “dirty”—siloed, flawed, and unstructured—making it largely unusable for machine-learning applications.

4. Policy and Guidance

The DoD has fallen behind on communicating with the public about how it will use AI under existing policy. This is partly due to a lack of AI understanding in the general public combined with unclear technical terminology. The conversation surrounding AI often uses the phrases artificial intelligence, autonomy, autonomous, and automation interchangeably. These concepts are distinct but overlapping, blurring the differences between systems. For example, is a suicide drone meaningfully distinct from a loitering cruise missile? Do rules-based systems of decades past count as AI when compared to machine learning-enabled systems? Moreover, due in part to the variety of terms included under the AI umbrella, the total number of AI projects that exist—let alone the dollar value of those projects—is unclear to the public.[30]

While section III. above demonstrates the Department is grappling with the policy and guidance issue, it is still in its infancy and lacking in the appropriate delineation of means (from the ends-ways-means template for strategy articulation) necessary to bring the Department's articulated desires to fruition. Similarly, structured concepts (beyond the Army's RAS strategy) illustrating how AI will be integrated into the seven joint warfighting functions (C2, Information, Intelligence, Movement and Maneuver, Fires, Sustainment, and Protection) have yet to be developed. While there is mention of aspects of these functions in the strategies discussed above, there still remains a dearth of cohesive articulation regarding how, and for what purposes, AI will be integrated with – and perhaps create new – warfighting functions and concepts of operation.

5. Budget Considerations

The necessarily labyrinthine and complex budgeting system for DoD is called the Planning, Programming, Budgeting and Execution System (PPBES) and includes all DoD components and Congress in the deliberation over current and future requirements, authorization from Congress on those desired requirements, and appropriation of funds from Congress to fund and implement DoD's budget request. A brief description of this process is provided below:

PPBE Phases, Actors, and Outputs[31]

PPBE comprises four separate, but interrelated phases: planning, programming, budgeting, and execution. Each phase typically involves certain actions, officials, and outputs:

- **Planning:** During the planning phase, the USD Policy assesses strategic guidance (e.g., the President's National Security Strategy; the Secretary of Defense's National Defense Strategy; and the CJCS's National Military Strategy) and coordinates the Defense Planning Guidance (DPG) detailing force development priorities that inform the programming phase
- **Programming:** During the programming phase, the Director of Cost Assessment and Program Evaluation (CAPE) reviews the Program Objective Memorandum (POM) developed by each DoD component. The POM is a funding plan that describes proposed resource requirements (forces, personnel, and funding) over five years and adjusts programs in the Future Years Defense Program (FYDP) database. At certain points throughout the year, OSD works with DoD components to make changes to programs through Resource Management Decisions (RMDs)
- **Budgeting:** During the budgeting phase, the DoD Comptroller reviews the Budget Estimate Submission (BES) developed by each DOD component. The BES covers the first year of the POM and adjusts amounts in the FYDP. The output is the DoD portion of the President's budget request to Congress. At certain points throughout the year, particularly in the fall, OSD works with the White House Office of Management and Budget (OMB) to make changes to budgets through Resource Management Decisions (RMDs)
- **Execution:** During the execution phase, officials in OSD and the DOD components adjust resources, typically through transfer and reprogramming actions that require congressional notification and/or prior approval.

Since budgeting within the Department is based upon five-year increments, the adaptability and flexibility necessary to fund advanced technology that evolves and matures in much shorter timelines is problematic at best. The processes including money allocation, planning lead times, and compromising among competing priorities present challenges to AI adoption. In an IBM and GovLoop survey of DoD and intelligence professionals on the challenges of data readiness and new technologies such as machine learning, forty-nine percent of respondents reported the budget was their primary constraint (the additional response options were lack of skills, unsure which is best, not a priority, and cultural issues). Additionally, strategy documents do not grant the CDAO the authority to allocate funding and resources. It can incentivize and support AI initiatives but cannot force the armed services to start AI projects. How the CDAO will encourage AI adoption is unclear, though mentioned above in very general

terms. Also, the U.S. government's planning period is too long to allow for immediate, widespread AI technology use, and the measures called for by various AI strategies require at least two years' lead time.[32]

6. Trust- *Individual/Organizational*

As with the adoption of any new technology or capability, trust will have to be earned both within DoD and across the political spectrum of the populace who elect officials as their representatives in DC. A lack of trust will either result in slow adoption of new capabilities, or a refutation of those capabilities' ethical or moral justification with potentially catastrophic effect to national security. In many cases as it pertains to AI, ignorance (in its truest, non-pejorative sense) coupled with sensationalist depictions in popular culture often warp public perception of what AI is, what it is capable of, and what it is not. Education and transparency within DoD and publicly will be the only way to ameliorate those fears and allow DoD to pursue this critical warfighting capability.

<u>Opportunities to Leverage</u>

The Council on Foreign Relations determined steps DoD could take to mitigate some of the challenges highlighted above:

- First, the department should modernize its computing infrastructure, software procurement efforts, and data architecture. The Defense Department needs modern IT as well as the flexibility to acquire and experiment with new software. The department should implement the recommendations provided in the DIB's Software Acquisition and Practices to address these challenges. Successfully tackling the dirty data challenge would significantly improve the department's ability to work with AI and provide valuable experience in solving a core problem that many AI users face.[33]
  Progress has been made on this front as described by the GovConWire website, where the Defense Advanced Research Projects Agency's Strategic Technology Office, is focusing on improving the agency's AI and Industrial Internet of Things capabilities by dismantling monolithic, centralized platforms in favor of a more distributed, disaggregated strategy referred to as "Mosaic Warfare." Additionally, despite cultural challenges, Maj. Gen. Matthew Easley, chief information security officer and director of cybersecurity for the U.S. Department of the Army, said the United States, across most key areas, remains a great competitor regarding AI capabilities. Also, recent strides in AI capabilities fostered through public-private collaboration include the Booz Allen Hamilton-Databricks partnership formed last year.

Databricks' Lakehouse Platform offers federal and industry customers a unified AI platform as a way to tackle the exponentially increasing financial burden of AI model training and enterprise integration.[34]

- Second, the DOD needs to actively invest in innovation where the private sector is not incentivized to focus. The department should prioritize research and investment in security, verification and validation, test and evaluation for machine-learning systems, and AI-specific microprocessors. Further, as the United States and its adversaries increasingly adopt AI technologies, the department should prioritize research on counter-AI techniques to protect its own assets and exploit vulnerabilities in targets.[35]

- Third, the department should task all organizations that have a stake in AI development and deployment with demonstrating return on investment of money allocated for AI. The department should prioritize efforts to identify metrics to accurately assess AI program success and routinely collect data related to the metrics it identifies. As the AI hype cycle slows and trade-offs are made among competing priorities, the department will need to account for its investment in AI to itself, Congress, and the American people.[36] Assessment is the coin of the realm for any initiative requiring funding and successful application. And if AI lives up to the promise of its abilities, then that assessment process will become far easier in the future.

- Fourth, the DOD should focus on the talent pipeline for both military and civilian personnel. First, it should address security clearance processing times and reform hiring authorities to better suit the realities of the information age job market. Though the 2020 National Defense Authorization Act requires processing times of 30 days or fewer for a secret clearance and 90 days or fewer for a top secret clearance by December 2021, the processing time for secret clearance averaged 234 days and top secret averaged 422 days as of mid–FY 2019. Second, because the DOD is at a disadvantage on salary for roles like software engineers compared to the technology sector, it should follow the example of the Department of the Treasury's Office of Financial Research, the Securities and Exchange Commission, and the Federal Reserve. In order to compete with the high-paying private financial sector, these federal entities have the authority to hire federal regulators on a pay scale separate from the General Schedule (GS) pay scale. Though maybe not equivalent to private sector pay, a dedicated STEM pay scale coupled with signing and performance bonuses would make the DOD more competitive for technical talent. Finally, placement, retention, and professional development are critical for keeping talent once hired. The department should create a STEM career track tailored to technical career growth milestones for both early- and mid-career professionals to address challenges in retention.[37]

  Discussions concerning talent management within the military have increasingly included the need to train and retain technologically gifted personnel. Beyond the pay disparity discussed above, the differences in warfighting roles between ground, air, or naval combatants, and those involved in the more technical realms of data science, cyber operations, space operations, and the adoption of AI-enabled operations, the standard fitness requirements and advancement milestones will have to be re-evaluated.

In addition to the opportunities the Department should explore above, the impetus to reconceptualize what warfare in the 21st Century should look like needs to be fostered and rewarded. Innovators from our past, like George Patton, Billy Mitchell, Curtis LeMay, Hyman Rickover, or Robin Olds, should be heard, embraced, advanced, and funded should their ideas have merit. While the need for legacy concepts of maneuver warfare will certainly play a role in the nation's security into the future, the instantaneity and simultaneity of the networked, interconnected, and information-soaked reality of our current era demands new prioritization in warfighting functions and concepts of operation. If Ukraine is to provide any lessons, it is that aggregated information warfare and new operational concepts integrated with legacy systems may just be the key to victory in future wars.

An Operational Approach for AI Adoption in DoD

The principles of joint operations and the joint warfighting functions captured in joint doctrine provide a useful template for illustrating and illuminating AI use in terms well-understood across the Department, and provides clarity on the various military purposes for which AI can be pressed into service. Above all, the adoption of AI into military applications must be tied to clearly understood capability objectives that govern the intended endstate; to whit, "for what ultimate operational purposes are we adopting AI?" This may be best framed by filtering this question through the lens of the Principles of Joint Operations:[38] These principles are as follows:

Objective

The purpose of military operations is to achieve the military objectives that support attainment of the overall political goals of any conflict. This frequently involves the destruction of the enemy armed forces' capabilities and their will to fight. The objective of joint operations not involving this destruction might be more difficult to define; nonetheless, it too must be clear from the beginning. Objectives must directly, quickly, and economically contribute to the purpose of the operation. Each operation must contribute to strategic objectives. JFCs should avoid actions that do not contribute directly to achieving the objective(s).

Establishing clearly defined capability objectives for AI integration into military applications should be the initial starting point for any exercise in developing and integrating AI technologies into DoD. Establishing clarity in our objectives focuses development efforts, saves precious time and RDT&E resources, short circuits the "complexity worship idea traps" often associated with solving wicked problems, and prevents mission creep into operational areas we are not trying to solve. The beginning of any mission analysis seeks to understand the operational environment using the tenets of JP 2-01.3, Joint Intelligence Preparation of the Operational Environment. This four-step process (Define the Operational Environment; Describe the Impact of the Operational Environment; Evaluate the Adversary and other Relevant Actors; and Determine Adversary and other Relevant Actor Courses of Action) aids in understanding the political, military, economic, social/cultural, infrastructure, informational, and geographic/meteorological realities surrounding the enemy's capabilities, location, will, etc. This creates shared understanding across the joint force to better enable knowledge of the political and military objectives required for successful military operations. In practical application for the integration of AI into military service, the notion of clarity of objective fits perfectly.

There are numerous operational applications where AI would be of tremendous benefit. Here are a few capabilities of most immediate impact:

- ***Differential Understanding Advantage*** (DUA) against adversaries. AI enabled data aggregation and analysis would enable friendly forces to rapidly inform accurate analysis of the operational environment, evolving threat forces, our own weaknesses and strengths, and battlefield opportunities as they arise
- ***Differential Decision Advantage*** (DDA) against adversaries. AI tasked with aiding in decision-making could assist commanders and their staffs in understanding the complexities of the operational environment faster than the enemy, to better develop courses of action for attainment of the tactical objective. AI decision making aids can help commanders cut through the uncertainty of current battlefield events "what's happening now" as well as projecting "what's about to happen," providing estimated percentages in accuracy and likelihood certainties so commanders can pick their best options instead of merely guessing. AI enabled DDA also helps commanders cut through the fatigue, distractions, fear, emotion and other human issues that come with making decisions in combat under prolonged duress
- ***Differential Execution Advantage*** (DEA) against adversaries. AI enabled commanders and their staffs could use AI enabled DEA to better orchestrate the maneuver of their organizations taking advantage of increased certainty of action and providing clearer, decisive orders. This would accelerate the "Clock-Speed" of battlefield tempo exponentially. DEA enabled commanders act faster, via the assurances provided by AI enhanced precision Situational Awareness, precision intell products, and an accelerated and more efficient Kill Chain methodology. Commanders will move faster than the enemy because they see the battlefield better than the enemy, can accept more risks than him, and can sustain constant pressure on the enemy he cannot contest
- ***Differential Coordination Advantage*** (DCA) against adversaries. JADC2/All-Domain Operations where the AI enabled network (or the internet of military things, or IoMT) would empower autonomous systems, decision-makers, and the joint force would enable commander to bring massed effects onto the objective with speed and relevance faster than the enemy
- ***Differential Strategic Advantage*** (DSA) against adversaries. In the case of political objectives, AI enabled DSA, through the use of informational, cyber, space, intelligence, and other non-kinetic means, could serve as a powerful deterrent to prevent adversaries from advancing toward open conflict. Essentially, our forces deployed forces would enjoy the advantage of support from an AI capability that sees and predicts threat forces' intent and movements before they can get into position, allowing other elements of national power, i.e. diplomacy and economic levers to either prevent the fight before it begins or prevent strategic/operational/tactical surprise should conflict begin.

Mass

In order to achieve mass, appropriate joint force capabilities are integrated and synchronized where they will have a decisive effect in a short period of time. Mass often must be sustained to have the desired effect. Massing effects of combat power, rather than concentrating forces, can enable even numerically inferior forces to produce decisive results and minimize human losses and waste of resources

The U.S. went away from quantity in favor of exquisite technological quality in the prosecution of its warfighting aims, but as the old saying goes, quantity has a quality all its own, especially in attrition-style warfare. What AI can bring to this principle is the merging of both; to whit, a "return of Mass to the battlefield." AI harnessed to battlespace management and assisting in command and control of maneuver and fires, for both crewed and uncrewed assets, will accelerate and enhance lethality. Many of the strategies listed above herald AI-enabled platforms' ability to provide long-range ISR, decoy or deception, distributed all-domain swarming, etc. This mass, coupled with the relatively cost-effective nature of those high-tech platforms should they be lost in the prosecution of their missions, will better preserve military end strength normally associated with crewed platforms conducting the same missions.

Offensive

Offensive action is the most effective and decisive way to achieve a clearly defined objective. Offensive operations are the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results. The importance of offensive action is fundamentally true across all levels of war.

In the future operating environment, gaining the initiative will mean the difference between victory or defeat. In the compressed timelines of hypersonic, algorithmic, and informational warfare, the battlespace geometry of the past measured in weeks, days, or hours will be compressed into minutes, seconds, and nanoseconds. He who sees first, understands first, and acts with precision and appropriate force will win. Comprehending, assessing, deciding, and then acting within this milieu will easily and rapidly overwhelm human cognition. Only a properly conceived application of AI capabilities and its attendant ability to process information at the speed of light will ensure the initiative can be sustained in offensive operations.

Surprise

Surprise can help the commander shift the balance of combat power and thus achieve success well out of proportion to the effort expended. Factors contributing to surprise include speed in decision-making, information sharing, and force movement; effective intelligence; deception; application of unexpected combat power; OPSEC; and variations in tactics and methods of operation.

As previously mentioned, AI and autonomous systems can assist with military deception, distributed operations to overwhelm an enemy's understanding and decision-making, provide flexible force allocation and delivery of effects across all the warfighting domains, and allow for assessment and reassessment based on data feeds and relevant enemy actions to recommend alternative force allocations or courses of action in real time.

Economy of Force

Economy of force is the judicious employment and distribution of forces. It is the measured allocation of available combat power to such tasks as limited attacks, defense, delays, deception, or even retrograde operations to achieve mass elsewhere at the decisive point and time.

Another central idea behind JADC2/All-Domain warfare. See Surprise above.

Maneuver

Maneuver is the movement of forces in relation to the enemy to secure or retain positional advantage, usually in order to deliver—or threaten delivery of—the direct and indirect fires of the maneuvering force. Effective maneuver keeps the enemy off balance and thus also protects the friendly force. It contributes materially in exploiting successes, preserving freedom of action, and reducing vulnerability *by continually posing new problems for the enemy.*

AI will help accelerate the clock speed of ground maneuver forces. US ground forces will operate inside the "OODA loop" (Observe, Orient, Decide, Act) of their enemies, as AI will enable commanders to understand the location and disposition of enemy forces early. From there, commanders will be able to see the battlefield with greater clarity and thus exploit enemy weaknesses. With AI assistance, ground forces will move to positions of advantage faster than their enemies, engage and destroy targets of their choosing, and exploit breakthroughs and pursuit of fleeing forces with greater security and confidence. A unit so equipped with AI will be like fighting an opponent who seemingly knows what you are going to do two moves before you do.

Unity of Command

Unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose. During multinational operations and interagency coordination, unity of command may not be possible, but the requirement for unity of effort becomes paramount. Unity of effort—the coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—is the product of successful unified action.

This is the driving premise behind all-domain operations and JADC2. As mentioned above, if AI were to be utilized within the JADC2 framework, then data aggregation between sensor platforms, sense-making, and decision-making would all take place much more quickly and efficiently facilitating speed of relevance actions in the time and space compressed battlefield of the future. Similarly, autonomous systems within the operating area would more quickly sense, detect, identify, target, and respond to threats than their human counterparts.

Simplicity

Simplicity contributes to successful operations. Simple plans and clear, concise orders minimize misunderstanding and confusion. When other factors are equal, the simplest plan is preferable. Simplicity in plans allows better understanding and execution planning at all echelons. Simplicity and clarity of expression greatly facilitate mission execution in the stress, fatigue, fog of war, and complexities of modern combat, and are especially critical to success in multinational operations.

If clarity is the essence of simplicity, then adequate information is the essence of clarity. As already described above, AI-enabled analysis and decision tools will distill otherwise chaotic and overwhelming data streams into clear analyses which will provide the clarity necessary for decision-makers and commanders to transmit their intent to subordinate or coalition forces. Complexities and the fog of war will always be a factor in warfare – AI is no magical panacea – but sound implementation, concepts, exercises, and adoption of AI capabilities will help mitigate the scope and impact of these realities.

Security

Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Staff planning and an understanding of enemy strategy, tactics, and doctrine enhance security. Risk is inherent in military operations. Application of this principle includes prudent risk management, not undue caution.

Autonomous systems will increasingly be able to perform tasks normally performed by human crewed systems. From defensive measures to protect rear area posts, or formations of units converging on an objective, to supply, reconnaissance, surveillance, medical evacuation, etc., autonomous vehicles and capabilities will remove scores of personnel from vulnerable or otherwise risky endeavors allowing for more focus on force protection and offensive operations.

Restraint

A single act could cause significant military and political consequences; therefore, judicious use of force is necessary. Restraint requires the careful and disciplined balancing of the need for security, the conduct of military operations, and the national strategic end state. For example, the exposure of intelligence gathering activities, such as interrogation of detainees and prisoners of war, could have significant political and military repercussions and should be conducted with sound judgment. Excessive force antagonizes those parties involved, thereby damaging the legitimacy of the organization that uses it while potentially enhancing the legitimacy of the opposing party.

This could arguably be the most potentially problematic principle when employing AI-related systems. Without a human in or on the loop to adjudicate target recommendations, there exists the possibility fully autonomous systems might erroneously engage targets, or otherwise misread or misinterpret actions in the operating area resulting in engagements inconsistent with the LOAC and IHL principles. This is one area where concepts of operation which detail the types, numbers, and environments in which AI systems are to be utilized is critical.

Perseverance

Perseverance involves preparation for measured, protracted military operations in pursuit of the national strategic end state. Some joint operations may require years to reach the termination criteria. The underlying causes of the crisis may be elusive, making it difficult to achieve decisive resolution. The patient, resolute, and persistent pursuit of national goals and objectives often is essential to success. This will frequently involve diplomatic, economic, and informational measures to supplement military efforts.

Robots do not sleep. They do not require sustenance (other than charging and periodic maintenance). They do not possess emotions or distractions from home during long deployments which could compromise their mission execution. In other words, AI-enabled capabilities are the ultimate persistence and presence options for sustained military operations. Long-term loitering, concealed long-term reconnaissance or intelligence gathering, or passive placement until sensing enemy movement and then reacting to contact, these are all possibilities on the future battlefield where the limitations and psychological stresses normally associated with human operators are obviated and replaced by robotic team members who can dispassionately “stand the watch.”

Legitimacy

Legitimacy, which can be a decisive factor in operations, is based on the actual and perceived legality, morality, and rightness of the actions from the various perspectives of interested audiences. These audiences will include our national leadership and domestic population, governments, and civilian populations in the operational area, and nations and organizations around the world.

Committed forces must sustain the legitimacy of the operation and of the host government, where applicable. Security actions must be balanced with legitimacy concerns. All actions must be considered in the light of potentially competing strategic and tactical requirements, and must exhibit fairness in dealing with competing factions where appropriate. Legitimacy may depend on adherence to objectives agreed to by the international community, ensuring the action is appropriate to the situation, and fairness in dealing with various factions. Restricting the use of force, restructuring the type of forces employed, and ensuring the disciplined conduct of the forces involved may reinforce legitimacy.

This can be considered in the context of restraint described above. While drone strikes in the past have raised questions about the legitimacy of U.S. actions abroad, the use of AI-related systems in future contexts will likely be even more vociferously questioned and denounced. Again, this will require the Department to engage in departmental, public, and international transparency using detailed rules of engagement, concepts of operation highlighting the types of AI-enabled capabilities and where, when, and how they will be employed (to the extent national security allows), to ameliorate doubt. If AI can be shown to statistically guarantee greater precision in targeting and lethal application than human controlled assets alone, there may an opportunity to show AI as an improvement to managing collateral damage. Again, it is the fog of war that so often leads to unintended death and destruction. AI may help clear battlefield uncertainties in specific use cases where humans alone might make more mistakes.

Joint Functions:[39]

Command and Control:

C2 encompasses the exercise of authority and direction by a commander over assigned and attached forces to accomplish the mission. The JFC provides operational vision, guidance, and direction to the joint force. The C2 function encompasses a number of tasks, including: (1) Establish, organize, and operate a joint force HQ. (2) Command subordinate forces. (3) Prepare, modify, and publish plans, orders, and guidance. (4) Establish command authorities among subordinate commanders. (5) Assign tasks, prescribe task performance standards, and designate OAs. (6) Prioritize and allocate resources. (7) Manage risk. (8) Communicate and ensure the flow of information across the staff and joint force. (9) Assess progress toward accomplishing tasks, creating conditions, and achieving objectives. (10) Coordinate and control the employment of joint capabilities to create lethal and nonlethal effects. (11) Coordinate, synchronize, and, when appropriate, integrate joint operations with the operations and activities of other participants. (12) Ensure the flow of information and reports to and from higher authority.

The benefit of AI-enabled C2 will be profound. In addition to being the engine to drive JADC2, AI will (1) expand the number of echelons and units commanders will be able to coordinate in the operational environment; (2) prepare and modify orders and guidance at the speed of relevance due to AI's enhanced capability to aggregate data and improve the timeliness of decision making; (3) more rapidly assign and, perhaps more importantly, reassign tasks as the situation develops; (4) better prioritize and allocate/re-allocate resources; (5) better manage risk through real time domain awareness and autonomous systems updates; (6) ensure the timely transmission of battle updates and reports to higher headquarters; (7) maintain persistence and the initiative against the enemy, overwhelming their decision making and ability to react to multiple vectors of attack across all warfighting domains.

Information:

The information function encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of military activities to achieve the commander's objectives and attain the end state.

Here, AI can perform not only critical military information requirements as described in the previous sections, but also assist the commander in achieving not only military but political objectives and endstates as well. Using AI-enabled information analysis, the joint force can monitor and discern patterns within enemy communications and data streams while simultaneously monitoring internet, social media, news, and other commercial data streams in an effort to confound enemy actions while simultaneously gaining unprecedented understanding of the social and political ramifications of military operations. Non-AI related information dominance has been recently witnessed in the Ukrainian conflict with Ukraine gaining the advantage in this important domain. AI-enabled information dominance will be even more dramatic.

Additionally, AI-enabled information operations will enhance: military deception through low-cost and attritable swarming techniques of robotic and autonomous systems; operational security through advanced reconnaissance and scouting machines and multi-vector approaches against enemy positions; cyber offensive and defensive operations through autonomous cyber capabilities; and AI monitoring, jamming, and frequency re-allocation in the electronic warfare domain while providing communication and operational capabilities in electronically denied or degraded EW environments.

Intelligence:

Understanding the OE is fundamental to joint operations. The intelligence function supports this understanding with analysis of the OE to inform JFCs about adversary capabilities, COGs, vulnerabilities, and future COAs and to help commanders and staffs understand and map friendly, neutral, and threat networks. Using the continuous JIPOE analysis process, properly tailored JIPOE products can enhance OE understanding and enable the JFC to act inside the enemy's decision cycle. Intelligence activities and assessments also occur while defending the homeland within the guidelines of applicable regulations and laws.

As mentioned earlier in this paper, using AI to aggregate multiple intelligence data streams to provide timely information to decision makers is key to maintaining situational awareness and the initiative on the battlefield. Additionally, AI-enabled vehicles will be able to loiter over, under, and in advanced reconnaissance positions on the battlefield to provide a common operating picture to units and the commander while providing recommendations for force and capabilities allocation and reallocation, thus maintaining pressure on enemy action and reaction decisions and times.

Fires:

To employ fires is to use available weapons and other systems to create a specific effect on a target. Joint fires are those delivered during the employment of forces from two or more components in coordinated action to produce desired results in support of a common objective. Fires typically produce destructive effects, but various other tools and methods can be employed with little or no associated physical destruction.

Like the joint principle of mass discussed above, AI-enabled fires from all warfighting domains, perhaps simultaneously, will confound the enemy's cognitive ability to defend or respond tactically, will demoralize the enemy and keep them on their heels under a persistent barrage of multi-vector fires which create effects in the physical *and* cognitive domains. Overwhelming force means not only firepower, but fires for effects in the operational environment from multiple vectors to achieve military and political objectives. AI-enabled capabilities will be able to synchronize and coordinate fires from the strategic down to the tactical levels of war in a near-seamless and timely manner.

Movement and Maneuver:

This function encompasses the disposition of joint forces to conduct operations by securing positional advantages before or during combat operations and by exploiting tactical success to achieve operational and strategic objectives. This function includes moving or deploying forces into an OA and maneuvering them to operational depths for offensive and defensive purposes. It also includes assuring the mobility of friendly forces.

From strategic movement of forces from the U.S. or in space, to the tactical maneuver of units to gain positional and cognitive advantage over the enemy, AI-enabled capabilities will play a critical role in streamlining actions, reducing manpower and manhours for deployment and employment concerns, and providing the situational awareness and informational advantage necessary for tactical success. AI capabilities will greatly reduce the tremendous amount of time and energy required for the development of the time-phased force deployment data (TPFDD) necessary for force and transportation feasibility analysis, and force generation and mobility requirements for deployment using autonomous systems (ships, trucks, aircraft, and data). Similarly, maneuver will be greatly enhanced through the use of robotic scouts and reconnaissance, the fusing of ground, aerial, seaborne, and space sensors, and the data aggregation capability AI will provide.

Protection:

Preserves the joint force's fighting potential in four primary ways. One way uses active defensive measures that protect the joint force, its information, its bases, necessary infrastructure, and LOCs from an enemy attack. Another way uses passive defensive measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy by reducing the probability of, and minimizing the effects of, damage caused by hostile action without the intention of taking the initiative. The application of technology and procedures to reduce the risk of friendly fire incidents is equally important. Finally, emergency management and response reduce the loss of personnel and capabilities due to isolating events, accidents, health threats, and natural disasters.

Uncrewed systems utilizing various levels of AI for the conduct of their missions inherently raise the protective measures necessary for security of the units engaged in battle. From uncrewed logistics convoys, to uncrewed defensive systems to provide anti-air, anti-missile, and other protective measures, to uncrewed scout and reconnaissance vehicles, and the military deception uncrewed swarming systems can provide, AI-enabled capabilities will reduce the number of personnel exposed to enemy fires.

Sustainment:

Sustainment is the provision of logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force. Sustainment provides the JFC the means to enable freedom of action and endurance and to extend operational reach. Sustainment determines the depth to which the joint force can conduct decisive operations, allowing the JFC to seize, retain, and exploit the initiative. The sustainment function includes tasks to: (1) Coordinate the supply of food, operational energy (fuel and other energy requirements), arms, munitions, and equipment. (2) Provide for maintenance of equipment. (3) Coordinate and provide support for forces, including field services; personnel services support; health services; mortuary affairs; religious support (RS); postal support; morale, welfare, and recreational support; financial support; and legal services. (4) Build and maintain contingency bases. (5) Assess, repair, and maintain infrastructure. (6) Acquire, manage, and distribute funds. (7) Provide common-user logistics support to other government agencies, international *organizations, NGOs, and other nations. (8) Establish and coordinate movement services. (9) Establish large-scale detention compounds and sustain enduring detainee operations.*

As mentioned above, sustainment is one of the many areas where AI-enabled systems can dramatically enhance joint force capabilities and timeliness through greater automation while minimizing personnel exposure to enemy action. As with the Amazon example earlier in this paper, that company is leading the way in robotic logistics and drone deliveries. The Department of Defense can learn from their lead and embrace similar approaches to military operations. Of most immediate impact, the integration of AI into the assistance of monitoring and reporting maintenance functions, using predictive analytics and predictive maintenance, will streamline what is otherwise a time, cost, and – in its most extreme implication – human life intensive endeavor. AI analysis can greatly reduce maintenance error or the loss of human life by predicting impending failure of critical vehicle systems. AI can generate supply chain demands ahead of need, based on predictive pattern memory and granular analysis of system supply and delivery needs.

By utilizing a design approach to determine the operational environment as it exists today, what the operational environment needs to look like in the future, the challenges which need to be overcome in order to achieve those desired conditions in the future, along with the opportunities that can be leveraged to achieve desired outcomes, a clear roadmap for DoD adoption and development of AI becomes clear. From there developing an approach for the Department using the logical path behind the principles of joint operations, the joint functions, and service-specific applications of the joint doctrine, for determining exactly what it is AI will be used for, and for what purpose the DoD seeks to achieve through the use of AI also becomes clear. After that, prioritizing and funding for capabilities highlighted in that approach becomes a relatively easy process.

Conclusion

With the rapid advances in technology witnessed over the past 30 years, capabilities and technological solutions have outpaced national security strategists in how best to integrate and operationalize those capabilities. While this is nothing new – witness the longbow in the battle of Hastings; the introduction of railroads and telegraph during the Napoleonic wars; the machine gun in the late 19th and early 20th centuries; the airplanes, tanks, and chemical weapons during WWI; the concept of Blitzkrieg and the adoption of undersea warfare, radar, code-breaking, nuclear weapons, and other advancements during WWII; etc. -- without the imperatives of full-scale war driving the impetus to innovate, the more recent advancements of the relatively static and peaceful late 20th and early 21st centuries have met with sclerotic and oftentimes unnecessarily delayed adoption. During that essentially unipolar moment, where the U.S. stood predominant economically and militarily, perhaps prudence and caution were warranted, or bureaucratic foot dragging was an inconvenience to be tolerated since no existential threat to the nation was on the horizon.

Today, the United States no longer stands in that enviable position. A rising and increasingly bellicose China espousing an ideology contra to those of western liberal democracies, a revanchist and actively militarist Russia, along with other spoiler nations such as North Korea and Iran, and other “non- aligned” nations such as India or Indonesia, have all created a geopolitical reality where the West and America no longer can assume the dominance of their influence, their militaries, or their economies. In a networked and highly interconnected world where cyberspace and open-source code have made many of the capabilities described above available to anyone with a connection and modicum of ability, the U.S. and the West can no longer abide with business as usual. If it is true in corporate boardrooms that the death knell of competitive advantage rests in the seven deadly words, “This is how we’ve always done it,” then the same will certainly hold true for the nation’s federal bureaucracy, with much higher stakes than shareholder profit. The key to holding battlefield dominance in future war will be held by the force that masters the integration of AI into its warfighting capabilities. The U.S. must act now to properly define its terms, objectives, requirements and warfighting concepts for this critical capability. Commercial technologies for both AI and autonomy applications exist, but they are challenged to make a difference without clarity and guidance from DoD. The purpose of this Whitepaper series is to take an important step toward changing the current dialogue. In this time of geopolitical reordering and change, where the impetus to re-think how warfare should be conceptualized faces a growing immediacy, it is time to embrace this immediacy and give everyone who has the ability and desire a chance to help and a voice in assisting with new ideas for AI integration, new applications, and new concepts of operation.

<u>End Notes:</u>

[28] Sheppard, Lindsey, ”Accelerating the Defense Department’s AI Adoption,” *Council on Foreign Relations Digital and Cyberspace Policy Program,* April 9, 2020, (Accessed September 16, 2022), https://www.cfr.org/report/accelerating-defense-departments-ai-adoption

[29] Ibid.

[30] Ibid.

[31] Congressional Research Service, *DOD Planning, Programming, Budgeting, and Execution (PPBE): Overview and Selected Issues for Congress”* Washington, DC: July 11, 2022

[32] Sheppard, April 9, 2020

[33] Ibid.

[34] Myatt, Summer, ” Artificial Intelligence-Related Challenges, Opportunities Drive Federal Defense Agency Priorities & Budget Concerns,” November 8, 2021, (Accessed September 16, 2022), https://www.govconwire.com/2021/11/ai-challenges-opportunities-drive-federal-defense-agency-priorities-budget/

[35] Sheppard, April 9, 2020

[36] Ibid.

[37] Ibid.

[38]Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations, Appendix A, Principles of Joint Operations,”* Washington, DC: June 18, 2022

[39] Ibid., pp. III-2 – III-52