

Artificial Intelligence Guided Battle Management: Enabling Convergence in Multi-Domain Operations

A Monograph

by

MAJ Sam H. Kriegler
US Army



School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2020

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 21-05-2020		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) JUN 2019 – MAY 2020	
4. TITLE AND SUBTITLE Artificial Intelligence Guided Battle Management: Enabling Convergence in Multi-Domain Operations			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) MAJ Sam H. Kriegler			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301			8. PERFORMING ORG REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Advanced Military Studies Program, School of Advanced Military Studies.			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The US Army in <i>Multi-Domain Operations 2028 (MDO 2028)</i> is the Army's future operating concept. It is a document that illustrates how the service anticipates it needs to adapt and evolve to maintain a competitive military advantage in the future fight. Critical components of the concept are the Tenets of Multi-Domain Operations – Calibrated Force Structure, Multi-Domain Formations, and Convergence – which enable the dis-integration of enemy anti-access and area denial systems and allow military forces to exploit short windows of superiority. It is a concept which hinges on the ability to continuously synchronize capabilities in time, space, and purpose, to achieve cross-domain synergy and create an exploitable window of superiority. The joint force's current process of converging capabilities by "episodic synchronization of domain-federated solutions," does not support the rapid and continuous integration of capabilities across multiple domains in the reoccurring cycle of competition and exploitation against a future peer-threat. Therefore, it is critical to consider what capabilities allow the military leader to overcome these technological and human cognitive limitations. One possible solution is the integration of artificial intelligence into the battle management process.					
15. SUBJECT TERMS Artificial Intelligence, Multi-Domain Operations, Multi-Domain Convergence, Battle Management, Autonomy					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON MAJ Sam H. Kriegler
a. REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)			19b. PHONE NUMBER (include area code) 912-332-6102

Monograph Approval Page

Name of Candidate: MAJ Sam H. Kriegler

Monograph Title: Artificial Intelligence Guided Battle Management: Enabling Convergence in Multi-Domain Operations

Approved by:

_____, Monograph Director
Dan G. Cox, PhD

_____, Seminar Leader
Aimee S. DeJarnette, COL

_____, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 21st day of May 2020 by:

_____, Deputy Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Fair use determination or copyright permission has been obtained for the inclusion of pictures, maps, graphics, and any other works incorporated into this manuscript. A work of the US government is not subject to copyright, however further publication or sale of copyrighted images is not permissible.

Abstract

Artificial Intelligence Guided Battle Management: Enabling Convergence in Multi-Domain Operations, by MAJ Sam H. Kriegler, US Army, 40 pages.

The US Army in *Multi-Domain Operations 2028 (MDO 2028)* is the Army's future operating concept. It is a document that illustrates how the service anticipates it needs to adapt and evolve to maintain a competitive military advantage in the future fight. Critical components of the concept are the Tenets of Multi-Domain Operations – Calibrated Force Structure, Multi-Domain Formations, and Convergence – which enable the disintegration of enemy anti-access and area denial systems and allow military forces to exploit short windows of superiority. It is a concept which hinges on the ability to continuously synchronize capabilities in time, space, and purpose, to achieve cross-domain synergy and create an exploitable window of superiority. The joint force's current process of converging capabilities by “episodic synchronization of domain-federated solutions,” does not support the rapid and continuous integration of capabilities across multiple domains in the reoccurring cycle of competition and exploitation against a future peer-threat.¹ Therefore, it is critical to consider what capabilities allow the military leader to overcome these technological and human cognitive limitations. One possible solution is the integration of artificial intelligence into the battle management process.

This monograph focuses on illustrating the need to integrate artificial intelligence into the battle management process to facilitate convergence in multi-domain operations. By analyzing multi-domain operations' convergence gaps, developments in artificial intelligence, and current command and control systems, the research intends to illustrate that the complexity of the continuous convergence of capabilities in multi-domain operations rapidly exceeds human cognitive abilities. Additionally, due to the fact that adversaries of the United States are heavily investing in artificial intelligence and autonomy, the question of merging artificial intelligence into the battle management process is not a matter of achieving superiority on the battlefield. Instead, it is a matter of possessing the ability to compete for temporary exploitable windows of advantage.

¹ United States Training and Doctrine Command, *Army Training and Doctrine Command Pamphlet (TRADOC PAM) 525-3-1, The US Army in Multi-Domain Operations 2028* (Washington, DC: Government Printing Office, December 2018), v.

Contents

Acknowledgements	v
Abbreviations	vi
Introduction	1
The Path to Multi-Domain Operations	2
AI on the Battlefield	6
Multi-Domain Convergence	9
Current Battle Management Systems	14
Methodology	19
Scope and Limitations	21
Strategic Framework (Scenario One & Scenario Two)	22
Scenario One - Corps Echelon	27
Scenario Two - Division Echelon	30
Implications	33
Conclusion	34
Bibliography	38

Acknowledgements

Dr. Cox for his enthusiasm, insight, and willingness to guide me along the monograph process.

COL DeJarnette for her mentorship, patience, and attention to detail – and for always pushing us to make progress.

My AMSP peers who always took the time to discuss ideas, provided suggestions, and motivated each other.

My family for providing encouragement, support, and never giving me a reason to second-guess the decision to pursue this profession.

Abbreviations

A2AD	Anti-Access and Area Denial
ABMS	Advanced Battle Management System
AI	Artificial Intelligence
C2	Command and Control
MDO	Multi-Domain Operations
MDO 2028	Multi-Domain Operations 2028
NDS	National Defense Strategy
NMS	National Military Strategy
NSS	National Security Strategy
TRADOC	US Training and Doctrine Command

Introduction

In short, speed matters in two distinct dimensions. First, autonomy can increase decision speed, enabling the U.S. to act inside an adversary's operations cycle. Secondly, ongoing rapid transition of autonomy into warfighting capabilities is vital if the U.S. is to sustain military advantage.

— DSB Report on Autonomy, 2016

The US Army in *Multi-Domain Operations 2028 (MDO 2028)* is the Army's future operating concept. It is a document that illustrates how the Army anticipates it needs to adapt and evolve to maintain a competitive military advantage in the future fight. Critical components of the concept are the Tenets of Multi-Domain Operations – Calibrated Force Structure, Multi-Domain Formations, and Convergence – which enable the dis-integration of enemy anti-access and area denial (A2AD) systems and allow military forces to exploit short windows of superiority. It is a concept which hinges on the ability of commanders to continuously synchronize capabilities in time, space, and purpose, to achieve cross-domain synergy and create an exploitable position of advantage.²

Currently, the joint force is converging capabilities by “episodic synchronization of domain-federated solutions,” a process that does not support the rapid and continuous integration of capabilities across multiple domains in the reoccurring cycle of competition and exploitation against a future peer-threat.³ Military leaders acknowledge this shortcoming, and the complexity of the task, and consequently introduce convergence considerations that call for the development of new military technology to fill critical gaps. Based on these gaps, future command and control systems need to provide commanders at all echelons with a complete common operating picture of all joint assets within a battlespace, and the ability to rapidly transmit reconnaissance and target data to prosecute proposed targets by both kinetic and non-kinetic means.

² US Training and Doctrine Command, *Training and Doctrine Command Pamphlet (TRADOC PAM) 525-3-1, The US Army in Multi-Domain Operations 2028* (Washington, DC: Government Printing Office, December 2018), v.

³ *Ibid.*, x.

However, enemy developments in autonomy and artificial intelligence (AI) drastically compress the time-window in which convergence must occur. Due to the short time window, the task of coordinating convergence efforts quickly exceeds human capabilities. Other factors, such as the need for munition optimization and capability reset times, increase the complexity of the task further. Therefore, it is critical to consider what capabilities military leaders need to possess to overcome these technological and human cognitive limitations. One possible solution is the integration of AI into the battle management process. Consequently, the challenge that convergence in multi-domain operations presents raises one key question: does the US Army need an AI guided battle management system to successfully converge capabilities in multi-domain operations against a peer competitor with an ability to field autonomous and AI guided capabilities?

Path to Multi-Domain Operations

The way we seek to get an advantage is to optimize all domains at a decisive space in order to affect the penetration.

— LTG Eric Wesley, Director, US Army
Capabilities Integration Center

A phenomenon of armed competition is the weaponization of technological innovations. From a military perspective, it is a critical progression that allows a nation's fighting force to maintain a competitive edge on the battlefield. To drive capability development, military leaders introduce future operating concepts. The concepts are documents that anticipate how the military needs to train, equip, and organize itself to compete and win against emerging threats. Currently, the US Army is in the process of a significant reformation. This reorganization will pivot the military towards large-scale combat operations and align forces to meet the demands outlined in the National Security Strategy (NSS), and the nested National Defense Strategy (NDS) and National Military Strategy (NMS).⁴ This change presents a paradigm shift for a military force

⁴ Office of the President, *National Security Strategy (NSS) of the United States of America* (Washington, DC: Government Printing Office, 2017).

that, for nearly two-decades, focused predominantly on counterinsurgency. For the US Army, it is an undertaking that validates the maxim that history does not repeat itself, but it rhymes. Mainly because the introduction of the current future operating concept, *MDO 2028*, prompts a transformation effort that is reminiscent of past reorganization cycles.⁵ One relevant example is the restructuring triggered by the introduction of *AirLand Battle* doctrine in the mid-1980s.⁶

AirLand Battle was the US Army's response to the Russian threat at the height of the Cold War. Published in 1986, it presented an operational framework that relies on the effective synchronization of capabilities in the land and air domain. Rising complexity, driven by technological advances that result in "an increased tempo of events," was the underlying premise.⁷ A key component of the document is the introduction of new language that reflects the evolving nature of warfare. One of these new terms was integrated battle – the concentrated employment of all capabilities to defeat the enemy – which relied on the ability to gain and maintain situational awareness.⁸ Based on the realization that emerging technology can provide an edge on the battlefield, *AirLand Battle* directed the integration of computer technology, which was rapidly evolving. Required innovation efforts were presented in the 1986 *Department of Defense's Annual Report to Congress*. The Joint Tactical Fusion Program (JTFP) and the Joint Surveillance and Target Acquisition System (JSTAS) are examples of the systems that ensued.⁹ Both systems were designed to provide commanders the ability to collect information from various sources and guide the employment of joint kinetic efforts in pursuit of ground targets. The need to develop these systems denote two truths.¹⁰ First, the systems demonstrate the integral

⁵ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, iii-v.

⁶ Douglas W. Skinner, "AirLand Battle Doctrine" (Center for Naval Analysis, Alexandria, VA, 28 December 1988), 1, accessed 12 September 2019, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a202888.pdf>.

⁷ Skinner, "AirLand Battle Doctrine," 1.

⁸ *Ibid.*, 16 - 18.

⁹ *Ibid.*, 22 - 26.

¹⁰ *Ibid.*, 20 - 27.

relationship between technology and warfare. Second, the systems highlight the military leaders' admission that, from this point forward, the speed and complexity required to effectively synchronize military capabilities on the battlefield exceeds human cognitive abilities. The current multi-domain operations concept carries this realization into the future.

Recognizing the US military's diminishing competitive advantage, Lieutenant General (Ret.) H.R. McMaster and then-Deputy Defense Secretary Robert O. Work called for the development of AirLand Battle 2.0.¹¹ General (Ret.) David G. Perkins, then commanding general of Training and Doctrine Command, answered the call and introduced Multi-Domain Battle. However, during the 2016 US Army Annual Meeting and Exposition, General (Ret.) Perkins pointed out that the concept is not a revamp of *AirLand Battle* or *Full-Spectrum Operations*, but depicts a revolutionary approach to warfare. One critical reason why Multi-Domain Battle was presented as revolutionary, is the fact that it called for a transformation in the way military forces operate. The underlying drivers of the new way of operations were rapid scientific and technological developments and the need to compete against a peer threat across all domains in a continuous cycle of competition, defeat, exploitation, and re-competition.¹²

Prompted by a return to great power competition, with China and Russia serving as a pacing threat, the 2017 NSS directs the military services to possess the ability to contest competitors across multiple domains at once. To build the capacity to contest the enemy across domains requires the development of "new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains."¹³ Reliable and timely cross-domain support from joint enablers is a critical requirement and implied task for successful

¹¹ Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story," *Modern War Institute* (October 2017), accessed 17 September 2019, <https://mwi.usma.edu/road-multi-domain-battle-origin-story/>.

¹² General (Ret.) David Perkins, "Multi-Domain Battle: Joint Combined Arms Concept for the 21st Century," *Association of the United States Army* (November 2016), accessed 14 October 2019, <https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms>.

¹³ Office of the President, *NSS*, 29.

competition. The resulting domain interdependency means that a “lack of access in one domain can have cascading effects in one or more domains.”¹⁴ Consequently, Dr. Jared Donnelly, assistant professor for the US Air Force’s Multi Domain Operational Strategist program, predicts future wars will be fought in a rapid and complex multi-domain continuum that does not rely on the sequential setting of conditions across a line of operations but requires the perpetual synchronization of capabilities across multiple domains.¹⁵ Consequently, an understanding of the capabilities that exist within the separate domains and how each can be leveraged to achieve temporary superiority is fundamental to successful multi-domain operations.¹⁶

Guided by the NSS and NDS, the US Training and Doctrine Command (TRADOC) introduced TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, in early 2018.¹⁷ It is a concept that, as former TRADOC Commander General Stephen J. Townsend highlights, recognizes the enemy’s ability to present challenges and contest the US military in a multi-layered stand-off with the intent “to separate US forces and our allies in time, space, and function in order to defeat us.”¹⁸

One reason why the concept presents an evolution of warfare is the way it visualizes the interaction of capabilities across multiple domains, which goes beyond maneuvering within different domains or possessing the ability to achieve cross-domain effects. Instead, the concept acknowledges that technological advances alter the interrelationship between domains and the

¹⁴ Brian Willis, “Multi-Domain Operations at the Strategic Level,” *Over The Horizon* (March 2018), accessed 18 September 2019, <https://othjournal.com/2018/03/02/multi-domain-operations-at-the-strategic-level/>.

¹⁵ Jeffrey Reilly, “Over the Horizon: The Multi-Domain Strategist,” *Over The Horizon* (November 2018), accessed 18 September 2019, <https://othjournal.com/2018/11/08/oth-mdos-reilly/>.

¹⁶ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, iii - v.

¹⁷ Ibid.

¹⁸ Dennis Boykin and Scott King, “Distinctly Different Doctrine: Why Multi-Domain Operations Isn’t AirLand Battle 2.0,” *Association of the United States Army* (February 2019), accessed 17 September 2019, <https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn-t-airland-battle-20>.

speed at which cross-domain connections occur. *MDO 2028* incorporates these changes in the concept's Tenets of Multi-Domain Operations – Calibrated Force Structure, Multi-Domain Formations, and Convergence – which enable the dis-integration of enemy anti-access and area-denial systems and allow military forces to create short windows of superiority.¹⁹ Combined, they set the conditions for commanders to converge capabilities in time, space, and purpose, to achieve cross-domain synergy and create an exploitable position of advantage. Furthermore, multi-domain convergence is a process that can be optimized and accelerated through the integration of AI guided systems.

AI on the Battlefield

We have to get used to the radical idea that we, human beings, will be just one species of intelligent beings.

— Alexander Kott, Chief, Network Science
Division, US Army Research Laboratory

AI is the ability of technological systems to perform tasks that until this point required human intelligence. These tasks include the ability to observe and identify patterns, learn through observation, predict events, or take action. China, one of the United States' main competitors, recognizes the way AI can skew the battlefield symmetry to their advantage. The country's heavy investment in the development of AI guided military capabilities, including autonomous weapon systems, serves as a testament.²⁰ To maintain a position of relative advantage in armed conflict requires the United States to develop counter-capabilities that tie AI into the decision-making process. Current US AI initiatives largely center on pattern recognition, which, enabled by the rapid increase in computing power, can analyze ever increasing amounts of data to create information.²¹

¹⁹ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 17 - 25.

²⁰ Bill Gertz, "China Developing Battlefield AI for High-Technology Warfare," *Washington Times*, 30 January 2019, accessed 10 September 2019, <https://www.washingtontimes.com/news/2019/jan/30/chinas-military-outlines-artificial-intelligence-p/>.

²¹ Ben Dickson, "What is Narrow, General and Super Artificial Intelligence" (May 2017), accessed 14 October 2019, <https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super->

One aspect of multi-domain operations is the need to collect and analyze vast amounts of data to observe and assess developments within the operating environment. Current military application of AI focuses on the support of logistical and transportation, and data analytics. However, the creation of the Joint Artificial Intelligence Center, and the White House's Select Committee on AI, both signal the expansion of AI into other areas within the Department of Defense.²² For example, the US Army Futures Command currently works on a number of initiatives that analyze how AI can improve a commander's ability to gain situational awareness and make informed decisions. One focus area is the development of capabilities that increase the speed at which US forces can synchronize effects and alleviate mundane cognitive tasks.²³ Emphasis on an iterative collaboration between the developers and the potential end-user sets the conditions that allows the service to develop AI guided systems which can "generate and help commanders explore new options," and enable them to focus on selecting advantageous courses of actions that minimize risk to force and mission.²⁴

Concerning the integration of AI into the battle management process, it is critical to differentiate between systems that place humans in-the-loop or on-the-loop. The definition of autonomy, according to the Joint Concept for Robotics and Autonomous Systems, is the "spectrum of automation in which independent decision-making can be tailored for a specific mission, level of risk, and degree of human-machine teaming."²⁵ The spectrum itself encompasses different degrees of autonomy. During the 2017 Mad Scientist Conference, hosted

artificialintelligence/.

²² White House Press, "Artificial Intelligence for the American People," accessed 14 October 2019, <https://www.whitehouse.gov/ai/>.

²³ Sydney Freedberg, "The Art of Command, the Science of AI," *Breaking Defense* (November 2019), accessed 14 October 2019, <https://breakingdefense.com/2019/11/the-art-of-command-the-science-of-ai/>.

²⁴ US Department of Defense, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy," 11.

²⁵ US Department of the Army, *Robotics, Artificial Intelligence & Autonomy: Visioning Multi-Domain Warfare in 2030-2050* (Washington, DC: Government Printing Office, December 2018), 15.

by the TRADOC and the Georgia Tech Research Institute, experts presented three degrees of autonomy – fully autonomous, supervised autonomous, and autonomy baseline.²⁶ A fully autonomous system operates independent from human real-time intervention and operates with the human out of the loop. With the supervised autonomous systems, humans maintain the ability to intervene and influence decision in real-time, and thus remain on the loop. Autonomy baseline is the current presence of autonomy in various existing systems. In military applications, this autonomy is present in human supervised weapons such as the Patriot and Aegis missile systems, or the AH-64D Apache attack helicopter longbow fire control radar, which independently “searches, detects, locates, classifies, and prioritizes multiple moving and stationary targets on land, air, and water.”²⁷

Richard Potember of the Mitre Corporation regards machine learning as the “foundational basis for AI,” which focuses on the ability of systems to learn unsupervised and create deep neural networks to support decision-making and the employment of robotics.²⁸ The integration of autonomy and AI is a process that inadvertently will result in the fact that “everything we formerly electrified, we will now ‘cognitize’.”²⁹ A critical technological development trend that supports the integration of an AI guided battle management system into multi-domain operations is the gradual shift of autonomy and learning from sensing to decision-making. In doing so, AI can mitigate the complexity inherent in MDO. One inherent complexity is the ability to integrate capabilities and make decisions spanning multiple domains not within minutes or hours, but seconds, if required.³⁰ Therefore, integrating AI into the decision and

²⁶ US Training and Doctrine Command, “*Robotics, Artificial Intelligence & Autonomy: Visioning Multi-Domain Warfare in 2030-2050*,” 15 - 18.

²⁷ Ibid., 18.

²⁸ Ibid., 32.

²⁹ Ibid., 39.

³⁰ Ibid., 55.

synchronization process provides to the potential to balance the observe-orient-decide-act cycle in the United States' favor.³¹

At the strategic level, AI guided systems can influence the decision that drive escalation and de-escalation across the varying domains. At the operational level, general AI can build situational awareness and synchronize effects.³² To support the convergence of capabilities across multiple domains, AI's ability to "process a flood of information from various platforms operating in multiple domains," directly contributes to two fundamental aspects of MDO warfare: speed and range.³³ The current status of AI supports the ability to strike faster and at further distances than the enemy. It is an ability that enables the analysis of a dynamic battlefield in real-time to set the conditions for a rapid strike with minimal risk to friendly forces. A 2016 study by Defense Science Board, supports the notion that AI systems are capable of integrating multiple battle-management, command and control, communications, and intelligence capabilities within a kinetic targeting cycle.³⁴ Furthermore, the board assesses that the cumulative effect of these AI guided systems can change the operational and strategic dynamic of the fight throughout the multi-domain convergence cycle.

Multi-Domain Convergence

AI is coming to the battlefield, it's not a question of if, it's when and who.
— GEN John Murray, Commanding General,
Army Futures Command

³¹ Erik Trautman, "How Artificial Intelligence is Closing the Loop with Better Predictions," accessed 12 October 2019, Editors Official, <https://www.eriktrautman.com/posts/how-artificial-intelligence-is-closing-the-loop-with-better-predictions>.

³² General Artificial Intelligence enables machines to display human intelligence behavior characteristics such as learning, the integration of prior knowledge into the decision-making process, problem solving, and innovation.

³³ Zachary Davis, "Artificial Intelligence on the Battlefield: An Initial Survey of Potential implications for Deterrence, Stability, and Strategic Surprise" (Center for Global Security Research Lawrence Livermore National Laboratory, March 2019), accessed 12 October 2019, https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf, 6.

³⁴ US Department of Defense, *Defense Science Board: Summer Study on Autonomy* (Washington, DC: Government Printing Office, 2016), 98 - 101.

In armed conflict, United States' competitors aim to integrate their A2AD systems to establish layered stand-off zones. The objective is to deny the US military joint forces the ability to synchronize effects in time and space. Russia's S-400 Triumf is representative of the type of systems US forces could face in large-scale combat. The S-400 is a mobile surface-to-air missile system that possesses the ability to engage various weapon systems ranging from UAVs to terminal ballistic missiles. The radar tracks targets at a range of 600 km, and has an engagement range of 100 km. One of the critical technological advances the system provides is the fully automated sensor to shooter loop that allows the system to track and engage up to eighty targets simultaneously.³⁵ This is one example supporting *MDO 2028*'s assumption that the US military cannot assume it has superiority in any domain at the onset of hostilities in large scale combat against a peer threat. To overcome the enemy's defense systems in a continuous cycle of competition, penetration, dis-integration, and exploitation, the US Army's multi-domain operations framework introduces three Tenets of Multi-Domain Operations – calibrated force posture, multi-domain formations, and convergence.³⁶

Calibrated force posture refers to the mix of forces and capabilities that can quickly adapt and change in response to the operating environment. The intent is to identify a potential weakness or create asymmetry on the battlefield to establish an exploitable window of local superiority. Forward presence forces support the rapid escalation of activities across the range of military operations to penetrate and dis-integrate enemy systems. The forces are arranged to provide mission command, fires, intelligence collection, sustainment, information activity, and special operations capabilities.³⁷ Expeditionary forces offer the ability to conduct joint forcible

³⁵ Missile Defense Project, "S-400 Triumf," *Missile Threat* (Center for Strategic and International Studies, 4 May 2017, last modified 15 June 2018), accessed 18 November 2019, <https://missilethreat.csis.org/defsys/s-400-triumf/>.

³⁶ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, iii.

³⁷ *Ibid.*, 17 - 18.

entry operations, if required, and set the conditions for follow-on forces. These forces deploy either by air and sea, within days or weeks.³⁸

The focus of multi-domain formations is to enable lower echelons to conduct offensive and defensive operations against a near-peer threat. The three capabilities that support multi-domain formations are the ability to perform independent maneuver, employ cross-domain fires, and maximize human potential. To support the achievement of objectives within a contested domain, *MDO 2028* recognizes that units at the corps, division, and brigade echelon need to operate independently and unconstrained by higher headquarters resourcing prioritization. Therefore, they need to possess organic logistical, maneuver, fires, medical, and communication networks that allow units to fight independently for a predetermined amount of time. The operating concept's current framework calls for these echelons to "maintain offensive operations for several days despite highly contested lines of communication."³⁹ The ability to maintain the offense is driven by the commanders' ability to employ cross-domain fires.

Cross-domain fire is the integration of fires capabilities with redundancy in the case of a temporary separation from higher headquarters' fires support. The process includes direct and indirect fire assets, protection capabilities, and electronic warfare devices, as well as "multi-spectral fused munitions, and cyberspace, space, and information related capabilities."⁴⁰ To enhance the decision-making process in the complex and rapidly evolving multi-domain operating environment requires the development of "man-machine interfaces, enabled by artificial intelligence and high-speed data processing."⁴¹ Both the calibrated force posture and the creation of multi-domain formations are geared to enable what this paper regards as a critical component of multi-domain operations, convergence.

³⁸ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 19.

³⁹ *Ibid.*, 16.

⁴⁰ *Ibid.*, 19.

⁴¹ *Ibid.*, 20.

MDO 2028 defines convergence as the “rapid and continuous integration of capabilities in all domains, the electro-magnetic spectrum, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy.”⁴² Though it may appear like an extension of the current integration and synchronization of joint capabilities, the concept differs significantly from present procedures. This is mainly because it is not the process of sequential de-confliction of effects in time and space, guided and limited by targeting cycles and tasking orders. Instead, it is the continuous synchronization of effects across all domains, in windows of opportunity, with great variance in both space and time. To compete in a peer-contested environment requires the ability to create temporary domain overmatch through cross-domain synergy. This synergy is concentrated at the decisive space. The decisive space is a physical, virtual, and cognitive location in time and space that allows US forces to attain an exploitable position of marked advantage.⁴³ Additionally, because military units expect to counter multiple threats simultaneously, multi-domain convergence requires the concurrent dis-integration and neutralization of systems, in a competition continuum across all domains.⁴⁴

Rapid command and control sets the conditions for commanders to achieve convergence through cross-domain synergy and layered options. Consequently, the ability of military commanders to possess holistic situational awareness of all joint enablers operating within a battlespace at any given point in time is a critical component of convergence. *MDO 2028* identifies two requirements that necessitate the development and integration of technologically advanced command and control systems into multi-domain formations to facilitate the process. The first is the need for “commanders and staffs at each echelon to visualize and command a

⁴² US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 20.

⁴³ *Ibid.*, C-7.

⁴⁴ Office of the President of the United States, NSS, 28 – 39; Headquarters, Department of the Army, “Concepts Drive Change,” accessed 14 November 2019, https://www.ausa.org/sites/default/files/ILW-CMF_MDO_general-slides.pdf.

battle in all domains,” and rapidly orient capabilities to achieve convergence.⁴⁵ The second is the ability to quickly coordinate the convergence of joint capabilities against a specific enemy vulnerability.⁴⁶

Critical to the commander’s ability to converge capabilities in purpose and time is the synchronization of five convergence elements – preparation time, planning and execution time, duration time, reset time, and cycle time.⁴⁷ Consideration of these elements allows commanders to calculate the time it takes a capability to achieve an effect from the initiation time, and the time that is required to reset the capability for a new cycle of re-competition. The process of converging multiple capabilities within this framework is further complicated by the varying capability usage rates. Whereas the cycle rate presents an infinite sequence of employment, the usage rate represents a diminishing asset that is tied to “munitions and expendable virtual weapons.”⁴⁸ Because logistics is contested and predictable resupply is not guaranteed, commanders face an additional challenge in multi-domain convergence. This challenge is the task of optimizing the use of available ammunition and align the ammunition use with the coordination of joint capabilities.

The current quantitative limitation of available munitions and the inability to establish stockpiles could result in critical shortfalls in future large-scale combat operations. In order to extend the endurance of military forces, especially when operating across contested lines of communication, requires the continued assessment of the status of weapon the various systems. The ability to “optimize and sequence fires” across all joint platforms within kinetic range becomes critical.⁴⁹ This optimization and sequencing process, again, rapidly exceeds the

⁴⁵ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, xi.

⁴⁶ *Ibid.*, xi.

⁴⁷ *Ibid.*, C-7 - C-8.

⁴⁸ *Ibid.*, C-18.

⁴⁹ *Ibid.*, F-3.

cognitive capability of human decision-makers, and presents a technological battle management system shortfall that adversely affects the effective convergence of joint capabilities.⁵⁰

Central to the US Army’s effort to achieve operational agility in a multi-domain battlespace is the ability to create understanding out of ever-growing aggregate data sets, while maintaining “superior decision speed.”⁵¹ Fog and friction will always exist on the battlefield, but shrinking the amount of time it takes to observe changes in the environment and orient forces accordingly enables a faster rate of decision and action. Improved awareness of the joint forces’ position within the various domains, relative to the enemy and their operational and tactical plans, is necessary to accelerate maneuver at lower echelons. Furthermore, short windows of opportunity require future battle management systems to rapidly match sensors to shooters.

Within the US Army’s modernization framework, emerging technology needs to provide a solution to two critical technological and organizational shortfalls. The first is the ability to maintain complete situational awareness of all joint military assets within an operational area. The second is the ability to rapidly establish redundant sensor to shooter loops that incorporate all available joint assets and consider the capabilities’ varying regeneration cycles. It is a task, based on the amount of data that needs to be processed to continuously synchronize joint military assets as they compete in a contested battlefield, which quickly surpasses human cognitive abilities. The integration of artificial intelligence into the battle management process can mitigate this human limitation.

Current Battle Management Systems

It’s not coincidental that one of our priorities for investment is the network... so we have the ability to communicate that kind of target very quickly to another domain.

— GEN John Murray, Commanding General,
Army Futures Command

⁵⁰ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, F1 - F3.

⁵¹ US Air Force, “Air Force Future Operating Concept: A View of the Air Force in 2035,” Washington, DC: Government Printing Office, September 2015.

One of the most critical steps to achieving multi-domain convergence is the development of joint command and control (C2) systems that link capabilities vertically, and horizontally, across the battlespace. In 2017, SYSTEMATIC Inc. was awarded the contract to design the US Army's new battle-management system, SitaWare. The US Army's Tactical Mission Command Manager, Lieutenant Colonel Shane Taylor, calls the system "an out-of-the-box solution to synching mission command data across echelons [which] provides a leap forward in the Army's goal of migrating to a common architecture."⁵² Some of the advances the system provides are simplified command post C2, improved interoperability with joint and coalition partners, and a standard warfighting function convergence framework. Another key function of the system is the ability to scale large amounts of data quickly and present it in a manner that increases the commanders' situational awareness.

Within the US Army's operating environment, SitaWare is a Command Post Computing Environment component that is expected to eliminate information and intelligence stove piping and can be integrated as a common operating platform. SYSTEMATIC Inc. acknowledges that future combat requires the rapid synchronization of intelligence, logistics, and combat systems. Consequently, the current system is designed to analyze large data sets and display relevant information on an intuitive user interface. As a result, it builds the commanders' situational awareness in real time and increases their decision-making speed. Additionally, the system software complies with various civilian and military interoperability standards, which makes it easier to link the system with other joint and coalition platforms.

To nest the system across echelons, SitaWare's user interface apps and displays are tailorable to meet the requirements of the operational environment. Vertical information sharing ensures that all echelons share common data across all echelons. To provide situational understanding at the tactical level, the system has friendly force tracking capabilities for light,

⁵² Systematic, "SITWARE C4I Suite," accessed 19 November 2019, <https://www.systematicinc.com/products/n/sitaware/>.

wheeled, and armored formations. Another key feature of the system is the integrated command layer. This is a feature that allows commanders to quickly disseminate updates and changes to the original orders, in response to changes in the operational environment. However, SitaWare is not designed to direct effects. Therefore, it does not adequately accelerate the sensor-to-shooter cycle in a manner that increases the commanders' ability to effectively converge joint capabilities in a contested environment against a peer threat with autonomous and artificial intelligence supported weapon platforms.

In another effort to address future multi-domain operations requirements, the US Army initiated an internal project that aims “to increase the integration between physical objects, data collection, data analysis and autonomous decision making into *The Internet of Battlefield Things*.”⁵³ The project is specifically designed to fill gaps US Army leaders assess are not being adequately addressed by commercially produced technology. Appropriately labeled *Project Quarterback*, experts at Virginia Tech predict that one of the projects main challenges is the ability to “juggle a number of complex variables,” which impact the ability to combine aspects ranging from game theory to distributed learning.⁵⁴ These challenges are amplified by the fact that current US Army technological development efforts focus on the fielding of capabilities with little regard to integrating software and hardware that allows these systems to communicate with various joint capabilities.⁵⁵

The focus of the project is to place an AI guided system in-the-loop to provide commanders with a synthesis of the vast amount of data collected across various sensor platforms operating in the battlespace. By collecting data from relevant sensor systems, analyzing the enemy capability distribution, and comparing it against the available friendly weapons systems,

⁵³ Nicholas West, “U.S. Military Seeks A.I. Quarterback to Call Plays for *The Internet of Battlefield Things*,” *Activist Post*, accessed 27 October 2019, <https://www.activistpost.com/2019/10/u-s-military-seeks-a-i-quarterback-to-call-plays-for-the-internet-of-battlefield-things.html>.

⁵⁴ *Ibid.*

⁵⁵ *Ibid.*

the system provides recommendations on how to achieve effects most effectively. In order for the process to operate effectively, commanders must abdicate a significant level of control because they allow the system to “select the most appropriate strategy for how to wage war.”⁵⁶ Despite this concern, Kevin McEnery, deputy director of the Army’s Next-Generation Combat Vehicle Cross Functional Team, acknowledges that AI is essential in multi-domain operations because it provides the ability reduce the current ninety-six hour division targeting cycle “down to ninety-six seconds.”⁵⁷ Overall, *Project Quarterback* is an effort to help commanders “understand exactly what is on the battlefield and then select the most appropriate strategy based on the assets available and other factors.”⁵⁸ The initiative is a significant step towards being able to effectively converge capabilities in a time-constrained decision space because it elevates AI beyond a data visualizer and makes it a battle strategy tool.

Concerns regarding the reliability of AI in the battle management process can be mitigated by rapid advances in cloud architectures and deep learning systems. Similar to human interaction, building trust in artificial intelligence and autonomous system-waged war requires time. Lieutenant Colonel Wisham, one of the Project Quarterback directors, states that it requires a deliberate strategy to demonstrate that the system is reliable and effective, which is complicated by the fact that it is difficult, or impossible, to trace the neural nets’ decision-making path.⁵⁹ However, Dieter Fox, a robotic researcher at the Nvidia Corporation, predicts that this is a problem with a solution, since researchers continue to develop new procedures that analyze the neural network and machine learning process.⁶⁰ To analyze the networks and learning process is

⁵⁶ West, “*U.S. Military Seeks A.I. Quarterback to Call Plays for The Internet of Battlefield Things.*”

⁵⁷ Ibid.

⁵⁸ Ibid.

⁵⁹ Patrick Tucker, “*The US Army Wants to Reinvent Tank Warfare with AI,*” Defense One, accessed 24 November 2019, <https://www.defenseone.com/technology/2019/10/us-army-wants-reinvent-tankwarfare-ai/160720/>.

⁶⁰ Ibid.

a critical aspect of AI because it allows developers to constrain autonomous self-learning systems within a set decision framework. Another service that recognizes the importance of developing AI enabled capabilities is the US Air Force.

As a result of identifying the need to develop multi-domain C2 systems, the US Air Force intends to replace its legacy Joint Surveillance Target Attack Radar System with a “whole new network of different sensors on satellites, manned aircraft, and drones.”⁶¹ The name of this new capability is the Advanced Battle Management System (ABMS). Despite the fact that the projects current focus is the linking of US Air Force assets, the ultimate goal of the effort is to develop a “digital nervous system of the future fight.”⁶² US Air Force Brigadier General David Kumashiro, the US Air Force Joint Force Integration Director, illustrates that their approach centers on the notion that if “you don’t follow the standards of an open systems architecture, you’re going to find yourself off on the sidelines and not being relevant for the fight.”⁶³ The ABMS structure builds on an existing cloud-based targeting assistant that is designed to effectively track targets and aircraft. By expanding upon that concept, US Air Force planners want to concentrate on networking machine to machine interaction. A guiding idea of the project is to develop systems that can “snap together like Lego blocks” to connect joint capabilities rapidly and effortlessly.⁶⁴

Overall, the need to integrate artificial intelligence into the battle management process is driven by an understanding that linking the US military services across the warfighting domains is necessary to maintain a competitive military advantage. Failing to follow the path of AI integration has the potential to adversely impact the US military’s ability to defeat near-peer

⁶¹ Amy McCullough, “*Life After JSTARS*,” Airforce Magazine, accessed 24 November 2019, <https://www.airforcemag.com/article/life-after-jstars/>.

⁶² Ibid.

⁶³ Ibid.

⁶⁴ Sydney Freedberg, “*Air Force ABMS: One Architecture to Rule Them All?*” Breaking Defense, accessed 05 December 2019, <https://breakingdefense.com/2019/11/air-force-abms-one-architecture-to-rule-them-all/>.

competitors in a future fight. The following two scenarios illustrate how an AI guided battle management system can affect the dynamic on the battlefield in multi-domain operations at the corps and division level.

Methodology

Long-term planning allows the military to focus research and developments efforts, and guides manning, training, and equipping decisions. Central to this process is the development of concepts that assess developing threats. *MDO 2028* is an example of a document that incorporates assumptions and predictions to drive military strategy. Joint Publication 5-0, *Joint Planning*, defines assumptions as “a supposition about the current situation or future course of events, presumed to be true in the absence of facts,” which are critical to advancing the planning process.⁶⁵ To provide a contextual framework that ties military capabilities and requirements to the anticipated future operational environment, military planners create scenarios to increase understanding. This process allows military leaders at all echelons to “get in contact with a probable unknown situation, to assimilate it,” and propose solutions.⁶⁶ As such, scenarios serve as a way to create a feasible framework that acknowledges technological evolution. It is important, however, to not confuse scenarios with concrete forecasts, but regard them as a tool to expand the realm of possibilities and recognize future opportunities based on anticipated technological evolutions. Additionally, it is important to realize that an underlying factor of scenario building is uncertainty.⁶⁷ To acknowledge the uncertainty and complexity, while keeping the scenario “somewhere between prediction and speculation,” requires the integration of historical and current information, the recognition of behavioral patterns, and the “structuring of a

⁶⁵ Headquarters, Chairman of the Joint Chiefs of Staff (CJCS), "Joint Publication 5-0, *Joint Planning*," Washington, DC: Government Printing Office, June 2017, V-8.

⁶⁶ Marius Potirniche, “*Military Scenario Development*,” *Vojenske Rozhledy*, 26. 33-40, 16 October 2016, accessed 15 September 2019, https://www.researchgate.net/publication/320588106_Military_Scenario_Development/citation/download.

⁶⁷ *Ibid.*, 34.

coherent [story] about the future.”⁶⁸ Other important considerations are the need for the scenario to be aligned with credible, real-life, conditions.

Marius Potirniche, a researcher for the Center for Defense and Security Studies at the National Defence University, Bucharest, created military-specific scenario classifications. The two categories he presents are strategic scenario and exercise scenario. Strategic scenarios are the broadest category and take into consideration military events and capabilities that can occur, and be employed, across the full range of military operations. Exercise scenarios are nested within the strategic scenario framework and are further subdivided into real and fictional. Real scenarios analyze a situation within a real-world mission set, using existing military capabilities, within the constraints of an existing operational environment. Fictional environments assess the current status of military capabilities, as well as anticipated future capabilities, and lay them over an anticipated threat environment that is based on published military operating concepts and modernization frameworks.⁶⁹

This monograph presents two fictional scenarios to illustrate the potential impact of integrating an AI guided battle management system in a future multi-domain fight. All scenarios are based on an in conflict environment against China. The first scenario is set at the corps echelon, and focuses on the convergence of air and naval kinetic strikes, and cyberspace activities “in support of corps scheme of maneuver or on behalf of subordinate echelons.”⁷⁰ The second scenario is set at the division echelon and focuses on the convergence of joint capabilities and the “tailoring of high-volume intelligence” which requires analysis and dissemination.⁷¹ China’s A2AD and military innovation efforts and the US Army’s *MDO 2028* and current modernization

⁶⁸ Arden Brummell, and Greg Mac Gillivray, “*Introduction to Scenarios*,” accessed 24 August 2019, <http://www.scenarios2strategy.com/pdf/Introduction%20to%20Scenarios%20and%20Scenario%0Plannig.pdf>, 2.

⁶⁹ Potirniche, “*Military Scenario Development*,” 33 - 38.

⁷⁰ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, C-6.

⁷¹ *Ibid.*, C-6.

initiatives are used as the contextual scenario background. The scenarios are nested and conclude with an assessment of whether the US Army can integrate AI into its battle management process to effectively converge capabilities in multi-domain operations under the current *MDO 2028* modernization framework, and the potential risks if the service fails to do so.

Scope and Limitations

The framework of this monograph is the US Army's multi-domain operations concept. The focus is not to discuss the legal and ethical ramifications and considerations of AI on the battlefield. Rather it seeks to evaluate how AI can assist in achieving the multi-domain element of convergence in an increasingly complex operating environment. Due to the rapid changes and developments in the field of AI, the evaluation is held at a conceptual level, without going too deep into the endless employments of AI at the tactical and operational level of war. The assessment of whether algorithms can guide the convergence of capabilities is based on current developments, as well as anticipated advances in the field of machine-learning, quantum computing, and autonomous machine-to-machine teaming. All of the information the monograph presents and uses as its foundation is solely pulled from sources that have been cleared for public release. Therefore, it is possible that classified documents exist that contradict the assumptions of this monograph.

Strategic Framework (Scenario One & Scenario Two)

It is 2035. Chinese military forces have initiated an invasion of Taiwan and have begun to block naval access to the South China Seas, under its One-China policy. To defend their interests, the Chinese military's missile defense force is on high alert. The integrated anti-access and area-denial network is supported by long- and mid-range missiles, various anti-aircraft and air defense weapons, as well as various long- and mid-range intelligence collection and surveillance capabilities. China's *New Generation Artificial Intelligence Development Plan* has guided the

development of military technology for the last fifteen years.⁷² At its introduction in 2017, the Chinese leadership declared that “AI has become a new focus of international competition. AI is a strategic technology that will lead into the future; ...the development of AI as major strategy to enhance national competitiveness and protect national security.”⁷³ Consequently, China invested over \$15 billion dollars annually in the development of “intelligentized technology,” focusing on artificial intelligence guided autonomous capabilities. Chinese artificial intelligence integration efforts go beyond the field of military robotics, and include autonomous military decision-making. Based on the potential in deduction, combat command, and decision-making, Zeng Yi, the head of a leading Chinese defense company, pushed developments with the view that “in the future intelligent wars, AI systems will be just like the brain of the human body.”⁷⁴ As a result, the US military faces a Chinese force with capabilities operating at the leading edge of machine-to-machine teaming.

Autonomous reconnaissance drones, attack aircraft, and missile launchers are integrated into an AI guided sensor to shooter network. These developments increase the speed of battle exponentially. Chinese systems can track and engage hundreds of targets simultaneously, and rapidly re-engage and re-task assets, if required. To compete and penetrate the redundant Chinese defense structure requires US forces to rapidly and continuously converge capabilities to penetrate and dis-integrate the Chinese A2AD umbrella. These actions enable the establishment of temporary windows of superiority that corps and division echelon forces can exploit by

⁷² Gregory Allen, “Understanding China’s AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security,” *Center for New American Security*, February 2019, accessed 16 October 2019, <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.

⁷³ The China State Council’s AIDP is available in English at Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania (translators), “Full Translation: China’s New Generation Artificial Intelligence Development Plan,” *New America*, August 1, 2017, accessed 05 October 2019, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-newgeneration-artificial-intelligence-development-plan-2017/>.

⁷⁴ Allen, “Understanding China’s AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security.”

maneuvering into the tactical support area and close area. Within these areas the echelon below corps can converge their organic capabilities against the enemy. This in turn enables the corps to re-compete and converge capabilities in the continuous cycle of penetration and dis-integration to set the conditions for exploitation by lower echelon forces.

In response to China's modernization efforts, the US Army, guided by national security strategies, AI directives, and multi-domain operation concepts invests heavily in machine-to-machine teaming. As a result, US military capabilities include a wide array of self-learning battle network systems that can sense, coordinate effects, and command and control. Individual autonomous robotic and drone systems, as well as larger unmanned aircraft, naval, and missile delivery systems are all operating as autonomous nodes within this framework. Significant advances in the areas of quantum computing by US-based private firms provides a competitive edge to the US military in the form of processing speed and response time. This provides a window of opportunity that allows friendly forces to observe, orient, decide, and act quicker than the enemy.⁷⁵ However, due to technological advances, John Boyd's OODA loop is no longer executed in minutes, but seconds or milliseconds.⁷⁶ These emerging threats cause the US to increasingly remove the human from the loop, which allows the joint force to "operate at a higher, more effective tempo than its adversaries."⁷⁷ However, constrained by ethical regulations concerning the use of autonomous guided systems and AI in warfare the US military still places the human into the decision-making loop. The result is the effective integration of human-machine teaming at the command and control level that allows commanders to choose between an

⁷⁵ Peter Layton, "*Fifth Generation Air Warfare*," (paper No. 43, RAAF Air Power Development Centre, Canberra, June 2017), accessed 16 October 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43Fifth-Generation-Air-Warfare.pdf>, 36.

⁷⁶ Former US Air Force fighter pilot COL (ret.) John Boyd created the observe, orient, decide, act (OODA) loop to allow pilots to enter the enemy's decision cycle and gain a position of advantage in a dogfight. He expanded the concept in a later writing and it is applicable at all echelons of the organization, as well as business organizations.

⁷⁷ Layton, "*Fifth Generation Air Warfare*," 37.

array of options in offensive operations during the competition continuum, while relying on autonomous AI guided action for protection.

The US Army's key command and control system is the AI guided battle management system. It is the hub of the US military's battlefield network. This system collects data from all joint sensors within the operational environment, and continuously pulls and pushes data from, and to, theater and national collection assets to build a common operational picture. This allows the system to analyze the position of enemy and friendly forces on the battlefield. Because the system is self-learning, it continuously assesses enemy actions and capabilities. Simultaneously, it has complete awareness of friendly force capabilities and their status, including the various systems regeneration times, ammunition consumption rates, and resupply statuses. Consequently, the system can identify enemy weaknesses and threats, and execute a continuous assessment cycle to predict how friendly joint capabilities can converge to create a temporary overmatch on the battlefield. In addition, the battle manager calculates munitions optimization, capability de-confliction, and the employment of capabilities that achieve the desired effect, while minimizing collateral damage and risk to force.

Within the battlefield network, the system is linked to joint capabilities across all domains. The various battle management systems itself are horizontally and vertically linked, which allows them to quickly task and re-task capabilities across multiple domains, without losing the ability to achieve their respective objectives. Being connected to all sensor and shooter, allows the system to control the sensor to shooter link, and task the best weapon system to achieve both kinetic and non-kinetic effects. In a protection role, the battle management system operates completely autonomous and controls the elimination of enemy threats to friendly forces and designated areas of protection. Because converging capabilities for the continuum of offensive competition must nest within higher headquarters objectives, the battle management system places the human-in-the-loop for offensive operations. In this role, the system analyzes

the various effects friendly capabilities can achieve by converging joint capabilities at the different echelons.

The multi-domain framework considers US Army corps as expeditionary forces. One of the critical roles at this echelon is the defeat and neutralization of long-range and mid-range systems. As such, they serve as an enabling force for the divisions that fall under their span of control. To compete against a peer threat it is critical to converge capabilities against China's air defense, long-range ground fires, and anti-ship missiles. Additionally, when required, the corps headquarters is responsible for the command and control of the multi-domain joint capabilities operating within their area of operations. The main objective of the converging of kinetic joint fires is the destruction of enemy mid-range weapon systems in order to facilitate the freedom of maneuver for division and brigade assets. Lastly, the corps is responsible for synchronizing the intelligence collection efforts of national, theater, and internal assets. Cyberspace capabilities are inherently integrated within the convergence efforts, including national and theater level assets. The overall intent is to layer the convergence efforts in order to provide multiple options and create various cross-domain synergy capability variations.

Within the competition cycle, corps focus on the penetration and dis-integration of enemy defense umbrellas. The penetration of China's A2AD umbrella includes the dis-integration of the enemy's long-range fire systems. This includes neutralizing radars and key command and control nodes, which can have a greater and longer-lasting impact than the destruction of the delivery systems. Another aspect of penetration is the contesting of enemy ground force maneuver and the synchronization of friendly "maneuver from operational and strategic distances" during windows of temporary superiority.

At the division level, forces focus on dis-integration and exploitation. At the onset of conflict, they can serve as forward presence or expeditionary forces. The primary role of the division is to set the conditions for lower echelon forces to maneuver and compete in the close area. Primary responsibility for the division is the convergence of "aviation, fires, EW, maneuver

support, and multi-brigade maneuver to achieve positions of advantage.”⁷⁸ Critical is the destruction or neutralization of the enemy’s mid-range fires assets. At this echelon, the division has the ability to synchronize organic assets with higher headquarters, and incorporate allocated joint air and naval capabilities. Against a peer-competitor with autonomous and AI guided systems, the success at both echelons is impacted by their ability to conduct multi-domain synchronization and the level of capability autonomy.

Scenario 1 – Corps Echelon

The 18th US Army Airborne Corps Headquarters is located in the operational support area. The primary role of the organization is to shape conditions on the battlefield that the divisions and enablers under its control can exploit to move into the close maneuver area.⁷⁹ Offensive actions center on four objectives – neutralization of enemy long-range air defense assets, dis-integration of China’s mid-range fire capabilities, deceleration of China’s ground forces, and the creation of “convergence at lower echelons by allocation resources, sequencing division maneuver, and incorporating it with depth.”⁸⁰ Although the distance to the close and deep maneuver area exceeds 1500 km, friendly forces are under a constant threat of kinetic targeting by Dongfeng intermediate-range ballistic missiles and non-kinetic targeting within the cyber and space domain.⁸¹

For protection, the 18th US Army Airborne Corps’ AI battle management system is continuously linking into national and theater collection assets to gather intelligence. Upon detection of an enemy threat, the battle management system automatically coordinates with

⁷⁸ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 23.

⁷⁹ *Ibid.*, 22.

⁸⁰ Dis-integration is the targeting of a sub-capability to interrupt and temporarily, or permanently, disable a fires capability. The sub-capability ranges from radar vehicles to command and control stations; US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 22 - 23.

⁸¹ The Chinese DONGFENG (“East-Wind”) missile-type is a high velocity ballistic cruise missile, with a range of 1200 - 1800 miles capable of hitting ground and naval targets.

theater and national sensors to identify the threat and facilitates a sensor hand-over that ensures collection overlap while mitigating unnecessary asset redundancy. Simultaneously, it identifies multiple delivery platforms across all domains to build a robust kill-chain that is executable in a time-constrained environment despite the potential loss of primary links.⁸²

Space sensors provide continuous updates to the system concerning the disposition of the various components of the enemy's long and mid-range fires capabilities. In the meantime, the battle management system identifies a naval destroyer as the asset with the highest probability of success in destroying the incoming missile. Simultaneously, the system identifies additional friendly assets that can respond to the threat and prioritizes them in accordance with its current assessment of the overall operational environment. Some of the factors the system considers based on its algorithm are: risk to force, probability of success, ammunition status, capability reset time, and collateral damage.

For protection efforts, the battle management system operates in a human-on-the-loop construct. This means the corps' operations center can observe the developments, and in an emergency, can intervene, but the process is designed for the battle management system to act autonomously.⁸³ The number of enemy threats, and the speed at which they can operate drives the need for autonomous operation. As soon as an incoming missile is detected, the battle management system executes the outlined sequence in a matter of seconds to destroy the enemy threat. This cycle occurs simultaneously and continuously in response to emerging threats. Three aspects make the autonomous operation of the intelligence guided battle management system in the defense critical. First, the ability to close the shooter-to-sensor link within seconds to counter threats operating at hypersonic speed. Second, the ability to build robust and redundant kill-

⁸² Ways for the primary method to become infeasible are destruction of the sensor or shooter platform, friendly maneuver, changes in the collateral assessment, or enemy movements.

⁸³ A criteria for the system to be operated with the human-in-the-loop is the event that autonomous decisions do not meet the protection requirements due to a failure autonomous observation-to-action loop.

chains that can quickly integrate alternate and contingent capabilities. Third, the ability to direct protection efforts while optimizing the use of resources that are limited and difficult to resupply. Simultaneously to protection operations, the system analyzes the operational environment to detect opportunities for offensive action.

For offense operations, the battle management system operates in a human-in-the-loop mode. US government policies on the ethical use of artificial intelligence and autonomous weapons, as well as public perception concerning the use of autonomous weapon systems guided by artificial intelligence, are the basis for the decision to leave humans in the decision chain. The US Army's *Project Quarterback* efforts provided the framework for the construct of the current battle management system. Similar to the protection efforts, the battle management system continuously pulls data from external and organic sensors. It then assesses how joint capabilities can converge to temporarily disable parts of the enemy's defense umbrella and allow subordinate units to advance and bring their organic assets into range.

Because the deconfliction of joint assets in time and space needs to be executed and synchronized in a matter of seconds, the battle management system continuously analyzes the operational environment. In the process, it restructures parts of the OODA loop concept to gain the ability to get into an autonomous enemy decision-cycle that occurs in seconds or milliseconds. The system achieves this by continuously observing the battlespace and simultaneously analyzing what friendly forces are oriented to respond to a threat, rather than observing and then orienting. The system then produces a series of available options to conduct an offensive strike. Within the corps' operation center, the options are displayed on an interactive display that allows the individual with the proper release authority to decide which action to take. By continuously analyzing and reconfiguring possible sensor-to-shooter loops, the system creates a decision space that mitigates the disadvantages of placing a human-in-the-loop against a peer-competitor who relies heavily on autonomous capabilities. After the proper authority in the operations center commits to target an enemy asset, the battle management system converges

capabilities from various selected joint enablers by synchronizing reliant effects in time and space.

In this case, prior to launching the friendly missile, the battle management system coordinates an offensive cyber action that floods the enemy radar with threat signals, which increases the missile's chance of successfully penetrating the enemy's anti-access and area denial umbrella.⁸⁴ As soon as the cyber effect is created, the battle management system directs the launch of the missile and observes the enemy response to relaunch another missile, if necessary, and to detect additional targeting opportunities. The missile finds its target and destroys it. As soon as the sensor confirms impact, the battle management system disseminates a message to media outlets aligned with the existing information operation line of effort. Simultaneously, the battle management systems re-calculates ammunition availability and recycling rates of friendly delivery platforms. This data is used to optimize ammunition usage for future strikes and to build a resupply prioritization list for sustainment forces.

This process is repeated continuously as friendly forces advance and the corps' shapes the deep maneuver area and the operational deep fires area. US Army divisions exploit the temporary windows of superiority and freedom of maneuver to advance and bring the enemy within the effective range of their organic weapon systems. This sets the conditions for competition in the close and deep maneuver areas, which shifts the battlespace boundaries and restarts the cycle of competition.

Scenario 2 – Division Echelon

After the 18th US Army Airborne Corps sets the conditions, the 3rd Infantry Division positions to maneuver into the close area and defeat enemy ground forces on Taiwan. This area is the first time military formations contesting for “control of physical space in support of campaign

⁸⁴ The sensor flooding can occur in the form of cyber infiltration or the use of swarming through the unmanned aerial vehicle emitters.

objectives,” operate within the close range to the enemy.⁸⁵ Because friendly ground units are expected to conduct independent maneuver in this contested space, it is critical to possess the ability to converge capabilities faster than the enemy in order to drive the tempo and maintain the initiative. The goal of ground maneuver units is to coordinate maneuver during windows of temporary advantage to “defeat enemy forces, disrupt enemy capabilities, physically control spaces, and protect and influence populations.”⁸⁶ Enemy forces in the close area depend on an interconnected network of autonomous intelligence, surveillance, and reconnaissance (ISR) strike systems, integrated air defense systems, and ground combined-arms formations. The integration of AI into the decision-making cycle drastically increases the enemy’s tempo of operations. To gain a position of advantage requires the continuous interruption of the enemy’s capabilities, preferably at their command, control, and sensor nodes.⁸⁷

As 3rd Infantry Division forces maneuver, the battle management system continuously collects and compares data to build a common operating picture that illustrates the composition and disposition of friendly and enemy forces. Based on the data, the system starts to analyze the enemy’s defense network to identify enemy sensors, ISR platforms, and information streams.⁸⁸ During this phase, ground forces operate dispersed, and the battle management system focuses on deception measures that force the enemy to expose their capabilities. As soon as the enemy exposes their systems, the battle management system synchronizes reconnaissance data collected by national and theater assets with those collected by organic and adjacent unit intelligence and reconnaissance capabilities. It then coordinates with the battle management systems of adjacent units and higher headquarters to de-conflict the engagement. This action ensures multiple assets

⁸⁵ HQDA, “Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040,” December 2017, accessed 17 December 2019, [https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20\(1\).pdf](https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf), 10.

⁸⁶ *Ibid.*, 10.

⁸⁷ *Ibid.*, 36 - 45.

⁸⁸ *Ibid.*, 38.

across echelon do not prosecute the same target.

As soon as the higher headquarters' battle management system pushes authority to the 3rd Infantry Division, the division's battle management system scans across organic capabilities to create a sensor to shooter link with the highest possibility of success. If the system is unable to develop a link, or the probability of success falls below predetermined thresholds, the system pushes the target back up to the higher headquarters' system to expand the array of available joint assets that can prosecute the target and raise the probability of success. When the threat can be pursued with organic assets, the division battle management system confirms the disposition of friendly forces to clear the ground, analyzes the munition status across the various weapon systems, and tasks the identified delivery platform. As soon as the sensor cycle is complete, the battle management system signals the selected weapon system to engage.

Immediately upon releasing the munition, the battle system updates the ammunition supply status, resets the regeneration cycle, sends a resupply request to the logistics combat support units, and tracks the threat until its destruction. It is a cycle that takes seconds, and occurs repeatedly during penetration and dis-integration efforts. As division forces advance, the battle management system pushes information operation messages across various media platforms that support the US narrative. Every kinetic engagement is accompanied by a messaging effort that is tailored to the demographics of the region. As operations progress, the system continuously assesses enemy information activities and presents proposed counter-messages that allow friendly forces to maintain the initiative in the information spectrum.

While friendly forces continue to compete within the enemy's anti-access and area-denial umbrella, the battle management system repeatedly identifies enemy sensors and establishes redundant kill-chains to defeat enemy ground forces. Every time an enemy ISR sensor is eliminated, the system assesses the impact the destruction has on the enemy's ability to engage friendly formations. The consequent establishment of temporary non-coverage areas is exploited by maneuver forces to advance their organic assets. Simultaneously, the battle management

system restarts the convergence of cyber, space, and drone sensors to detect a new target, and converge capabilities to establish a new temporary window of opportunity that can be exploited to advance the maneuver division ground forces.

These activities occur within seconds, and events occur at a speed that by far exceeds the human cognitive cycle. As operations progress, the self-learning algorithms of the battle management systems continue to analyze and identify patterns within the enemy's behavior. As a result, the system enables a cycle of continuous competition against Chinese ground forces and their defensive efforts.

Implications

The willingness of US adversaries to integrate and merge autonomy and AI drives the need for the US military to develop and employ competitive capabilities. These developments raise the need to execute multi-domain convergence in rapid succession when facing a peer threat. Because converging joint capabilities across multiple domains requires the analysis of vast amounts of information, the process pushes a human-led synchronization process outside of the enemy's decision-making cycle. Furthermore, multi-domain convergence involves the establishment of redundant kill-chains. It is not enough to establish a single sensor to shooter convergence chain through deconfliction. Instead, convergence requires the identification and employment, if necessary, of redundant capabilities that can prosecute a target, or provide protection efforts. Establishing redundant kill-chains which synchronize joint-capabilities quickly is a critical and simultaneous effort due to the continuously shrinking timeframe in which windows of superiority exist.

Overall, future battle-management systems must link horizontally and vertically across joint platforms to meet multi-domain operation requirements and possess the ability to coordinate operations in seconds or milliseconds. In addition, to converge capabilities, an AI guided battle management system can close the capability gap of ammunition optimization in a contested

resupply environment. The systems achieves this by continuously assessing the optimal target-to-munition combination and avoiding target overkill that expends munitions unnecessarily. Unfortunately, the current method of developing command and control platforms which largely occurs along service stovepipes will slow the ability to establish the technical framework required to converge capabilities in a future fight.

Conclusion

The impact AI and autonomy has on the tempo of battle supports Lieutenant Colonel (Ret.) Robert L. Leonhard's claim that "time is increasingly becoming [war's] critical dimension."⁸⁹ The merging of AI with autonomous capabilities allows a military force to drastically increase the frequency at which activities occur, which in turn drives the tempo of sequence and shortens the windows of opportunity. It is a relationship that further accelerates when artificial intelligence guides autonomous systems without a human in the observation-decision-action loop. Time, and the ability to observe and act faster than the enemy, becomes a critical factor in the execution of convergence that enables friendly forces to achieve a temporary position of advantage.

The United States has not faced a peer rival since the proliferation of computer networks, tactical data links, and satellite communications. Current efforts in the area of quantum technology, artificial intelligence, and autonomy challenge the ability of US military services to operate independently within their respective dominion. Consequently, as the US Army's *MDO 2028* concept anticipates, the ability to create a temporarily exploitable advantage on the battlefield relies on the ability to converge joint capabilities across multiple domains. Currently, this process is primarily executed by coordination cells whose main task is to converge

⁸⁹ Chris Field, Reading For War: Fighting By Minutes: Time and the Art of War by Robert Leonhard, 4 July 2017, accessed 8 January 2020, <https://cove.army.gov.au/article/fighting-minutes-time-and-the-art-war-robert-leonhard>.

capabilities by “episodic synchronization of domain-federated solutions.”⁹⁰ However, the complexity of converging against a peer competitor whose AI guided and autonomous weapons systems shorten the decision and synchronization loop to minutes or seconds requires the development of new technology. *MDO 2028*’s architects acknowledge this shortcoming, and the complexity of the task, and list convergence considerations that call for the development of new military technology to fill this critical gap.⁹¹

Consequently, future C2 systems need to provide commanders at all echelons with a common operating picture of all joint assets within a battlespace that is as close to complete as possible. Additionally, the systems need to rapidly transmit reconnaissance and target data to prosecute proposed targets with kinetic and non-kinetic means. However, even if future C2 systems can provide commanders and their staffs with the data that allows them to converge capabilities across multiple domains, the vast amounts of information associated with the task of converging capabilities within rapidly fleeting windows of opportunity quickly exceeds human cognitive abilities. Additionally, other factors such as ammunition optimization requirements and varying capability regeneration windows further increase the complexity of converging capabilities in multi-domain operations.⁹²

Current efforts to meet the emergent threats show that the US military services are still slow to develop and field Department of Defense wide capabilities. The fact that the US military is in a restructuring process presents an opportunity to create systems that focus on fighting a war that requires nested and linked C2 systems that facilitate the rapid handover and integration of joint enablers. Failure to build these capabilities now will result in the development of a force that is multi-domain in name only, because instead of converging capabilities as envisioned in *MDO*

⁹⁰ US Training and Doctrine Command, *TRADOC PAM 525-3-1*, 20.

⁹¹ *Ibid.*, A1 - B2.

⁹² *Ibid.*, 20, C7 - C8.

2028, military forces will fallback-on established processes of deconfliction and synchronization, which is a procedure that is too slow and inefficient to stay competitive.

As this paper illustrates, the only way to stay competitive against a peer-threat with AI guided and autonomous weapons systems is to develop similar capabilities that can establish and execute a redundant sensor-to-shooter link within seconds. Integration of AI into the battle management process is not a question of maintaining domain superiority, but ensures that the US military can compete to create short windows of advantage in a continuous cycle of competition, exploitation, and re-competition that plays out in seconds across all warfighting domains.

Bibliography

- Allen, Gregory. "Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security." *Center for New American Security*, 6 February 2019. Accessed 16 October 2019. <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.
- Boykin, Dennis and King, Scott. "Distinctly Different Doctrine: Why Multi-Domain Operations Isn't AirLand Battle 2.0." *Association of the United States Army* (February 2019). Accessed 17 September 2019. <https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn-t-airland-battle-20>.
- Brummer, Arden, and Gillivray Greg Mac. "Introduction to Scenarios." N.d. Accessed 24 August 2019, <http://www.scenarios2strategy.com/pdf/Introduction%20to%20Scenarios%20and%20Scenario%0Plannig.pdf>, 2.
- Center for Strategic and International Studies. Missile Defense Project, S-400 Triumph: Missile Threat. *Missile Defense Project*, 4 May 2017, last modified June 15, 2018. Accessed 18 November 2019. <https://missilethreat.csis.org/defsys/s-400-triumf/>.
- CNA Analysis and Solutions. "Impact of Unmanned Systems to Escalation Dynamics." Accessed 3 September 2019. https://www.cna.org/CNA_files/PDF/Summary-Impact-of-Unmanned-Systems-to-Escalation-Dynamics.pdf.
- Davis, Zachary. "Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise." Center for Global Security Research Lawrence Livermore National Laboratory, March 2019. Accessed 12 October 2019. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf, 6.
- Dickson, Ben. "What is Narrow, General and Super Artificial Intelligence." Accessed 14 October 2019. <https://bdtechtalks.com/2017/05/12/what-is-narrow-general-and-super-artificialintelligence/>.
- Endsley, Mica. *Autonomous Horizons: System Autonomy in the Air Force—A Path to the Future, Volume 1: Human-Autonomy Teaming*. Washington, DC: Department of the Air Force, 2015.
- Field, Chris. "Reading For War: Fighting By Minutes: Time and the Art of War by Robert Leonhard." 4 July 2017. Accessed 8 January 2020. <https://cove.army.gov.au/article/fighting-minutes-time-and-the-art-war-robert-leonhard>.
- Freedberg, Sydney. "The Art of Command, The Science of AI." *Breaking Defense* (November 2019). Accessed 14 October 2019. <https://breakingdefense.com/2019/11/the-art-of-command-the-science-of-ai/>.
- . "Air Force ABMS: One Architecture To Rule Them All?." *Breaking Defense* (November 2019). Accessed 05 December 2019. <https://breakingdefense.com/2019/11/air-force-abms-one-architecture-to-rule-them-all/>.

- . “Faster than Thought: DARPA, Artificial Intelligence, and the Third Offset Strategy.” *Breaking Defense*, 11 February 2016. Accessed 2 September 2019. <https://breakingdefense.com/2016/02/faster-than-thought-darpa-artificial-intelligence-the-third-offset-strategy/>.
- Garcia, Ecatarina. “The Artificial Intelligence Race: U.S. China and Russia.” *Modern Diplomacy*, 19 April 2018. Accessed 21 August 2019. <https://moderndiplomacy.eu/2018/04/19/the-artificial-intelligence-race-u-s-china-and-russia/>.
- Gertz, Bill. “China Developing Battlefield AI for High-Technology Warfare.” *Washington Times* (30 January 2019). Accessed 2 September 2019. <https://www.washingtontimes.com/news/2019/jan/30/chinas-military-outlines-artificial-intelligence-p/>.
- Gunning, David. “Explainable Artificial Intelligence (XAI).” Defense Advanced Research Projects Agency. Accessed 19 August 2019. <https://www.darpa.mil/program/explainable-artificial-intelligence>.
- Hoffmann, Achim. “Can Machines Think? An Old Question Reformulated.” *Minds and Machines* 20, no. 2 (June 2010): 203–212.
- The Association of the United States Army. “Concepts Drive Change.” PowerPoint Presentation, Association of the United States Army, 4 October 2018. Accessed 14 November 2019. https://www.ausa.org/sites/default/files/ILW-CMF_MDO_general-slides.pdf.
- . “Integrating Army Robotics and Autonomous Systems to Fight and Win.” *Institute of Land Warfare* 17, no. 2. (July 2017): 1–4. Accessed 5 September 2019. <https://www.ausa.org/sites/default/files/publications/SL17-2-Integrating-Army-Roboticsand-Autonomous-Systems-to-Fight-and-Win.pdf>.
- Kania, Elsa. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power*. Washington, DC: Center for a New American Security, 2017.
- Layton, Peter Layton. “Fifth Generation Air Warfare” Paper No. 43, RAAF Air Power Development Centre, Canberra, June 2017. Accessed 16 October 2019. <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43-Fifth-Generation-Air-Warfare.pdf>
- Lynch, Ricky, and Michael McGee. “Military Applications of Artificial Intelligence and Robotics.” *Military Review* 66, no. 11, (December 1986): 50-56.
- Lorenz, Bernd, and Raja Parasuraman. “Automated and Interactive Real-Time Systems.” In *Handbook of Applied Cognition*. 2nd ed., edited by Francis T. Durso, Raymond S. Nickerson, Susan T. Dumais, Stephan Lewandowsky, and Timothy J. Perfect, 414-441. Chichester, UK: John Wiley & Sons, 2007.

- Mainzer Klaus. "Toward a Theory of Intelligent Complex Systems: From Symbolic AI to Embodied and Evolutionary AI." In *Fundamental Issues of Artificial Intelligence*, edited by Vincent C. Müller, 241-259. Cham: Springer, 2016.
- Maneuver, Aviation, and Soldier Division, Army Capabilities Integration Center. *The US Army Robotic and Autonomous Systems Strategy*. Fort Eustis, VA: Government Printing Office, March 2017.
- McCarthy, John. "Programs with common sense." In *Proceedings on the Symposium on Mechanization of Thought Processes*, Vol. 1, edited by D. V. Blake and A. M. Uttley, 75 - 84. London: Her Majesty's Stationery Office, 1958.
- McCoy, Kelly. "The Road To Multi-Domain Battle: An Origin Story." *Modern War Institute* (October 2017). Accessed 17 September 2019. <https://mwi.usma.edu/road-multi-domain-battle-originstory/>.
- McCullough, Amy. "Life After JSTARS." *Airforce Magazine*, 21 March 2019. Accessed 24 November 2019. <https://www.airforcemag.com/article/life-after-jstars/>.
- Nilsson, Nils J. *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Cambridge: Cambridge University Press, 2009.
- Office of the President of the United States. *National Security Strategy of the United States of America*. Washington, DC: Government Printing Office, December 2017. Accessed 18 September 2019. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- Perkins, David. "Multi-Domain Battle: Joint Combined Arms Concept For The 21st Century." *Association Of The United States Army* (November 2016). Accessed 14 October 2019. <https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms>.
- . "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." US Department of Defense. Last modified 21 July 2017. Accessed 7 September 2019. <https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computeralgorithms-to-war-zone-by-years-end/>.
- Potirniche, Marius. "Military Scenario Development." *Vojenske Rozhledy*, no. 26 (October 2016): 33-40. Accessed 15 September 2019. https://www.researchgate.net/publication/320588106_Military_Scenario_Development/citation/download.
- Rabunal, Juan R., and Julian Dorado. *Artificial Neural Networks in Real-Life Applications*. Hershey, PA: Idea Group, 2006.
- Reilly, Jeffrey. "Over the Horizon: The Multi-Domain Strategist." *Over The Horizon* (November 2018). Accessed 18 September 2019. <https://othjournal.com/2018/11/08/oth-mdos-reilly/>.
- Russell, Stuart. "Rationality and Intelligence: A Brief Update." In *Fundamental Issues of Artificial Intelligence*, edited by V. C. Müller, 7-28. Cham, Switzerland: Springer International Publishing, 2016.

- Skinner, Douglas R. "AirLand Battle Doctrine." Center for Naval Analysis, Alexandria, VA, 28 December 1988. Accessed 12 September 2019.
<https://apps.dtic.mil/dtic/tr/fulltext/u2/a202888.pdf>.
- Systematic. "SITWARE C4I Suite." N.d. Accessed 19 November 2019.
<https://www.systematicinc.com/products/n/sitaware/>.
- Thompson, Christopher. "The Future of Fires Software: AFATDS and JADOCS." N.d. Accessed 17 November 2019. https://sill-www.army.mil/firesbulletin/archives/2018/mayjun/articles/183_6_Thompson.pdf.
- Townsend, Stephen. "Accelerating Multi-Domain Operations: Evolution of an Idea." *Military Review* 98, no. 5 (September-October 2018): 4-7. Accessed 2 September 2019.
<https://www.armyupress.army.mil/Journals/Military-Review/EnglishEditionArchives/September-October-2018/>.
- Trautman, Erik. "How Artificial Intelligence is Closing the Loop with Better Predictions." Accessed 12 October 2019. <https://www.eriktrautman.com/posts/how-artificial-intelligence-is-closing-the-loop-with-better-predictions>.
- Tucker, Patrick. "The US Army Wants to Reinvent Tank Warfare with AI." *Defense One*, 18 October 2019. Accessed 24 November 2019.
<https://www.defenseone.com/technology/2019/10/us-army-wants-reinvent-tankwarfare-ai/160720/>.
- . "What Is Machine Learning - A Complete Beginner's Guide." Bernard Marr & Co. 2018. <https://www.bernardmarr.com/default.asp?contentID=1140>.
- US Air Force. "Air Force Future Operating Concept: A View of the Air Force in 2035." Washington, DC: Government Printing Office, September 2015.
- US Department of Defense. "Summary of the 2018 Department of Defense Artificial Intelligence Strategy." Washington, DC: Government Printing Office, December 2018.
- . "Defense Science Board: Summer Study on Autonomy." Washington, DC: Government Printing Office, June 2016.
- . Chairman of the Joint Chiefs of Staff, Joint Publication 5-0, *Joint Planning*. Washington, DC: Government Printing Office, June 2017.
- US Training and Doctrine Command. Army Training and Doctrine Command Pamphlet 525-3 1, *The US Army in Multi-Domain Operations 2028*. Washington, DC: Government Printing Office, December 2018.
- . Army Training and Doctrine Command Pamphlet 525-3-3, *The US Army Functional Concept for Mission Command 2020-2040*. Washington, DC: Government Printing Office, 2017.
- . "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, December 2017. Accessed 17 December 2019.
[https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20\(1\).pdf](https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf).

- . *Robotics, Artificial Intelligence & Autonomy: Visioning Multi-Domain Warfare in 2030-2050*. Washington, DC: Government Printing Office, December 2018.
- Weisgerber, Marcus. “General: Project Maven Is Just the Beginning of the Military’s Use of AI.” *Defense One*, June 28, 2018. Accessed 19 August 2019. <https://www.defenseone.com/technology/2018/06/general-project-maven-just-beginning-militarys-use-ai/149363/>.
- West, Nicholas. “U.S. Military Seeks A.I. Quarterback to Call Plays for The Internet of Battlefield Things.” *Activist Post*, 22 October 2019. Accessed 27 November 2019. <https://www.activistpost.com/2019/10/u-s-military-seeks-a-i-quarterback-to-call-plays-for-the-internet-of-battlefield-things.html>.
- . “The Pentagon’s New Artificial Intelligence Is Already Hunting Terrorists.” *Defense One*, 21 December 2017. Accessed 19 August 2019. <https://www.defenseone.com/technology/2017/12/pentagons-new-artificial-intelligence-already-hunting-terrorists/144742/>.
- Weiss, Gerhard. *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*. Cambridge, MA: The MIT Press, 2000.
- White House Press. “Artificial Intelligence For The American People.” Accessed 14 October 2019. <https://www.whitehouse.gov/ai/>.
- Willis, Brian. “Multi-Domain Operations at the Strategic Level.” *Over The Horizon* (March 2018). Accessed 18 September 2019. <https://othjournal.com/2018/03/02/multi-domain-operations-at-the-strategic-level/>.