THEATER ARMY ROLE IN MULTI-DOMAIN OPERATIONS INTEGRATED RESEARCH PROJECT

Gregory L. Cantwell, Ph.D., Colonel, US Army, retired
Faculty Team Lead and Editor

UNITED STATES ARMY WAR COLLEGE

Theater Army in Multi-Domain Operations

Integrated Research Project

Gregory L. Cantwell, Ph.D.

Faculty Lead and Editor

Faculty Advisors

Mark Balboni	**Lieutenant Colonel**	**U.S. Army**
Dr. John Bonin	**Professor of Concepts and Doctrine**	
Ms. Megan Casey	**Research Librarian**	
Dr. G.K. Cunningham	**Professor of Strategic Landpower**	
Mr. Gregory D. Hillebrand	**Professor of Space and Cyberspace**	
Mr. Ben Leitzel	**Professor of Cyberspace**	
Paul Mikolashek	**Senior Mentor, Professor**	
	Lieutenant General	**U.S. Army, Retired**
Dr. James Morningstar	**Visiting Professor**	
Dr. John Eric Powell	**Visiting Professor / Liaison Officer MSCoE**	
Dr. Bert B. Tussing,	**Professor of Homeland Defense and Security**	
Mr. Peter Whalen	**Visiting Professor**	

Students

Darren Buss	**Colonel**	**U.S. Army**
Dan Harris	**Lieutenant Colonel**	**U.S. Air Force**
Michael Hays	**Lieutenant Colonel**	**U.S. Marine Corps**
Eric Jacobson	**Colonel**	**U.S. Army**
Brian Newill	**Colonel**	**U.S. Army**
Shawn Underwood	**Colonel**	**U.S. Army**
Michael West	**Colonel**	**U.S. Army**

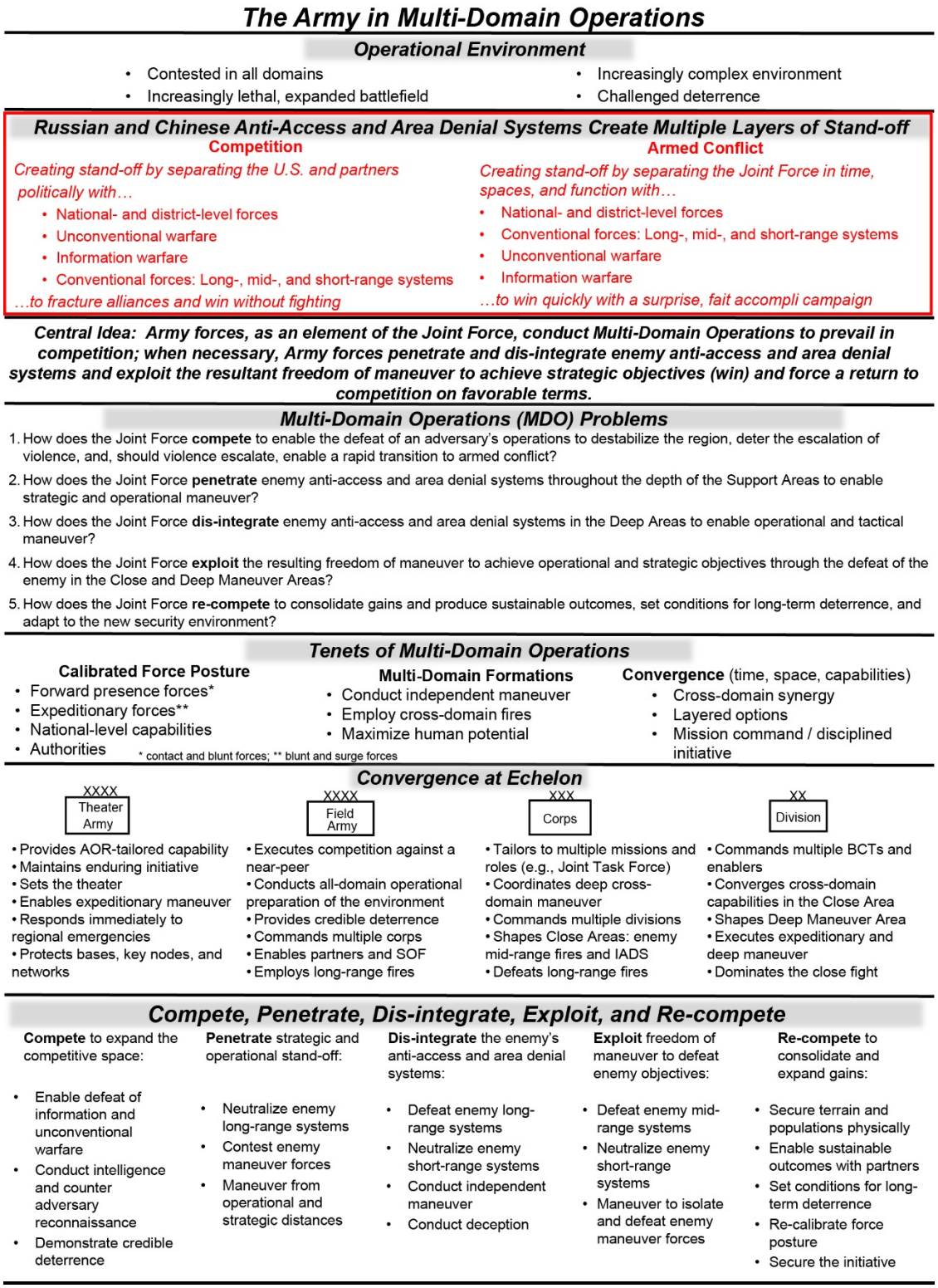

Figure 1. Logic Chart, Army in Multi-Domain Operations[1]

[1] U.S. Army Training and Doctrine Command, The U.S. Army in Multi-Domain Operations 2028, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), v.

Table of Contents

Acknowledgements and Methodology

This Integrated Research Project (IRP) was made possible by the works of many dedicated faculty members and Army professionals serving across the globe. Without their interest and support, this research would not have been possible. This project grew from the Strategic Studies Institute's (SSI) request for topics that the Army War College should research for the next year. I proposed that the Army War College should address the professional military education (PME) gap of understanding the roles, responsibilities, and authorities of the Army Service Component Commands (ASCC) and the theater army. How these roles are addressed in the Multi-Domain Operations (MDO) Concept are central to the future application of strategic Landpower.

The US Army War College (USAWC) embraced the study proposal and I assumed faculty lead for the effort. The Faculty team in the Strategic Landpower and Futures Group (SLFG) in the Center for Strategic Leadership (CSL) graciously offered their expertise to assist in this analysis. Members of the Department of Military Strategy, Plans, and Operations (DMSPO) also offered their expertise. The students self-selected to participate in this yearlong effort of more than 45 seminar contact hours.

The IRP team also participated in the Futures Study Program (FSP) Strike-Table Top Exercise (TTX) in support of Army Futures Command and the Mission Command Center of Excellence (MCCoE) at Fort Leavenworth, Kansas. Many thanks to COL Tim O'Sullivan and Mr. Duane H. Riddle and their team of professionals for including us in the program. The students attended the overview briefing and discussions in the seminar break out rooms, as their schedules permitted. Leaders of the exercise stated

the few hours spent in seminar with the USAWC IRP Students was the most productive time of the week. We examined many challenges that they will incorporate into their future experiments and exercises. Similarly, the students and faculty enjoyed the opportunity to participate in a relevant exercise that may shape the future MDO doctrine for the Army and Joint force.

Special recognition is required for members of the staff and faculty that made this project possible. Many members of the SLFG selflessly gave their time to the students to help them with their research and writing. Their contributions were in addition to their position requirements in an effort to support the students and make relevant contributions to the Army. Dr. John Bonin has been serving the Army for nearly forty years and has become a renowned authority on Army force structure, concepts and doctrine, and Joint doctrine. He was influential in providing a basis of knowledge for understanding the authorities, roles, and missions of the theater army and echelons above brigade (EAB). LTC Mark Balboni also assisted with many of the concepts and doctrine related subjects and the conduct of the seminars. Ms. Megan Casey provided assistance as the research librarian and presented a seminar session on research methodology. Professor Gregory Hillebrand and Professor Ben Leitzel provided seminars on space and cyber space operations to converge capabilities in Multi-Domain Operations. LTG(R) Paul Mikolashek reviewed all the seminar research topics and facilitated a seminar on his experience as a Theater Army Commander and the projected role of the ASCC in MDO. Mr. Pete Whalen provided a presentation on intelligence and the future operating environment. Dr. Eric Powell and Dr. Bert Tussing facilitated a discussion on homeland defense and homeland security. Dr. James

Morningstar provided editing and assistance to the students along their research journey throughout the year.

The DMSPO Department Chair, COL Douglas Winton, also supported the idea and encouraged participation of the DMSPO faculty. Dr. G.K. Cunningham recruited student participation in the program and combined the effort with his scheduled Landpower elective course. He also provided a seminar presentation on component operations.

The students recorded a podcast for the Army War College “War Room” which provided a brief overview of their key points from their research. Additional thanks to Mr. Granieri and Mr. Haberichter for helping to coordinate, conduct, and edit this session to make it available in an audio format. COL Darren Buss also provided assistance in coordinating, rehearsing, and completing this recording.

Finally, all the IRP students should be commended for their professionalism in volunteering to conduct extra work and learn about the science of how the Army prepares for large scale combat operations at the strategic level. They also provided recommendations for the USAWC Core curriculum to include some of the MDO IRP lessons next year. Understanding MDO, and the related modernization initiatives, will likely remain important for the remainder of the students’ Army careers.

Introduction

In TRADOC Pamphlet 525-3-8, the Multi-Domain Operations Concept, LTG Lundy expressed that a generation of Army leaders have experienced counter-insurgency and stability operations in combat in Iraq and Afghanistan. The Army transformed from a division centric to a brigade centric force to meet the challenges of these protracted conflicts. Many Army units at echelons above brigade (EAB) underwent reductions in strength to fully resource operations at the brigade level. This focus on small unit operations has let the skills required for the Army to conduct large scale combat operations (LSCO) to atrophy. He also proposed, LSCO are more probable now than at any time since the end of the Cold War.[2]

Near peer adversaries have taken advantage of our resource commitment to brigades and modernized their militaries. Some reports suggest that at least 17 major capability gaps exist between both China, Russia, and the United States. These gaps give China and Russia an advantage over the United States. Further, both nations have improved their defenses and increased the range, quality, and quantity of their indirect fire and missile systems. China and Russia both have established anti-access, area denial (A2/AD) capabilities to guard their homelands against an expeditionary army or attacking force. This capability provides Russia and China almost unlimited freedom of action beneath their defensive umbrella of fires and A2/AD. In response to these

[2] U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, *TRADOC Pamphlet 525-3-1* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), iv. https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018

gaps, Multi-Domain Operations (MDO) Concept addresses the challenges of LSCO against a near peer adversary.[3]

The MDO concept defines a future operating environment with three conditions. They are: near peer adversaries in constant competition below armed conflict, armed conflict, and a return to competition below armed conflict. Specifically, "Competition below armed conflict occurs when two or more actors in the international system have incompatible interests but neither seeks to escalate to open conflict."[4] Adversaries will continue to use all means available to achieve their goals without triggering an armed conflict. However, the current capability gaps provide an advantage to the near peer adversary operating within their A2/AD environment.[5]

Actions taken in the competition phase before armed conflict become increasingly important because they set the conditions in the theater that determine the strategic options available to the Combatant Commander (CC). In fact, the goal should be to succeed in setting the theater in the competition phase to deter the adversary and avoid conflict completely. The theater army, field army, corps, and division headquarters will have increased roles in competition and large scale combat operations than they have had in recent conflicts. Specifically, the theater army maintains the only forward presence in many regions and is responsible for completing all coordination and agreements with partner nations to provide a credible deterrent force. Should

[3] TRADOC Pamphlet 525-3-1, 10.

[4] TRADOC Pamphlet 525-3-1, 14.

[5] The United States Institute for Peace (USIP), *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission (NDSC)* (Washington, DC, November 18, 2018), iv.

deterrence fail and conflict emerge, the theater Army may be the only land component headquarters available to respond to a crisis.

The theater army headquarters also serves as the Army Service Component Command (ASCC) for the CC. The ASCC also is responsible for all the Title 10, USC Service responsibilities in the theater. This includes Army support to other Services (ASOS) and executive agent responsibilities. Joint Publication 3-31 provides the doctrinal role of a Theater Joint Force Land Component Command (TJFLCC). Six of the seven CCs have identified their ASCC as the Theater Joint Force Land Component Command (TJFLCC). Admiral Locklear, Commander of US Pacific Command was among the first to designate the theater army as the TJFLCC. In his Initiating directive he specified the role for the JFLCC, as stated in Joint doctrine.

> The primary responsibilities of the theater JFLCC may be to provide coordination with other theater-level functional components, to provide general support to the multiple JFLCCs within the AOR, to conduct theater-level contingency planning, or to conduct joint reception, staging, onward movement, and integration (JRSOI) for the entire joint land force.[6]

The theater army headquarters must also be able to assume an operational headquarters role in case of armed conflict. However, no additional resources have been allocated to help the theater army with this role. In fact, the theater army headquarters manning has been reduced as much as 68 percent from their authorized strength as part of the Focused Area Review Group (FARG) headquarters reduction

[5] S.J. Locklear, Memorandum for Commanding General, US. Army Pacific Command; Commander Marine Forces Pacific, SUBJECT: Initiating Directive - Designation of Theater Joint Force Land Component Commander and Deputy (September 12, 2013), 1.

initiatives to increase efficiency and fully resource brigade combat teams required for rotations in Iraq and Afghanistan while meeting force structure ceilings.[7]

In the MDO operating environment, the US will be contested and disrupted in all domains including space and cyber in theater and in the homeland. Disruption of the reserve mobilization and DoD supply chains by cyber-attack could dramatically reduce forces and material arrival in theater. Understanding the science of mobilization and Joint reception, staging, onward movement, and integration (JRSOI) is essential to determining vulnerabilities. The theater army conducts most of the planning for the CC with a minimal staff. The staffing levels lack the capability and skillset to simultaneously manage an operational campaign without augmentation. The deployment of an additional headquarters and augmentation forces is required. Against a near pear adversary, there may not be sufficient time or capability available to arrive in theater before the adversary reaches their objectives and ends the period of conflict on their terms.[8]

Overcoming these challenges and obstacles is critical to the successful application of the MDO concept. Winning in competition requires more resources than are currently allocated. Additional attention is needed to understand the roles, missions, and authorities at the theater army for it to successfully achieve national objectives. The National Commission on the Future of the Army study for the President and the Congress found, “the COCOMs and their Army Service Component Commands

[7] Under Secretary of the Army, *2013 Focus Area Review Group Reclama and 25 Percent Final Reduction Decisions* (Washington, DC: US Department of the Army, April 2, 2014), 2. https://armypubs.army.mil/publications/administrative/pog/CPOG.aspx

[8] USIP, 17.

(ASCC) are at high risk to effectively execute mission command with current capability."[9] They further recommended reducing the Army by 2 brigade combat teams (BCTs), if required, to offset the manning requirements for the shortages identified.[10]

The actions taken to "set the theater" determine the strategic options that will be available to achieve our national objectives. Those individuals that are not involved in the tough government work that ensures the right resources and agreements are in place prior to the start of an operation may not appreciate the efforts these actions require. At the tactical and operational levels, many of these activities are conducted by units assigned at EAB, which are invisible to many and just make things appear like magic. Like "magic", the true efforts that create the illusion are transparent to the observer. The theater headquarters that coordinate the access and agreements, provide the resources, and perform the "magic" are not considered "the tip of the spear". Many people, even some in uniform, consider these organizations "unnecessary headquarters" and "redundant overhead". This lack of understanding has been identified in defense studies and reflects a gap in our professional military education.[11]

Understanding these requirements, rather than assuming support will appear like "magic" to the Joint Force, is essential to the discussions of MDO. Some recent assessments indicate, against a near peer adversary, that we lack a credible strategic military response option short of escalation to global nuclear war.[12] If true, this statement challenges the core rationale for the future organizational design of the

[9] National Commission on the Future of the Army, *Report to the President and the Congress of the United States* (Washington, DC, January 28, 2016), 54.

[10] National Commission on the Future of the Army, 2.

[11] Mark Thompson, "Starry, Starry Fight: The Pentagon's General Bloat" *Time Magazine* (May 15, 2016), 3. https://time.com/4336563/military-generals-congress/

[12] USIP, 15.

Department of Defense. The National Defense Strategy Commission included in their report a summary that also questions military superiority:

> Put bluntly, the American people and their elected representatives must understand that U.S. military superiority is not guaranteed…. The choices we make today and in the immediate future will have profound and potentially lasting consequences for American security and influence. If we do not square up to the challenge now, we will surely regret it.[13]

This statement is part of a report to the President and the Congress, but can also be applied to the military leadership. Best military advice and planning to aid prioritization of the finite resources available for military modernization is also essential. MDO requires Joint collaboration and parochial recommendations are counterproductive and further dilute our ability to overcome the capability gaps that exist between the U.S. military and China and Russia. Unity of effort must occur between all elements of government. An authoritarian regime can quickly achieve unity of effort. In a democracy, unity of effort is much more difficult to maintain. The theater army headquarters coordinates many of the diverse set of actions in support of the embassies in theater. However, this is not an equal substitute for a coordinated and unified government effort.

The USAWC is responsible for educating the next generation of senior leaders on the application of strategic Landpower. This cannot be accomplished without providing a thorough understanding of the roles of the theater army. This integrated research project provided the students with a foundational understanding that exceeds their contemporaries. They have all earned the Strategic Landpower Area of Concentration designation based on their successful study this year. Their research

[13] USIP, 3.

focused on one of the challenges facing the Joint force in applying the MDO concept to the future operating environment. Their research and recommendations presented in this study identify many areas for additional study.

Abstracts

Echelons above Brigade Headquarters in Multi-Domain Operations: Field Army Alternatives

By

Colonel Darren W. Buss, United States Army

The Army's future operating concept, Multi-Domain Operations (MDO), envisions activating standing field armies as an intermediary echelon of command between corps and theater armies. According to the concept, field armies execute a threat-focused campaign against near-peer adversaries during competition and, if needed, rapidly transition to armed conflict as a multi-corps land component command. The creation of Active Component field armies, however, requires either growing the force or rebalancing between Active and Reserve Components. The questionable validity of this underlying assumption demands consideration of alternatives to standing field armies. Four likely alternatives exist: cadre-level field armies, theater army operational command posts (OCPs), forward stationed corps, and U.S. based corps. Comparing these alternatives suggests the Army continue exploring options to assign corps to select theaters, authorize OCPs for theater armies, change forward stationed corps to active-duty only headquarters, and establish a corps headquarters in the reserve component. (6256 words, 31 pages)

Convergence of Military Deception in Support of Multi-Domain Operations

By

Lieutenant Colonel Michael G. Hays, United States Marine Corps

The U.S. national security and military policy has refocused on a 'return to great power competition' after emphasizing counterinsurgency operations for the last 18 years of conflict in the Middle East. This policy shift demands a reconsideration of the art and science of military deception across all levels of war. China and Russia's military modernization, increased use of information warfare, and the rise of anti-access area denial (A2AD) environments have resulted in an erosion of a relative U.S. military advantage against near peer competitors. Multi-Domain Operations (MDO) offers a competing concept that leverages joint force capabilities across all domains. For MDO to be successful, the planning and application of military deception through competition and armed conflict must be fully integrated in order to provide the convergence necessary to ensure actions are believable, effective, and verifiable. Despite increases in Intelligence, surveillance, and reconnaissance (ISR) capabilities that challenge deception approaches, these emerging technologies provide new opportunities to exploit an adversary's decision making processes. Embracing military deception must focus on both organizational culture and structure, training, and continued capability development, while adhering to legal requirements. (7244 Words, 31 Pages)

Winning in the Gray Zone: Utilizing Multi-Domain Operations in Competition

By

Colonel Daniel W. Harris, United States Air Force

U.S. strategic documents, beginning with the National Security Strategy, call for action to counter China and recognize that the approach required must incorporate the whole-of-government. These documents further describe current interactions with China as not fully peace, but also not fully war, occurring in what some call the gray zone. China actively attempts to keep interactions in the gray zone to achieve its strategic goals incrementally rather than conduct dramatic moves that invite backlash. To address this challenge, the United States requires a new overarching framework to integrate whole-of-government action, a void the emerging Multi-Domain Operations (MDO) concept could fill. While the current MDO concept touches on competition, it largely focuses on armed conflict. Recognizing the importance of MDO for effective deterrence and armed conflict, this paper proposes the United States use an expanded MDO concept for whole-of-government integration. This concept could fill a void in U.S. strategy and provide a structure for effective competition with China. Absent coordinated action the United States will remain structured to lose international power to China in small increments each passing day. (5976 Words, 29 Pages)

Army Special Operations Forces (ARSOF) in Competition in MDO

By

Lieutenant Colonel Eric Jacobson, U.S. Army

For the United States to protect and promote its national interests in a multi-polar world against near-peer adversaries, the Army must expand Army Special Operations Forces (ARSOF) offensive competition capabilities in terms of authorities, permissions, and force structure. Thus reinforced, ARSOF can become an effective tool in realist U.S. policy to secure and expand a global network of partners and allies in offensive competition in Multi-Domain Operations (MDO) against Russia and China. National level policy makers and senior military leaders must understand that failure to make such reforms risks losing competitive space and global influence to international adversaries. (5901 Words, 22 Pages)

Leveling Up: Improving Army Fires and Targeting for Multi-Domain Operations

By

Lieutenant Colonel Brian J. Newill, United States Army

With new lethal and non-lethal capabilities on the horizon extending the operational reach of the land component beyond the land domain, the Army is poised to become a leader in providing multi-domain fires for the Joint force. Acceptance of this new role requires the Army to master Joint integration to truly achieve multi-domain convergence; the third, and arguably most challenging, of the three tenets of the Multi-Domain Operations (MDO) concept. This paper contends the Army's success depends on it fully embracing the Joint targeting process through education, training, and execution by incorporating recent lessons learned and improving upon current efforts. Moreover, the Army's ability to conduct mission command in MDO relies on supporting the development of a Joint networked architecture and creating a framework for force structure to enable the integration of multi-domain fires. Recommendations include updates to doctrine, improved training and education, robust exercises, and a modernized C2 architecture with the organizational structure capable of handling the complexities of integrating multi-domain fires. (7696 Words, 33 Pages)

Multi-Domain Operations: Modernizing Reserve Force Mobilization Capabilities

By

Colonel Shawn Patrick Underwood, United States Army

The United States faces near-peer competitors in the world today who leverage advancements in all domains and environments to counter American power. Addressing new concepts like Multi-Domain Operations (MDO) to prepare for potential large scale combat operations (LSCO) places additional training and deployment requirements on an already busy reserve force (National Guard and Army Reserve). Moreover, the ability of the Army to identify, create, refine, and validate MDO reserve component force packages is critical to success of the overall MDO concept. Reserve force formations expected to participate effectively in MDO operations will require additional resources, training time, and validation exercises. Changes to force structure, training, and requirements, take time to address and the allocation of resources should be deliberate. Modifications in these areas could improve readiness to support Combatant Command requirements for reserve forces as part of a MDO force to deter and defeat future near-peer threats. (4975 Words, 24 Pages)

Information Operations and Information Warfare: Is the United States Prepared?

By

Colonel Michael R. West, United States Army

Information operations have tremendous impacts on the ways in which political goals are attained around the world. State and non-state actors are utilizing many information operation techniques and procedures to influence populations within their own countries, regions, and around the globe. The Multi-Domain Operations (MDO) concept depicts information operations remaining prominent in the future operating environment. Adversaries are conducting information operations on a different level than the United States. They are fighting a street fight with no rules, and the United States is fighting a strictly regulated and officiated match. This study focuses on understanding information operations and information warfare (and the many other facets like cyber warfare, hostile social manipulation, misinformation, disinformation, and propaganda) from the U.S. perspective and those of our adversaries. It also identifies examples of agencies and organizations and their use of information operations and information warfare. Finally, it concludes with some recommendations on how the United States, and our partners and allies, can improve our performance in the information environment to effectively compete in Multi-Domain Operations (MDO). (5879 Words, 32 Pages)

Integrated Research Team Papers

Echelons above Brigades Headquarters in Multi-Domain Operations:

Field Army Alternatives

by

Colonel Darren W. Buss, United States Army

After progressively reducing both the quantity and size of operational headquarters since the end of World War II, the U.S. Army recognized that the resultant gaps between echelons above brigade (EAB) commands could hinder competition and armed conflict with near-peer adversaries. Since 1974, the U.S. Army has leveraged three echelons of headquarters for tactical and operational command and control above brigade: theater armies, corps, and divisions.[1] It now proposes in *The U.S. Army in Multi-Domain Operations 2028* and the supporting *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* to reestablish an echelon of command above corps that has been dormant for almost 50 years – the field army.[2]

---

[1] John Bonin, "Echelons Above Reality: Armies, Army Groups, and Theater Armies/Army Service Component Commands (ASCCs)," in *Essential to Success: Historical Case Studies in the Art of* Command *at Echelons Above Brigade*, ed. Kelvin Dale Crow and Joe R. Bailey (Fort Leavenworth, KS: Army University Press, 2017), 261, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/essential-to-success-historical-case-studies-in-the-art-of-command-at-echelons-above-brigade.pdf.

[2] U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf; U.S. Army Training and Doctrine Command, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons*

Field armies remain a historical fact as well as a future concept, but exist in the present only as a doctrinal addendum despite the existence of one field army, Eighth U.S. Army, in the active force structure since 2012.[3] Field armies previously served between theater armies and corps as the senior operational headquarters.[4] Reconstituting field armies could relieve the burden on geographically focused theater armies by designating a command to plan and execute a persistent campaign of competition against strategic competitor nations, namely Russia and China, or regional actors, such as Iran and North Korea. The forward presence of a field army also reduces risk during the critical transition to armed conflict. It provides the Combatant Command and theater army with a dedicated multi-corps land component command (MC-LCC) capable headquarters for large scale ground combat operations (LSGCO). Conceptually and doctrinally, field armies provide the ideal solution to the Army's capability gap.

Converting concepts and doctrine into reality, however, will likely prove a daunting task for the U.S. Army. Limited resources require the Army to make difficult choices about force structure mix without ideal solutions. Culturally and historically, the

Above Brigade 2025-2045, TRADOC Pamphlet 525-3-8 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-8.pdf.

[3] For Eighth U.S. Army, see “History,” U.S. Eighth Army, last updated March 27, 2020, https://8tharmy.korea.army.mil/site/about/history.asp; for current doctrine on field armies, see U.S. Department of the Army, *Theater Army, Corps, and Division Operations*, Field Manual 3-94 (Washington, D.C: Department of the Army, 2014), 1-3, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm3_94.pdf. Pending draft revision of FM 3-94 excluded from consideration.

[4] For summary of field armies between 1942 and 1974, see Bonin, “Echelons Above Reality,” 255-264.

Army dislikes large headquarters, a characteristic unlikely to change in the future.[5] For over a decade Army corps headquarters have operated at a reduced manpower capacity and rely on the Reserve Component (RC) to man approximately 12% of the authorized positions. Also, the structure of theater armies limits them to only responding to contingencies and not managing operational campaigns. So, after reducing EAB headquarters' manpower over the preceding decades, the Army now proposes to expand the usage of a rarely employed echelon within the hierarchy. This expansion increases competition for the most limited resource within the Army, experienced manpower.

Given the likelihood of constrained manpower resources into the future, the Army should explore alternative methods of establishing standing forward stationed field armies. Options to consider include amending theater army force structure to reestablish the previously authorized operational command post, converting corps headquarters assigned to theater armies to purely active-duty component, and generating a corps headquarters in the RC.

This study begins with an overview of the Army's Multi-Domain Operations (MDO) concept and the vital role that EAB formations contribute to the concept. Contesting neither the concept nor the role provided by EAB formations, the study then challenges a critical underlying assumption to the concepts, that the Army will adequately resource the required formations. After providing an overview of the Army's

[5] As a historical example, see Kent Roberts Greenfield, Robert R. Palmer, and Wiley, Bell I., *The Organization of Ground Combat Troops*, The U.S. Army in World War II: The Army Ground Forces, CMH Pub 2-1 (Washington, D.C: U.S. Army Center of Military History, 1987), 364, https://history.army.mil/html/books/002/2-1/index.html. This example shows how even during World War II senior U.S. Army leaders attempted to minimize the size and quantity of field armies.

organizational development and change process, the study notes three recent resource-informed force management decisions that directly limit current Army headquarters corps and above. With an expectation that, although desired, the Army will be unable to man standing forward stationed field armies for select theaters, the study then describes possible alternatives and recommends further detailed examination by the institutional and operational Army. The analysis begins, as does the Army's force management process, with an overview of the future operation that's fueling change across the Army, Multi-Domain Operations.

Multi-Domain Operations: Competing Against Near-Peer Threats

The Army's MDO concept, as described in *The U.S. Army in Multidomain Operations 2028*, explores methods to compete against adversarial "states contesting international norms."[6] Russia serves as the Army's immediate pacing threat for MDO concept development, with China likely surpassing Russia around 2030.[7] These two near-peer threats and the regional adversarial states of North Korea and Iran have developed technology and employed hybrid strategies to generate stand-off and achieve strategic gains while operating below the threshold of armed conflict.[8] Threat investments in and employment of numerous technologies, notably "anti-access/area denial capabilities, long-range fires, electronic warfare and deception capabilities,

[6] TRADOC, *MDO at EAB 2025-2045*, 6.

[7] U.S. Army Training and Doctrine Command, *The Operational Environment and the Changing Character of Warfare*, TRADOC Pamphlet 525–92 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2019), 13–14, https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf; for examples of how MDO concept details Russian strategies across the competition continuum, see TRADOC, *MDO 2028*, 9–15.

[8] TRADOC, *Changing Character of Warfare*, 11–12.

space-based sensors and anti-space weapons, advanced forms of information operations, weapons of mass destruction, and cyber capabilities."[9] Coupled with these facts, "hybrid strategies have fractured the U.S. concept of joint, phased, multi-domain operations."[10] Even if the Army does not directly fight state-based threats in the coming decades, it will likely see these adversarial states' technology and tactics employed by other adversaries.[11] Therefore, the development of concepts, doctrine, and organizations to counter these threats demands attention.

The Army describes MDO as "an operational-level military concept designed to achieve U.S. strategic objectives articulated in the *National Defense Strategy*, specifically deterring and defeating China and Russia in competition and conflict."[12] The Army, through MDO, seeks to deter armed conflict by integrating and converging effects across all domains – air, land, sea, space, and cyber--, the electromagnetic spectrum (EMS), and the information environment during *competition short of armed conflict*. Should competition escalate to armed conflict, then the Army intends to converge multi-domain effects to "*penetrate* and *dis-integrate* enemy anti-access and area denial systems and *exploit* the resultant freedom of maneuver to achieve strategic objectives (win) and force a *return to competition* on favorable terms [italics mine]."[13] The MDO

[9] TRADOC, *Changing Character of Warfare*, 12.

[10] TRADOC, *Changing Character of Warfare*, 13.

[11] TRADOC, *Changing Character of Warfare*, 11–14.

[12] TRADOC, *MDO 2028*, 24; for information on the competition continuum, see U.S. Chairman of the Joint Chiefs of Staff, *Competition Continuum*, Joint Doctrine Note 1-19 (Washington, D.C: U.S. Joint Chiefs of Staff, 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

[13] TRADOC, *MDO 2028*, 17.

concept, then, explains the Army's approach as part of the Joint force to addressing these five military problems of near-peer competition and armed conflict summarized by the following tasks: compete, penetrate, dis-integrate, exploit, and re-compete.[14]

The MDO concept proposes three tenents to overcome these problems: calibrated force posture, multi-domain formations, and convergence. Calibrated force posture seeks to optimize forward presence and capable expeditionary forces with national-level capabilities and appropriate authorities to prevent adversaries from quickly obtaining strategic objectives. Through multi-domain forces, the Army intends for all echelons of Army forces to maneuver independently, even in contested environments, and employ cross-domain fires while maximizing the potential of soldiers and leaders within the unit. The third tenent, the convergence of capabilities from all domains, the EMS, and the information environment, generates synergistic effects across multiple layers to defeat enemy anti-access/area denial capabilities. Army formations, brigade and above, must converge multi-domain effects at echelon to achieve strategic success through MDO.[15]

The MDO concept's focus on near-peer threats and associated combat operations required to defeat their multi-layered stand-off techniques marked a significant cultural shift for a brigade-centric Army previously consumed with stability operations. To hasten a requisite cultural shift and mitigate doctrinal gaps, the Army published a revised Field Manual (FM) 3-0, *Operations,* migrating certain aspects of the

[14] TRADOC, *MDO 2028*, 15–17.

[15] TRADOC, *MDO 2028*, 17–24.

MDO concept into doctrine in 2017.[16] The updated FM 3-0 beckoned the Army to prepare for LSGCO against near-peer threats. It also expanded the Army's brigade centered gaze towards the broader role that divisions and above provide during LSGCO.

Echelons above Brigade: Essential Elements of MDO

The Army considers EAB headquarters vital to competing against near-peer adversaries, particularly during LSGCO. Senior Army leaders stressed this perspective in the revised FM 3-0 and associated journal articles. The Army even published a compendium book providing historical case studies titled *Essential to Success: Historical Case Studies in the Art of Command at Echelons above Brigade* to educate and reinforce this message.[17] These products articulated the importance of existing EAB headquarters (division, corps, and theater army), but, except for a few historical chapters in *Essential to Success,* none mentioned field army headquarters.

Current published Army doctrine only fleetingly addresses field armies. Historically, when field armies served as the pinnacle tactical formation for the Army, an entire chapter of FM 100-15, *Larger Units: Theater Army-Corps,* described their operations.[18] With the shift to a corps centric Army and elimination of standing field armies from the force structure, FM 100-15 changed to *Corps Operations*, and doctrine

[16] Mike Lundy and Rich Creed, “The Return of U.S. Army Field Manual 3-0, Operations,” *Military Review* 97, no. 6 (December 2017): 14–15.

[17] Kelvin Dale Crow and Joe R. Bailey, eds., *Essential to Success: Historical Case Studies in the Art of Command at Echelons above Brigade* (Fort Leavenworth, KS: Army University Press, 2017), https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/essential-to-success-historical-case-studies-in-the-art-of-command-at-echelons-above-brigade.pdf.

[18] U.S. Department of the Army, *Larger Units: Theater Army-Corps*, Field Manual 100-15 (Washington, D.C: Department of the Army, 1973), chap. 7.

related to theater armies and field armies practically disappeared.[19] The 1986 version FM 100-5, *Operations*, briefly described field armies in an appendix and acknowledged that theater army commanders could constitute field armies from existing forces.[20] After resurrecting theater armies and field armies back into the standing force structure, the Army published in 2014 the supporting doctrine in FM 3-94, *Theater Army, Corps, and Division Operations*.[21] Beyond identifying the unique circumstances supporting Eighth U.S. Army's designation as the only standing field army, the current version of FM 3-94 only addresses the possibility of establishing a field army for very large-scale combat operations. All other references to field armies in the manual relate to the theater army's inability to perform the role of a field army and the theater army's responsibilities to field armies when constituted.[22]

To understand field armies, then, one must turn to MDO concepts. These concepts describe how echelons above brigade, considered "the linchpin"[23] of MDO, perform their roles as the "orchestrators of multi-domain combined arms operations."[24] Future EAB headquarters must evolve to meet the operational demands of MDO while continuing to perform administrative service requirements, like today's EAB

---

[19] Bonin, "Echelons Above Reality," n. 50.

[20] U.S. Department of the Army, *Operations*, Field Manual 100-5 (Washington, D.C: Department of the Army, 1986), 185–86.

[21] U.S. Army, *Theater Army, Corps, and Division Operations*.

[22] U.S. Army, *Theater Army, Corps, and Division Operations*, 2-4, 2-13 – 2-15.

[23] Eric J. Wesley, "Foreword," in *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*, TRADOC Pamphlet 525-3-8 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), iii.

[24] TRADOC, *MDO at EAB 2025-2045*, 26.

headquarters. One must grasp these continuities and required modifications to all EAB headquarters before individually assessing each echelon.

Echelons above brigade must integrate both service-related administrative requirements and joint force operational requirements, a demanding and persistent challenge affecting future headquarters design. Theater armies, as the Army Service Component Command (ASCC) for their assigned Combatant Command, direct subordinate Army headquarters in the execution of service-related responsibilities. The senior Army headquarters of a JTF, designated as the Army Forces (ARFOR) headquarters, similarly performs functions as the ASCC does for the Combatant Command. These administrative duties include service-specific Title 10 responsibilities, Army support to other services, and Department of Defense executive agent responsibilities. Operationally, Army EAB headquarters conduct planning and provide guidance and direction to subordinate forces in one of the following roles: intermediate headquarters, ARFOR, Joint Forces Land Component Command (JFLCC), or Joint Task Force (JTF) headquarters.[25] MDO concepts assume these competing responsibilities endure and influence internal EAB staff composition and procedures.[26]

The Army, while acknowledging the continued tension of dual-focused EAB headquarters, assesses that these headquarters must evolve into warfighting formations to meet the operational requirements of MDO. Current EAB headquarters, operating independently from subordinate organizations according to the modular construct, lack the warfighting capability to fight near-peer threats. In his foreword to

[25] U.S. Army, *Theater Army, Corps, and Division Operations*, 1-24 – 1-26.

[26] TRADOC, *MDO at EAB 2025-2045*, 74–75.

U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045, Lieutenant General Eric Wesley, director of Army Futures and Concepts Center, stated that modular and independent EAB headquarters must become "more than headquarters."[27] They must be "multi-domain capable formations that converge capabilities in all domains and environments during competition and armed conflict, focused on near-peer threats able to win in large-scale ground combat."[28] Unlike historically rigid force structures, MDO EAB formations must agilely adjust their composition to integrate and transfer subordinate units, including from partner nations.[29]

In seeking to design agile formations, the Army must evaluate what capabilities inherently reside within the headquarters and what enabling capabilities EAB headquarters must obtain from their subordinate commands. The specific composition of these enabling formations requires a separate study effort. However, a relevant example demonstrates the challenges of designing EAB formations and documents a current capability mismatch between EAB headquarters. Currently, corps headquarters contain their own signal company, but theater army headquarters rely on signal support from their enabling theater signal command.[30] The allocation of this capability adds to the corps independence at the cost of an increased structure. In contrast, theater armies conserve manpower but must task their enabling subordinate command for any

[27] Wesley, “Foreword,” iii.

[28] Wesley, “Foreword,” iii.

[29] TRADOC, *MDO at EAB 2025-2045*, 26–27.

[30] U.S. Army, *Theater Army, Corps, and Division Operations*, 2-19, 3-4 – 3-5, 4-17.

operational or expeditionary signal support. As the Army looks to build field army headquarters and their enabling commands, decisions such as this affect the force design process and operational employment capabilities of the EAB formations.

Identifying the relationship between the 'larger units' of MDO, the echelons above division, helps to identify the necessary change processes the Army must undertake in the coming years. Looking first at the vision for corps and theater armies helps one understand the gap field armies intend to bridge, and the gap that will drive the force management process.

Corps

The MDO EAB concept classifies "*corps as the linchpin of EAB versatility and agility*."[31] MDO requires corps to primarily conduct LSGCO against a near-peer adversary as intermediate tactical headquarters. The Army intends to structure corps headquarters to principally perform this combat function while remaining capable of serving as a JFLCC or JTF headquarters for operations requiring less than a field army. This priority reverses current corps headquarters focus, and the MDO concept acknowledges that corps headquarters structure must be adjusted to accommodate this new focus.[32] To reduce operational risk associated with the variety of missions expected of corps, the Army intends to man corps with tactically experienced senior personnel trained in both joint and Army doctrine. Corps headquarters staffs also prepare to quickly integrate Army and joint augmentees to expand the headquarters to meet mission requirements. An expeditionary command component capable of short-

[31] TRADOC, *MDO at EAB 2025-2045*, 53.

[32] TRADOC, *MDO at EAB 2025-2045*, 80.

notice global deployment supported by the main command element enables the corps to execute its numerous roles and functions.[33]

Theater Armies

Theater armies, tailored for the specific theater they support, provide persistent capabilities to retain the initiative, to respond to emergencies, and to set the theater, much as they do according to current doctrine.[34] The MDO concept, however, stresses "the pivotal role" played by theater armies in "winning the competition below armed conflict," and setting the theater with "protected operational positions of advantage" for friendly forces to operate from should armed conflict occur.[35] As such, the MDO EAB concept notes prioritization of the theater army, and the field army, ahead of other EAB formations for capability development.[36]

Designed for leading during competition below armed conflict, the theater army headquarters only consists of a main command component and a contingency command component. This structure allows the theater army to respond to short-notice contingencies while continuing to set and sustain the theater on behalf of the Geographic Combatant Commander. It does not provide an operational command capability. Despite this shortage, the MDO EAB concept still expects future theater army

[33] TRADOC, *MDO at EAB 2025-2045*, 53–54.

[34] For further information on setting the theater, see U.S. Army, *Theater Army, Corps, and Division Operations*, 2-9 – 2-10; Joseph John Shimerdla and Ryan Kort, “Setting the Theater: A Definition, Framework, and Rationale for Effective Resourcing at the Theater Army Level,” *Military Review*, 98, no. 3 (June 2018): 55–62.

[35] TRADOC, *MDO at EAB 2025-2045*, 51.

[36] TRADOC, *MDO at EAB 2025-2045*, n. 59.

formations to provide a JFLCC capability for LSGCO, even against a near-peer threat, unless assigned a field army formation.[37]

Field Armies

The MDO EAB concept, recognizing the extreme task load placed upon theater armies, recommends standing threat-focused field armies forward postured in theaters to assist the theater army to compete with and deter near-peer threats persistently. These field armies "enable a rapid transition to, and execution of, LSGCO."[38] Field armies could, in addition to their historical role as multi-corps command and control headquarters, provide the core of a JFLCC, a JTF, or a multi-national headquarters.[39] Joint doctrine finds field armies ideally suited for land component command.[40]

Simply put, the Army sees field armies as the organizational solution to fill capability and capacity gaps between corps and theater armies. Theater armies remain geographically focused on setting the theater during competition and consolidating gains after an armed conflict. They rely on forward stationed threat-focused standing field armies to compete against and rapidly transition to armed conflict with near-peer adversaries, while retaining a small capacity to respond to regional contingencies. Corps remain essential, versatile formations bridging operational and tactical realms with a propensity towards LSGCO. All three of these headquarters must balance

[37] TRADOC, *MDO at EAB 2025-2045*, 78–80.

[38] TRADOC, *MDO at EAB 2025-2045*, 52.

[39] TRADOC, *MDO at EAB 2025-2045*, 52–53.

[40] U.S. Chairman of the Joint Chiefs of Staff, *Joint Land Operations*, Joint Publication 3-31 (Washington, D.C: Joint Chiefs of Staff, 2019), II-10 – II-11, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_31.pdf.

operational and administrative requirements through separate chains of command. They also operate as warfighting formations with associated units providing capabilities to execute MDO. These factors steer the Army's organizational change process.

Force Management: Converting Concepts into Reality

The Army must employ its force management process and associated organizational life cycle model to "recast the current EAB headquarters into interdependent, echeloned multi-domain warfighting formations…."[41] The Army's force management process is a collection of numerous processes executed by multiple organizations that systematically manage change within the Army; it translates strategic guidance into combat-ready formations available for employment by the Geographic Combatant Commanders. The force development process, force management's first sub-system, determines the organization's mission and structure based upon strategic guidance and operational concepts. Repetitive experimentation and senior leader reviews during this phase perform multiple functions: refine concepts into doctrine; design the structure for organizations; determine training, leader development, and education requirements; define personnel requirements; implement supporting policy. Based on the findings of these experiments, the Army then evaluates the required capabilities and organizational design to perform the mission. It finally obtains senior leader authorization for those capabilities as constrained by fiscal and manpower resources. Senior Army leaders seek to maintain a balanced and affordable force structure while mitigating operational and organizational risk. The Army Organizational

[41] Michael D. Lundy, "Preface," in *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*, TRADOC Pamphlet 525-3-8 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), i.

Life Cycle Model demonstrates how authorized organizations continue through the force integration and force generation phases of the force management process.[42]

The Army, through the force management process, must convert the current force structure into its desired force structure over time with congressional approval and oversight. Significant tension occurs as the Army must balance modernizing equipment with personnel authorizations, for which the Army must subsequently recruit, train, and retain Soldiers.[43] The Army seeks to avoid hollowing itself out or authorizing more force structure than it can fill with personnel.[44] This tension plays a significant issue as the Army looks to create new headquarters to support its future operating concept, Multi-Domain Operations.

Realization of the Army's MDO concept relies upon a questionable assumption of adequate resourcing through force growth and "rebalancing of active and reserve components."[45] While an appropriate assumption for conceptual experimentation, history demonstrates that this assumption rarely proves valid without incurring risk in other areas. By 2020, the Army found its budgetary plans to grow the force derailed at the risk of causing a hollow force, a concern likely to intensify given the fiscal impacts of

[42] Tony Caldwell, "Chapter 3 – Force Management," in *How the Army Runs: A Senior Leader Reference Book*, ed. Ed Filberti, 2017th–2018th ed. (Carlisle Barracks, PA: U.S. Army War College), accessed March 29, 2020, http://publications.armywarcollege.edu/pubs/3550.pdf; U.S. Department of the Army, *Force Development and Documentation Consolidated Policies*, Army Regulation 71-32 (Washington, D.C: Department of the Army, 2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN8238_AR71_32_FINAL.pdf.

[43] For balancing of competing demands, see Caldwell, "Chapter 3 – Force Management," 1–1

[44] Andrew Feickert and Stephen Daggett, "A Historical Perspective on 'Hollow Forces,'" CRS Report No. R42234 (Washington, D.C: Congressional Research Service, February 9, 2012), sec. Summary, https://crsreports.congress.gov/product/pdf/R/R42334.

[45] TRADOC, *MDO at EAB 2025-2045*, 8.

the ongoing corona-19 virus pandemic.[46] Three resource-informed force management decisions of the past decades still hinder today's EAD formations from operating under MDO: contingency versus operational command posts for theater armies, U.S. based corps assigned to TAs/ASCCs, and multi-component corps headquarters.

First, under modularity initiatives, the Army eliminated the operational command post (OCP) element from theater army headquarters.[47] Although effecting all theater armies, the experience of Third Army (3A) / U.S. Army Central Command (USARCENT) best underscores the impact of this reduction. In support of Operation Enduring Freedom from 2001-2002, 3A/USARCENT relied upon an already deployed active-duty Army division to assist the headquarters in performing Combined Forces Land Component Command (CFLCC) duties for U.S. Central Command (USCENTCOM).[48] Lessons learned through this deployment allowed the 3A/USARCENT staff to augment itself with personnel to independently perform duties as CENTCOM's JFLCC for Operation Iraqi Freedom in 2003.[49] This structure served as the basis of the theater armies OCP. 3A/USARCENT successfully employed this OCP structure, which it had retained via an exception from the Army, to establish the initial command structure for

[46] For 2020 budget, see Mark Cancian, "U.S. Military Forces in FY 2020: The Struggle to Align Forces with Strategy," Analyses, Center for Strategic and International Studies, September 24, 2019, https://www.csis.org/analysis/us-military-forces-fy-2020-struggle-align-forces-strategy; for coronavirus impact, see David Barno and Nora Bensahel, "After the Pandemic: America and National Security in a Changed World," *War on the Rocks* (blog), March 31, 2020, https://warontherocks.com/2020/03/after-the-pandemic-america-and-national-security-in-a-changed-world/..

[47] U.S. Army, *Theater Army, Corps, and Division Operations*, 1-5.

[48] John A. Bonin, "U.S. Army Forces Central Command in Afghanistan and the Arabian Gulf During Operation Enduring Freedom: 11 September 2001-11 March 2003" (Monograph 1-03, Carlisle Barracks, PA, The Army Heritage Center Foundation, 2003), 10.

[49] Bonin, "USARCENT During OEF," 28–35.

Operation Inherent Resolve in 2014 before transitioning the command to III Corps.[50] With the elimination of the OCP from its authorized force structure, 3A/USARCENT now requires a rotational division headquarters, currently sourced from the Army National Guard (ARNG), to command and control the multiple units supporting Iranian deterrence operations under Operation Spartan Shield.[51] So, as a result of Active Component (AC) force structure reductions, the Army now commits an ARNG division headquarters from its operational reserve to sustain an extended competition campaign against Iran.

Other theater armies face similar challenges commanding and controlling subordinate formations due to lack of adequate authorized force structure coupled with lower prioritization for assignment of personnel. The U.S. Army Europe (USAREUR), for example, relies upon its subordinate administrative training command, Seventh Army Training Command (7th ATC), to provide training and readiness oversight to USAREUR's assigned tactical brigades.[52] This factor, reduced strength of an already inadequate force structure, drives TAs/ASCCs to rely on subordinate assigned headquarters or request allocation of rotational forces to assist them in managing

[50] U.S. Army Center for Army Lessons Learned, "ARCENT Transition to Combined Joint Task Force - Operation Inherent Resolve," Initial Impressions Report (Fort Leavenworth, KS: Center for Army Lessons Learned, March 9, 2016), 1–2, https://usacac.army.mil/sites/default/files/publications/16-10.pdf.

[51] U.S. Army Center for Army Lessons Learned, "USARCENT Intermediate Division Headquarters (IDHQ) Operation Spartan Shield 29th Infantry Division Observations Report," Observation Report (Fort Leavenworth, KS: Center for Army Lessons Learned, April 2018), 2, https://usacac.army.mil/sites/default/files/publications/17683.pdf.

[52] John Bonin and Mark Balboni, "What's in a Name?," US Army War College War Room (blog), January 2, 2020, https://warroom.armywarcollege.edu/articles/whats-in-a-name/; 7th Army Training Command Public Affairs, "7th Army Training Command," official website, accessed March 29, 2020, https://www.7atc.army.mil//.

theater activities, even during competition short of armed conflict.[53] Both USAREUR's and 3A/USARCENT's approaches, neither good nor bad, demonstrate how force structure reductions in senior theater-level headquarters cascade effects into the Army's operational reserve or training organizations.

Europe provides another recent example of resource-constrained force management decision making, the assignment of Army corps headquarters stationed in the continental United States (CONUS) to theater armies. With the inactivation of V Corps in the summer of 2013, the Army reduced its pool of versatile operational command headquarters to just three CONUS-based corps.[54] Recognizing the challenges faced by theater armies described above, the Army began assigning corps headquarters to priority theaters in 2015 with the assignment of I Corps to U.S. Pacific Command.[55] The Army recently announced it will reactivate V Corps for assignment to U.S. Army European Command but will station its headquarters in Kentucky and forward position a command element from the corps in Europe manned by personnel on a rotational basis from the main headquarters.[56] This approach provides some additional support to USAREUR to manage competition activities. However, it does not

[53] For further information on how USAREUR lacks structure, see U.S. Army Center for Army Lessons Learned, "Strategic Landpower in Europe Special Study," Special Studies Report 18-05 (Fort Leavenworth, KS: Center for Army Lessons Learned, December 2017), 10, https://usacac.army.mil/sites/default/files/publications/17587P.pdf.

[54] Daniel Cole, "V Corps Inactivates after Nearly a Century of Service to U.S. Army," U.S. Army, June 13, 2013, https://www.army.mil/article/105339/v_corps_inactivates_after_nearly_a_century_of_service_to_u_s_army; U.S. Army, *Theater Army, Corps, and Division Operations*, 1-2.

[55] Robert B Brown and Jason N. Adler, "I Corps: U.S. Pacific Command's Newest Asset," *Joint Force Quarterly*, no. 77 (Quarter 2015): 115.

[56] "Army to Activate New Corps Headquarters," Association of the United States Army, February 12, 2020, https://www.ausa.org/news/army-activate-new-corps-headquarters.

provide USAREUR a multi-corps capable command element, a likely requirement according to the MDO concept.[57] It also demands the corps to balance a plethora of responsibilities from numerous commands. Corps headquarters must perform installation senior commander functions at their CONUS based installations and respond to U.S. Army Forces Command (FORSCOM) administrative requirements while attempting to support their theater army operational requirements.[58] This economy of force approach delivers a limited solution for theater armies. It, however, pales in comparison to the concept of a forward postured field army to compete against a near-peer threat, as described in MDO and MDO EAB concepts.

As the Army began aligning and assigning corps to assist theater armies, it also imposed a 25% personnel reduction in corps headquarters structure to meet personnel constraints imposed by sequestration. Beginning in 2015, the Army converted corps headquarters into a multi-component unit (MCU) incorporating U.S. Army Reserve (USAR) members. Current corps headquarters retain active duty positions to fulfill at least one shift of all functions in the main command element and an active-duty only tactical command post. For full operational capacity, significantly reduced over the last decade, the corps must mobilize its USAR Main Command Post – Operational Detachment (MCP-OD). [59] To integrate MCP-OD members, corps must forecast training

[57] Jose Luis Calvo Albero et. al., *Friendly Force Dilemmas in Europe: Challenges Within and Among Intergovernmental Organizations and the Implications for the U.S. Army* (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2018), 11-15, https://publications.armywarcollege.edu/pubs/3538.pdf.

[58] U.S. Department of the Army, *Army Command Policy*, Army Regulation 600–20 (Washington, D.C: Department of the Army, 2014), 7–11, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r600_20.pdf.

[59] Stuart Deakin, Irene Zehmisch, and Wesley M. Good, “The Identity Crisis Facing Echelons Above the Brigade - Building the Future by Remembering the Past,” *Military Intelligence Professional Bulletin* 44, no. 1 (March 2018): 20–21; Stephen Dalzell et al., “Main Command Post-Operational Detachments

and deployments twelve to twenty four months in advance and manage mobilization rates to comply with Army policy. The Army could explore policy adjustments for corps headquarters, but this will likely reduce recruitment and retention for MCP-OD Soldiers. The Army observed similar recruitment challenges at the division level, especially for intelligence specialists. Evidence from the same division-level analysis also suggests that forward stationing a corps overseas would further complicate the recruitment and retention issue.[60] While the MCP-OD provides a better alternative than the complete elimination of authorized positions, the MCU composition places additional internal strains on an already task saturated corps headquarters.

These force structure and force allocation decisions partially account for the assessment that current EAD formations are unsuitable for the requirements of MDO. They also underscore that the Army must prioritize resources and select where to assume risk when unable to obtain sufficient resources of funds, personnel, equipment, or a combination thereof. Changing priorities based on a changing political conditions makes a lack of resources a presumable condition given today's uncertain economic times. Similar to recommendations that the Department of Defense forecast future budgets along multiple projection paths, the Army should evaluate alternative force

(MCP-ODs) and Division Headquarters Readiness" (Santa Monica, CA: RAND Corporation, 2019), 20–25, https://www.rand.org/pubs/research_reports/RR2615.html.

[60] For specialty recruitment, effect of stationing, and mobilization procedures, see Dalzell et al., "MCP-ODs and Division Readiness," 54, 61–63, 79–80.

structure against the force structure proposed in the MDO concept as the assumption of growth rests on unstable footing.[61]

Alternatives to Field Army

In light of force management decisions over the past decade and a questionable assumption of authorized growth with which to generate field army headquarters, this study compares four possible field army alternatives. None of the alternatives provide the same capabilities and capacity as a standing field army, and, therefore, constitute a less than desirable option. These alternatives, however, permit incremental force management decisions over time and provide the theater army with assigned forces from which to constitute a field army should the campaign require it before the Army assigns an independent standing field army. They offer the seed or core upon which to expand into a full standing field army as tensions escalate, a concept preferable according to joint doctrine, and the historical method for creating field armies since their elimination from standing Army force structure.[62] Comparing these alternatives against attributes of a standing field army informs future experimentation and force management decisions. The four alternatives to a standing field army, described in further detail below, include cadre-strength field army headquarters, theater army OCP, and either forward stationed, or CONUS based, corps headquarters.

[61] For defense spending forecasting, see Matt Vallone, "Forecasting Defense Spending in an Age of Uncertainty," *War on the Rocks* (blog), March 20, 2020, https://warontherocks.com/2020/03/forecasting-defense-spending-in-an-age-of-uncertainty/.

[62] U.S. Chairman of the Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication 3-33 (Washington, D.C: Joint Chiefs of Staff, 2018), II-2 – II-3, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_33.pdf.

Activating select field armies at cadre-level constitutes the first alternative. This method, listed in the EAB concept and proposed for other headquarters, signifies intent and provides the skeleton from which to expand as situations warrant.[63] The 7th ATC, described above, makes the most likely candidate for this option. Under this model, the Army activates field armies with minimal staff. It also designates a commander of another equivalent command to serve as the field army commander or deputy (i.e., dual hatting). Cadre strength units need other units, preferably colocated, to support them administratively. They also possess minimal ability to oversee subordinate units' training and readiness. This option would, however, provide the nucleus of a staff, which, if protected, could refine the plans and internal staff processes for future growth.

The second option employs a previously authorized element of theater armies, the operational command post. The previously described 3A/USARCENT headquarters evolution provides the best case study for this option. Reconstituting this headquarters element empowers the theater army headquarters to plan and execute a threat-focused campaign across the competition continuum while leveraging efficiencies of the existing theater army staff. As the OCP operates under authorities delegated to a theater army's deputy commander, the OCP could oversee subordinate formations at the division echelon and below. Command of corps and multi-corps formations would require the broader theater army headquarters, however. This option authorizes, and with adequate manning realizes, increased capacity within the theater army headquarters to manage both theater and threat specific tasks. Risk exists, given the diverse requirements for and frequent reduced manning of the theater army headquarters, that the theater army

[63] TRADOC, *MDO at EAB 2025-2045*, 78; Bonin and Balboni, "What's in a Name?"

command group and staff would divert OCP efforts away from their threat aligned focus to complete theater-related tasks or respond to contingencies.

The last two alternatives use corps headquarters to command MDO formations during competition and convert to field armies or MC-LCC during armed conflict. Corps headquarters, which have more authorized personnel than either the draft field army headquarters or previous OCP designs, bring the most staff resources and appropriate general officer leadership to command MDO formations. In addition to requiring the least augmentation to reach a field army equivalent, corps provide the most experience commanding subordinate divisions and brigades while training for joint operations. By delegating authorities through an establishing directive and augmenting corps headquarters with appropriate personnel, Combatant Commanders and theater army commanders can convert a corps headquarters into a field army headquarters or MC-LCC.

Designating and training assigned corps to serve as the theater's field army or MC-LCC relieves the operational burden from the theater army. However, it transfers risk to the operational and upper tactical levels. An inadequate supply of existing corps headquarters impedes the adoption of this alternative. Corps, only resident in the AC and fully committed to each theater or the Joint Force, perform a demanding role converging capabilities at echelon as described in the MDO concept. Converting a corps to field army equivalent organization during the early stages of armed conflict places tremendous strain on the corps' staff that will likely exceed the capacity of one headquarters. As an example, the transition from intermediate tactical command during combat operations to assuming joint command for stability operations exceeded V

Corps capacity during Operation Iraqi Freedom.[64] Similarly, the transition from a service command during competition below armed conflict to MC-LCC during LSGCO against a near-peer threat will likely saturate corps headquarters without relief from corps-level responsibilities. While possible to mitigate these effects through training and exercises, relying on corps to step up and fill the field army requirement just pushes the risk down to the corps headquarters and its subordinate formations.

The split basing of corps headquarters deserves additional consideration as this appears to be the Army's current approach. This variant, described in the preceding section of this report when discussing the reactivation of V Corps, provides the Army some strategic flexibility to reassign corps between theaters with less impact. This split-based option, though, places significant additional burdens on the corps headquarters managing rotation of personnel forward in support of the theater mission and supporting CONUS installation needs.

Comparison Results and Methodology

Full evaluation and comparison between alternative headquarters options demand detailed experimentation to sufficiently inform Army force management decisions. Such evaluation exceeds the scope of this study, as do numerous other influential factors.[65] A review of published concepts, however, permits a broad, subjective comparison between these headquarters options and the associated risks and benefits of each. Although such comparison lacks the rigors of the scientific

[64] For an assessment on V Corps transition to CJTF-7 during OIF, see Donald P. Wright and Timothy R. Reese, *The United States Army in Operation Iraqi Freedom, May 2003-January 2005: On Point II: Transition to the New Campaign* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 164–65.

[65] Factors beyond scope of this study include political, inter-service, intergovernmental, and cultural.

method, exploration and summation of findings encourage further intellectual debate to fuel subsequent research and experimentation by both the institutional and the operational Army. The description of the evaluation methodology follows the comparison of alternatives results displayed in Table 1.

Table 1. Subjective Comparison of Field Army Alternatives

		Headquarters Options				
Category	Factor	FA (Standing)	FA (Cadre)	TA - OCP	Corps (Fwd)	Corps (Split)
Threat	Compete	1	4	3	2	5
	Transition	1	5	4	2	3
	Penetrate / Dis-Integrate	1	5	4	2	3
	Category (Rank / Avg)	1 / 1	5 / 4.67	3.5 / 3.67	2 / 2	3.5 / 3.67
Friendly	Relieve TA	1	5	3	2	4
	MC C2	1	5	2	3	4
	Strategic Flexibility	5	4	3	2	1
	Internal Focus	1	2	3	4	5
	Category (Rank / Avg)	1 / 2	5 / 4	2.5 / 2.75	2.5 / 2.75	4 / 3.5
Personnel	Qty (est)	530	~150	300	650	650 (200 Fwd)
	Qty (Rank)	3	1	2	4	4
	Admin Efficiency	3	2	1	4	5
	Category (Rank / Avg)	3 / 3	1.5 / 1.5	1.5 / 1.5	4 / 4	5 / 4.5
Summary (Rank / Avg)	Factors Equal[a]	1 / 1.89	4 / 3.67	2.5 / 2.78	2.5 / 2.78	5 / 3.78
	Categories Equal[b]	1 / 2	4 / 3.39	2 / 2.64	3 / 2.92	5 / 3.89
	Category Rank Order[c]	1 / 1.67	4 / 3.83	2 / 2.5	3 / 2.83	5 / 4.17

Sources: Data based on author's subjective assessment; John A. Bonin, "Theater Army Employment," (lecture, United States Army War College, Carlisle Barracks, PA, January 9, 2020); John A. Bonin, personal conversation, March 20, 2020; John A. Bonin, email message to author, March 31, 2020.

Note: Lower score better.

[a] Calculated by averaging of all nine criteria.

[b] Calculated by averaging the average category score.

[c] Calculated by averaging the category ranks.

Evaluation metrics fall into three broad categories: threat, friendly, and personnel requirements. Rank ordering headquarters alternatives from lowest to highest for each evaluation criteria demonstrate a subjective preference for the specific criteria. The threat category relates to the headquarters ability to remain threat-focused across the

competition continuum, especially during the initial three of six challenges facing EAB formations.[66] Future EAB formations must compete below the threshold of armed conflict, rapidly transition to armed conflict, and then penetrate and dis-integrate the threat's multi-layered stand-off systems. Forward stationing provides better means to compete and transition. A more robust and established organization independent of the theater army favors the "penetrate" and "dis-integrate" tasks.

The friendly evaluation category considers capabilities the headquarters provides to higher Army and Joint commands and the internal challenges for the headquarters. From a theater command perspective, the headquarters should relieve the burden on the theater army and provide the means to command multiple corps, whether Army, joint, or multi-national, as a land component. Strategic flexibility considers that the greater quantity of forces committed to a specific theater decrements the Army's strategic flexibility to respond to crises in other theaters. For example, a field army stationed in Europe structured to compete and fight against Russia provides little assistance to the Army should the need arise for an additional corps to fight in the Pacific. Lastly, levying more requirements on a headquarters increases the frequency and scope of the headquarters' internal processes; a headquarters scoped to a narrower role allows focus, and informed, timely decision making.

Lastly, personnel requirements always influence headquarters decisions. In general, headquarters smaller in size that can leverage administrative efficiencies through shared staff structures prove easier to justify as they reduce the tooth-to-tail

[66] For the six challenges of EAB in MDO, see TRADOC, *MDO at EAB 2025-2045*, 16–17.

ratio.[67] As specific headquarters compositions remain pre-decisional and subject to tailoring for assigned theaters, this study used broad estimates obtained from draft documents for aggregate comparisons of size and capabilities. As noted previously, headquarters organically lacking desired capabilities must force tailor required capabilities from enabling commands.

Assessment

Two significant findings emerge from comparing the headquarters alternatives. For starters, a forward-deployed corps and a theater army operational command post provide similar assistance across the competition continuum and in support of friendly forces. As the corps most closely replicates a field army in size, structure, and experience of personnel, then logically, it rates well in the threat category. Conversely, a theater army OCP assists the theater army headquarters during competition with reduced force structure but must grow significantly to perform armed conflict against a near-peer threat.

The second finding relates to a split based corps and establishing a field army at cadre strength. Each of these commits a minimal level of force structure directly to the problem. The corps headquarters performs numerous tasks until deployed and committed. However, the corps has manned force structure available to dedicate to the problem, whereas the cadre of a field army headquarters requires drastic augmentation from some unidentified manpower pool.

[67] For tooth to tail ratio, see John J. McGrath, *The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations*, The Long War Series Occasional Paper 23, (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), 4–8, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/mcgrath_op23.pdf.

From the results, one may also infer a few items worth further research and experimentation. First, the incremental establishment of the various headquarters options over time provides deterrent options for the theater, spreads resource growth over time, and retains strategic flexibility for the Army. When viewed in this light, the Army's decision to activate V Corps begins the growth process at a higher level of commitment and support than merely designating Seventh Army Training Command as a cadre-level field army. It retains strategic flexibility and escalatory deterrent options while providing the seeds for USAREUR to plan and exercise.

Next, combining headquarters, such as a corps headquarters and a theater army OCP, may provide a robust regionally experienced staff and leadership to perform duties as a MC-LCC capable field army successfully. This option deserves additional experimentation, and, if validated, suggests the Army explore reconstituting OCPs for select theater armies such as USAREUR and USARPAC. The authorization of an OCP and assignment of a corps provides theater armies inherent capabilities from which to form field army equivalents during exercises and in preparation or response to emerging large-scale contingencies.

Rebalancing between components provides another avenue for further exploration, especially concerning corps headquarters. The Army should assess whether the current MCU composition for corps headquarters remains sustainable if the corps positions forward or converts to a field army. The MCU construct for corps assumed a CONUS based force with routine deployments. Given the challenges of recruiting and retaining RC soldiers to fill U.S. stationed headquarters, one must

assume even more significant difficulties for a forward stationed headquarters.[68] Some forward stationed headquarters, like the 2d Infantry Division in Korea and USAREUR in Germany, leverage host nation soldiers to form combined staffs during the competition phase.[69] With further exploration, experimentation, and approval of prerequisite agreements and authorities, this avenue may compensate for capacity that the RC cannot fill.

As an alternative to RC authorizations in corps, the authorization of a RC corps headquarters deems further research. If theater assigned corps convert to a field army equivalent upon transition to armed conflict, then a void exists in the availability of corps-level headquarters. With only one AC corps unassigned to theaters, the creation of a RC corps headquarters, at least at reduced strength, in place of MCU corps may provide some reserve capacity.

Finally, the Army should reassess assumptions underlying MDO. If end strength growth and rebalancing prove incapable of generating the required force structure, then other reorganization initiatives may need exploration, such as consolidation of ASCCs. Much like the U.S. Air Force and U.S. Navy provide consolidated service headquarters for European Command and Africa Command, the Army may need to consolidate U.S.

---

[68] For explanation of RC stationing impact on MCU recruiting, see Dalzell et al., "MCP-ODs and Division Readiness," 61–63.

[69] For 2d Infantry Division, see Michelle Tan, "South Korean Troops Form Combined Division with U.S. Army," *Army Times*, January 14, 2015, sec. Your Army, https://www.armytimes.com/news/your-army/2015/01/14/south-korean-troops-form-combined-division-with-u-s-army/; Ellen M. Pint et al., "Review of Army Total Force Policy Implementation" (Santa Monica, CA: RAND Corporation, 2017), 41, https://www.rand.org/pubs/research_reports/RR1958.html; M. L. Cavanaugh, "In Search of Seamless Interoperability in Korea: The First Year of the R.O.K-U.S. Combined Division," Commentary, *War on the Rocks* (blog), June 24, 2016, https://warontherocks.com/2016/06/in-search-of-seamless-interoperability-in-korea-the-first-year-of-the-r-o-k-u-s-combined-division/; for USAREUR, see Dan Stoutamire, "USAREUR Bids Farewell to First-Ever German Chief of Staff, Welcomes Second," *TCA Regional News*, January 26, 2017, ProQuest.

Army Africa and U.S. Army Europe to free up authorization for field armies or OCPs.[70] Numerous options merit consideration to generate as many options for the Army's senior leaders.

Conclusion

The MDO concepts, like the preceding analysis, provides a starting point for further experimentation. These concepts promote the Army's goal of developing EAB warfighting formations capable of converging multi-domain effects at echelon to compete against and defeat the "2+3" threat's multi-layered stand-off capabilities. Over the past four years, the Army, recognizing the significant role EAB formations perform across the competition continuum, began operationalizing the MDO concept by transferring key aspects to doctrine and by implementing organizational changes. However, achieving the MDO's aspired structure of a forward stationed standing field army formation for each near-peer theater necessitates massive organization growth accompanied by modifications to AC/RC force structures. Historical trends, current fiscal constraints, and uncertain future strategic forecasts questions the validity of growth and rebalancing as assumptions. The Army must, therefore, explore lesser included alternatives to its desired force structure.

A subjective review of four alternatives to standing field armies generated findings and recommendations worthy of further detailed research and experimentation. Given the MDO concept's suggested prioritization of theater and field armies, the Army should initially consider generating up to three theater army OCPs. The allocation of an

[70] For U.S. Air Force, see "USAFE-AFAFRICA Mission and Organization," U.S. Air Forces in Europe and Air Forces Africa, accessed on April 3, 2020, https://www.usafe.af.mil/About-Us/Mission-and-Organization/; for U.S. Navy, see "About Us," U.S. Naval Forces Europe-Africa / U.S. 6th Fleet, accessed on April 3, 2020, https://www.c6f.navy.mil/About-Us/.

OCP provides the TA/ASCCs with dedicated resources to campaign against their aligned near-peer or regional threat and from which to establish a field army equivalent headquarters with the theater assigned corps. To mitigate the resultant risk at the corps level, the Army should consider constituting a corps headquarters in the RC and reversing the MCU construct of today's corps. While none of these alternative headquarters configurations equates to the MDO's envisioned force structure, they provide incremental growth opportunities that can also serve as deterrent options should competition with regional and near-peer adversaries escalate. Other MDO assumptions, such as the assignment of separate ASCCs for each GCC, merit further research.

As the Army sees an increased risk of LSGCO in the coming decade, Army leaders need to critically examine these assumptions and innovate solutions over the coming decade. As the former Commander of the U.S. Army's Combined Arms Center, Lieutenant General Michael Lundy wrote in his preface to the Army's MDO EAB concept,

> The time is now to prepare our Army for these demands and adapt to the multi-domain battlefield of tomorrow. Only through enhancing EAB formations and evolving its warfighting culture can the U.S. Army remain the world's most lethal ground combat force capable of winning anywhere, anytime.[71]

Culture can only take the Army so far. Tough organizational decisions lie ahead.

[71] Lundy, "Preface," i.

This Page Intentional Left Blank

Convergence of Military Deception in Support of Multi-Domain Operations

by

Lieutenant Colonel Michael G. Hays, United States Marine Corps

> All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away; that you are near. Offer the enemy a bait to lure him; feign disorder and strike him.
>
> —Sun Tzu[1]

Military deception (MILDEC) operations are as old as warfare itself. For most, the classical example of the Trojan Horse represents a well-known tale of deception that resulted in a dramatic reversal of events. Regardless of whether the story is true or fictional, the very name itself has been adopted within the context of the current operating environment and now represents a form of malware intended to deceive the unsuspecting user of its true intentions. This example illustrates not only the enduring character and relevancy of military deception in warfare, but also the continuous process of adaptation resulting from technological advances and their influence on how we fight. Technology offers creative solutions to both age-old problems and new emerging challenges that require different conceptual approaches to account for the changing strategic landscape.

The 2018 National Defense Strategy (NDS) acknowledges a strategic landscape characterized by the erosion of a U.S. military advantage due to sustained low intensity

[1] Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), 66.

combat and the “reemergence of long-term, strategic competition.”[2] In the past 19 years of combat in Iraq, Afghanistan, and Syria, the U.S. has enjoyed overwhelming military superiority against our adversaries across all domains and has not needed to rely on deception to preserve combat power and operational freedom of maneuver. The recent return of great power competition signifies an inflection point in which military leaders must ask how the character of warfare has changed, where is it the same, and how must one adapt? In response, the U.S. Army developed the Multi-Domain Operations (MDO) concept which attempts to counter the growing anti-access area denial (A2AD) threat posed by reemerging powers and the rapid proliferation of new technologies. At its core, MDO seeks to converge capabilities from every warfighting domain in order to reinforce and assure a U.S. military advantage during competition and armed conflict. This concept also attempts to inform a change of Army culture to incorporate more deception planning and operations into future plans. Changing the Army culture may be more difficult than organizational and Material modernization. Military deception will be essential to supporting the MDO concept. Advances in information related technologies and the growing reliance on multi-source information to feed decision making present increased vulnerabilities that can be exploited through military deception. The return of great power competition against peer adversaries with advanced A2AD capabilities requires a refocus on the employment of military deception to counter the erosion of U.S. military advantage by leveraging emerging technologies to compete with adversaries within the information environment. This paper seeks to address how

[2] Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: US Department of Defense, 2018), 2. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

MILDEC can enable MDO and why U.S. military leaders should reinforce a strategy that embraces and incorporates military deception operations to sustain a decisive military advantage.

Military Deception (MILDEC)

At its foundation, military deception is about influencing or misleading decision-making capability. As a result, it falls under the overall umbrella of Information Operations (IO) as a core Information Related Capability (IRC). Deception is traditionally employed by forces perceived to be in a position of strategic or operational disadvantage to achieve one or a combination of four effects; to achieve surprise, preserve friendly combat power, induce an adversary to unnecessarily expend resources, or adopt a preferred course of action. Current joint doctrine defines military deception as "actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[3] Military deception operations span all levels of war and all phases of operations, and are comprised of physical, technical and administrative tactics, techniques, and procedures (TTP's).[4] Military deception works by either increasing or decreasing ambiguity within the adversary decision making cycle and is reliant on an in-depth understanding of the process of how information flows to the intended deception target. While this has historically focused on the cognitive realm of the commander as the deception target, current trends forecast a transition of decision making into the

---

[3] Joint Publication 3-13.4, *Military Deception* (Washington, DC: U.S. Joint Chiefs of Staff, February 14, 2017), I-1.

[4] Joint Publication 3-13.4, *Military Deception,* I-1.

virtual space where artificial intelligence (AI) enabled systems either make the decision or feed the decision-making cycle. Figure 1 offers a quick synopsis of MILDEC tactics and techniques that will be examined throughout the paper.

If military deception is in fact an enduring character of war, then the U.S. may have a need to refocus on military deception. Like any skillset, it must be practiced or the skills will atrophy. Military deception skills must also be practiced and exercised to remain as viable options for integration into a strategy. A 2002 RAND study asserted that while appreciated, deception was "surprisingly understudied" with "few resources tasked to support deception operations."[5] Since the time frame of the study, the U.S. military has been engaged in sustained combat operations against irregular and hybrid forces, without needing to rely on deception for a strategic or operational advantage. A historical review of deception operations within the past century reveals that traditionally "weaker powers tend to favor the use of deception to overcome a stronger opponent."[6] Although not limited to attack or defense, deception is primarily employed as a means to "even the odds" of success. Deception may not be a considered in a strategy until an opponent is faced with a threat that cannot be easily defeated.[7] To an extent, even the U.S. national independence owes a debt of gratitude to the deceptive capabilities of George Washington. He relied heavily on deception to hide critical shortage of supplies, inflate troop strength, conceal unit movements, and exploit internal political

[5] Scott Gerwehr and Russell W. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations*, The RAND Corporation, February 10, 2003, xi. https://ebookcentral-proquest-com.usawc.idm.oclc.org/lib/usawc/detail.action?docID=202801

[6] Christopher M. Rein, *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations.* Vol. 98. Fort Leavenworth: U.S. Army CGSC, 2018, 3.

[7] Jon Latimer, *Deception in War*, (Woodstock and New York: Overlook Press, 2001), 3.

discords within adversaries.[8] Fast forward to the fall of the Soviet Union in 1991, and the U.S. found itself as the lone global superpower. The need for deception capabilities in this security environment was overshadowed by the newfound technological superiority driven by decades of strategic competition. However, the hiatus was merely temporary. Today, nearly all U.S. security and intelligence assessments describe an environment where U.S. military advantage has been eroded with the reemergence of Chinese and Russian threats and projects a challenging U.S. future without appropriate action to contest these threats. Ultimately, the RAND study concluded that "deception techniques are as important as improvements in speed, armor, and weapons," which begs the question why they don't get as much attention as technological advances?[9] With the return of great power competition, military modernization, and an environment where U.S. military dominance is challenged, it is fitting to rethink and analyze the utility of military deception on the modern battlefield. In order to address the employment of military deception, one must first understand the emerging threats. Figure 1 below provides some definitions of the tactics and techniques that may be employed in Military deception (MILDEC).

MILDEC Tactics and Techniques	
Tactics	**Techniques**
1. Amplifying signatures to make a force appear larger and more capable or	1. Feint: offensive action involving contact with the adversary conducted for the purpose of

[8] Amy Zegart, "George Washington Was a Master of Deception," The Atlantic, November 25, 2018. https://www.theatlantic.com/ideas/archive/2018/11/george-washington-was-master-deception/576565/

[9] Gerwehr and Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations,* xi.

simulate the deployment of critical capabilities. 2. Suppressing signatures to make a force appear smaller and less capable or to conceal the deployment of critical capabilities. 3. "Dazzling" adversary sensors by overloading them with multiple false indicators and displays to distract or dissipate their collection assets. 4. "Repackaging" known organizational or capability signatures to generate new or deceptive profiles that increase or decrease the ambiguity of friendly activity or intent. 5. "Conditioning" to desensitize the adversary to particular patterns of friendly behavior and induce adversary perceptions that are exploitable at the time of friendly choosing.	deceiving the adversary as to the location and/or time of the actual main offensive action. 2. Demonstration: Show of force where a decision is not sought and no contact with the adversary is intended. A demonstration's intent is to cause the adversary to select a COA favorable to friendly goals. 3. Ruse: designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary. 4. Display: the simulation, disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the MILDEC story. Such capabilities may not exist, but are made to appear so (simulations) (e.g., show of force).

Figure 1. MILDEC Tactics and Techniques[10]

Erosion of U.S. Military Advantage

The collapse of the Soviet Union and the effective end to the Cold War in 1991 ushered in a period of supreme U.S. military dominance. The U.S. was now the sole global superpower enabling an opportunity for what President H.W. Bush described as a "new world order."[11] At the same time, the world bore witness to the overwhelming firepower and destruction resulting from a well-trained, well equipped, and modern U.S.

[10] Joint Publication 3-13.4, I-8 – I-9. (Figure created by author).

[11] Herbert W. Bush, "Address Before a Joint Session of Congress," September 11, 1990. https://millercenter.org/the-presidency/presidential-speeches/august-8-1990-address-iraqs-invasion-kuwait

military. The 1991 Gulf War saw the first combat employment of the M1 Abrams main battle tanks, M2 and M3 Bradley fighting vehicles, AH-64 Apache attack helicopters, M270 Multiple Launched Rocket Systems (MLRS), Patriot air defense missile systems, HMMWVs, and F-117 Night Hawk stealth fighters.[12] Although periodically modernized, 30 years later, these same systems makeup a large portion of the U.S. military conventional capability.

The Gulf War revealed the full might of the new, post-Vietnam U.S. military, and signaled the technological gap between its closest competitors. Competing nations had to notice this technological gap and make plans to overcome the U.S. capabilities. They were able to implement their plans uncontested while the U.S. was focused on counter insurgency operations in Iraq and Afghanistan for almost 18 years. In 2017, former Chairman of the Joint Chiefs of Staff, General Dunford, reinforced this point by directly stating that "Russia and China have examined U.S. Operations since the Gulf War and invested in capabilities and doctrines to counter America's conventional overmatch."[13] In his assessment, the U.S. military still enjoyed a military advantage over both Russia and China, but the U.S. competitive edge was eroding due to Russian and Chinese aggressive modernization efforts.

While both Russia and China have executed military modernization efforts, China has outpaced Russia in development largely due to its vast economic power. With a rapid rate of economic growth over the past decade, China has now surpassed the U.S.

---

[12] William T. Allison, *The Gulf War, 1990-91*, (New York: Palgrave MacMillan, 2012), 59-60.

[13] Jim Garamone, "Dunford: U.S. Military Advantage Over Russia, China Eroding," DoD News, Defense Media Activity, accessed February 28, 2020. https://www.jcs.mil/Media/News/News-Display/Article/1374604/dunford-us-military-advantage-over-russia-china-eroding/

and ranks first globally in GDP considering purchasing power parity, and demonstrates an average annual growth rate of approximately 7% based on CIA data.[14] Despite spending significantly less than the U.S. on defense, China's People's Liberation Army (PLA) is "undergoing its most comprehensive restructuring" in its history with the goal of being capable of fighting "in all military domains" to defend it national interests.[15] During the last decade China has heavily invested in technological modernization to the PLA to include, 4th and 5th generation aircraft, anti-ship cruise missiles (ASCM), ballistic missile defense (BMD), anti-satellite (ASAT), precision strike weapons, armed UAV's, space, cyber, and EW capabilities.[16] The People's Liberation Army Navy (PLAN) is now the largest regional navy with 300 ships including three aircraft carries, 60 submarines, and eight amphibious ships. With the world's largest shipbuilding capacity, China is poised to continue rapid development of modern vessels.[17] Not to be left behind, the PLA Air Force (PLAAF) is now the third largest in the world with more than 2,700 aircraft.

Internally, China has made dramatic organizational and structural changes to increase function and efficiency. In 2018, the PLA was broken down into five

[14] The World Factbook 2020, Washington, DC: Central Intelligence Agency, accessed February 28, 2020, https://www.cia.gov/library/publications/resources/the-world-factbook/geos/ch.html

[15] Danial Coats, "Worldwide Threat Assessment of the US Intelligence community," Office of the Director of National Security, Statement for the Record, Senate Select Committee on Intelligence, January 29, 2019, 26. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[16] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, (Washington, DC, May 2, 2019). 31-65. https://media.defense.gov/2019/May/02/2002127082/-1/1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

[17] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 98.

geographically oriented theaters with Combined Arms Brigades as the primary maneuver force. Within the PLAAF, an airborne corps was assigned to provide rapid employment via air assault. Within the PLAN, there are plans to triple the size of the Marine Corps from 10,000 to 30,000 personnel by 2020 in order to conduct expanded expeditionary operations. Lastly, the PLA Rocket Force (PLARF) has been organized with a variety of short, medium, and intermediate range ballistic missiles to provide a layered defensive belt capable of ranging past the second island chain.

The U.S. now asserts the relevancy of the information environment within modern conflict, in much the same way, China has also adopted a strategic shift in how they view information. In 2003, the PLA adopted the “Three Warfares” (TW) strategy consisting of psychological, public opinion, and legal warfare.[18] The TW strategy is designed to influence perceptions, opinions, and decision making in order to enhance a strategic advantage. In 2016, China further reinforced their information strategy by creating the Strategic Support Force (SSF); a single national level organization designed to fuse all information related capabilities to include space and cyber domains. The SSF’s role in armed conflict is to achieve information dominance against adversary capabilities, centralize planning, and create “operational synergies”.[19] Not limited to state level adversaries, the TW strategy is not constrained by U.S. policy restrictions on military information operations. China maintains an information advantage based on a unified approach controlled by an authoritarian government. Additionally, China can

[18] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 112.

[19] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 48.

target their own population without concern for any competing narrative from the state controlled media.

In total, the modernization and organizational efforts indicate a PLA that has an expanding capability and capacity to conduct operations outside of their territorial boundaries to expand Chinese influence. China's investment in new technologies, advanced A2AD technologies, and information warfare capabilities provide the means to deny or degrade an adversary's freedom of movement and provides China with operational and strategic standoff against adversaries. A 2018 PLA document revealed China has a two phased approach to complete military modernization efforts by 2035. Phase two will conclude with the PLA becoming a "world class" military by the year 2049.[20] With the economic power to resource their modernization, China has the momentum to sustain their course towards this long term goal. The U.S. must explore and develop creative solutions to prevent continued erosion of U.S. military power. Military deception operations, leveraging emerging technologies, offer the potential to overcome the challenges of A2AD.

Emerging Technologies Impact on MILDEC

Military deception has evolved and adapted over the centuries to the changing character of war and ever advancing technological improvement. The Quaker Guns of the American Civil War, the inflatable tanks of WWII, and the "routine" military exercises along the Suez Canal in 1973, are all examples of military deception despite advances in technology. The convergence of emerging technologies today offer military deception

[20] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 14.

practitioners increased opportunities for deception. In his foreword address to the Multi-Domain Operations publication, U.S. Army Chief of Staff General Milley included artificial intelligence (AI), machine learning (ML), and robotics as "driving fundamental change in the character of war."[21] Although not intended to be a comprehensive assessment of emerging technologies as agents of change, it is worthwhile to examine their potential future applications and implications to military deception.

Commanders and their staffs have long sought to increase situational awareness, reduce uncertainty, and achieve information dominance to counter Clausewitz's "fog of war." The current trend of ever-increasing amounts of information available provide a challenge, and insatiable desire, to fuse together information into something meaningful that can aid decision making. The 2019 National Intelligence Strategy states that the intelligence community will be challenged to "collect, process, evaluate, and analyze such volumes of data quickly enough" to be relevant.[22] Intelligence fusion, battle tracking, and surveillance seek to provide decision makers a clear understanding of the operational environment through information technologies. While there are clear advantages gained by more information, there are also unforeseen vulnerabilities. The statement, "the more information you need, the more vulnerable you are to deception" implies that the emerging technologies also have

[21] US Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1: *The U.S. Army in Multi-Domain Operations 2028*, (Fort Eustis, VA, December 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

[22] Office of the Director of National Intelligence, *National Intelligence Strategy 2019* (Washington DC, 2019), 5. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

vulnerabilities.[23] Consider what will happen when decision makers can no longer trust the information they are being presented? In 2015, the U.S. Director of National Intelligence outlined a critical future threat involving the manipulation of "electronic information in order to compromise its integrity."[24] He stated that in the future, "decision making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."[25] While Artificial Intelligence (AI) offers a means to deal with massive amounts of data, the question remains of whether the data, and subsequent conclusions, can be trusted?

Artificial Intelligence and the increasing demand for an interconnected battlefield provide the means and conduit to exploit information systems and ultimately decisions. According to some observers, AI applications of the future could offer the ability to create "fog of war machines" designed to exploit flaws in Intel fusion, automatically dispense misinformation, or alter data rendering exquisite collections processes useless and paralyzing decision makers.[26] Policy researchers from the RAND Corporation even went so far as to suggest that AI could usher in a "deception-dominant world" in the

[23] Christopher M. Rein et al., *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations*, (Fort Leavenworth, KA: Army University Press, 2018), 246.

[24] James R. Clapper, "Worldwide Cyber Threats," Office of the Director of National Intelligence, Statement for the Record, House Permanent Select Committee on Intelligence, September 10, 2015, 5. https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf

[25] James R. Clapper, "Worldwide Cyber Threats," 5.

[26] Edward Geist and Marjory Bluementhal, "Military Deception: AI's Killer App," War on the Rocks, October 23, 2019. https://warontherocks.com/2019/10/military-deception-ais-killer-app/

near future where countries cannot distinguish tradeoffs in offensive or defensive actions due to uncertainty.[27]

AI incorporated deception could take several forms. On the high end of the spectrum, a cyber enabled intrusion could insert an AI deception program designed to manipulate or spoof actual data and provide a false display of force disposition, location, and capabilities. In such a scenario, deception could serve to either increase or decrease ambiguity based on the intended target and decision-making process. Minor alterations of data would at times be preferable to shutting down an adversarial network and forcing an enemy to transition to a different information system or process. Following the fourth U.S. Navy collision at sea in less than a year in 2017, questions were raised as to whether the USS John McCain had been effectively "hacked" by adversaries intending to alter location data and disrupt maritime operations in the Pacific.[28] While the possibility of the hack was officially discounted, the capability to manipulate data of a piece of equipment, weapon, or command and control system remains a potential vulnerability which can be exploited.

On the other end of the spectrum, deception can be employed by manipulating existing AI technologies without changing the actual data input, but rather using specific data to achieve a desired effect. The 2019 Worldwide Threat Assessment states that "AI enhanced systems are likely to be trusted with increasing levels of autonomy and

[27] Edward Geist and Marjory Blumenthal, "Military Deception: AI's Killer App."

[28] Christopher Woody, "The Navy's 4th Accident this Year is Stirring Concerns About Hackers Targeting US Warships," Business Insider, August 24, 2017. https://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8

decision making."[29] If an AI enhanced system is actually making a decision; its own algorithm can be effectively used against it. Knowing the data or the algorithm is akin to knowing exactly how an enemy commander thinks and how he makes decisions. An Army Research Laboratory scientist recently said that "if I know your data, I can create ways to fake out your system."[30] As an example, in a recent social experiment, a man in Germany carted 99 active cell phones across a bridge in a small wagon creating a virtual traffic jam on Google Maps, which then re-routed all local vehicles.[31] The AI used within the application design decided to recommend traffic take an alternate route based on data collected from 100 cell phones moving slowly across the bridge. Although a small example, the concept could potentially be applied to aircraft or military air defense systems causing them to perceive a virtual threat. Using the same concept, imagine the effect upon an adversary AI enabled information system by a swarm of miniaturized UAV's mimicking a mass of vehicles, aircraft, or personnel. Each case seeks to use information to lead the decision maker, whether human or automated, to make an incorrect conclusion.

As an extension of AI, Machine Learning (ML) offers both defensive and offensive deception capabilities. ML tools can be used to identify false or modified data

[29] Danial Coats, "Worldwide Threat Assessment of the US Intelligence community," Office of the Director of National Security, Statement for the Record, Senate Select Committee on Intelligence, January 29, 2019, 15. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[30] Sydney J. Freedberg Jr., "Big Bad Data: Achilles' Heel of Artificial Intelligence," Breaking Defense, November 13, 2018. https://breakingdefense.com/2018/11/big-bad-data-achilles-heel-of-artificial-intelligence/

[31] Malik, Daniyal, "Man Creates Virtual Traffic Jam on Google Maps With a Few Dozen Smartphones, Google Reponds," Digital Information World, 5 February 2020. https://www.digitalinformationworld.com/2020/02/artist-creates-virtual-traffic-jam-on-google-maps-with-a-few-dozen-smartphones.html

for counter deception operations. However ML tools are not infallible. They depend upon the learning model and complexity of the data used to 'train' them. ML can also be used to produce what is now commonly referred to as "deep fakes", which are altered video and/or audio files designed to mimic individuals or recorded events. They are primarily designed for entertainment purposes. However, potential military applications for subversive use by an adversary has security professionals concerned. In 2019, the Director of National Intelligence included deep fakes within his remarks on the future information environment and potential implications.[32] To address the security risk, the Defense Advanced Research Project Agency (DARPA) now maintains a funded program referred to as Media Forensics (MediFor) to identify manipulation, and develop technologies to counter what it assesses as an environment that "favors the manipulator."[33] Although deep fake examples found on the internet are currently easily identifiable, state sponsored manipulation in the near future could be much more sophisticated. Consider the impact of manipulated communications disseminated globally during periods of escalated tensions or times of crisis. The power of information operations can sway a population for, or against, an adversary and threaten mission accomplishment. ML enabled deep fakes combined with the rise of social media disinformation has the potential to further blur the lines between fact and fiction. Harnessing these potential systems for future deception could yield a decisive

[32] Danial Coats, "Worldwide Threat Assessment of the US Intelligence community," 7.

[33] Matt Turek, "Media Forensics (MediFor)," Defense Advanced Research Projects Agency, accessed February 12, 2020. https://www.darpa.mil/program/media-forensics

advantage to the side that acts first. The other side, that did not act first, would need considerable effort to overcome the effects of the disinformation.

Although a topic of increased attention, AI is not new, but is rapidly evolving. Any future employment of deception should incorporate the employment of AI and ML technologies. In his 2019 statement before the Senate Intelligence Committee, the Director of National Intelligence, indicated that "advanced AI systems could lead to unexpected outcomes that increase the risk of economic miscalculation or battlefield surprise."[34] As China continues to modernize the PLA and create an "information-ized force" with expanded information systems to command and control across all domains, they also open additional conduits to exploit through AI and ML enabled deception.[35] In their effort to compete militarily, China's increased reliance on technology serves to expand U.S. deception opportunities, which includes increased susceptibility to other emerging capabilities such as advanced decoys.

The emergence of unmanned autonomous vehicles provides another means to exploit deception operations through multi-purpose decoys. Decoys on the battlefield have long been a staple of military deception. From the employment of plywood constructed aircraft of World War II, to the most recent examples of fake wooden BMP's in Iraq by ISIS, decoys have served to mislead adversaries or induce them to expend resources. Unmanned autonomous vehicles breathe life into these otherwise motionless "ghost armies."[36] Instead of just visually looking the part, unmanned vehicles now offer

[34] Danial Coats, "Worldwide Threat Assessment of the US Intelligence Community," 16.

[35] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 63.

[36] Ghost Armies refers to the 23rd Headquarters Special Troops employed during WWII.

the ability to maneuver, sound, transmit, and virtually appear more realistic. Unmanned autonomous vehicles also offer certain advantages over conventionally manned platforms. Whether on land, air, or sea, unmanned assets provide extended endurance at a much lower: risk to force, and potential cost savings than manned systems. For demonstrations to be effective in the past, friendly forces were exposed to potential enemy contact. Unmanned autonomous vehicles can conduct demonstration tasks without exposing friendly forces to enemy contact by mimicking designated radars, acoustics, or electromagnetic signals. Additionally, both the MDO and the Marine Corps' Expeditionary Advance Base Operations (EABO) concepts currently call for forward postured forces distributed within the adversary's A2AD engagement range. Suppressing unit signatures, as well as mimicking or amplifying false signals, will be key to their survivability. A recent author advocated "the urgent need for [electromagnetic] decoys."[37] Decoys can now be employed in all domains.

Over the past two decades, Unmanned Aerial Vehicles (UAV's) have dramatically increased in both numbers and capability, but many have retained a focus on intelligence, surveillance, and reconnaissance (ISR) capabilities. With increased production reducing overall costs, UAV's can now be used to swarm and confuse enemy systems in an A2AD environment. UAV's can also simulate deep strikes or large-scale airborne insertions to penetrate and confuse enemy defenses.[38] While technically not considered a UAV, the AGM-160 Miniature Air Launched Decoy (MALD)

[37] Walker Mill, "A Tool for Deception: The Urgent Need for EM Decoys," War Room: United States Army War College, February 27, 2020. https://warroom.armywarcollege.edu/articles/tactical-decoys/

[38] Joel Harding, "Military Deception Using UAVs," To Inform is to Influence, March 21, 2017. https://toinformistoinfluence.com/2017/03/21/military-deception-using-uavs/

is a programmable long range air launched craft that mimics the flight profile and signature of designated U.S. aircraft to enemy radar and integrated air defense systems (IADS).[39] Another deception option is to convert or retrofit manned aircraft to unmanned status to provide additional realism. The U.S. Navy recently conducted a demonstration of an E/A-18G Growler in a manned and unmanned team.[40] Retrofitted legacy aircraft could be used in deception as a sacrificial "shoot down" scenario to divert adversary attention and resources to recover the downed aircraft.[41] The U.S. military's historical use of air power lends additional credibility to aerial deception operations. Expanding the role of UAV's beyond ISR can increase enemy uncertainty, divert resources, and stimulate enemy responses, making them vulnerable to counterattacks.

The utility of unmanned vehicles for deception purposes also extends to the maritime domain. A 2013 RAND Corporation study identified 62 mission sets for the employment options of unmanned surface vehicles (USV's) and evaluated them along a scale of suitability broken down by highly, possibly, and less suitable.[42] Of the 62 mission sets, six were characterized as deception, with five of the six found to be highly

[39] "MALD Decoy," Raytheon, accessed February 27, 2020, https://www.raytheon.com/capabilities/products/mald

[40] David Larter, "US Navy and Boeing use manned Jet to control drone Growlers," C4ISRNET, February 4, 2020. https://www.c4isrnet.com/naval/2020/02/04/us-navy-and-boeing-demonstrate-controlling-unmanned-aircraft-with-a-manned-jet/

[41] Phyllis Nixon, "Deceiving the Enemy: These are not the drones you are looking for?" (Research Report, Air Command and Staff College, Air University, Maxwell Air Force Base, AL, 2016). https://apps.dtic.mil/dtic/tr/fulltext/u2/1040765.pdf

[42] Scott Savitz et al., "U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs)," The RAND Corporation, (Santa Monica, CA, 2013), xiv. https://www.rand.org/pubs/research_reports/RR384.html

suitable for USV future employment options.[43] The study showed significant future potential for deception regarding disposition, communications, radar, acoustics, and counter decoy operations. The report further concluded that "USVs could be highly effective in overcoming challenging anti-access/area-denial (A2/AD) environments" by employing military deception.[44]

Advances in ISR and collection capabilities have complicated the ability to conduct deception operations without being detected, yet they have far from rendered it obsolete. Given sufficient time, multi-source intelligence collection using differing capabilities would likely be able to discover a ruse executed in only one domain. In the rapidly changing environment of armed conflict, collection resources will be stretched thin across prioritized requests. Deception operations will be much more difficult to uncover when integrated into a comprehensive plan across all domains. Emerging technologies and the want for additional information have opened new opportunities for deception. The challenge now is how to achieve the convergence of assets required to render the deception credible, verifiable, believable, and consistent.[45] Incorporated throughout the concept, Multi-Domain Operations offers "a way" to leverage deception to enhance a U.S. capabilities.

[43] Scott Savitz et al., "U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs)," xxiv – xxv.

[44] Scott Savitz et al., 34.

[45] The terms credible, verifiable, believable, and consistent reference deception criteria listed in Joint Publication 3-13.4, *Military Deception*.

Multi-Domain Operations Overview

In December 2017 the U.S. Army released *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century*. Its intended purpose was to "drive change and design for the future Army" that would find itself contested in all domains in a growing complex and lethal environment.[46] A year later following the release of the 2018 National Defense Strategy, Multi-Domain Battle was replaced by *The U.S. Army in Multi-Domain Operations 2028,* aligning it to the NDS and expanding upon the concept's scope and scale. Specifically, the new concept directly identified Chinese and Russian aggression in similar fashion to the NDS. The concept also addressed the central problem of "layered standoff" created by A2AD capabilities that will restrict force projection and employment options.[47] The concept's assessment of the A2AD operational environment posed five central questions outlined in figure 2 below. These questions are intended to drive future capability development. Multi-Domain Operations attempts to counter the threat through the application of three core tenets: calibrated force posture, multi-domain formations, and convergence.[48]

Multi-Domain Operations Problems
1. How does the Joint Force ***COMPETE*** to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict 2. How does the Joint Force ***PENETRATE*** enemy anti-access and area denial systems throughout the depth of the Support Areas to enable strategic and operational maneuver?

[46] US Army Training and Doctrine Command (TRADOC), *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, Version 1.0* (Fort Eustis, VA, December 2017), i.

[47] US Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, vii.

[48] TRADOC Pamphlet 525-3-1, vii.

3. How does the Joint Force ***DIS-INTEGRATE*** enemy anti-access and area denial systems in the Deep Areas to enable operational and tactical maneuver?

4. How does the Joint Force ***EXPLOIT*** the resulting freedom of maneuver to achieve operational and strategic objectives through the defeat of the enemy in the Close and Deep Maneuver Areas?

5. How does the Joint Force ***RE-COMPETE*** to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

Figure 2. Multi-Domain Operations Problems[49]

Another interesting change occurred between the release of Multi-Domain Battle and Multi-Domain Operations concepts. In 2017, Multi-Domain Battle referenced "deception" a grand total of seven times throughout the document. By comparison, Multi-Domain Operations listed it 41 times. While not specifically addressed, it is likely that the wargames, simulations, and assessments that took place post Multi-Domain Battle's release, greatly informed the need to better incorporate military deception as a critical enabling capability to accomplish MDO objectives. The question to consider now is, how the U.S. Army and the Joint Force can leverage deception to overcome the challenges of the threat and emerging technologies?

MDO's Core Problem Sets

As listed in Figure 2 above, Multi-Domain Operations asks five core questions to drive the implementation of the concept. Common to all questions is an effective deception story that weaves all the elements together. The deception story forms the foundation that paints a complete picture for the adversary decision maker to visualize, assess, and make a judgement that corresponds to the intended purpose sought by the

[49] TRADOC Pamphlet 525-3-1, v. (Figure created by author).

deceiver. According to U.S. joint doctrine, to be effective it must meet four criteria.[50] First it must be “believable”, such as the possibility of an amphibious assault presented by U.S. Marines during the Gulf War. Next it must be “verifiable” taking into account the adversary’s collection resources, systems, and processes. The case during WWII when the Allied Forces transmitted false radio traffic indicating a landing at Calais vice Normandy during Operation FORTITUDE. Third, it must be “consistent” regarding the assessed doctrine, strategy, and tactics of the force employing the deception. Lastly it must be “executable” given not only friendly capabilities, but also the adversary’s understanding of those capabilities. A deception story based on unrealistic capabilities such as teleportation or flying tanks is unlikely to work. An effective deception story requires detailed planning, integration, and resourcing, and therefore cannot be treated as an afterthought when addressing the MDO’s core questions holistically.

The implication for Multi-Domain Operations in achieving the four basic deception criteria is that in order to be successful the joint force must be transparent enough, regarding capabilities, concepts, and strategies, while protecting future deception goals. This requires significant foresight based on a strategic assessment of when, where, and how the U.S. envisions the next large-scale combat operation. Next deception operations must be integrated in planning across all domains. Increased availability of sensors and collection platforms require that the deception story be reinforced by all actions to be believable and verifiable. This requires staffs to be appropriately organized, trained, and equipped with resident authorities to plan, coordinate, and

[50] Joint Publication 3-13.4, I-5.

converge deception operations systematically, and at decisive points. Due to the time and resources required to align these actions, they must be initiated during competition and not left for initial consideration during the transition to conflict.

With a refocus towards great power competition with near peer adversaries, the 2018 NDS advocates a strategic approach to "expand the competitive space."[51] It requires a focused and consistent approach that recognizes near peer advantages and develops innovative counter measures and activities to provide operational and strategic overmatch. During competition, military deception supports multi-domain operations by creating strategic ambiguity and by setting conditions for the successful transition to armed conflict. Due to the rapid pace and lethality of modern combat, a failure to plan and execute military deception during competition will unnecessarily forfeit a potential advantage to the adversary. Competition therefore is the most important phase to ensure future deception operations are believable, verifiable, consistent, and executable.

The design of units that can converge military deception activities across all domains is critical in the competition phase. Multi-domain Operations defines convergence as the "rapid and continuous integration of capabilities in all domains, the EMS, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative."[52] The increasing complexity and speed of warfare demands organizations that can harness and synchronize both current and

[51] Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, 4.

[52] TRADOC Pamphlet 525-3-1, 20.

aforementioned emerging technologies into unified action. Military deception proponency currently resides within the J-39 Deputy Director for Global Operations (DDGO) and is synchronized with combatant commanders through the Joint Information Operations Warfare Center (JIOWC).[53] This top-down driven process ensures the Joint MILDEC tenet of "centralized planning and control," yet relies on the full integration at subordinate echelons for execution across all domains.[54] Without robust subordinate organizations to fuse military deception into integrated operations, the risk of potential compromise, unnecessary expenditure of resources, and friendly confusion increases.

Once established, echelons of command must be empowered with appropriate authorities to execute military deception operations while ensuring adherence to, and synchronization with, operational and strategic deception goals. The classified Joint Policy for Military Deception (CJCSI 3211.01) governs both the approval process and authority to execute deception operations. It should be revaluated to ensure responsiveness at all echelons to account for emerging capabilities in MDO organizations.[55] The 2017 activation of Marine Expeditionary Force Information Groups (MIG) represented a step forward to operationalize all elements within the information environment under a single command and provided a centralized focal point for deception coordination. In similar fashion, the U.S. Army is experimenting with a proposed Theater Information Command (TIC) with subordinate Information Warfare

[53] Joint Staff, *Chairman of the Joint Chiefs of Staff Instruction 5125.01, Charter of the Joint Information Operations Warfare Center*, (Washington, DC: Joint Staff, September 1, 2011), A-1. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205125.01%C2%A0.pdf?ver=2017-02-08-175018-130

[54] Joint Publication 3-13.4, I-8.

[55] Joint Publication 3-13.4, VI-I.

(IW) commands at the field army and corps level.[56] Regardless of the resulting force design outcome, future formations must be capable of planning, coordinating, and integrating deception operations both vertically and horizontally across domains to achieve the level of convergence necessary to plan and execute deception operations.

During the competition phase, training exercises with integrated deception serve two fundamental purposes in support of multi-domain operations. First, exercises serve as a conduit to demonstrate capabilities (real or perceived) to adversary collection agencies. If well integrated into a long-term deception strategy, exercises can serve to condition adversary expectations of behavior, thus enabling a future exploitation at a decisive point. Where, when, with whom, and how the U.S. conducts large scale training exercises sends strategic messages to potential adversaries. Done effectively, exercises can reinforce behavior, set future conditions, or enhance deterrence through the creation of strategic ambiguity. Regarding competition with peer adversaries: multi-national exercises, site survey's, military engagements, access requests, positioning of assets, and weapons testing, can potentially signal a preferred course of action or operational approach. In fact, no such operational approach may be desired other than to deceive the adversary of our true intentions, tactics, or objectives. In these scenarios, one must balance the tradeoff between training as one may want to fight, versus signaling to the adversary a message. Train as you will fight has long been the army standard to maximize training opportunities.

[56] Gregory Cantwell, "Presentation to the Theater Army in MDO Integrated Research Project Team," Carlisle Barracks, PA, February 24, 2020.

Exercises integrating deception further support MDO during competition by both exposing and countering internal U.S. vulnerabilities to adversarial deception techniques. One can assume that the U.S. will be contested within the information environment by a near peer threat. Further, the enemy will employ all the available technologies previously discussed to gain a position of relative advantage. Senior leaders must be comfortable operating in uncertainty and recognize the potential for misleading information to enter their decision-making cycle. They must develop robust counter-deception tools and techniques to guard against responding to false information created by the enemy. The challenge however is that effective adversary deception in training exercises could dramatically impact the accomplishment of preplanned training objectives and create significant confusion. Imagine the confusion and risk involved with a combined arms live fire training exercise in which adversarial AI has manipulated friendly force tracking data. In this scenario the exercise would likely grind to a halt, yet this is the exact impact that an adversary will try to achieve. During the competition phase, the U.S. must experiment and exercise with deception to educate the force and instill the appropriate frame of mind to prepare for the future should deterrence fail, and the U.S. is forced to transition to armed conflict.

During armed conflict, multi-domain operations are designed to enable the joint force to rapidly penetrate and dis-integrate adversary A2AD threats and exploit friendly freedom of maneuver. Throughout this phase, military deception capabilities developed and exercised during competition, help offset enemy advantages posed by operational standoff and a layered defense of long-range precision fires by influencing the

adversary's key strategic and operational decisions. The following brief scenario highlights how the convergence of military deception can support MDO.

Upon transitioning to armed conflict, network cyber deception paired with information security supports deployment of forces by preserving the integrity of data necessary for the mobilization of forces, while virtual mobilization of fake units creates confusion within adversary force posture. Administrative deception techniques in the form of false multi-national basing, staging, access, and overflight requests creates strategic ambiguity in national intent and operational approach. Conditioned methods of operation carried out during competition are exploited through a systematic replacement of autonomous air, ground, surface, and sub-surface vehicles to reinforce enemy perceptions. Forward postured forces are concealed and protected by decoy air, land, and maritime signal emitters designed to stimulate adversary systems, sow doubt, and prompt the unnecessary expenditure and exposure of enemy weapons and resources. Offensive cyber enabled deception manipulates both enemy data and AI algorithms presenting a false operational picture, enabling U.S. maneuver, and eroding senior leader trust in the information in their systems. Key strategic messages from senior leaders (documents, video, audio) are altered and rebroadcast creating increased confusion and exploiting dissention.

Although the list of potential deception possibilities is endless, this brief example is designed highlight four key themes. First, emerging technologies offer tremendous opportunities to reinvigorate military deception options for the future but must be integrated during the competition phase to be relevant. Second, in order to successfully execute the overall deception story and achieve the desired effect, the future joint

environment requires the convergence of deception capabilities in all domains. Organizations at each echelon must work in close coordination to synergize effects and preserve the underlying reality. Third, all echelons of command must have the requisite deception authorities to maintain pace with the evolving security environment and threat. Lastly, the rapid and continuous application of deception operations can have a deteriorating effect on the reliability of an adversary's information systems which can degrade, if not paralyze, their decision making. When these four themes can be executed effectively, they can provide a significant advantage over an adversary.

Implications and Risk

A refocus on military deception to enable MDO requires a commitment to invest in the research, development, and fielding of future capabilities. Emerging technologies offer tremendous potential; however, they are not the only solution. Tried and true low-tech solutions continue to provide cost-effective means to achieve effects. For example, Russian forces employing the deception doctrine of maskirovka continue to heavily invest in rapid deployable realistic inflatable decoys. By one account, Russia can setup a battalion of T-80 main battle tanks in two and half hours.[57] Whether decoy's, signal emitters, or cyber enabled deception, future investments should reflect a mixture of low and high-tech deception capabilities in a contested environment where forces may be required to operate in a degraded environment. Additionally, future investments must also consider the need to invest in counter deception capabilities. Increased reliance on information technology systems expose the U.S. to similar vulnerabilities as the

[57] Kyle Mizokami, "A Look at Russia's Army of Inflatable Weapons," Popular Mechanics, October 12, 2016. https://www.popularmechanics.com/military/weapons/a23348/russias-army-inflatable-weapons/

adversary. China's embrace of the 'Three War fares' information operations strategy, and Russia's continued use of disinformation require commanders to treat counter deception measures as seriously as "their own deception schemes."[58]

A commitment to invest and refocus on deception carries the same fundamental opportunity cost as the actual employment of deception without any guarantee of success. However, military deception operations have the potential to achieve significant results indirectly. These results may be achieved at a much smaller cost than a direct military confrontation in lives and resources. These benefits far outweigh the cost of investment and favor an indirect approach. However, if deception operations are unsuccessful, the net outcome may be costly in a resource constrained environment because the resources spent on deception could have been applied elsewhere.[59] U.S. defense budgets are expected to decrease or remain flat, deception can offer low cost solutions that may produce the same effect of degrading the adversary's decision making ability. Currently, since 2017 and the pivot back to great power competition, military deception funding is on the rise. Increasing from approximately three million dollars in 2017 to 15 million dollars in 2020. Procurement, research, development, testing, and evaluation (RDT&E) initiatives are gaining additional significance as key capabilities.[60] Yet, official numbers represent a minuscule amount of the overall U.S.

[58] Latimer, *Deception in War*, 303.

[59] Edward Geist and Marjory Bluementhal, "Military Deception: AI's Killer App," War on the Rocks, October 23, 2019. https://warontherocks.com/2019/10/military-deception-ais-killer-app/

[60] National Defense Authorization Act 2017, Public Law 114-328, 114th Cong., (December 23, 2016), 130 STAT. 2001, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf; National Defense Authorization Act 2020, Public Law 116-92, 116th Cong., 1st sess. (December 20, 2019), https://www.congress.gov/bill/116th-congress/senate-bill/1790/text

defense budget of 750 billion dollars and warrant reevaluation based on their potential future benefit.[61]

Some have a moral objection to deception operations. Their argument offers deception at its foundation is a lie. The U.S. Army as an institution should not promote behavior that is dishonest. They argue, an institution viewed as untruthful, will lose the trust and support of the nation. These are two elements the U.S. military seeks to preserve. As an example, the DoD Office of Strategic Influence (OSI) launched in 2002 to influence foreign audiences was quickly shut down amid public backlash.[62] An expansion of deception efforts within the competition phase therefore carries with it the underlying risk of the U.S. military losing support of either the population or multi-national partners. Within this environment, U.S. military deception organizations, may need to integrate and partner with interagency partners equipped with appropriate authorities. However, failing to conduct deception operations during competition risks losing the information war prior to conflict and forfeiting any potential advantages.

One author has argued that deception is in fact morally permissible based on the presumption that its intended goal is to hasten war termination and restore a "just and lasting peace."[63] Both the Hague Convention and Geneva Convention specially allow for deception on the grounds that should be expected and considered common practice,

---

[61] National Defense Authorization Act 2017, Public Law 114-328, 114th Cong., (December 23, 2016), 130 STAT. 2001, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf

[62] Michel Chossudovsky, "War Propaganda: Fake News and the Pentagon's Office of Strategic Influence," Global Research, December 17, 2017. https://www.globalresearch.ca/war-propaganda-fake-news-and-the-pentagons-office-of-strategic-influence-osi/562284

[63] John Mattox, "The Moral Limits of Military Deception." Journal of Military Ethics 1, no. 1 (2002): 4-15. https://www-tandfonline-com.usawc.idm.oclc.org/doi/abs/10.1080/150275702753457389

but it is not without limits.[64] Referred to as perfidy, military deception is not permitted in cases where the deception goal is to influence the enemy into believing they are allowed legal protection under the law of war.[65] Using a protected symbol such as the Red Cross or feigning a peace negotiation would be clear violations of these conventions. Future U.S. deception therefore must be executed within the Law of Armed Conflict (LOAC) and incorporate appropriate legal reviews prior to initiation.

Conclusion

In a recent interview, the Commander for U.S. Pacific Air Forces, criticized the U.S. military's "gadget" culture and advocated for the DoD to "start paying more attention" to the use of deception to counter China and create doubt in their decision making.[66] A return to great power competition demands a refocus on the art and science of military deception across all levels of war. China and Russia's military modernization, increased use of information warfare, and the rise of A2AD threats have resulted in an erosion of a relative U.S. military advantage against these competitors. Multi-Domain Operations offers a competing concept that leverages joint force capabilities across all domains. For MDO to be successful, the planning and application of military deception operations, from competition through armed conflict, must be fully integrated in order to contribute to the convergence of Joint capabilities to provide the adversary with multiple simultaneous dilemmas that overwhelm his capabilities.

---

[64] John Mattox, "The Moral Limits of Military Deception." 8-9.

[65] Joint Publication 3-13.4, I-11.

[66] Charles Brown, Interview by Defense Writers Group, George Washington University's Project for Media and National Security, December 17, 2019. https://nationalsecuritymedia.gwu.edu/project/general-charles-q-brown-jr-commander-pacific-air-forces-air-component-commander-u-s-indo-pacific-command-executive-director-pacific-air-combat-operations-staff-joint-base/

Despite increases in ISR capabilities that challenge conventional deception methods, emerging technologies provide new opportunities to exploit the decision-making systems of an adversary. While the complexity of conducting military deception operations has increased, the future application of deception operations is only limited by one's imagination. Embracing military deception must focus on both organizational structure, training, and continued capability development, while ensuring adherence to legal requirements. For planners, military deception also requires an in depth understanding of potential vulnerabilities to guard against with counter deception techniques and capabilities. Ultimately for MDO, one of the most critical targets will remain the decision-making capability of our adversary. The convergence of military deception operations provides one of most effective means to overwhelm and influence an adversary's cognitive environment and provide a U.S. advantage.

Winning in the Gray Zone: Utilizing Multi-Domain Operations in Competition

by

Lieutenant Colonel Daniel W. Harris, United States Air Force

Nested throughout U.S. strategic documents, from the *National Security Strategy* (NSS), through the *National Defense Strategy* (NDS), *National Military Strategy* (NMS), *Capstone Concept for Joint Operations: Joint Force 2030* (CCJO) and both the Department of Defense's and Department of State's Indo-Pacific strategies is the call to address China's strategy of coercion across the globe.[1] Furthermore, these documents portray that this is not solely a U.S. military problem and that solutions must also integrate all the instruments of U.S. national power. Additionally, the problem requires integration of the efforts of allies and partners.[2] Phrased in the NDS as "expanding the competitive space," the NDS describes the United States relationship with China as competition, instead of, either war or peace.[3]

Since the release of the Multi-Domain Battle concept and its successor and current Multi-Domain Operations (MDO) concept, as outlined in TRADOC Pamphlet 525-3-1, there has been a robust discussion of these concepts as a model for

[1] White House, *National Security Strategy* (Washington, DC: White House, 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, 25. This need to address a revisionist China is first identified in the National Security Strategy as the top-level strategic guidance document. Subordinate documents mentioned are nested and mirror this assessment.

[2] White House, *National Security Strategy,* 3, 26. Subordinate strategy documents identified in the previous sentence mirror this assessment of the need to involve all instruments of national power.

[3] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), https://dod.defense.gov/ Portals/1/ Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 4. See also: White House, *National Security Strategy,* 28.

countering the anti-access, area denial (A2AD) challenges presented by Russia and China.[4] The most recent version of MDO presents five multi-domain military problems labeled by one-word descriptors: compete, penetrate, dis-integrate, exploit, and re-compete.[5] In this framework, "compete" occurs before the onset of armed conflict and "re-compete" describes the consolidation of gains in the aftermath of cessation of hostilities.[6] However, "penetrate," dis-integrate," and "exploit" occur in the context of defeating the adversary once decisively engaged in large scale armed conflict against a near peer adversary.[7]

Historian Jack Watling, former U.S. military officer Daniel Roper from the Royal United Services Institute for Defence and Security Studies, and others, have remarked that the MDO concept focuses primarily on armed conflict problems, with less attention paid to the "compete" problem.[8] For US forces to provide a credible deterrent effect, there must be corresponding equipment, personnel, skills, concepts, and doctrine for

---

[4] US Army Training and Doctrine Command (TRADOC), *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, Version 1.0* (Fort Eustis, VA, December 2017), https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf; US Army Training and Doctrine Command (TRADOC), *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA, December 2018), https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

[5] US Army Training and Doctrine Command (TRADOC), *TRADOC Pamphlet 525-3-1*, iii.

[6] *TRADOC Pamphlet 525-3-1*, iii.

[7] *TRADOC Pamphlet 525-3-1*, iii.

[8] Russell W. Glenn, "Mismatch: U.S. Preparation for Future Conflict During China's Second Cultural Revolution," Small Wars Journal, accessed March 6, 2020, https://smallwarsjournal.com/jrnl/art/mismatch-us-preparation-future-conflict-during-chinas-second-cultural-revolution; Jack Watling and Daniel Roper, *European Allies in US Multi-Domain Operations* (London: Royal United Services Institute for Defence and Security Studies, October 2019), https://www.ausa.org/sites/default/files/publications/SR-2019-European-Allies-in-US-Multi-Domain-Operations.pdf, 21.

this potential high-end fight. Without these elements of power, the United States loses the ability to compel Chinese behavior by force in areas under their A2AD bubble. However, successful deterrence of China from fighting a major conflict may lead them to use other means to achieve their national ends. As a result, U.S. national security documents prominently reflect a concern for the consequences of alternate Chinese strategies.[9] While armed conflict with China may be the United States' most dangerous threat, losing in competition is probably the most likely threat.

Deterring China from armed conflict with the United States is still necessary, but alone is not sufficient to maintain the relative global strategic position pf the U.S. or to achieve U.S. national security goals. The United States must also deter China to constrain actions to expand its competitive space and reduce the U.S. competitive space. The concept of MDO, appropriately expanded in scope and focus, could serve as the backbone of an effective whole-of-nation strategy towards China, and more generally towards other countries. Working towards a whole of government approach to achieving U.S. national objectives capitalizes on current efforts and processes associated with MDO and advances a concept that not only deters armed conflict, but

---

[9] White House, *National Security Strategy*, 25. This concern, identified in the top national security policy document, the National Security Strategy, is also reflected in subordinate documents. See: Chairman, Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2030* [UNCLASSIFIED], (Washington, DC: U.S. Joint Chiefs of Staff, September, 2019), 4; Department of Defense, *Indo-Pacific Strategy Report* (Washington, DC: Department of Defense, 2019), https://media.defense.gov/2019/Jul/01/ 2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF, 8-9; Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America,* 2; Department of State, *A Free and Open Indo-Pacific* (Washington, DC: Department of State, 2019), https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf, 5, 23; Joint Chiefs of Staff, *Description of the National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, 2018), https://www.jcs.mil/ Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf, 2.

also wins in competition. This paper establishes a description of the MDO concept in its current form. Then, it will describe the relevance and importance of deterring China from armed conflict, and if deterrence should fail, defeating her. This paper will then describe the gray zone and China's actions to compete in this space. Following that, it will describe and characterize the U.S. response to date. Finally, this paper will recommend modifications to the MDO concept to better compete in the gray zone. First, it is important to have a full understanding of the current vision of the MDO concept under development.

Multi-Domain Operations Concept

Multi-Domain Operations, as outlined in TRADOC Pamphlet 525-3-1, is the U.S. Army's concept for countering the challenges posed by the emerging operational environment and specifically, the problem of an adversary's layered standoff and A2AD.[10] While the TRADOC pamphlet identifies Russia as the near-term pacing threat, the MDO concept also recognizes that the concepts are equally applicable to China.[11] Important as well, as GEN Milley stated in the pamphlet's foreword, it is an evolving concept and not intended to be mature doctrine.[12] The concept of MDO centers around addressing five multi-domain military problems: 1) Compete; 2) Penetrate; 3) Dis-Integrate; 4) Exploit; and, 5) Recompete.[13] The MDO concept further includes three

[10] *TRADOC Pamphlet 525-3-1*, iii, vi.

[11] *TRADOC Pamphlet 525-3-1*, 11.

[12] *TRADOC Pamphlet 525-3-1*, Foreword.

[13] *TRADOC Pamphlet 525-3-1*, iii.

tenants: 1) calibrated force posture; 2) multi-domain formations; and, 3) convergence.[14] The MDO concept models the five military problems as phases to organize operations in a MDO campaign, and explicitly discusses the transition from compete to some combination of penetrate, dis-integrate, exploit, and then back again to competition.[15] Compete is the first phase in the MDO model and is worth additional consideration.

Compete occurs below the level of armed conflict and references the concept of "expanding the competitive space" as well as deterring aggression and enabling a transition to armed conflict.[16] While the TRADOC pamphlet addresses generalities about: the use of unconventional war; information operations; the interagency and allies; and, partners to expand competitive space; this discussion primarily focuses on setting conditions for the joint force in the case of transition to armed conflict.[17] Competition can also set the conditions to successfully deter an adversary or achieve national objectives without armed conflict. The next three problems in the MDO model focus on actions after a transition to armed conflict.

Penetrate, dis-integrate, and exploit, attempt to address how to achieve U.S. objectives in armed conflict when faced with an adversary's established A2AD capabilities. The A2AD problem is the genesis of the MDO concept as well as its main focus. These "phases" describe in detail the ways the joint force might respond

---

[14] *TRADOC Pamphlet 525-3-1*, iii.

[15] *TRADOC Pamphlet 525-3-1*, 31, 45.

[16] *TRADOC Pamphlet 525-3-1*, 16, 24-25.

[17] Glenn, "Mismatch: U.S. Preparation for Future Conflict During China's Second Cultural Revolution;" *TRADOC Pamphlet 525-3-1*, 24-25; Watling and Roper, *European* Allies *in US Multi-Domain Operations*, 21.

systematically to: gain access to areas defended by A2AD capabilities; mitigate and reduce these threat capabilities; and, enable operational maneuver to achieve the strategic objectives of the campaign.[18] However, the MDO concept involves quickly neutralizing enemy long-range systems. In the case of China, this would likely require kinetic strikes inside their homeland, which may appear as a strategic attack. The degree of potential escalatory effect and subsequent response from the adversary, based on the adversary's perception of threat, is difficult to control.[19] Therefore, avoiding escalation remains a significant concern during the penetrate, dis-integrate, and exploit phases. Following these phases, the problem of recompete addresses war termination and subsequent return to competition short of armed conflict.

The return to competition, or recompete, problem provides a new operating environment or post conflict conditions that are likely different than they were in pre-hostilities.[20] This recognition drives the joint force to seek three primary objectives: 1) consolidate the gains achieved during conflict; 2) deter future conflict; and, 3) posture the force to favorably compete in the new post-conflict strategic environment.[21] This concept relies on the belief that in armed conflict between two nuclear powers, the end state is unlikely to be total capitulation of either side. Instead a return to competition

[18] *TRADOC Pamphlet 525-3-1*, 25.

[19] Terrence Kelly, David C. Gompert, and Duncan Long, *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression* (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/ pubs/research_reports/RR1359.html, 9; *TRADOC Pamphlet 525-3-1*, 32.

[20] *TRADOC Pamphlet 525-3-1*, 45.

[21] *TRADOC Pamphlet 525-3-1*, 45.

under post hostility conditions may be more likely below the threshold of armed conflict.[22]

The MDO concept addresses these five problems in conjunction with three separate, but mutually reinforcing tenants. These tenants are: calibrated force posture, Multi-Domain formations, and convergence.[23] Calibrated force posture combines the informed positioning of forces with the capacity to rapidly move over strategic distances to deter or counter an adversary.[24] Forward presence demonstrates U.S. resolve and creates a dilemma for adversaries to consider whether their national objectives are worth the risk of killing, capturing, or isolating U.S. forces. The Marine Corps Expeditionary Advanced Base Operations is an example of a concept that applies this informed presence and mobility to complicate an adversary's decision making.[25] While calibrated force posture describes stationing or deploying units, the tenant of multi-domain formations expands on the concept by suggesting tactics and techniques regarding organizing, training, and equipping these units for flexible employment.

Designing units to be able to employ the concepts of MDO, and also organize in such a way as to be more resilient, is the tenant of Multi-domain formations.[26] MDO

---

[22] *TRADOC Pamphlet 525-3-1*, 44.

[23] *TRADOC Pamphlet 525-3-1*, vii.

[24] *TRADOC Pamphlet 525-3-1*, 17.

[25] Jake Yeager, "Expeditionary Advanced Maritime Operations: How the Marine Corps can Avoid Becoming a Second Land Army in the Pacific," War on the Rocks, December 26, 2019, https://warontherocks.com/2019/12/expeditionary-advanced-maritime-operations-how-the-marine-corps-can-avoid-becoming-a-second-land-army-in-the-pacific/.

[26] *TRADOC Pamphlet 525-3-1*, 19.

units' key tasks include the ability to: independently maneuver; avoid and take advantage of adversary actions; be proficient at the employment cross-domain fires; and, maximize human potential through both technical means and careful selection of leaders who will thrive in complex situations.[27] Development of these units are already underway. The Army multi-domain task force (MDTF) pilot program is one of these test programs.[28] Furthermore, the Army has plans to create several more task forces over the next several years for employment on the U.S. west coast, Europe, and in the Pacific.[29] Convergence addresses the combat employment of these properly located, organized, trained, and equipped units.

Convergence focuses on the integration of actions across multiple domains to achieve coordinated effects and impose complexity on the enemy.[30] Convergence utilizes the concepts of: cross-domain synergy; layered options; mission command; convergence at echelon; and, multi-domain command and control.[31] Convergence threatens an adversary in multiple domains simultaneously with multiple dilemmas.[32] Challenging an adversary's capability in multiple domains has a complementary effect, can be overwhelming, and is at the core of what multi-domain operations intends to

[27] *TRADOC Pamphlet 525-3-1*, 19-20.

[28] Sean Kimmons, "Army to build three Multi-Domain Task Forces using lessons from pilot," Army News Service, October 11, 2019, https://www.army.mil/article/228393/army_to_build_three_multi_domain_task_forces_using_lessons_from_pilot.

[29] Sean Kimmons, "Army to build three Multi-Domain Task Forces using lessons from pilot."

[30] *TRADOC Pamphlet 525-3-1*, 20-23.

[31] TRADOC Pamphlet 525-3-1, 20-23.

[32] *TRADOC Pamphlet 525-3-1*, 20-23.

accomplish.[33] However, convergence is exceptionally challenging to achieve even for a single U.S. commander in charge of Joint capabilities. The challenge increases when capabilities must be integrated between the U.S. interagency, allies, and partners. Seldom does a commander have the ability to control all the capabilities available across all domains. Overall, these three tenants endeavor to focus efforts on the MDO concept and further its development for use in conflict in A2AD environments.

If successfully applied, the current MDO concept would close a critical gap in the U.S. capabilities to attack, disable, and maneuver within A2AD systems in support of U.S. objectives. This mission provides focus for training, exercising, and equipping the force for armed conflict. While the MDO concept identifies how the United States might pursue objectives in an A2AD threat environment, the real value of employing the MDO concept may be for its deterrent effect. Credible MDO capability sends a powerful message of U.S. resolve to challenge the impenetrability of A2AD systems and provide a challenge to the leadership in contested regions of the world. The lack of a U.S. credible deterrent would likely result in emboldened actions by revisionist states, unencumbered by the threat of U.S. action. If, however, deterrence does fail, none of the solutions to the military problems presented in the MDO concept are easily overcome. Conceptualizing, procuring, fielding, and training to overcome the military capabilities of a near peer adversary, or China, in armed conflict present significant challenges to the nation. Economic expense alone may make fielding a Joint MDO force infeasible.

[33] *TRADOC Pamphlet 525-3-1*, 20-23.

Deterring and Defeating China in Armed Conflict

While war with the United States would likely also be costly for China or an adversary, the United States government must prepare appropriately for existential threats. The most likely possibility for large scale combat operations may arise from a miscalculated action that involves China crossing a vague U.S. red line.[34] Furthermore, the MDO concept may foster escalation as many capabilities are applied simultaneously. An MDO strike may occur very quickly and raise additional alarm because both adversaries possess operational nuclear weapons.[35] Recent years of increased Chinese investment in A2AD capabilities raises concerns over cost benefits of U.S. military responses in the Pacific.

Increased Chinese interest in the concept of A2AD traces back to the 1995-1996 Taiwan Straits Crisis. The United States demonstrated resolve by sailing two carrier strike groups to the area. The Chinese chose not to counter due to an unacceptable level of risk.[36] In response to this inability to counter this U.S. action, China has been developing its A2AD capabilities in line with its national interests to challenge the U.S. ability to project power.[37] As these A2AD capabilities mature, the resultant reduction in U.S. ability to project power translates into a less credible deterrent against Chinese

[34] Daniel Altman, "Is Fait Accompli the Primary Challenge for Deterrence in the 21st Century?" (Recorded lecture with accompanying slides, SMA STRATCOM Academic Alliance Speaker Series, December 12, 2018), https://nsiteam.com/is-the-fait-accompli-the-primary-challenge-for-deterrence-in-the-21st-century/, slide 22.

[35] Kelly, Gompert, and Long, *Smarter Power, Stronger Partners, Volume I*, 9.

[36] Kelly, Gompert, and Long, 44.

[37] Kelly, Gompert, and Long, 44.

actions. This raises the possibility of the Chinese conducting aggressive acts, such as denying access to the global commons which are protected by their A2AD bubble. With fewer options, the U.S. may be more likely to escalate in response to signal resolve.[38] Such a scenario is fraught with danger on both sides. Either side could unintentionally initiate an armed conflict that neither side desired. While regrettable from a U.S. perspective, it is nonetheless logical that China has taken actions to mature their A2AD capabilities.

A2AD offers several advantages to China. First it capitalizes on the strength of the defense. A2AD requirements are to simply deny access, while and adversaries force projection requirements are much greater and require gaining control.[39] Secondly, current technological trends favor air and sea target survivability over ground targets. Additionally, technology favors the first strike of an offense vice defense against surviving a first strike (e.g. missile technology is outpacing missile defense).[40] These considerations provide an advantage to the defender as an A2AD capability is both easier to develop and less expensive than the power projection capabilities required to defeat A2AD.[41] However, the United States should not abandon efforts to protect its forces. Cutting-edge technological solutions may provide a new calculus to evaluate these challenges. Nevertheless, protective or leap ahead technologies will not be attainable in the short term and that the United States should not count on a

[38] Kelly, Gompert, and Long, 4, 41.

[39] Kelly, Gompert, and Long, xiii.

[40] Kelly, Gompert, and Long, xiv

[41] Kelly, Gompert, and Long, xiv

technological silver bullet to solve all problems.[42] The last advantage of A2AD results from the simple matter of geography. China has the advantage of interior lines operating in the Pacific. Power projection, almost by definition, requires transit and logistical lines. The longer the support lines, the higher the expense, vulnerability, and the more time the adversary has to react and optimize its defense.[43] The western Pacific particularly has expansive space and challenging long lines of communications for an expeditionary force across the air, sea, and land domains. Overall, China's A2AD efforts are a cause of concern, requiring a carefully considered response.

Given China's increasing A2AD capabilities, the United States should, at minimum, continue work on the MDO concept as currently conceived. To deter armed conflict, the MDO concept: penetrate, dis-integrate, and exploit, phases are particularly important to signal a credible and capable deterrent to China. To ignore the problem and abandon all efforts to counter A2AD will leave the United States in a demonstrably weaker geopolitical situation. It is important to consider the ability to deter armed conflict is necessary, but not sufficient, in today's strategic environment. While the United States must prepare for armed conflict for all of the reasons discussed above, neither the United States nor China sees armed conflict with each other as the proximate solution to their differences.[44] A general understanding of the negative economic impacts of armed conflict support an assessment of the relative unlikelihood of

[42] Kelly, Gompert, and Long, 8.

[43] Kelly, Gompert, and Long, xii-xiv.

[44] Eric Kuznar and George Popp, *China's Perception of the Continuum of Conflict* (Boston: NSI, Inc, September 2019), https://nsiteam.com/chinas-perception-of-the-continuum-of-conflict-a-future-of-global-competition-and-conflict-virtual-think-tank-report/, 2.

voluntarily entering into a conflict without significant consideration. Further reinforcing this assertion is the capitalist peace theory, which argues that countries that trade extensively with each other tend to not go to war with each other.[45] However, the combination of these structural factors and successful U.S. deterrence does not mean that China will abandon pursuit of their national interests; successful deterrence at higher levels of conflict simply means that China will pursue different ways to achieve their national goals.

China's Competition in the Gray Zone

Instead of armed conflict, China is using an integrated whole-of-society approach to achieve its objectives. This approach is operating in, exploiting, and expanding what has been called the "gray zone," the space between the U.S.'s traditional duality of peace and war.[46] Describing the strategy China is using to compete in the gray zone has been the subject of much academic work using many similar terms, including: gray zone conflict, integrated strategic deterrence, strategic gradualism, political warfare, coercive gradualism, and comprehensive coercion.[47] "Coercive gradualism" is a

---

[45] Erich Weede, "The Capitalist Peace and the Rise of China: Establishing Global Harmony by Economic Interdependence," *International Interactions, 36* no. 2 (2010), 206-213, https://doi.org/10.1080/03050621003785181, 206.

[46] United States Special Operations Command (USSOCOM), *White Paper: The Gray Zone* (Tampa, FL: USSOCOM, September 2015), https://www.soc.mil/swcs/ProjectGray/ Gray%20Zones%20-%20USSOCOM %20White%20Paper%209%20Sep%202015.pdf, 1.

[47] The following sources are associated with their respective descriptive terms:

1. Grey zone conflict: Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: Strategic Studies Institute, December, 2015), https://publications.armywarcollege.edu/pubs/2372.pdf, 58.

2. Integrated strategic deterrence: Daniel J. Flynn, "China's Evolving Approach to "Integrated Strategic Deterrence" in *Chinese Strategic Intentions: A Deep Dive into China's Worldwide Activities* (Boston: NSI, Inc, December 2019), https://nsiteam.com/chinese-strategic-intentions-a-deep-dive-into-chinas-worldwide-activities/, 26.

particularly descriptive term that incorporates the idea of China as a coercive, not cooperative actor interested in advancing its position, taking actions that are to the detriment of adversary countries' strategic interests.[48] Secondly, this term highlights China's strategic intention to act through a series of small incremental steps, to remain in the gray zone and inside the bounds of competition.[49] Furthermore, China's efforts to remain in the gray zone guards against escape beyond escalatory thresholds which would result in armed conflict.[50]

Importantly, rooted in traditional Chinese strategic doctrine is implementation of strategies to influence a competitor through integrated use of primarily non-military tools.[51] It represents an update to Chinese traditional doctrine for the 21st century rather than something new.[52] Furthermore, China's fundamental structure lends itself to this form of conflict; noted academics Mahnken, Babbage, and Yoshihara argue China

---

3. Strategic Gradualism: Mazarr, *Mastering the Gray Zone*, 38.

4. Political Warfare: Mazarr, 48.

5. Coercive Gradualism: William G. Pierce, Douglas G. Douds, and Michael A. Marra, "Understanding Coercive Gradualism," *Parameters 45* no. 3 (Autumn 2015): 51-61, https://publications.armywarcollege.edu/pubs/3710.pdf, 52.

6. Comprehensive Coercion: Thomas G. Mahnken, Ross Babbage and Toshi Yoshihara, *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018), https://csbaonline.org/uploads/documents/Countering_Comprehensive_Coercion,_May_2018.pdf, 4.

[48] Pierce, Douds, and Marra, "Understanding Coercive Gradualism," 52.

[49] Pierce, Douds, and Marra, 52.

[50] Mazarr, 58.

[51] Mahnken, Babbage and Yoshihara, *Countering Comprehensive Coercion*, 26-27.

[52] Mahnken, Babbage and Yoshihara, 27.

"perceives their political warfare campaigns to be a permanent feature of their strategic postures."[53] Some would consider the indirect approach another tactic available to achieve national objectives without firing a shot.

As an element of its strategic posture, China's autocratic society fosters harmonic coordination across society and their instruments of national power to implement strategies to compete in the gray zone. China utilizes, but also attempts to subvert, the western rules-based international order. This is what U.S. Army strategists Isaiah Wilson III and Scott Smitson call "a globalizing insurgency challenging the foundational regime of the current advanced industrial nation-state based (and largely Western) international system and order." [54] China challenges or finds gaps and ambiguities in international norms, while ensuring that their actions do not cross bright international legal lines that would give clear justification for a particular adversary or the international community to respond against them.[55] Furthermore, China justifies some of its tactics by calling attention to recent actions by other nations in the international community. For example, China argued the NATO intervention in Libya violated international norms and therefore obviated the legitimacy of any criticism leveled at China for similar actions.[56] Additionally, China increasingly employs its significant

[53] Mahnken, Babbage and Yoshihara, 58.

[54] Isaiah Wilson III and Scott Smitson, "Solving America's Gray-Zone Puzzle," *Parameters 46* no. 4 (Winter 2016-2017): 55-67, https://publications.armywarcollege.edu/pubs/3298.pdf, 59.

[55] Pierce, Douds, and Marra, 53; John Stevenson, *NSI Concept Paper, Gray Zone Deterrence: What It Is and How (Not) to Do It* (Arlington, VA: Strategic Multi-layer Assessment (SMA), 2017), http://nsiteam.com/sma-publications-grayzonedeterrencel/, 2.

[56] Wilson III and Smitson, "Solving America's Gray-Zone Puzzle," 63.

economic power, utilizing it to turn countries away from the United States and towards China. One example is China's debt-trap economics, where loans offered for the construction of major infrastructure are beyond the abilities of the recipient countries to service.[57] Default in this debt results in eventual Chinese ownership of the infrastructure which becomes a coercive means for China to gain increased influence in the economic realm.[58]

China also recognizes the value of gradualism in pursuit of their goals.[59] Coercive gradualism or strategic gradualism highlights the idea of achieving gains through designing a series of small steps that individually do not engender significant competitor response. However, aggregated over time these gains represent a strategically significant changes.[60] The DoD in its Indo-Pacific strategy recognizes this incremental nature in China's activities to control disputed maritime spaces in the Pacific.[61] These activities have drawn complaint from the United States, but as per Chinese design, fall short of inciting enough ire to motivate a military response sufficient to modify Chinese behaviors.[62]

---

[57] "Workshop Summary: 5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks," Lawrence Livermore National Laboratory, November 14, 2018, https://cgsr.llnl.gov/content/assets/docs/Deterrence_Workshop_Summary_Final2018.pdf, 5.

[58] "Workshop Summary: 5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks," 5.

[59] Pierce, Douds, and Marra," 51.

[60] Mazarr, 38; Pierce, Douds, and Marra, 52.

[61] Department of Defense, *Indo-Pacific Strategy Report*, 8.

[62] Department of Defense, *Indo-Pacific Strategy Report*, 8.

As the United States and the international community fail to demonstrate the will to respond in a significant way, they embolden the Chinese towards more dramatic steps, reinforcing their belief they "can get away with aggression."[63] In addition, since in gray zone competition responding with overt military action is a form of escalation, this simultaneously limits potential responses to avoid being labeled the aggressor.[64] This also highlights the need for non-military response options.[65] Lastly, as the competition continuum approaches the brink of armed conflict, China's increasing A2AD capabilities complicate deterrent signaling at acceptable risk to U.S. interests. The increased risk further reduces the chances of considering a U.S. military response due to assessments of expected costs, casualties, and outcomes. However, it is also important to consider that China's strategy may affect its calculation of risk as well.

China's competition in the gray zone is reason for concern, but it also presents competitors with some opportunities. First, consider the problem of escalation control. Neither side can be entirely sure which action will lead to an international crisis, escalation to conventional armed conflict, or worse.[66] In addition, when countries see China implement their gray zone strategies as a response to U.S. provocation, it fosters a fundamental lack of common understanding that could encourage a series of

[63] Pierce, Douds, and Marra, 53.

[64] Kapil Bhatia, "Coercive Gradualism Through Gray Zone Statecraft in the South China Seas: China's Strategy and Potential U.S. Options," *Joint Forces Quarterly 91* (4th Quarter 2018): 24-33, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-91/jfq-91_24-33_Bhatia.pdf, 30.

[65] Bhatia, "Coercive Gradualism Through Gray Zone Statecraft in the South China Seas: China's Strategy and Potential U.S. Options," 30.

[66] Pierce, Douds, and Marra, 56.

escalating actions that cannot be easily controlled.[67] Finally, competing in the gray zone is expensive financially, but also may have unintended political or international opinion effects.[68] In China's case, some of its neighbors are looking more towards the United States for strategic partnerships.[69] China's main form of competition with the United States has been in the gray zone, but it is also important to consider what actions the US has taken in the region.

United States Response in the Gray Zone

Considering that the United States can expect the primary form of international competition with China will be in the gray zone, it begs the question whether U.S. ability to prevail in armed conflict is enough. Lt Col Christopher Forrest of the U.S. Air Force's strategic studies group CHECKMATE stated:

> While being prepared to fight and win a future war and deter adversaries' actions in full-scale conflict is vital, it may no longer be sufficient if Chinese (and Russian) objectives are to achieve wins below traditional armed conflict in the gray zone.[70]

If China is making gains in this space right now, it is important to examine why. As seen through the lens of Clausewitz's classic equation, resistance equals means multiplied by will.[71] China endeavors to act on both means and will, to drive down U.S. resistance to

---

[67] Mazarr, 112.

[68] Mazarr, 88.

[69] Mazarr, 88.

[70] Christopher D. Forrest, "Refocusing US Capabilities to Compete in the Gray Zone" in *Chinese Strategic Intentions: A Deep Dive into China's Worldwide Activities*, 157.

[71] Carl von Clausewitz, *On War*, eds. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), Book 1, Part 5.

their gray zone actions. In this context, A2AD developments affect relative capability in a military sense, while actions in the gray zone primarily act on U.S. will and assessment of risk.[72] Overall, these tools intend to drive the United States to judge the risk of intervention as too high when compared with the consequences of allowing the Chinese action to remain functionally unchallenged. Further complicating the analysis is a potential disparity in the degree of risk tolerance between United States and China. China may be willing to accept much more risk in the pursuit of their strategic objectives, both strategically and operationally, than the United States will. [73] In the cases when China assumes "certainly no one will start a war for [insert Chinese action here]" and is proved correct, these events change the situation incrementally and move U.S. calculus towards a less favorable assessment of the risk equation.[74] This unwillingness to counter China's actions undermines U.S. resolve, which is exactly China's intent.[75] Further, U.S. unwillingness to act raises questions about the credibility of a response to future actions by China and undermines future deterrence. Despite future deterrent signals the United States communicates, China can argue that the U.S> lacks the will to act based on past experiences.[76] China, and the international community, are watching the actions of the U.S. and utilizing this understanding to challenge the U.S. in areas of perceived weakness.

[72] Kelly, Gompert, and Long, 22.

[73] Mahnken, Babbage and Yoshihara, 57.

[74] Mazarr, 61.

[75] Mazarr, 61.

[76] Mazarr, 115-116.

Some structural considerations the U.S. from effective coordinated action to counter China. First there are disparate views of the states of peace and war in the U.S. and international community. In general, authoritarian states see war as enduring and peace as transitory, where democratic nations generally see peace as the prevailing state of being and war as an anomaly.[77] Ignoring its societal impacts, this belief benefits China and limits the United States in a national security context. Perpetual armed conflict is unpopular in democratic societies. Policymakers, therefore, have a difficult time advocating for potential enduring actions to counter China.[78] Also, U.S. agencies and the international community find it difficult to find clarity in applying policies in complex ambiguous situations. The boundaries of war and peace are hard to apply to situations that do not neatly fit either category.[79]

Second, and more importantly, is the structural disparity in the ability to coordinate across the whole-of-government or whole-of-society. In short, authoritarian societies, because they are authoritarian, can centralize and direct actions across the government and society at a level that is impossible in a democratic state.[80] The U.S. DoD establishes policies in support of the national objectives. Joint doctrine is authoritative within DoD only, but similar Chinese doctrine applies across society.[81]

---

[77] Mahnken, Babbage and Yoshihara, 59.

[78] Bhatia, 29.

[79] United States Special Operations Command (USSOCOM), *White Paper: The Gray Zone*, 6.

[80] Mahnken, Babbage and Yoshihara, 28; White House, *National Security Strategy*, 27-28.

[81] Dean Cheng, "Chinese Views of Information and Implications for the United States" in *Chinese Strategic Intentions: A Deep Dive into China's Worldwide Activities*, 13.

Although a disparity in resources often results in DoD leading other agencies due to its size. However, DoD does not dictate interagency doctrine or policy. It also has no control over resources or budgets beyond DoD.[82] Civil control over the military in a democracy is paramount to serving as professionals.[83]

Other structural factors affect implementation as well, for instance, organizations focus on what they view as their core tasks. The U.S. military has focused more on full-spectrum conflict vice competition, one particularly relevant example is that the latest version of the MDO concept regressed from previous versions when discussing, intra- and non-governmental participation.[84] Additionally, the U.S. is challenged to develop a consistent long-term and focused strategy across years of different administrations. The changing priorities further disrupt the information environment and the need to ensure messaging from the government is consistent.[85] Attempting to provide a consistent message further exposes the political differences within the government that can be exploited by our adversaries. Further challenges exist based on the organization of the U.S. government.

In the U.S. system, the National Security Council (NSC) is the first level that coordinates the instruments of national power. Following the Iran-Contra scandal, the

[82] USSOCOM, White Paper: The Gray Zone, 7.

[83] Glenn.

[84] Forrest, 157; Glenn.

[85] Hal Brands, "Paradoxes of the Grey Zone," Foreign Policy Research Institute, February 5, 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/; Mazarr, 125; Wilson III and Smitson, 61.

"consensus view" is that it should not be the agency that executes policy.[86] This lack of oversight of execution can lead to lack of integration of resources or unity of effort. To provide one example, in 2013 China unilaterally declared an Air Defense Identification Zone (ADIZ) in the East China Sea, essentially requiring aircraft entering that particular airspace to coordinate with Chinese air-traffic controllers.[87] The U.S. military took several steps to send a message of non-recognition of this Chinese action. In addition to statements of "deep concern," B-52's conducted freedom of navigation flights through the disputed area where the aircraft intentionally did not comply with the newly established ADIZ procedures.[88] However, separately, the Federal Aviation Administration issued a directive for U.S. civil aircraft to honor the newly established ADIZ.[89] Whether this was a coordinated and risk-based decision based on aviation safety or a failure of coordination across agencies is irrelevant. The conflicting actions of the government sent mixed signals to China about the resolve of the United States to challenge this Chinese action.

Overall, the opinion that coordination across the whole-of-government and whole-of-society is lacking and improvements need to be made to protect U.S. national

[86] I. M. Destler, "How National Security Advisers See Their Role," in *The Domestic Sources of American Foreign Policy: Insights and Evidence*, ed. James McCormick, 6th ed., (Lanham MD: Rowman and Littlefield, 2012), 216; Russell W. Glenn and Ian M. Sullivan, "Why the U.S. Government Is No Longer Capable of Ensuring National Security," The National Interest, March 31, 2018, https://nationalinterest.org/feature/why-the-us-government-no-longer-capable-ensuring-national-25160; Brandon Morgan, "Dropping Dimes: Leveraging All Elements of National Power On the Multi-Domain Battlefield," Modern War Institute at West Point, September 18, 2019, https://mwi.usma.edu/dropping-dimes-leveraging-elements-national-power-multi-domain-battlefield/.

[87] Bhatia, 29.

[88] Bhatia, 29.

[89] Bhatia, 29.

security in the strategic environment of the future is not a new idea. This sentiment appears in U.S. strategic documents from the NSS, NDS, NMS, and CCJO to the DoD and DoS Indo-Pacific strategy and a breadth of academic writing on the subject of competition with China.[90] Despite this, the U.S. government is not as coordinated as it could or should be. While a galvanizing event, such as a terrorist attack or major armed conflict might be the impetus for increased coordination, this is precisely the type of event gray zone competitors are avoiding. It becomes vitally necessary to develop an overarching whole-of-government vision and plan to improve coordination. The concept of multi-domain operations offers a framework to improve this coordination.

Recommendations for Improving the MDO Concept

As previously discussed, the current MDO concept focuses primarily on armed conflict despite reference to the military problem of compete as a precondition to armed conflict. However, it is a concept, not mature doctrine, and has the attention of Army leaders. Appropriately expanded, resourced, and broadened, the concept could facilitate the synchronization of all the instruments of national power across the whole-of-government, allies, and partners. So constructed, the MDO concept would serve as the organizing concept for a U.S. approach to China's activities as well as gray zone competitions elsewhere. MDO can incorporate additional emerging concepts under development that may hold keys for the competition phase in other agencies or parts of

[90] Bhatia, 30; Chairman, Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2030,* 4; Department of Defense, *Indo-Pacific Strategy Report* ,16, 54; Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America,* 4; Department of State, *A Free and Open Indo-Pacific*, 4; Jim Garamond, "Dunford Details Implications of Today's Threats on Tomorrow's Strategy," DoD News, August 23, 2016, https://www.defense.gov/Explore/News/Article/Article/923685/dunford-details-implications-of-todays-threats-on-tomorrows-strategy/; White House, *National Security Strategy,* 3, 26.

government. Ideas, such as comprehensive deterrence, gray zone deterrence, or strategic shaping, could address ways to limit escalation and complicate or manipulate the adversary's calculation of risk and cost benefits, or induce doubt in an adversary's mind as to their capability to successfully execute their plans.[91] Through modifications to the three tenants, an expanded MDO concept could serve as the coordinating framework that enables unity of effort across varied organizations.

Expansion of the MDO concept broadens the purview of its three existing tenants of convergence, multi-domain formations, and calibrated force posture to a whole-of-government view. Multi-domain formations would not solely include military forces that operate in the traditional military domains. They could also include the interagency formations that can leverage capabilities across all elements of national power, further expanding the tools available to their leaders. Calibrated force posture would not only look at locations of Army and Joint force capability, but also incorporate DoS Foreign Service officers, treasury officials, commerce department personnel, non-governmental personnel, and others into an integrated posture plan. The integration of actions would not necessarily require new authorities or challenge existing civil-military relationships. The NSC still has the authorities needed to achieve unity of effort across the government. Once the U.S. has established a viable approach to multi-domain operations, then the international community could look for opportunities for cooperation

[91] For more information on these ideas, see: John Stevenson, *NSI Concept Paper, Gray Zone Deterrence: What It Is and How (Not) to Do It*, 4; Terrence J. O'Shaughnessy, Matthew D. Strohmeyer, and Christopher D. Forrest, "Strategic Shaping: Expanding the Competitive Space," *Joint Forces Quarterly 90* (3th Quarter 2018): 10-15, https://ndupress.ndu.edu/ Portals/68/Documents/jfq/jfq-90/jfq-90_10-15_OShaughnessy-et-al.pdf?ver=2018-04-11-125441-307, 11; United States Army Special Operations Command (USASOC), *White Paper: Comprehensive Deterrence* (Ft. Bragg, NC: USASOC, April 2016), https://www.soc.mil/Files/ ComprehensiveDeterrenceWhitePaper.pdf, 5.

in areas of mutual benefit. Execution of these first two tenants would facilitate the third tenant, convergence. Rapidly "converging" all elements of national power and the efforts of allies and partners against an adversary's gray zone actions would have an exponential impact beyond the traditional military sphere.

The benefit of using the MDO concept as a starting point is that it both obviates the need to start from scratch and permits synergistic efforts across the whole of government that can benefit the nation in armed conflict and gray zone competition. For instance, advancements in Joint all-domain command and control (JADC2) would not only improve the military's ability to target enemy systems in the penetrate phase, but it would also facilitate the convergence of other systems like economic tools, diplomatic warnings, and a military action to influence an adversary's behavior. In general, preparation for armed conflict should occur in the competition phase before the capability is needed. Coordination in competition gets easier through exercises and habitual relationships formed between the joint, intergovernmental, and coalition teams. Further, U.S. led military deterrence becomes more credible as demonstrated capabilities increase between agencies and multinational teams. In theory, deterrence should reduce the chances of armed conflict. However, developing these relationships will require change and cultural acceptance at the highest levels of the government and each agency. Bureaucratic resistance to change, structural obstacles, and a lack of resources and consistent support will create challenges to achieving any lasting effects. Collaboration in the competition phase is essential to success in any of the other phases of the MDO Model.

A bureaucratic change is vital to the success of MDO in order to utilize it across the spectrum of conflict. This paradigm requires coordinated action under the leadership of a single organization, to achieve unity of effort in competition. Some ideas include a new Washington, D.C. office attached to DoS or the NSC, raising the possibility or probability that this organization's leader would not be a military officer.[92] Regardless, a MDO concept, developed largely in a DoD stovepipe and then presented as the way forward for whole-of-government integration will likely find a poor reception by other agencies. MDO concept developers would need to get the interagency, allies, and partners involved in a substantive way early on, so that the final concept has some initial by in from these agencies prior to any attempt for implementation. Inability to overcome institutional culture and resistance to change could lead to the worst outcome, an anemic organization unable to integrate action. Failure to integrate actions would provide additional opportunities for Chinese information operations and media exploitation. Finally, considering the gray zone challenge China poses to U.S. interests under the MDO concept could provide a forum to promote efforts to develop the capabilities needed for gray zone competition.[93] Many forums exist for the advocacy of the capabilities needed for armed conflict, little attention in the military industrial community is placed on the capabilities for competition.

The way forward for implementation of an idea for change is fraught with challenges, but the power of the idea begins with recognition that military capabilities

[92] Glenn and Sullivan, "Why the U.S. Government Is No Longer Capable of Ensuring National Security;" Mazarr, 134.

[93] Mazarr, 132.

are not sufficient for competition with China, or a near peer adversary. The U.S. military must recognize that it is losing the next war in the gray zone, and the U.S. is losing its relative strategic position and national power. Just as the U.S. military accepted the capability gaps that exist in Joint capabilities as a result of focused operations in Iraq and Afghanistan, it must accept that what is coordinated in competition will establish the conditions that determine success or failure in armed conflict. The military must still prepare readiness for large scale combat operations (LSCO) and armed conflict. At the national leadership level, this requires a recognition that the paradigm that has kept the United States in its advantageous position since the end of the Cold War is fraying, requiring new solutions and structures. Driving leaders across the interagency to recognize this threat and internalize the sense of urgency required for significant change must come from the top, or else it is nearly certain that the U.S. will not achieve the unity of effort required for effective implementation.

Conclusion

China is winning in the Gray zone through a combination of manipulating U.S. will to act and capitalizing on their structural advantages in integrating their elements of national power across their government and society. Expanding and operationalizing the MDO concept for this realm of competition may begin to reverse this trend and help the US compete effectively. Maintaining, and as necessary recovering, the credibility of U.S. statements of will should involve a coordinated approach across the whole-of-government. The United States must coordinate red lines with U.S. allies and partners, communicate them clearly, and must demonstrate the national resolve to enforce them.[94] Enforcement must not rely solely, and perhaps not primarily, on the military instrument of power. True whole-of-government integration is vital to sending a credible signal of will to China that the United States will defend its interests. To signal this will, the United States should reconsider its view of risk in competition. Assuming additional risk in a systemic and calculated way will redefine the boundaries between Chinese actions and U.S. responses. Accepting risk and demonstrating better whole-of-government integration may induce uncertainty in China's understanding of U.S. decision-making and provide the United States a competitive advantage when pushing back against Chinese gray zone actions.

Offered as the backbone of that integration mechanism, what may drive an expanded MDO concept's success or failure may be inter-governmental friction more than any action by China. Exploring the bureaucratic, legal, and political challenges of

[94] Bhatia, 30.

assigning an office within the U.S. government that would have the authority necessary to compel a whole-of-government approach is an area for further research. The current MDO concept may require considerable changes to enable integration of all aspects of national power at the speed required for effective action against a near peer. Within the Joint force, realizing the MDO concept as executable doctrine still necessitates overcoming considerable challenges. Many of these challenges are technical ones, but the management of organizational change and bureaucratic obstacles are at least as difficult to overcome, if not more so.

Failure to address the issue of Chinese competition in the gray zone in a comprehensive way will leave the United States in a markedly worse strategic position in the future. China will continue to exploit our vulnerabilities and achieve their strategic objectives. The United States consumes limited resources in an uncoordinated effort overseas every day. The current strategy, and execution of policy, for competition fundamentally facilitates the United States to lose in small increments every day. The end result will be a loss of strategic power to China and eventually a general inability to shape Chinese behavior through effective deterrence or coercion by military force.

This Page Intentional Left Blank

Army Special Operations Forces (ARSOF) in Competition in MDO

by

Lieutenant Colonel Eric Jacobson, U.S. Army

The Army Special Operations Forces (ARSOF) will require new authorities, permissions, and force restructuring to succeed in the type of offensive competition against near-peer adversaries envisioned in the National Security Strategy. As a first step, the Army must define ARSOF's role in supporting the Joint Force in Multi-Doman Operations (MDO) in future competition to both defeat adversary destabilization operations and deter any escalation of violence.[1] Moreover, the Army must address a legacy of cultural, legal, and political issues that have made U.S. policy historically reactive in competition below armed conflict and now inhibit global competition against Russia and China.[2] Only through such a reframing of policy and doctrine can the Army empower ARSOF with the necessary authorities, permissions, and force structure to execute successful offensive competition.

The United States Army has yet to fully define the Multi-Domain Operations (MDO) concept, which focuses more on winning in conflict then winning through offensive competition. TRADOC Pamphlet 525-3-1 instructs Army Forces to seize and retain the initiative in the competition phase, however the predominant description of

[1] Training and Doctrine Command, *Training and Doctrine Command Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations* (Fort Eustis, VA: Training and Doctrine Command, December 2018), 27.

[2] *Training and Doctrine Command Pamphlet 525-3-1*, 27

Army operations in competition focuses on doctrinal tasks such as deter and deny.[3] Deter and deny are fundamentally defensive operations and imply that the United States will be defensive in competition to counter near-peer adversaries while creating a favorable environment for a rapid transition to armed conflict if deterrence fails. The United States, utilizing a whole of government effort, should instead approach the current state of competition with a mindset towards offensive competition.

To effectively compete against near-peer adversaries the U.S. will need to address and adjust not just concepts, doctrine, force design, and budgets, but also authorities and permissions required to win in competition to prevent large scale combat operations (LSCO). Traditionally, the U.S. military has focused its future concepts, force design, and budgets around a model of traditional warfare and has not focused on offensive competition. The creation of organizational models primarily focused on conflict has occurred at the expense of organizations intended for competition with China and Russia below the level of armed conflict.[4]

Over the past 20 years the United States has actively engaged in conflict against Violent Extremist Organizations (VEO). Although Russia has also participated in military operations in Syria and the Balkans, Russia and China have mainly focused on offensive competition against the post-World War II Western establishment. America's competitors have redefined how to compete below the level of armed conflict with all elements of national power. Economically, China has expanded their 'Belt and Road

[3] *Training and Doctrine Command Pamphlet 525-3-1*, viii

[4] Christopher D. Forrest, Chinese Strategic Intentions: A Deep Dive into China's Worldwide Activities: A Strategic Multilayer Assessment (SMA) White Paper (Washington, DC: Joint Chiefs of Staff and Department of Defense, December 2019), 157.

Initiative' to gain access into markets in order to economically exploit other nations.[5] China is building and militarizing man-made islands in the South China Sea to expand their competitive space. Interference in the 2018 U.S. elections was another example of Russian offensive competition against the western establishment.[6] These examples demonstrate the broader offensive competition executed by Russia and China and come at the expense of American interests.

Only offensive competition can meet the intent of the 2018 National Security Strategy (NSS) and support America's vital national interests. The NSS directs the nation to promote American prosperity, preserve peace through strength, and advance American influence. This new NSS directs a return to principled realism through a zero-sum global competition strategy marked by winners and losers.[7] Winning in competition requires America to conduct offensive competition – confronting Russia and China in MDO below the threshold of state-on-state armed conflict and expanding the network of allies and partners around the globe, at the expense of both Russia and China.

To compete offensively also requires a fundamental shift in how the U.S. Government and the military view risk. The military traditionally views risk as something to mitigate. To win in offensive competition, risk should be considered as something

---

[5] Somik V. Lall, Mathilde Sylvie Maria Lebrand, *Policy Research Working Paper* 8806: *Who Wins, Who Loses? Understanding the Spatially Differentiated Effects of the Belt and Road Initiative (English)* (Washington, DC: World Bank Group, 2019), 1.

[6] Robert D. Blackwill, and Philip H. Gordon, *Containing Russia, How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge*, *Special Report No. 80* (Washington, DC: Council on Foreign Relations, January 2018), vii.

[7] Donald J. Trump, *A New National Security Strategy for a New Era* (Washington, DC; The White House, December 18, 2017), 1, https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.

taken to gain a competitive advantage. Risk taken in offensive competition expands the sphere of American influence around the globe, both to strengthen allies and reduce the effectiveness of an adversaries' actions. MDO provides a concept to better integrate SOF and conventional efforts during competition prior to having to respond to an adversary's actions.

Offensive Competition against Russia: Case Study Sudan

> In competition short of armed conflict, revisionist powers and rogue regimes are using corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground. Some are particularly adept at exploiting their economic relationships with many of our security partners. We will support U.S. interagency approaches and work by, with, and through our allies and partners to secure our interests and counteract this coercion.[8]

The scenario Secretary Mattis described above, is the new normal for our adversaries conducting offensive actions to undermine U.S. influence in competition. The U.S. and NATO response to Russian aggression against Ukraine has been defensive, deploying more conventional and SOF forces to the region to deter further Russian aggression.[9] America is preparing our allies to defend against Russian aggression, but defense, by its static nature, allows an adversary with an offensive mindset to retain the initiative. Training with allies is crucial to building strong and capable partners to deter future Russian expansion by visibly demonstrating American

[8] Jim Mattis, *Summary of the 2018 National Defense Strategy* (Washington, DC: Department of Defense, 2018), 5.

[9] Stephanie Pezard, and Ashley L. Rhoades, *What Provokes Putin's Russia, Deterring Without Unintended Escalation (*Santa Monica, CA: Rand Corporation, January 2020), 12, https://www.rand.org/pubs/perspectives/PE338.html.

and NATO resolve. While forward presence and combined training must continue, deployments and training are insufficient alone for a long-term strategy of offensive competition.

To gain and maintain the initiative in competition against near-peer adversaries the U.S. must take immediate actions utilizing ARSOF forces to conduct offensive competition to counteract coercion by our adversaries, as stated by Secretary Mattis. ARSOF can conduct many different operations that all involve competition below the level of armed conflict. These ARSOF efforts are compatible with Multi-Domain Operations because they will create multiple dilemmas for our adversaries.

Case Study: Sudan

In Africa, Russia has deployed private military contractors (PMC) to several countries, including the Central African Republic and Sudan.[10] Currently Sudan hosts approximately 300 Russian PMCs who are assisting the Sudanese government to stabilize their rule and secure key mines. With a small investment, Russia has gained access to critical natural resources and has increased influence in a nation that borders a U.S. ally, Egypt. Officially, the Russians in Sudan are private contractors, however their actions take place with the knowledge, aid, and instruction of the Russian Government.[11] The PMC operations in Sudan present an opportunity to utilize ARSOF forces to create a dilemma for Russia.

---

[10] "Russia/Africa: Alleged torture case renews focus on Russian Military Contractors in Central Africa," *Asia News Monitor Bangkok,* February 15, 2019*,* 1.

[11] Russia/Africa: 2.

The U.S. policy's desired end state of conducting offensive competition with ARSOF in Sudan is to gain an ally and maintain a favorable balance of power in the region. Two key priorities in the 2018 National Defense Strategy are to ensure the balance of power in key regions remains in our favor, and to advance an international order that is most conducive to our security and prosperity.[12] Egypt is a critical and stabilizing ally in both Africa and the Middle East, having a Russian backed and friendly government in Sudan, on the southern border of Egypt, threatens to upset the balance of power in this key region of the world. Offensive competition against Russia in Sudan would strengthen and build U.S. relations with South Sudan and weaken Russia's influence in Sudan. Additionally, any international order that is heavily influenced by Russia is not conducive to either the U.S. or allies' security and prosperity.

The Government of South Sudan recently reached a peace agreement that ended several years of civil war and has formed a new Unity Government.[13] Since South Sudan became independent from Sudan in 2011, the U.S. has been a strong supporter of this new and fragile nation. Gaining South Sudan's permission to conduct offensive competition from its territory will likely require diplomatic efforts and an increase in economic support to this new government. This young nation needs powerful and strong allies, which makes it likely that the Unity Government of South Sudan would authorize and support the U.S. request to conduct offensive competition operations from within their country.

---

[12] Mattis, *Summary of the 2018 National Defense Strategy,* 4.

[13] Max Bearak, *"South Sudan forms new Unity Government in bid to end Civil War that has killed 400,000," The Washington Post*, February 22, 2020.

The National Defense Strategy that demands innovative operational concepts requires changes in the way the Army organizes and deploys forces.[14] An innovative operational concept to conduct offensive competition in Sudan could be the deployment of a small, cross-functional ARSOF team to South Sudan. This cross-functional team could include a 12-man Special Forces Operational Detachment-Alpha (ODA), a four-person Civil Affairs team (CAT), and a three-person tactical psychological operations team (TPT). Working together this ARSOF team could execute operations along three lines of effort: (1) recruit, train, equip, and employ a surrogate force to conduct subversion and sabotage in Sudan against Russian PMCs; (2) conduct an information campaign in Sudan to create civil unrest of the populace and cause public opinion to turn on Russian contractors; (3) provide humanitarian aid to the local villages where the surrogate force reside.

An ODA would be responsible for training and developing the surrogate force. South Sudan has one of the poorest economies in the world and there is a long-standing animosity between South Sudan and Sudan.[15] These factors are important motivations for determining the viability of raising a small, but effective surrogate force in South Sudan. Once trained in the basic Soldier skills, the primary focus of training would be on clandestine subversion and sabotage operations. Once trained, the surrogate force could infiltrate into Sudan in small, two to four-man teams in civilian vehicles. The surrogate force could then proceed to conduct limited operations against

[14] Mattis, *Summary of the 2018 National Defense Strategy*, 7.

[15] Jason Patinkin, "International Funding Needed to Rescue South Sudan's Economy," Africa, Voice of America, April 28, 2016, https://www.voanews.com/africa/international-funding-needed-rescue-south-sudans-economy.

Russian interests. Targets could include generators that support mining operations and Russian or Sudanese vehicles that transport precious metals.

The intent would not be to kill or target Russians, but to consistently interfere with the Russian priority of guarding mines to produce and transport raw materials. If the Sudanese government perceives Russia is failing at their assigned task, the Sudanese Government may look for assistance elsewhere. To expand a potential rift in the Russian-Sudanese relationship, American diplomatic efforts conducted through Arab League allies could intensify to move Sudan away from Russian support, causing a dilemma for Russia. Offensive competition against Russian is both feasible and can be integrated into the whole of government approach in Sudan and the region.

Concurrent with the training of the surrogate force, a TPT could utilize multiple sources to conduct a psychological campaign into Sudan claiming Russia is stealing their critical resources. The TPT could utilize the Sudanese cell phone network to broadcast messages and photos of Russians “stealing” Sudan’s natural resources. The TPT could utilize multiple domains to reinforce this message and work by, with, and through vetted personnel in Sudan who have access and placement to local internet cafes to conduct the messaging. Information campaigns work best when tied to physical events, so part of the task of the surrogate force could be to document their subversion and sabotage efforts and display Russia’s inability to protect Sudanese mines.

While the Sudanese government has demonstrated a willingness to use force against civilians who demonstrate, the TPT could also provide external support to

strategic nonviolent movements.[16] As occurred in Poland in the 1980s, history is replete with examples of oppressed but resilient populations sustaining the motivation to resist against their oppressors.[17] Psychological Operations teams could target both university students and academics with messaging about foreign theft of Sudan's wealth by Russia with the goal of causing protests against the Sudanese government, demanding the removal of Russian PMCs from their country.

The Civil Affairs team can also be instrumental toward the success of the ARSOF cross-functional team conducting offensive competition. Most unconventional warfare operations cannot be successful without the support of the local population. Because ARSOF forces will be operating from South Sudan, a third country, their support and that of the population would enable a relative "safe zone" as a prerequisite. The local towns and villages in rural South Sudan are impoverished. A coordinated effort to provide food, medicine, and other humanitarian aid to villages that provide the surrogate force would enable an even deeper recruiting pool and maintain the support of both the population and the government of South Sudan.

Authorities, Permissions, and Rules of Engagement Required for Offensive Competition

Case Study: Syria

[16] Jehanna Henry, "They Were Shouting 'Kill Them': Sudan's Violent Crackdown on Protestors in in Khartoum," Human Rights Watch, November, 2019, https://www.hrw.org/report/2019/11/17/they-were-shouting-kill-them/sudans-violent-crackdown-protesters-khartoum#84ffd6.

[17] Maciej Bartkowski, *Poland's Solidarity Movement (1980-1989)* (Washington, DC: International Center on Nonviolent Conflict, December 2009), 2, https://www.nonviolent-conflict.org/polands-solidarity-movement-1980-1989/.

To conduct offensive competition will require not just a shift away from the United States' current defensive mindset, but also a shift in the process of requesting specific authorities. The Congressional Research Service researched whether the recent challenges by Russia and China call for new authorities and a reprioritization of security cooperation funding, which is currently focused on counterterrorism threats.[18] The authorities required by ARSOF to execute timely operations just below the threshold of armed conflict are necessary before an opportunity passes or a crisis develops. These authorities are traditionally requested by the Department of Defense after a crisis has developed. This lag time in obtaining the necessary authorities cedes the initiative, and offensive, to Americas' competitors.

Congressional authorities allowing the U.S. military to conduct operations with foreign partners, surrogates, or proxy forces, have actually limited the Department of Defense. For example, the FY2015 NDAA, Section 1209, "Assistance to the Vetted Syrian Opposition" authorization passed over a year after ISIS had captured Raqqa, Syria, and proclaimed the city as the capital of their caliphate.[19] Section 1209 limited what the military could and could not do to support the Syrian Opposition. Acknowledging the mandatory requirement and need for legislative oversight in the United States, section 1209 requires DoD report to eight different House and Senate subcommittees.[20] If the U.S. is going to effectively compete against Russia and China,

---

[18] Congressional Research Service, *DOD Security Cooperation: An Overview of Authorities and Issues,* 114th Cong., 2nd sess. (Washington, DC, August 23, 2016), 17.

[19] House Armed Services, Emerging Threats and Capabilities Subcommittee Hearing On FY2019 Budget Request For U.S. Special Operations, 115th Cong., 2nd sess., 2018, 3. Proquest.

[20] *DOD Security Cooperation*, 25.

authorities need to be less restrictive and broader to enable the Department of Defense to agilely employ ARSOF around the globe to offensively compete.

Authorizations to conduct offensive competition are also piece-meal and incomplete. A review of DoD Security cooperation authorities demonstrates numerous issues. The current allocation of resources, for example, does not align with the strategic guidance of the NSS, NDS, or NMS. Section 1206 of the 2019 NDAA states:

> Report on the use of security cooperation authorities. It is the sense of Congress that the Secretary of Defense should utilize appropriate security cooperation authorities to counter malign influence campaigns by strategic competitors and other state actors that are directed at allied and partner countries and that pose a significant threat to the national security of the United States.[21]

However, there is no specific amount of funding authorized to conduct these counter malign influence campaigns. Section 1206, along with numerous other sections of the 2019 NDAA, detail authorizations to specific countries or regions regarding security cooperation efforts.[22] The majority of the authorizations focus on counterterrorism and not offensive competition. The intent of Congress in Section 1206 is clear. It directs the Department of Defense to conduct operations to counter malign actors and malign state actors, but current security cooperation authorities do not provide the necessary legal authority for offensive competition. DoD requires additional overarching and broad authorization and funding to conduct operations utilizing surrogates, proxy forces, and partner forces (state and non-state) across the globe. In 2016, Congress authorized up

---

[21] National Defense Authorization Act 2019, Public Law 115-232, 115th Cong., 2nd sess. (August 13, 2018), 132 STAT. 1733, https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

[22] *DOD Security Cooperation, 7.*

to 50 million dollars for operations to eliminate the Lord's Resistance Army, a long standing insurgency in Central Africa, which was not an immediate threat to vital U.S. interests.[23] Offensive competition with Russia and China are threatening U.S. vital interests and Congress should authorize significantly more than 50 million dollars to compete effectively against these well-resourced near-peer adversaries.

Authorities to conduct information operations may be difficult to obtain, but authorities to conduct information operations in the cyber realm may be even more difficult to obtain. In combat environments, military commanders often withhold the authority to execute cyber operations to inform or influence populations to the general officer level. Under the current structure, this process slows U.S. information operations response times and thereby diminishes their immediate effectiveness in response to an event. In non-combat locations, many Ambassadors and Combatant Commanders are risk adverse and withhold permission for anything other than very generic and ineffective messaging. To increase effectiveness will require a shift in the mindset of the senior U.S. leadership. They will need to support approval of both information operations and psychological operations through a more responsive system or delegate a level of authority. Synchronization of psychological operations is a requirement that must occur for operations to be effective. An offensive mindset in competition will require utilizing all of the means to their best effect. Information warfare is a relatively inexpensive means to achieve the goals of the nation and should be embraced, rather than feared by senior leaders.

[23] *DOD Security Cooperation,* 24.

An alternative approval system may allow an ARSOF tactical psychological operations team to develop an overarching messaging theme and submit a CONOP for approval. Once the CONOP is approved, then the team should be able to execute the approved information campaign with all means available. This will increase flexibility for execution of the program and offensive information campaigns will be more timely and effective. Further, this system still requires civilian oversight of the military team, but retains the approval at the campaign level, rather than at the tactical level of requiring approval for all messages and medium used.

There are numerous examples of effective competition in strategic communications on the internet. ISIS mastered the simple, clear message (duty to join or support the jihad), communicated through an internet-enabled grass roots network without constraints to the messages. ISIS was able to respond to world events and capitalize on opportunities much faster than the western world news or military sources. ISIS, in effect, could make up a story supporting their information narrative without the constraints of fact checking sources or conducting investigations. ISIS was able to gain tens of thousands of recruits through their efforts without the U.S. or allies taking effective counter actions.[24] They employed an offensive competitive operations while the western world provided defensive actions in competition which had to respond to ISIS claims or misinformation.

[24] James F. Forest, *Influence Warfare* (Westport, CT: Praeger Security International, May 14, 2009), 351.

Understanding that democracies abide by the rule of law and that authoritarian and terrorist organizations do not follow many western norms or laws. The U.S. should not cede the competitive space regarding information simply because of different legal systems. Consider the example, in war both sides must do things that would not normally be accepted. At one extreme, nations kill the citizens of the opposing nation. This is a terrible thing, but terrible things happen in war. China and Russia are fighting a war for their national interests and using near unlimited state sponsored resources to achieve a whole of government approach. They have chosen to exploit the U.S. reluctance to conduct information warfare and U.S. reliance on an international set of western ideals to provide order. China and Russia are not limited by these ideals and can make swift decisions to gain an advantage over populations in the competition phase by exploiting opportunities, like poverty and poor conditions, to their benefit.

U.S. strategic messaging has become laden with bureaucratic and legal constraints on messages and messengers. It is a complex process slowed down by policy, process, and various agencies which results in a slow and often competing ineffective messaging.[25] Of course, the U.S. cannot simply abandon its form of government and conduct unilateral information operations without authorities, permissions, and oversight. The U.S. must change practices and limit agencies and organizations which can veto information campaigns aimed at Russia and China. Streamlining approvals and limiting those who can veto information operations will allow the U.S. to become more proactive in competition against near-peer adversaries.

[25] Curtis Boyd, "The Future of MISO," *Small Wars Journal* 24, no. 1 (January/February 2011): 7.

The previous fictional ARSOF operation to employ surrogates and proxy forces from South Sudan into Sudan would currently require permissions from multiple layers of various organizations. Obtaining permission to conduct offensive competition cannot be guaranteed for ARSOF operations at this time. In the Sudan scenario, after the proper authorities pass in Congress, ARSOF forces would require permission to execute operations from the Secretary of State and Ambassadors in South Sudan and Sudan (along with Chiefs of Station at both locations). Permission is also required from the Commander of US Africa Command and most likely from the Director of the Central Intelligence Agency. For SOCOM to coordinate and acquire approval from every one of these organizations, each with potential veto power, currently would take weeks to months. The President, through the Department of Defense could empower the functional combatant commander of SOCOM to be able to execute offensive competition across the globe in a more rapid and aggressive manner. Consultation with key stakeholders would still be necessary to mitigate unwanted second and third order effects, but streamlining the approval process and limiting veto power is required.

Case Study: Uighur Region

The MDO concept projects that China, with its expanding economy and military, will soon replace Russia as the primary pacing threat.[26] However, China is still vulnerable to offensive competition below the level of armed conflict. For example,

[26] *Training and Doctrine Command Pamphlet 525-3-1*, 7.

ARSOF forces could proactively support the National Defense Strategy by building capacity in the Uighur Region Forces to cause unrest and disturbances inside China.

The ethnic Uighur minority in Eastern China has been the target of oppression for decades by the Chinese Government. Reports of mass re-education camps and tens of thousands of Uighurs sentenced to serve in Chinese prisons for minor offenses such as having a beard too long provide the probable existence of a sympathetic portion of the Uighur population. ARSOF could likely assist efforts to train this group to conduct a vast array of operations to cause multiple dilemmas during competition for the Chinese government.[27] Conducting surrogate operations in China may be considered too provocative, but a vast array of other operations can be conducted to create internal dissent in China. Offensive competition requires the U.S. to further develop ARSOF capabilities now, in order to be able to provide credible options for the nation in the future.

One of the primary methods of conducting near-term offensive competition against China could be through engaging and building partner capacity. ARSOF units could conduct training deployments to potential partner nations where China is currently conducting construction, mining, or operations that could lead to debt exploitation. These deployments would support the U.S. national strategy of building partner capacity. The ARSOF teams would gain valuable intelligence that could be used to document, expose, and inform, host nation populations of China's exploitation of their

[27] "UN Panel says millions of Chinese Uighurs living in Massive Internment Camp," Radio Free Europe, Radio Liberty, August 11, 2018.

resources and corrupt intentions. This information would also support a broader global campaign to raise international awareness about some of the disadvantages associated with partnering with China. Psychological operations are an example of one of the activities in offensive competition that may create dilemmas for China without resulting in armed conflict. One theme that might be explored could question if a Chinese firm building a railroad in a developing nation with Chinese and local workers might be spreading the deadly coronavirus to the indigenous population. The fear associated with the virus may deter nations considering partnerships with China from future cooperation.

Task Organizing ARSOF for Competition and Multi-Domain Operations

To more effectively operate in a competitive, multi-domain environment, the U.S. Special Forces should conduct a thorough Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) review of the current force structure from the bottom up. This review should begin with the current, 12-man Special Forces Operational Detachment-Alpha (ODA). The traditional warfighting unit for Special Forces (SF) has been the 12-man ODA, but it lacks the required skills to operate across all domains. For example, the SF organization has no MOS for cyber. Instead of adding these emerging skills to the duties of the SF communications sergeant, the Army should consider adding another position to the ODA to facilitate operations in the cyber domain. A Special Forces cyber sergeant could also become skilled in artificial intelligence and robotics as those areas provide capabilities that will be employed by the ODA. These emerging technologies could enhance the ability of an ODA to operate from a permissive or semi-permissive

environment into a denied environment (A2AD) to advise and assist resistance or operating forces. Additional skills are needed for offensive competition against Russia and China today, as well as other emerging adversaries.

There is only one Special Forces intelligence sergeant (MOS 18F) per ODA. There needs to be a second intelligence sergeant on each ODA. Intelligence sergeants understand and employ various intelligence gathering techniques, however human intelligence (HUMINT) duties can quickly overwhelm one person due to the time required to effectively conduct, analyze, and document HUMINT. A second 18F could also specialize in signal intelligence. Understanding signal intelligence and open source information to synchronize sources of intelligence is growing in complexity and scale. The second 18F could also help leverage the rapidly evolving capability to process “Big Data” for the ODA. The ODA must add the second intelligence sergeant to enable successful operations in offensive competition.

A third additional member, a second commissioned officer, may be required for a 15 person ODA to be optimized to win in MDO. Traditionally, Special Forces recruit, assess, select, and train first lieutenants to serve on an ODA after one year as a successful platoon leader in the conventional Army. By adding a second commissioned officer to the ODA, the Special Forces Regiment will be able to develop officers with four years of experience on a team, or twice the amount of time they now can serve.

The Army has three components which build effective leaders over the course of their career: training, education, and experience. Serving four years on an ODA, conducting offensive competition, and MDO, will enrich the experience of future leaders

in ARSOF. Team Leaders could remain captains, but would be more experienced and better able to employ all the capabilities of their ODA to succeed in offensive competition and conflict.

The number of personnel authorized in a Special Forces Advanced Operating Base, (AOB) has remained unchanged for decades. The AOB, commanded by a major, has proved in combat operations to be a critical command and control organization. In Syria, one AOB commanded over 700 American forces and provided combat advisement to over 30,000 indigenous Syrian Democratic Forces (SDF) as the main effort in defeating ISIS in the Middle Euphrates River valley.[28] To succeed in Syria, the AOB required significant augmentation in both, the number of personnel, and the specific capabilities it lacked organically. To operate effectively in offensive competition and the future operating environment, the AOB requires restructuring.

The re-organization and composition changes to the AOB must also consider the DOTMLPF-P impacts and potential long-term effects on the total force. There are currently no cyber, robotics, or space, specialists in the AOB organization. Additionally, added capacity in intelligence support and a fires cell could provide the AOB more effective command and control of the ODAs and indigenous partners. This reorganization of the AOB would also provide more effective support to ARSOF cross-functional teams that could be conducting offensive competition against Russia and China.

[28] Special Forces Major, interview by author, March 12, 2020.

Rebasing ARSOF Units to Support Offensive Competition

The past four years in Syria have displayed the successful effects of Special Forces (SF), Psychological Operations (PO), and Civil Affair (CA) working together as cross-functional teams to defeat ISIS and consolidate gains. Despite this battlefield success, there is room to improve pre-mission training. The 5th Special Forces Group, based at Fort Campbell, Kentucky, formed cross-functional teams for Operation Inherent Resolve (OIR) with PO and CA units based at Fort Bragg, North Carolina. These units rarely conducted pre-mission training together and often met for the first time on the battlefield. With a 'train as we fight' logic, it would make sense that we improve integration prior to deploying for combat. Personal relationships and trust enhance operations in both competition and conflict, but take time to develop. When SF, PO, and CA teams have not trained together it takes weeks for them to develop relationships built on trust. It also takes time for young captains to learn about and understand the value of other ARSOF skills. Lack of education, training and experience results in sub-optimal integration of capabilities. Without habitual relationships, developed over months and years of combined training at home station and the Combat Training Centers, ARSOF units risk disappointing learning curves in future offensive competition.

The Army should consider rebasing O5 level tactical PO and CA units in the active duty component. Offensive competition requires CA and PO units participate with SF units conducting offensive competition against near-peer competitors. Prioritization is required with the limited capability that exists in PO and CA. Based on current priorities, SF units working in U.S. European Command (EUCOM) and U.S. Indo-Pacific

Command (INDOPACOM) should receive a higher amount of this limited resource. U.S. Southern Command (SOUTHCOM) and U.S. Africa Command (AFRICOM) would likely see reductions in accordance with the priorities in the National Security Strategy, National Defense Strategy, and National Military Strategy. Alternatively, as we confront China and Russia on a global scale, additional CA and PO units should be formed to meet the global demand for offensive competition. No part of the globe is not impacted by the current competition between Russia, China, and the U.S. for resources as part of the global economy. Reductions of capabilities to CENTCOM, AFRICOM, SOUTHCOM, or other commands, comes at a cost and associated risk. Forming more units may be preferred to reducing capabilities.

Authority to move units at the O5 level to another Army Post resides with the Secretary of the Army. Identifying PO and CA training requirements, work locations, and resources required at the new installations is critical before any re-basing decisions are considered. The current 90% fill at all active duty SF Groups enables an ability to consolidate undermanned ODAs. In order to expand an ODA from 12 to 15 personnel, most SF companies will have to adjust from 6 organic ODAs to 5 ODAs. This consolidation of ODAs will create working space for incoming PO and CA teams. Once physically moved to the new post, they will become OPCON/ADCON to the SF Group.

A critic of this proposal could argue that without dedicated and operational PO and CA groups, the recruiting for these low density MOS's, especially among the officer ranks, will decrease. This could give rise to the perception that without "real" O6 level commands, PO and CA officers will not have an opportunity to achieve General Officer ranks, therefore hurting their recruiting efforts. To mitigate the perception that PO and

CA are career ending MOSs, ARSOF could open senior positions at the five Special Forces and re-code them to allow for PO and CA officers to fill positions such as Group Executive Officer and Group Deputy Commander. This would increase the opportunity for upward mobility for these branches.

The O6 level group headquarters for PO and CA could remain at Ft. Bragg as O6 Commands, however, they would not have any organic units. Instead the group headquarters would right-size to enable them to deploy to support a 2-Star Special Operations Joint Task Force (SOJTF) to provide specialized staff in their respective fields. Additionally, demand for SF, CA, and PO officers in planning and operational assignments far exceeds the supply. Supporting major exercises, training events, and operational assignments could also exercise the staff capabilities.

Not all SF groups should look the same. It has been a long-standing tenant of military operations to weight the main effort. The NSS, NDS, and NMS all provide clear strategic guidance that the main effort of our national security focuses on Russia as the pacing threat and China as the future threat. With limited numbers of ARSOF formations, ARSOF should weight the main effort. Since the 10th and 1st Special Forces Groups are responsible for EUCOM and INDOPACOM respectively, they should each have one additional line battalion (an increase from three to four). With limited growth in overall Army size and flattening budgets, this move may have to come at the expense of 7th and 3rd Special Forces Groups (SOUTHCOM and AFRICOM) since those two regions are less of a priority within the SF community. The U.S. Central Command aligned 5th Special Forces Group would remain unchanged since it is the primary region to conduct counter-violent extremist organizations, a mission expected to continue into

the foreseeable future. Alternatively, Redesign of the Army may make additional slots available to increase SF, PO, and CA organizations. For SF rightsizing and rebasing select ARSOF units to conduct offensive competition against Russia and China will support the United States national strategy.

Conclusion

For the United States to protect and promote its national interests in a multi-polar world against near-peer adversaries, the Army must expand ARSOF's offensive competition capabilities in terms of authorities, permission and force structure. Thus reinforced, ARSOF can become an effective tool in realist U.S. policy to secure and expand a global network of partners and allies in offensive competition against Russia and China. National level policy makers and senior military leaders must understand that failure to make such reforms risks losing competitive space and global influence to international adversaries.

Page Left Intentionally Blank

Leveling Up: Improving Army Fires and Targeting for Multi-Domain Operations

by

Lieutenant Colonel Brian J. Newill, United States Army

The advent of AirLand Battle doctrine in the 1970s and 1980s represented a revolutionary shift in how Services and the Joint force operated to address the conventional Soviet threat. Many observers note the similarities between the development of AirLand Battle and the Army's new Multi-Domain Operations (MDO) concept in how the Army matches capability development to the threat.[1] Conventionally limited in range and capability, AirLand Battle provided ways for the Army to leverage capabilities of the Joint force to achieve objectives. However, with new lethal and non-lethal capabilities under development extending the operational reach of the land component beyond the land domain, the Army is poised to become a leader in providing multi-domain fires for the Joint force under MDO.[2] This transition has implications for how the Army: develops Service doctrine and informs Joint doctrine; trains and educates about Joint integration and processes; and, enables command and control (C2). This paper argues the Army's success in MDO depends on it fully embracing the Joint targeting process through education, training, and execution by incorporating recent lessons learned and improving upon current efforts. Moreover, the Army's ability to conduct mission command in MDO relies on supporting the development of a Joint

[1] Scott King and Dennis Boykin, IV, "Distinctly Different Doctrine: Why Multi-Domain Operations Isn't AirLand Battle 2.0," Association of the United States Army, February 20, 2019, https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn't-airland-battle-20.

[2] Sydney Freedberg, Jr., "Aiming the Army's Thousand-Mile Missiles," Breaking Defense, September 11, 2018, https://breakingdefense.com/2018/09/aiming-the-armys-thousand-mile-missiles/.

networked architecture and creating a framework for force structure to enable the integration of multi-domain fires.

Divided into two parts, the first part of this study examines the idea of how convergence impacts the Army's approach to Joint targeting in MDO and includes a brief review of lessons from recent operations and exercises. This first part also looks at current Army initiatives to improve how the Army trains, educates, exercises, and plans Joint targeting in the competition phase of MDO. The second part of this paper analyses ways the Army integrates and manages multi-domain fires by assessing recent concepts in C2 such as Joint All-Domain Command and Control (JADC2) and nascent organizational structure under the Fires complex. The second part also applies lessons from recent operations and exercises to inform developments. This paper concludes with a summary of recommendations contained throughout to improve the Army approach to Joint targeting and the integration of multi-domain fires.

The U.S. Army's MDO 2028 concept provides a framework for addressing the problem of layered standoff through rapid and continuous integration of all domains of warfare in competition and armed conflict. The concept offers three tenets critical to the Army's success in MDO: calibrated force posture, multi-domain formations, and convergence. Calibrated force posture calls for the global positioning of forces to give the Army greater operational reach and the ability to project power over strategic distances. Multi-domain formations give the Army capability and capacity at every echelon across all domains to disrupt and defeat adversaries. While these first two tenets are crucial components, the third tenet – convergence – arguably poses the biggest challenge for the Army due to its complexity in planning and execution.

TRADOC Pamphlet 525-3-1 defines convergence as "the rapid and continuous integration of capabilities in all domains, the EMS, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative."[3] The ability for the Joint force to converge Service-specific and Joint capabilities in MDO demands a more sophisticated degree of Joint coordination, integration, and synchronization than AirLand Battle required or recent operations in Iraq, Afghanistan, and Syria demanded.[4] Convergence must occur at a speed which complicates an adversary's decision cycle, presents multiple dilemmas, and creates windows of opportunity for friendly forces to exploit. To help achieve convergence, the Army must fully integrate capabilities with the Joint targeting process and develop systems and force structure to enable command, control, and battlespace management.

It's Time the Army Fully Embrace Joint Targeting

To rapidly transform to an organization capable of MDO, the Army must leverage the existing Joint Targeting Cycle to achieve Joint integration.[5] The Joint Targeting Cycle is a six-phase, iterative process that methodically analyzes, prioritizes, and assigns lethal and nonlethal capabilities against targets to create effects that will

[3] U.S. Army Training and Doctrine Command, *The Army in Multi-Domain Operations: 2028*, TRADOC Pamphlet 525-3-1 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, December 2018), 20.

[4] Dan Goure, "The Army's 'Multi-Domain Operations in 2028' Is an Important Doctrinal Development," *RealClear Defense*, May 3, 2019, https://www.realcleardefense.com/articles/2019/05/03/the_armys_multi-domain_operations_in_2028_is_an_important_doctrinal_development_114389.html.

[5] Michael Jacobson, "In the Opening Days of War, Let the Army Lead on Targeting," *War on the Rocks*, October 17, 2019, https://warontherocks.com/2019/10/in-the-opening-days-of-war-let-the-army-lead-on-targeting/.

contribute to achieving the Joint Force Commander's objectives.[6] In many operations and exercises, the Joint Force Commander, due to lack of capability and capacity, designates the Joint Force Air Component Command (JFACC) as the executive agent, or supported command, for leading the Joint targeting process, with the other functional or Service components playing a supporting role. However, as Michael Jacobson, a strategist with the Fires Division of Futures and Concepts Center, Army Futures Command, offers in his article *In the Opening Days of War, Let the Army Lead on Targeting*, the Joint force may need the Army to lead the targeting process when the air component's ability to maneuver is severely restricted or denied in an Anti-Access/Area Denial (A2/AD) environment.[7]

The Army Service-specific targeting process, Decide-Detect-Deliver-Assess (D3A), nests with the Joint Targeting Cycle. Therefore, the Army should resist any efforts to invent a new targeting process, or system, and fully embrace the Joint Targeting Cycle. In his article on *Targeting in Multi-domain Operations*, U.S. Army officer Kyle Borne, a targeting expert, cautions, "Attempting to create a new targeting process has proven to just create confusion and resistance from Joint partners."[8] For example, in the Rim of the Pacific (RIMPAC) 2018 exercise, he noted the Army tried to invent a new targeting process, bypassing the Combined Air Operations Center's (CAOC) responsibility to synchronize fires for the Joint Force Commander (JFC) and

---

[6] U.S. Joint Chiefs of Staff, *Joint Fire Support,* Joint Publication 3-09 (Washington, DC: U.S. Joint Chiefs of Staff, April 10, 2019), xi, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf.

[7] Jacobson, "In the Opening Days of War, Let the Army Lead on Targeting," 11.

[8] Kyle Borne, "Targeting in Multi-Domain Operations," *Military Review* 99, No. 3 (2019): 63, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-19/MJ-19-Book-1.pdf.

the Joint Targeting Cycle, leading to confusion and inefficiency.[9] Instead of inventing new processes, Borne and Jacobson suggest the Army expand its focus, from primarily conducting land-centric targeting with lethal fires, towards supporting the Joint force with multi-domain capabilities through the Joint Targeting Cycle.[10] With future Army lethal and non-lethal capabilities growing and Army targeting capacity expanding under modernization efforts, the Army must become a more active participant in the Joint Targeting Cycle at both the strategic and operations levels. Recent smaller scale operations and exercises fail to realistically stress the Army's capabilities in the Joint targeting process and mostly relegate the Army to submitting target nominations and requesting cross-domain fires. However, there are several lessons learned from Operation Inherent Resolve (OIR) and recent exercises that can help the Army become a more significant partner in the Joint targeting process for MDO.

Lessons Learned in Recent Operations and Exercises

While MDO is still a fledgling concept, the idea of operating in a multi-domain environment is not new to the Army. The Army can draw upon recent real-world operations and exercises to help inform the development of the Army's role in the application of Joint fires and targeting at the strategic and operational levels. Although the Joint force operates largely uncontested in most domains in the Middle East, the 101st Airborne Division's recent experience in Operation Inherent Resolve (OIR) as the Combined Joint Force Land Component Command (C/JFLCC) provides several lessons for further examination. As the Gulf War helped validate AirLand Battle Doctrine in the

[9] Borne, "Targeting in Multi-Domain Operations," 63.

[10] Borne, "Targeting in Multi-Domain Operations," 67.

early 1990s, the 101st Airborne Division's experience helped to prove many of the emerging concepts of Multi-domain Battle (MDB) – the precursor to MDO. In their article on *Theater Land Operations: Relevant Observations and Lessons from the Combined Joint Land Force Experience in Iraq*, authors Lieutenant General Gary Volesky and Major General Roger Noble offer three major observations with respect to multi-domain concepts in fires and targeting.

First, lethal fires were comprehensively integrated, and the result approached very close to the MDB ideal. The fires solution was effectively "Service agnostic," and was often selected from a range of capabilities sourced from across a coalition Joint force."[11] According to the Volesky and Noble, the integration and synchronization of lethal and non-lethal capabilities across all domains from strategic to tactical, including information operations (IO), electronic warfare (EW), public affairs (PA), and lethal strikes, enabled the 101st Division to secure Qayyarah Airfield West.[12]

Second, the authors note that many of the capabilities they employed came from non-military agencies, other countries, and other actors. Consequently, targeting moved beyond traditional "silos" into "all available means" merging multiple domains to dismantle enemy systems.[13] This resulted in a new, holistic approach to targeting which amplified the overall effect on the adversary.

---

[11] Gary Volesky and Roger Noble, "Theater Land Operations: Relevant Observations and Lessons from the Combined Joint Land Force Experience in Iraq," *Military Review*, June 27, 2017, 24, https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/Volesky-v2.pdf.

[12] Volesky and Noble, "Theater Land Operations: Relevant Observations and Lessons from the Combined Joint Land Force Experience in Iraq," 24.

[13] Volesky and Noble, "Theater Land Operations: Relevant Observations and Lessons from the Combined Joint Land Force Experience in Iraq," 24.

Third, the implications of the first two lessons above required a level of integrated planning and decentralized action. The land component, and even the Joint force, did not own, control, or have authority over some of the capabilities employed. Nevertheless, the staffs coordinated to achieve effects on the enemy in support of the commander's objectives. Integrated planning provided a process and common framework by which the land component could coordinate, integrate, and synchronize multi-domain capabilities without having centralized control over the assets involved. However, Volesky and Noble emphasized the integrated planning process does not substitute for, nor alleviate, the need for command direction and staff orchestration of traditional military functions.[14]

These three lessons highlight some of the challenges with MDO and help develop a framework solution for targeting and the convergence of lethal and non-lethal capabilities. While the Army can extrapolate these lessons for MDO 2028, the scale and speed of large-scale combat operations (LSCO) in the future present a more complex targeting challenge at the strategic and operational levels. In the future Joint Operating Environment (JOE) 2035, peer adversaries possess the ability to contest Joint capabilities in all domains at a scale previously unseen to deny access to the theater of operation.[15] The recent experiences of the Multi-Domain Task Force (MDTF) in the Indo-Pacific Theater in exercises such as Yama Sakura, Pacific Sentry, Rim of the

---

[14] Volesky and Noble, "Theater Land Operations: Relevant Observations and Lessons from the Combined Joint Land Force Experience in Iraq," 24-25.

[15] U.S. Joint Chiefs of Staff, *Joint Operating Environment 2035 (JOE 2035), Version 1.0* (Washington, DC: U.S. Joint Chiefs of Staff, July 14, 2016), 4-20, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2 017-12-28-162059-917.

Pacific and Valiant Shield, provide some insight into how the Army should approach MDO targeting in the future contested operating environment.

In these exercises, the MDTF discovered that strict adherence to the Service-centric targeting process failed to maximize integration with the Joint force. Specifically, the MDTF duplicated targeting efforts of the Combined Air Operations Center (CAOC) which led to deconfliction and coordination issues with the other Service components, particularly in the space, cyber, and air domains.[16] Historically limited in capability, the Army's targeting process provincially focused on the land domain against an adversary's land-based force. However, the MDTF gives the Joint force expanded capabilities to operate in a contested air and sea environment with speed and agility. The MDTF, working for the Theater Joint Force Land Component Command (T/JFLCC) in these scenarios, found it critical to adhere to the Joint Targeting Cycle to facilitate coordination, deconfliction of airspace, and synchronization of cyber and space effects.[17] The MDTF planners adjusted to the Joint Targeting Cycle which: 1) developed a common framework; 2) integrated and synchronized capabilities with the Joint force's actions; 3) achieved a convergence of capabilities; and, 4) created windows of opportunity for exploitation.[18]

The lessons from OIR and the MDTF will help develop future MDO targeting doctrine at the Service and Joint levels. However, these lessons represent less of a paradigm shift and more of an evolution in Army targeting. The Army's always had a

[16] U.S. Army Center for Army Lessons Learned, *Initial Impressions Report: Multi-Domain Operations in RIMPAC 2018* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, October, 2018), 20-21.

[17] U.S. Army Center for Army Lessons Learned, Initial Impressions Report: Multi-Domain Operations in RIMPAC 2018, 21.

[18] Borne, "Targeting in Multi-Domain Operations," 61.

role in the Joint Targeting Cycle, but limitations in range and capabilities consigned the Army to submitting target nominations, requesting Joint fire support for land objectives, and firing in support the Joint Force Commander. The creation of formations such as the MDTF coupled with ongoing developments to improve Army long-range precision fires provide the Army with greater capability and capacity to support the Joint force commander. Essentially, the Army is evolving from a consumer of Joint multi-domain capability, to a provider of capabilities to the Joint force in all domains.[19] As Jacobson remarks in his article, "Current Joint doctrine does not acknowledge the outsized role that Army artillery will play in the opening days of such a conflict."[20] The Army must work to update Service doctrine to reflect these best practices and inform the development of Joint and multi-Service doctrine to effect better integration with the Joint targeting process.

Training, Educating, and Exercising Joint Targeting for MDO

Updating doctrine alone is insufficient. As the U.S. Army's Pacific Pathways MDTF pilot program and the Air Force's Doolittle Exercise Series revealed, training, education, and exercises are critical to improving Joint integration in MDO.[21] The Air Force's Doolittle Series 18 exercise noted the lack of Army personnel with knowledge and experience of command and control (C2) structures and Joint processes. The report called for the Army to adapt its training, education, and exercises to a more Joint

---

[19] Sydney Freedberg, Jr., "Aiming the Army's Thousand-Mile Missiles."

[20] Jacobson, "In the Opening Days of War, Let the Army Lead on Targeting," 5.

[21] Sean Kimmons, "Army to Build Three Multi-Domain Task Forces Using Lessons From Pilot," U.S. Army, October 15, 2019,https://www.army.mil/article/228393/army_to_build_three_multi_domain_task_forces_using_lessons_from_pilot.

integrated environment for MDO.[22] The after-action reports for the MDTF pilot program identify similar concerns.[23] Participants in Yama Sakura 73 remarked on how the limited knowledge and experience of cyber and space officers on the staff challenged the integration of capabilities in the targeting process.[24]

Fortunately, as early as 2014, the Army recognized the growing gap between Army and Joint targeting and created the Army Multi-domain Targeting Center (AMTC) at Fort Sill, Oklahoma. The Army charged the AMTC with aligning Army targeting with Joint standards and requirements.[25] In response, AMTC established the Army's first Joint targeting training pipeline to train a new cadre of Joint certified soldiers with accredited courses in Joint Intermediate Target Development (JITD) and Target Material Production Course (TMP).[26] These courses ensure the Army conducts technical target development in accordance with the Joint standards; as well as, helps eliminate errors and speed up the targeting process.

Creating technically skilled soldiers is absolutely critical, but the Army needs to go further in creating Joint qualified leaders and staff officers/NCOs at the theater, field army, and corps levels with expertise in Joint integration and processes to conduct largescale combat operations (LSCO) in the new operating environment. The Army

---

[22] U.S. Air Force Lemay Center for Doctrine Development and Education, *Doolittle Series 18: Multi-Domain Operations, Lemay Papers 3* (Maxwell Air Force Base, AL: U.S. Air Force Air University, January, 2019), 7.

[23] Kimmons, "Army to Build Three Multi-Domain Task Forces Using Lessons From Pilot."

[24] U.S. Army Center for Army Lessons Learned, *Multi-Domain Operations in the Pacific: Insights from Yama Sakura 73* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, July, 2018), 31.

[25] "Army Multi-Domain Targeting Center Multi Domain Operations," U.S. Army Fort Sill, accessed January 8, 2020, https://sill-www.army.mil/amtc.

[26] "Army Multi-Domain Targeting Center Multi Domain Operations," U.S. Army Fort Sill."

should leverage existing Joint and Service training and educational opportunities such as: The Joint Air Operations Senior Staff Course (JSSC) and Joint Targeting Staff Course (JTSC). Additionally, the Army War College should increase elective opportunities for Joint certification courses, including fires and targeting, for resident students focused on the challenges of MDO and Joint integration. The Army's Command and General Staff Course (CGSC) also provides opportunities to educate and certify officers on Joint processes and capabilities earlier in their career than the senior Service colleges. A thorough review of the Joint challenges of MDO may also warrant changing the basic and advance PME certification courses. For example, infusing more rigorous Joint training and education in fires and targeting in the Captain's Career Course level curriculum may better prepare Field Artillery company grade officers for operational level broadening assignments following battery command. Extending instruction by a week or two could alleviate the burden on units sending officers Temporary Duty (TDY) for training or spending money for Mobile Training Team (MTT) support. At the senior levels, the Joint Force Land Component Command Course (JFLCC) at Carlisle Barracks educates the General/Flag officers on MDO, and theater warfighting command. Joint targeting and Joint fires education would also help better prepare them to: integrate Joint capabilities; and, chair Joint targeting and other joint decision boards in operational commands.

Of course, educating personnel takes time, money, and resources, and while resident institutional PME presents a great opportunity to educate leaders, enrollment is limited, and schools take leaders out of the operating force for up to a year. Therefore, the Army must invest in sending personnel on temporary duty to complete courses

and/or provide more resources to course directors to execute Mobile Training Teams (MTT). Units have an important responsibility in selecting soldiers for training and education with potential to succeed at the operational and strategic levels in Joint environments. Often, however, units have neither the money nor the time to educate soldiers outside the unit. Shifting the paradigm requires supportive leaders and increased funding. Unit leadership must enthusiastically support personnel attending schools understanding the loss may temporarily affect current operations but benefit the unit – and the Army – in the longer term. The Army should increase funding for units and Human Resource Command (HRC) to send personnel to training courses in transit to assignments, as well as, ensuring incoming personnel are properly trained and certified.

Furthermore, the Army can take steps under its new Army Talent Management initiative to ensure it selects personnel with the right training, skills, expertise, and motivation for assignments specialized positions. The Army places a premium on command and key developmental positions at the brigade and below level for career advancement. While these assignments are important for succeeding in tactical operations, they do not necessarily endow the skills and expertise needed for to be successful in MDO. The Army may consider modifications to career development paths. For example, labeling certain fires and targeting positions on theater and field army staffs as key developmental assignments for field grade officers will entice greater talent with the prospect of remaining competitive for selection to key positions. Selecting leaders for staff positions based on the centralized selection board process for which potential candidates undergo cognitive assessments is another way the Army can

attract innovative, strategic thinkers. Additionally, like the pre-command course requirement for battalion and brigade commanders, mandating the completion of specific training and education prior to an assignment would also ensure organizations receive qualified personnel for these key positions.

While individual training and education create capable professionals, those individuals make up staffs who need collective training in realistic environments with challenging scenarios. The degree of sophistication and integration in multi-domain operations require larger-scale exercises at the operational and strategic levels with cross-component, interagency, and multinational participation whenever feasible. A broader integration of multi-domain organizations, operators, and capabilities in more expansive training and exercise environments fosters better training opportunities, provides personnel with much needed experience, and allows for greater experimentation. For example, following the Doolittle Exercise 18 series, participants suggested greater realism with less scripting and recognized the need for a global communications system to simulate a real-time environment.[27]

To this end, the Indo-Pacific exercises has significantly informed the development of MDO doctrine and the MDTF. A recent RAND study concluded, geography restricts the Army's ability to project precision long-range fires and non-lethal capabilities in the East Asia-Pacific region.[28] Therefore, the Pacific-focused exercises stress maritime integration with the land and air domains – an underappreciated and

---

[27] U.S. Air Force Lemay Center for Doctrine Development and Education, *Doolittle Series 18: Multi-Domain Operations, Lemay Papers 3*, 7.

[28] Timothy Bonds et al., *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?* (Santa Monica, CA: RAND Corporation, 2017), 113-114.

underdeveloped aspect of doctrine.[29] The Pacific theater also lacks a multinational defense alliance such as NATO with widely accepted standards for operating, relying chiefly on bilateral alliances/partnerships. These binary relationships create a significantly more challenging atmosphere for integrating MDO given differing capabilities and foreign disclosure issues. Several nations, including Japan, South Korea, Australia, and the Philippines, are experimenting with MDTF-like formations and multi-domain capabilities. Strengthening cooperation with Allies and seeking new partnerships promotes interoperability in MDO and multi-national fires.[30]

With another MDTF planned for Europe in 2021, many lessons learned in Pacific may extend to the European theater. However, several distinctions exist affecting how the Army may employ the MDTF and other multi-domain fires capabilities in Europe. In an interview with Defense News in September 2019, Army Chief of Staff, General James McConville, and Lieutenant General Eric Wesley of the Army Futures and Concepts Center (FCC) both agreed the MDTF in Europe must be tailored to the mission and optimized with ground-based platforms for movement and agility.[31] While the terrain-limiting geography of the Pacific theater requires substantial air-maritime integration, the geography of the Euro-Atlantic region requires significantly more air-land and maritime-land integration – again, an underdeveloped aspect of Army and Joint doctrine. The presence of NATO also demands a higher degree of technical,

---

[29] Bonds et al., *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?*, xxi.

[30] Kimmons, "Army to Build Three Multi-Domain Task Forces Using Lessons From Pilot."

[31] Jen Judson, "US Army's Multidomain Force Emerges in Europe," Defense News, September 8, 2019, https://www.defensenews.com/land/2019/09/08/us-armys-multidomain-force-emerges-in-europe/.

procedural, and human interoperability for planning and integrating multi-domain fires. NATO's training facilities, ranges, and exercises limit the extent to which NATO can train in multi-domain fires – the extended range and improved lethality of future U.S. Army systems and munitions under development further compound the issue. This problem is not unique to Europe, either, as most U.S. ranges, simulation, and training centers are insufficient for the scale of MDO.[32] Therefore, experimenting and testing future capabilities to achieve convergence requires a modern simulated environment with increased rigor, robust support, and challenging scenarios.

Acknowledging the need to revamp training and exercises to accommodate MDO, the Army recently began investing in larger-scale, globally integrated exercises by expanding the breadth and scope of current exercises. Recent exercises such as EUCOM's Defender 20 and NATO's Trident series seek to test the Army's ability to fight multi-domain operations. These promising exercises bring in new organizations and capabilities such as NATO's Cyber Operation Command (CyOC) and the U.S. recently activated 41st Field Artillery Brigade – the precursor to a European MDTF planned for 2021.[33] EUCOM and NATO must continue to look for new opportunities at the strategic and operational levels to train MDO such as wargames and tabletop exercises (TTX). These exercises should include strategic level military and political leadership in order

[32] Dennis Wille, "The Army and Multi-Domain Operations: Moving Beyond AirLand Battle," New America, last updated October 1, 2019, https://www.newamerica.org/international-security/reports/army-and-multi-domain-operations-moving-beyond-airland-battle/dedicate-a-brigade-level-experimental-task-force-to-army-futures-command.

[33] Paul McLeary, "Massive NATO Wargame Seeks to Shore Up Fraying Alliance," Breaking Defense, October 14, 2019. https://breakingdefense.com/2019/10/massive-nato-wargame-acquisitions-seek-to-shore-up-fraying-alliance/.

to develop more detailed plans, rehearse the targeting cycle, and codify decision-making authorities.

The new U.S. Globally Integrated Exercises involve greater collaboration amongst the Geographic and Functional Combatant Commands focusing on global plans, operations, deterrence, command and control, messaging, and fires. While the U.S. built the first two exercises on top of existing scenarios, the next exercise will be constructed from the ground up.[34] The Army Futures Command's five-year Future Study Program campaign – formerly Unified Quest – gives the Army's senior leaders an exercise platform to help make informed strategic decisions regarding Army modernization efforts, including long range fires and targeting at the operational and strategic levels. These exercises also help refine battlefield development plans (BDP), calibrate MDO force packages (FP), and approve operational and organizational concepts to shape the future force and inform modernization efforts.[35] Furthermore, to help synchronize and integrate emerging concepts and capabilities in these and other exercises, the Army created a Cross Function Team (CFT) dedicated to providing opportunities for increased experimentation in Synthetic Training Environments.[36]

These promising innovative approaches to MDO training and exercises indicate the Army is serious about validating the concept, identifying potential gaps in

[34] Colin Clark, "Gen. Hyten On The New American Way of War: All-Domain," Breaking Defense, February 18, 2020,https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/.

[35] Stephen Rogers, "U.S. Army Futures Command presentation on Multi-Domain Operations," filmed June 6, 2019 at the Army Medical Department Center and School, TX, YouTube video file, 69:53, https://www.youtube.com/watch?v=NbkeQ1UJNPw.

[36] Wille, "The Army and Multi-Domain Operations: Moving Beyond AirLand Battle."

understanding the future OE, and informing Army modernization. The Army must continue to invest in these types of exercises to remain competitive. To effectively train in multi-domain fires, the Army must push for increased Joint and multinational participation in exercises, focusing on command post level exercises to train staffs without the need for operational forces beyond those units with strategic and operational level capabilities (e.g. MDTF). Multi-Service participation enables the Joint force to integrate domain layers and build redundancy and resiliency in the Joint kill chain. Future redundancy is imperative to achieving convergence in a contested environment.[37] Exercise scenarios must also contain the depth, rigor, and complexity to challenge commanders and staffs. Whenever possible, exercises should incorporate real-world plans to validate battlespace design, targeting, and fire plans. Perhaps, the Army may consider the development of an experimental task force akin to the former Army's Force XXI concept or the Army Evaluation Task Force (AETF) to experiment with next generation multi-domain fires capabilities.[38] The MDTF may serve that purpose now; however, as its real-world employment expands, its role as an experimental unit may fade.[39]

Joint Targeting Preparedness in Competition

In helping to set the theater, preparedness and readiness entails more than expanding training and education; theater-level commanders must consider targeting all

[37] Eric Wesley, "Transcript: A Discussion with Lt. Gen. Eric Wesley of the Army Futures Command," interview by Rebeccah Heinrichs, Hudson Institute, June 17, 2019, https://www.hudson.org/research/15103-transcript-a-discussion-with-lt-gen-eric-wesley-of-the-army-futures-command.

[38] Wille, "The Army and Multi-Domain Operations: Moving Beyond AirLand Battle."

[39] Wille, "The Army and Multi-Domain Operations: Moving Beyond AirLand Battle."

the time across the conflict continuum, particularly during competition[40] Success demands commanders have the options and authorities MDO requires on a globally integrated scale at the start of armed conflict. In competition, GCCs must coordinate pre-approved Joint fire support plans, target folders, and authority matrixes into campaign and operations plans to facilitate the integration of Joint fires at speed and repetition. Targeting specialists to the greatest extent possible, should develop electronic target folders in the Joint Targeting Toolkit (JTT) through the advanced target development (ATD) phase. Commanders should agree on authorization for target approval (TAA) and target engagement (TEA) and delegate to the lowest levels acceptable to expedite approval and execution of a target using appropriate lethal and non-lethal means. According to Lieutenant General Wesley in a 2019 interview with the Hoover Institute, authorities reside at various levels and requesting approval takes time. He explains:

> There will be opportunities on a very lethal future battlefield that is hyper lethal … where decisions will have to be made and resources applied that we won't be able to wait weeks and months to get certain targets approved. So we need to think through what capabilities within those domains can either have pre-approved ….[41]

To operate with speed and agility in armed conflict, the Army needs to determine what authorities it needs in competition and push those authorities downward.[42] From the Doolittle Series in 2018, the Air Force found authorities held at unnecessarily higher levels complicated C2 structures and slowed down decision-making in MDO. While delegating authority assumes greater risk, exercise participants and observers

[40] Borne, "Targeting in Multi-Domain Operations," 67.

[41] Wesley, "Transcript: A Discussion with Lt. Gen. Eric Wesley of the Army Futures Command."

[42] Wesley, "Transcript: A Discussion with Lt. Gen. Eric Wesley of the Army Futures Command."

recommended pushing authorities to the lowest level capable of integrating MDO capabilities and better defining support relationships. They suggested that a more agile C2 structure built on conditions-based authorities for conducting targeting and employing multi-domain fires will allow for faster reactions to known scenarios.[43]

Enabling C2 of Multi-Domain Fires

With expanding cross-domain capabilities redefining the dimensions of battlespace geometry, the complexity on integrating and converging MDO fires requires networked command and control systems and expert personnel sufficiently organized to operate with speed and agility. Additionally, future MDO targeting will exceed the limits of human cognitive capacity forcing decision makers to increasingly rely on automation and artificial intelligence, potentially introducing greater risk with less accountability.

Multi-domain Command and Control (C2)

In recent MDO-focused exercises, observers frequently commented on the inadequacy of personnel and systems to deconflict fires and clear airspace. Moreover, the increase in cyber and space capabilities available to Theater and Land Component Commanders illuminated gaps in cross-component coordination. Observers in RIMPAC 2018 noted a challenge with digitally clearing cyber and space engagements and recommended improving communication between U.S. Strategic Command

[43] U.S. Air Force Lemay Center for Doctrine Development and Education, *Doolittle Series 18: Multi-Domain Operations, Lemay Papers 3*, 8.

(USSTRATCOM) and the CAOC.[44] The Pacific Sentry 17-03 report highlighted issues with the integration of lethal and nonlethal capabilities in planning and mission threads/execution.[45] While the issues MDO creates for battlespace management are complex, the struggle of coordination within the Joint force – particularly between the land and air components – is a historical source of friction which MDO could exacerbate in the absence of proper C2 framework, structures, and tools.

In Operation Iraqi Freedom (OIF), the pace and complexity of operations, at times, overwhelmed the coalition forces' capabilities to effectively command, control, and integrate Joint fires. For example, disagreement between the JFACC and CFLCC over placement and management of the Fire Support Coordination Line (FSCL) gave targets sanctuary from land fires that could have been serviced by air assets.[46] Additionally, disputes over the interpretation of the "deep" area led to a lengthy, cumbersome coordination process that hampered timely and effective employment of surface fires and airpower.[47] The operational reach of MDO fires threatens to compound such problems across multiple domains if not managed properly. However, MDO also presents an opportunity to correct parochial differences and widens the aperture toward

---

[44] U.S. Army Center for Army Lessons Learned, *Initial Impressions Report: Multi-Domain Operations in RIMPAC 2018*, 21.

[45] U.S. Army Center for Army Lessons Learned, *News from the Front: Multi-Domain Battle in Pacific Sentry 17-03*, 13.

[46] Michael Choe, "Achieving Cross-Domain Synergy: Overcoming Service Barriers to Joint Force 2020" (master's thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2014), 80-81.

[47] Clay Bartels, Tim Tormey, and Jon Hendrickson, "Multidomain Operations and Close Air Support: A Fresh Perspective," *Military Review* 97, no. 2 (2017): 10-122,https://www.armyupress.army.mil/ Portals/7 /military-review/ Archives/Englis h/MilitaryReview_ 20 17430_ art001.pdf.

an increasingly integrated, rapid, and agile approach to targeting and fire support coordination in which all components/domains are viewed as equal partners and mutually enabling.[48] To this end, the Army and Joint force developed the concept of "any shooter, any (or best) shooter" – a central idea the concept of convergence.

The "any sensor, any (or best) shooter" concept seeks to digitally link any sensor to any shooter with any C2 node in near-real time to converge multi-domain capabilities against a target.[49] Ultimately, the idea aims to connect every soldier, device, and weapons platform. This concept materialized as Joint All-Domain Command and Control (JADC2) – software-enabled C2 capability with the goal of linking every sensor to every shooter via a military "Internet of Things".[50] Given its vast experience with coordinating across domains, the Air Force anticipated the challenge with C2 early in the MDO concept development and began work on a Multi-Domain Command and Control (MDC2) system initially termed the Air Battle Management System (ABMS).[51] Recognizing the Air Forces' expertise and initial advancements in MDC2, Gen Milley permitted the Air Force to spearhead the development of JADC2. The Air Force touted ABMS as the possible answer to the JADC2 problem, and embarked on a campaign to

---

[48] Bartels, Tormey, and Hendrickson, "Multidomain Operations and Close Air Support: A Fresh Perspective," 10-12.

[49] Theresa Hitchens, "All-Domain Ops Require Rethinking Combatant Commands: Goldfein," Breaking Defense, March 10, 2020, https://breakingdefense.com/2020/03/all-domain-ops-require-rethinking-combatant-commands/.

[50] Hitchens, "All-Domain Ops Require Rethinking Combatant Commands: Goldfein."

[51] Sydney Freedberg, Jr., "Air Force ABMS: One Architecture to Rule Them All?" Breaking Defense, November 8, 2019, https://breakingdefense.com/2019/11/air-force-abms-one-architecture-to-rule-them-all/.

collaborate on ABMS development with the other Services.[52] Although the Services agree on the general concept for JADC2, they do not share a universal understanding of what it entails or the output.

In his testimony before the House Armed Services Tactical Air and Land Forces Subcommittee in March 2020, the Army Futures Command's General John Murray emphasized that all the Services agreed to the basic concept of JADC2 but differed on solutions to achieve it.[53] Reinforcing General's Murray's point, Lieutenant General Eric Smith, commanding general for Marine Corps Combat Development Command, supported the idea of a common system in which to feed data, but argued against forcing Services to adopt a specific methodology for passing data.[54] Perhaps, Lt. Gen Smith believes, as the Army suggests, the Air Force is attempting to push its solution to JADC2 on the other Services too fast, too soon. The Air Force's decision to rename its Air Battle Management System to *Advanced* Battle Management System (ABMS) to incorporate Joint aspects may confirm the Army's suspicion.

Although eager to collaborate with the Air Force and the other Services to develop a solution, the Army advised against simply acquiescing to the Air Force's proposal as the sole solution. Seen as perhaps too air-centric, Lieutenant General Wesley, Commander for the Army's Future and Concepts Center (FCC), cautioned against a sole solution due to a difference in scale between the Air Force and Army and

---

[52] Freedberg, Jr., "Air Force ABMS: One Architecture to Rule Them All?"

[53] Lauren Williams, "Services grapple with 'any sensor, any shooter' network concept," Federal Computer Week, March 6, 2020, https://fcw.com/articles/2020/03/06/jadc2-shooter-sensor-williams.aspx.

[54] Williams, "Services grapple with 'any sensor, any shooter' network concept."

unique Service requirements.[55] While his warning could be construed as inter-Service bickering to protect Service equities and maintain control over material acquisition, it's important the solution meets Army requirements.

The Army must also avoid levying unnecessary or unrealistic requirements in search of a panacea which prolongs material development and shuns viable alternatives as occurred with the Future Combat System (FCS). A 2012 RAND study into the Future Combat System (FCS) concluded the Army failed to develop requirements appropriately and lacked "a sound technical feasibility analysis" overly relying on assumptions of what capabilities the science and technology, and acquisition communities could ultimately produce.[56] According to the report, the Army allowed parochial self-interests to impede capability development, neglecting to adjust to changing conditions.[57]

In another example, the Army's ongoing struggle with combining the capabilities of the Advanced Field Artillery Tactical Data System (AFATDS) and the Joint Automated Deep Operations Coordination System (JADOCS) highlights the difficulties with attempting to field one system to meet all tactical and operational Joint fire support requirements. Multiple theaters have employed both systems successfully according to their intended use, but the Army aims to merge JADOCS capabilities with AFATDS

---

[55] Sydney Freedberg, Jr., "ABMS Can't Be 'Sole Solution' For Joint C2, Army Tells Air Force," Breaking Defense, January 22, 2020, https://breakingdefense.com/2020/01/abms-cant-be-sole-joint-c2-solution-army-tells-air-force-exclusive/.

[56] Christopher Pernin et al., *Lessons from the Army's Future Combat Systems Program* (Santa Monica, CA: RAND Corporation, 2012), xx.

[57] Pernin et al., *Lessons from the Army's Future Combat Systems Program*, xx-xxii.

despite some evidence from the field the endeavor may prove too difficult. For example, between August 2016 and August 2017 over the course of three exercises, the 210th Field Artillery Brigade identified several limitations with AFATDS' ability to replicate JADOCS' capabilities. Similarly, in March 2016, the 197th Field Artillery Brigade produced a list of shortfalls with AFATDS later validated by the program managers and Fort Sill. Much of problem stems from trying to develop a one-size-fits-all solution to a poorly scoped requirement. Many competing equities determine the way ahead in a complex acquisition process. The lack of specific requirement statements and uncertain availability of technology in the future often lead to new products being produced with the best technology that was available years ago. This imbalance causes frustration and discontent, but the products were manufactured to the written government specifications. Perceptions that a system needs to be all things for all Services, is unrealistic and impractical. Each system operates as mandated, so perhaps in this case, the Army is attempting to solve a training or procedural issue with technology.[58]

Today, Services and functional components communicate via various wave forms and use multiple systems for transmitting data. Not all systems for intelligence, fires and targeting connect to one another forcing users to employ workarounds and analog methods of passing information which injects human error into the process. Moreover, the prevalent – and often risky – use in many commands of Microsoft PowerPoint and Excel spreadsheets for managing targets, fire missions, fire support

[58] Christopher Thompson, "The Future of Fires Software: AFATDS and JADOCS," *Fires* 644, no. 18-3 (2018): 34-35, https://sill-www.army.mil/firesbulletin/archives/2018/may-jun/articles/18-3_6_Thompson.pdf.

coordination measures, airspace coordination measures, amplifies a lack of interoperability and training. On smaller scale operations, these procedures may work, but in large-scale combat operations in a degraded and contested MDO environment, the process can quickly become overwhelming. In an MDO environment against a near peer adversary, digital or automated solutions for passing data will be required by the speed of operations needed in order to succeed. Furthermore, not all forms of communication will work with our partner nations to employ fires. For example, high frequency communication for sending targeting data requires the approval of all countries whose electromagnetic spectrum is affected. This approval also takes time to coordinate and may be difficult to obtain in conflict if not previously approved.

Recognizing the challenge with inter-Service interoperability in bringing the "any-sensor, any-shooter" concept to fruition, the Army and Air Force embarked on creating prototype software to translate message formats between different systems involving AFATDS. After developmental testing in a virtual environment, Beale Air Force Base and the 101st Airborne Division successfully demonstrated the technical feasibility of machine connectivity between Air Force sensors and Army shooters in 2019. Standard workflows and properly formatted messages streamlined the process and bypassed organizational layers allowing for faster prosecution of targets. The lessons learned from this endeavor will help inform future software development as the Army looks to better coordinate with the other Services for a truly Joint, multi-domain solution.

Additionally, expanding these types of exercises to other Services over greater distances between sensors and shooters will promote further advancement.[59]

Considering these examples, the Army must work to balance the need to meet future requirements with the risk of chasing a ubiquitous solution to a potentially ill-conceived problem. The Army should consider closely the wisdom and necessity of linking every sensor to every soldier/shooter. The ability to process targets and integrate fires at the speed and scale of multi-domain operations will require leveraging artificial intelligence and the ability of tactical commanders to make quick decisions with strategic implications. The increased speed of actions and complexity introduces additional risk for military and political leaders. Decentralizing execution and distributing C2 potentially sacrifices accountability and judgement for speed and agility. In the end, perhaps the most important goal of any multi-domain C2 system architecture should be to improve battlespace management decision-making to outpace the adversary's decision cycle through unity in action and effort. Multiple interoperable computer hardware and software solutions that meet each Service's needs may be preferable to one Joint solution. The development of a JADC2 system should focus first and foremost on those requirements and capabilities which enable the convergence of capabilities and create windows of opportunities to extend the Joint force's operational reach.

[59] Isaac Lewellen, James Patrick, and Larry Jennings, "From Sensor to Shooter, Faster," U.S. Army, June 7, 2019, https://asc.army.mil/web/news-alt-jas19-from-sensor-to-shooter-faster/.

Building Operational and Organizational Capacity for MDO

In general, networks and computer systems facilitate and enable command and control, but ultimately at some level, humans – whether in or on the loop – are planning, managing, or executing processes. Therefore, warfighting entities require organizational structure to operate efficiently and effectively. With new Army strategic and operational fires on the horizon, the Army must have adequate force structure for employing multi-domain fires at echelon, particularly at the theater and field army levels. Observations from recent MDTF-related exercises noted the lack of Joint billets to effect Joint integration, especially when assigned or attached to a Joint task force.[60] Participants in the Doolittle Series also found a shortfall of personnel with Joint experience and expertise.[61] Echoing these lessons, Lieutenant General Wesley spoke to Defense Media in August 2019 of the need for the Army to build capability and capacity at echelon:

> I think what you're going to see is after we get these MDTFs out into theater…and as we go through total Army analysis what you'll see is that we'll start building out those echelons we've talked about. You'll need to have a theater fires command; you'll need to have an operational fires command. You'll need to have cyber capacity at echelon. You'll need to have access to space assets at echelon.[62]

[60] U.S. Army Center for Army Lessons Learned, *Initial Impressions Report: Multi-Domain Operations in RIMPAC 2018*, 13, 25-26.

[61] U.S. Air Force Lemay Center for Doctrine Development and Education, *Doolittle Series 18: Multi-Domain Operations, Lemay Papers 3*, 7.

[62] Erik Wesley, "This 3-star Army General Explains What Multi-domain Operations Mean for You," interview by Todd South, *Army Times*, August 11, 2019, https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/.

Lieutenant General Wesley clearly indicated a need for fires headquarters and appropriate manning for successful operations in an MDO environment.

The Theater Fires Command (TFC) and Operational Fires Command (OFC) are the U.S. Army's initial answers to the problem of integrating multi-domain fires for large-scale combat operations (LSCO). Fort Sill's Concept Development Division built the TFC and OFC concepts to give the Army capability and capacity to plan, coordinate, and employ precise and responsive fires at the strategic and operational levels through an integrated "Fires complex".[63] Using an integrated fire control network, each organization is designed to maximize organic delivery capability and conduct multi-domain targeting. The OFC provides the corps or field army commander with ground-based operational lethal and nonlethal fires. The TFC is the senior fires command headquarters that can coordinate, or combine, with the MDTF and other Theater enablers to provide the theater land component commander with unique capabilities to combat the A2/AD threat.[64]

The Army Air and Missile Defense Command (AAMDC) is one of those potential theater enablers that could combine with the TFC. Under this proposed combined concept, the TFC commands and controls offensive and defensive fires. As a combined headquarters, combining staff functions common to both the TFC and AAMDC headquarters could reduce some overhead. However, adding offensive fires

---

[63] Chris Compton and Lewis Lance Boothe, "The Fires Complex: Organizing to win in large-scale combat operations," *Fires* 644, no. 18-3 (2018): 5, https://sill-www.army.mil/firesbulletin/archives/2018/may-jun/may-jun.pdf.

[64] Compton and Boothe, "The Fires Complex: Organizing to win in large-scale combat operations," 6.

coordination to the traditional roles of the AAMDC may prove unwieldy and incur too much risk for one commander. The AAMDC is also the deputy area air defense commander, theater air and missile defense coordinator, and senior commander for all air defense forces. Each of these responsibilities are significant. This proposed concept warrants further development and evaluation prior to endorsement. While a commander can be dual and triple hatted with responsibilities, the staff capacity to perform all these planning, coordination, and execution responsibilities quickly becomes overwhelmed without significant augmentation. The protection risk is also significant to friendly forces if any of these staff functions are compromised.

Furthermore, with the Army refocused on the corps as the senior tactical warfighting echelon for the future operating environment, both the Air Force and the Army are examining the need to reestablish Air Support Operations Centers (ASOC) at corps headquarters. This reverses the decision to shift from corps-centric to division and brigade-centric operations made by the Army in 2011. The Air force accommodated the Army's request and reorganized its Air Support Operations Squadrons (ASOS) to provide Army divisions with ASOC capability.[65] Left with a small Air Force Tactical Air Control Party (TACP) and virtually no ability to control airspace, the requirement for corps assigned airspace all but disappeared from doctrine. With the Army's increased emphasis on corps-centric operations under MDO, and the decision to create another Army corps, the Army recognized this need to provide airspace control at the corps

[65] U.S. Army Combined Arms Center and U.S. Air Force Air Combat Command, *The Joint Air Ground Integration Cente*r, ATP 3-91.1/AFTTP 3-2.86 (Fort Leavenworth, KS: U.S. Army Combined Arms Center, April, 2019), v, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN16449_ATP%203-91x1%20FINAL%20WEB.pdf.

level. This creates a new requirement on the Air Force for solutions without stripping Army divisions of the capability to control their own airspace as well.

The call for more Joint billets and LNOs; the creation of three MTDFs; the potential need for fires commands at echelon in the Pacific and Europe; the reemergence of corps-level ASOCs; and, the increase of cyber and space support personnel; all translate potentially to thousands of more operators required across the Joint force. However, generating force structure often comes with a price. In a resource-constrained environment, the addition of personnel from one organization likely equates to a loss for others. Moreover, during periods of downsizing, force managers recently have made cuts to strategic and operational level headquarters to meet the mandated end strength. As the MDO concept further materializes, the Services' appetite for more organizational capability and capacity will undoubtedly grow. Consequently, the lack of a unified framework could lead to inter-Service strife as they attempt to balance requirements and resources. Careful analysis and right sizing of all Service components is favorable to myopic piecemeal approaches. It is difficult to achieve greater capability at the Theater Army level while simultaneously cutting personnel in other areas of the headquarters. Perhaps, a revised and expanded Theater Air-Ground System (TAGS) model to encompass MDO developments could help provide a framework to enable multi-domain fires C2 and guide the development of organizational capacity that meets each Service's requirements.

The TAGS combines each Service's command and control (C2) and airspace management systems into a unified framework to create a synergistic effect when conducting Joint operations. Since it's not a formal system, the Joint force commander

can tailor the TAGS, through Theater policies and plans, to support operations.[66] However, in general, the components consistently follow a basic design, tactics, techniques, and procedures, so that other components in the Joint force can plan and operate habitually – essentially, a plug-and-play model. To make the TAGS functional, each Service operates its component to the system augmented with Joint personnel support to enable integration across the Joint force. Components typically exchange liaison officers and operational communications (less formal than liaisons) equipped with appropriate C2 systems.

As originally intended, this system promotes Joint integration in the conventional sense of components supporting one another with Joint fire support in the traditional domains of air, land, and sea – as in the example of the Air Force supporting the Army with close air support (CAS). However, with the expansion into the: domains of space and cyberspace; and, 2) the information environment; the system does not integrate the multi-domain fires well. The expansion of Department of Defense (DoD) organizations and Joint force enablers available at the strategic and operational levels further compounds the problem of integrating the sensors and shooters across the Joint community. The Joint Force Commander needs a modernized network capable of facilitating greater integration and C2 of multi-domain fires.

Transforming TAGS into a multi-domain fires integration system would provide a new unified framework for Joint fires. A new, expanded model can account for ongoing

[66] U.S. Air Land Sea Application Center, TAGS: Multi-Service Tactics, Techniques, And Procedures For The Theater Airground System, *ATP 3-52.2* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, June, 2014): 1, https://jdeis.js.mil/jdeis/alsa_pdf/alsa_tags.pdf.

developments in lethal and non-lethal capabilities, the creation of Space Force, and developments in multi-domain command and control, such as JADC2 and ABMS. The revision of TAGS should nest various targeting processes like the Joint Targeting Cycle, Joint Air Tasking Cycle, and Cyberspace Tasking Cycle to streamline deliberate targeting. Revisions could also include simplifying systems for dynamic support requests such as the Joint Air Request Net (JARN), Air Support Request (ASR), and Cyber Effects Request Form (CERF) with standard workflows and message formats to promote speed from sensor to shooter. Operating within an agreed, unified framework fosters inter-Service cooperation by encouraging Joint solutions and the development of future concepts and capabilities for the integration of multi-domain fires.

Recommendations and Conclusion

Throughout, this paper offers recommendations for how the Army can enhance its role in the conduct of Joint targeting and the integration of multi-domain fires to support the Joint force in achieving convergence. Updates to Service targeting and fires support doctrine must incorporate more aspects of the Joint Targeting Cycle and account for developments in lethal and nonlethal capabilities. While air- land Joint integration is well defined and practiced, maritime-land integration is less understood or practiced between the Navy and the Army and requires renewed focus. As new capabilities emerge, established joint doctrine, systems, practices, and procedures may require refinement or complete revision to enable convergence of capabilities across all domains to achieve the desired effects upon an adversary. To capitalize on AMTC's recent success in training Joint targeting, the Army should invest more in Joint-focused training courses and expand PME to incorporate multi-domain concepts. In line with its

Army Talent Management initiative, the Army must modernize its leader development systems and career paths to attract top talent and prepare leaders with the required skillset and acumen to operate in a Joint environment. The Army must expand existing ranges and construct new training environments to accommodate technological advancements. Additionally, the Army must leverage current exercises, such the Pacific Pathways series, and create new opportunities to train the integration of Joint targeting and multi-domain fires at the strategic and operational levels. These exercises should include Joint, interagency, and multi-national partners and contain sufficient rigor to stress and evaluate systems, networks, and concepts.

A modernized C2 architecture capable of handling the complexities of integrating multi-domain fires presents an enormous challenge for the Army. The goal of linking every sensor with every shooter depends on the Army properly managing the acquisition process in coordination with the other Services and combatant commands to avoid repeating past failures or pursuing uncoordinated efforts. A Joint architecture may represent the best, and most costly, prospect to achieve multi domain integration. However, a costly system could fail due to inter-Service rivalries or future budget cuts. The creation of new force structure to enable the planning, coordination, and execution of multi-domain fires is also a required, and potentially expensive, undertaking. As with the creation of a multi-domain C2 network, the Army must construct requirements in conjunction with the other Services. Adapting and expanding the TAGS as a framework to combine multi-domain activities may help ensure Services coordinate the Joint development of their organizations and minimize bureaucratic inefficiencies.

In conclusion, the Army's recent efforts to improve fires and targeting clearly demonstrate an appreciation for the enormity and complexity of the task ahead to realize MDO. The Army leadership has the opportunity to lead the Joint community as it tackles the concept of all-domain operations based principally on the Army's MDO concept. The MDO 2028 concept, avoids land-centric language and Service-specific answers to the Joint challenges of A2/AD. Solutions must be developed from Joint requirements and evaluated in Joint environments to provide the greatest possibility of obtaining the speed, agility, and scale required to achieve Joint capability convergence. The Army must regain the capability to converge joint capabilities against all adversaries to achieve our national objectives. The A2AD challenge requires a Joint solution. To fail to meet the challenges of the future would break the sacred trust that the nation has placed in the Army. The Army must be able to win the nation's wars without exception. Competing demands for modernization and readiness resources will create significant obstacles to achieving a consistent long term approach to achieve a Joint solution. The MDO concept may help articulate the need for consistent Joint cooperation and promote unity of effort.

Multi-Domain Operations: Modernizing Reserve Force Mobilization Capabilities

by

Colonel Shawn Patrick Underwood, United States Army

The time has come when we must proceed with the business of carrying the war to the enemy, not permitting the greater portion of our armed forces and our valuable material to be immobilized within the continental United States.

—George C. Marshall[1]

The United States faces multiple near-peer competitors in the world today leveraging advancement across all Space, Cyberspace, Air, Land, and Maritime domains and Information and Electro-Magnetic Spectrum environments to counter American power. China and Russia have capitalized on the fact the U.S. and its allies have been in continuous conflict over more than two decades inside Iraq and Afghanistan. All the while, they have observed and reviewed US and allied capabilities to leverage, adapt, and modernize Chinese and Russian capabilities to outpace the United States. The Chinese and Russian threats remain formidable and center on integrated fires capabilities paired with modernized air, land, and maritime forces that form an anti-access/area denial (A2AD) structure which generates standoff against U.S. and Joint Force capabilities.

United States forces struggle in the competition phase of Multi-Domain Operations against Chinese and Russian near-peer threats from modernized air, land, and maritime anti-access/area denial (A2AD) systems. Moreover, current U.S. Army

[1] "Times-Herald" (Washington, D.C.), (p.1), March 3, 1942." George C. Marshall Quotes, AZ Quotes, accessed April 1, 2020, https://www.azquotes.com/author/9510-George_C_Marshall?p=2.

efforts lack an effectively credible, integrated reserve component (AC/RC) force structure for Multi-Domain Operations because of changing operational environments. This competition degrades US Army readiness due to constant deployments affecting all three US Army components. Many key enablers and capabilities at echelons above brigade reside in the reserve component and must be considered for reallocation to the active component if required in future MDO war plans. Additionally, the threat of large-scale ground combat operations (LSGCO) potentially places new training requirements (e.g. maneuver, live-fire, command and control) and does not increase available training and readiness preparation time for National Guard and reserve composition units when allocated to Active Duty combatant commanders for war plans. This burden on the Total Army Force led the Chief of Staff of the Army, General Mark Milley, to develop a new initiative to help reduce deployment requirements on brigades. One of these initiatives was the Security Force Assistance Brigades (SFAB) program in both the active and reserve component.

While employing SFAB's reduces constant brigade combat team deployment time for both active and reserve components, it also allows brigade combat teams to focus on readiness, emerging threat training, and continued force preparations. Army senior leaders should still identify an efficient Multi-Domain Operations credible force to include the active and reserve components (AC/RC) within the competition phase. Otherwise, US forces will struggle with current mobilization process challenges across all domains to successfully compete in the Multi-Domain Operations during the competition phase.

Multi-Domain Problems

The Army is currently postured as a force well versed in "counter-insurgency and other stability operations" but is also operating at a degraded readiness condition due to constant deployments affecting all three components of our U.S. Army forces. [2] Current Army Chief of Staff, General James C. McConville, expressed his intention to continue to employ SFAB units in MDO. He stated "…We're going to have to create those types of organizations [SFABs]. Part of multi-domain operations is competing, and we want to compete below the level of armed conflict."[3] We are already in competition around the globe with our adversaries, below the level of armed conflict. To achieve our national objectives requires a total Army effort before we may have to fight and win in the emerging operational environment.

The operational environment requires a more modernized Army and Joint Force to respond to the potential threat of large-scale combat operations. The Army initiated and is improving the *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons above Brigade 2025-2045* to operate against a near-peer competitor during in competition.[4] The threat of large scale ground combat operations (LSGCO), however, places new training and readiness requirements on U.S. forces across all three

[2] Department of the Army, Training and Doctrine Command, Pamphlet 525-3-8: The U.S. Army Concept: Multi-Domain Combined Operations at Echelons Above Brigade (Washington DC: Department of the Army, December 21, 2018).

[3] "The Army Cannot do what it does without the National Guard." National Guard 73, no. 10 (10, 2019): 24-26. https://search.proquest.com/docview/2311511343?acountid=4444.

[4] Department of the Army, Training and Doctrine Command, Pamphlet 525-3-8: The U.S. Army Concept: Multi-Domain Combined Operations at Echelons Above Brigade (Washington DC: Department of the Army, December 21, 2018).

compositions (Composition I – Active duty; Composition II – National Guard; and Composition III – U.S. Army Reserve). While the active duty forces carry the burden of initial modernization efforts and continuous deployment to counter this threat, the real challenge resides with the reserve forces in composition II and III and their ability to modernize, train, and conduct LSGCO if required by the combatant commander.

Addressing new concepts like Multi-Domain Operations as part of potential LSGCO places additional training and readiness requirements on an already strained reserve force (National Guard and Army Reserve). Moreover, the ability of the Army to quickly identify, create, and validate MDO force packages consisting of RC forces as detailed and deliberate as possible is critical to overall MDO concept success. Units participating in MDO operations will require additional resources, training time, and validation exercises during the Mobilization and Execution Process. Consequently, the scholars, planners, and Army senior leaders should identify and address the Army's ability to deliver these forces into a contested theater. Further, they should identify the associated training and the required timelines to meet readiness requirements. While force structure changes take time to address, applying scarce resources should be deliberate, especially as modifications in these areas could improve readiness to support Combatant Command requirements and future threats globally.

Background: Multi-Domain Operations Concept

The United States (US) Armed Forces has enjoyed the role of a global superpower since the Cold War, but the ability of the armed forces (to include the Joint Force) to operate uncontested is coming to an end. The technological and equipment advancements of U.S. adversaries alter the balance of power to create a near peer and

peer capable environment. The world is transforming and the operating environment will become more contested than ever before and require U.S. policy and defense adjustments in order to remain a global power. America's adversaries, (China and Russia), as stated in the *2018 National Defense Strategy,* have reduced and, in some domains, even removed the technological and force advantage once held by U.S. Armed forces.[5] During the last 18 to 19 years of continued conflict in Iraq and Afghanistan, America's rivals have studied the U.S. Army and our Joint Force capabilities, increased their own technological military advantages, and developed new capabilities that generate standoff from the U.S. and Allied forces. Dan Gouré, a military journalist, maintains "These systems, generally described as anti-access/aerial denial (A2AD), are intended to dominate combat in nearby theaters while protecting their homelands and forces from attack." [6] These A2AD systems overwhelm U.S. capabilities and inhibit U.S. and Allied combined and Joint operation across multiple domains.

[5] Jim Mattis, Summary of the 2018 National Defense Strategy of the United States of America (Washington, DC: US Department of Defense, 2018), 1-14, https://www.defense.gov/Portals/1/Documents/pubs/2018National-Defense-Strategy- Summary.pdf.

[6] Dan Gouré, "The Army's "Multi-Domain Operations in 2028" Is an Important Doctrinal Development" Real Clear Defense, May 3 2019, https://www.realcleardefense.com/articles/2019/05/03/the_armys_multi-domain_operations_in_2028_is_an_important_doctrinal_development_114389.html

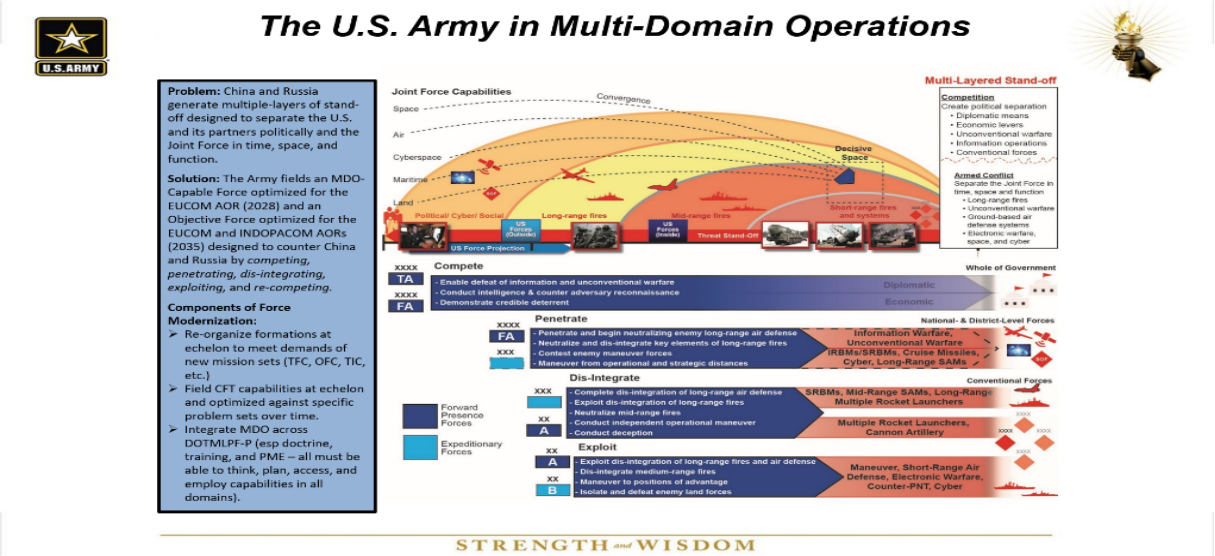

Figure 1. The U.S. Army in Multi-Domain Operations[7]

The MDO concept acknowledges A2AD existence and requires the Army, as part of the Joint Force, to "Maintain U.S. interests, deter conflict, and, when necessary, prevail in war."[8] The MDO concept not only focuses on peer and near-peer competitors such as China and Russia, but also outlines their national strategies in the U.S. National Security Strategy (NSS) and the National Defense Strategy (NDS). In response to the challenges presented by an adversary A2AD system, the MDO concept provides a model for organizing activities into five phases. The five phases outlined above in figure one are: competing, penetrating, dis-integrating, exploiting, and a return to competition phase. (See Figure 1).[9]

[7] Dr. Gregory L. Cantwell, "The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 (lecture, US Army War College, Carlisle, PA, 2019).

[8] Department of the Army, Training and Doctrine Command Multi-Domain Battle: Evolution of Combined Arms for the 21 Century; 2025-2040, version 1.0, (Washington DC: Department of the Army, December 2017, page i.

[9] Dr. Gregory L. Cantwell, "The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 (lecture, US Army War College, Carlisle, PA, 2019).

The Army forces of the future, regardless of composition, will operate in all domains, operating environments, and the five phases outlined in the MDO concept. TRADOC Pamphlet 525-3-8 describes six challenges confronting our Army components at Echelons above Brigade, and is displayed in Figure 2, which describes some necessary actions to win against a near peer threat.[10]

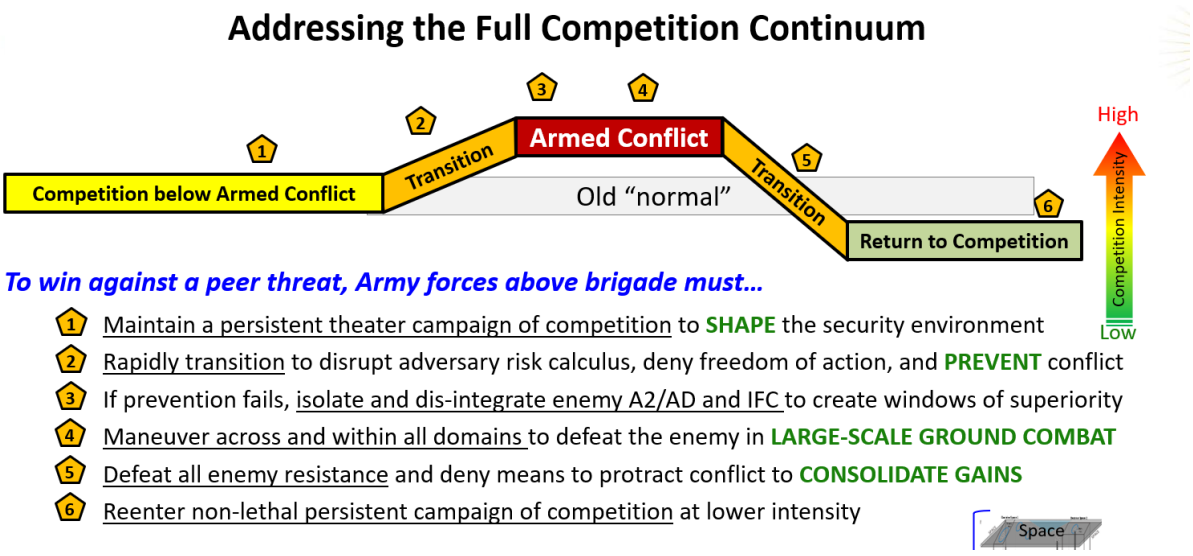

Figure 2. Six Challenges Confronting EAB Formations[11]

The ability to address these challenges at echelons below brigade presents similar, but perhaps more time sensitive, challenges for the reserve component forces. Training requirements, limited resources, and time for active and reserve training alike. The inability to predict the future further compounds the challenge to determine the potential demands placed on U.S. troops. The three tenets of MDO (calibrated force posture,

[10] Department of the Army, Training and Doctrine Command, Pamphlet 525-3-8: The U.S. Army Concept: Multi-Domain Combined Operations at Echelons above Brigade (Washington DC: Department of the Army, December 21, 2018.

[11] Dr. Gregory L. Cantwell, "The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 (lecture, US Army War College, Carlisle, PA, 2019).

multi-domain formations, and convergence) provide the Services the ability to execute operations across domains. These future cross domain Joint operational capabilities are challenging for active duty organizations to achieve with a daily training regimen. Active duty formations have more training resources and time available than the reserve forces. However, many of the reserve component forces are the enablers and sustainment forces for the active duty forces. The Army should consider the training requirements associated with MDO concept and provide additional training time and resources for the reserve forces prior to prepare prior to their mobilization for active duty. Updates in technology supporting MDO could also increase training requirements and time prior to mobilization for the reserve component. These new challenges have increased risk to mission accomplishment in an A2AD operating environment.

One identified risk, and an emerging development cost associated with MDO, is a network architecture to support collaboration. Existing network structures and systems are not adequately secure, resilient or scalable for simultaneous multidomain operations at the speed required to confront a near peer adversary. The network requirement generates an additional cost that includes operational and sustainment costs associated with new technological advances, potentially at the expense of pre-existing capabilities.[12] At a recent symposium on MDO, an audience member asked, “Are we willing to dismantle things like the [Marine Air Ground Task Force], carrier strike group,”

[12] Department of the Army, Training and Doctrine Command, Pamphlet 525-3-8: The U.S. Army Concept: Multi-Domain Combined Operations at Echelons Above Brigade (Washington DC: Department of the Army, December 21, 2018, appendix D, pg. 73.

or other similar service-specific constructs in favor of a joint multi-domain construct.[13] Leadership will likely face criticism when a new idea or concept is proposed that threatens an existing capability, however this obstacle should not overshadow the need for modernization and new concepts such as MDO.

Many senior leaders understand the requirement to adapt US forces to excel in warfare and to seek a marked advantage for U.S. forces in all domains and environments. The Department of Defense (DoD) realigned the Army Capabilities Integration Center (ARCIC) to the Futures and Concept Center (FCC) which resides in the Army Futures Command (AFC) to synchronize new and future concepts with doctrine, organization, training, materiel, leadership and education, personnel, and facility solution (DOTMLPF) for the Army. Senior leaders within the AFC and across DoD believe the MDO concept is a means to address capable peer threats. The Director of the FFC, LTG Eric Wesley in March 2020 affirms, "[W]e've enjoyed a period where problems posed by near-peers or adversaries have not adversely affected the United States or partners and allies' abilities to influence the world on behalf of our national security interests. . . . [W]ell, we find that's changing."[14] His statement rings true across all domains for the entire Army force, and to fight and win, all components should be ready when called upon regardless of composition.

AC / RC Force Mix

[13] Mark Pomerleau, "In the move to multi-domain operations, what gets lost?", C2/Comms, C4ISRNET, April 11, 2018, https://www.c4isrnet.com/c2-comms/2018/04/11/in-the-move-to-multi-domain-operations-what-gets-lost/ accessed on 21 FEB 20.

[14] "Wesley: Army Guard Key to Future Operations," Association of the United States Army, accessed March 9, 2020, https://www.ausa.org/news/wesley-army-guard-key-future-operations.

The Army's force structure and its readiness underscore how critical they are to the success of defending the Nation. Army senior leaders have placed readiness as the number one priority for all forces. The topic of appropriate force structure and force mix is not new to senior civilian leaders or the Army as they often discuss the "Abrams Doctrine" as an example to generate and justify discussion. Military Historian at the Army Heritage Education Center, Dr. Conrad Crane, in 2015 asserted:

> The Abrams Doctrine…intentionally placed a significant amount of logistics support structure in its reserve components so that if the president of the United States sent the Army to war, he would be forced to mobilize the reserves, thereby requiring him to get the support of the American people.[15]

The National Commission on the Future of the Army (NCFA), January 2016, stated:…

> However, no primary evidence supports the assertion that General Abrams consciously set out to structure the force to ensure domestic support for future wars. General Abrams' actions were designed to address the strategic challenge of the Soviet threat within manpower and budgetary constraints, nothing more.[16]

The senior leaders of the Army should consider the spirit of the Abrams Doctrine when recommending, proposing or deciding on changes to the force mix. Movement of forces from one component to the other have inherent force implications and create additional readiness requirements to be able to deploy rapidly.

The operational environment readiness, time available for training, and mobilization time concerns are additional factors to consider when designing a force

[15] Conrad Crane and Gian Gentile, "Understanding the Abrams Doctrine: Myth Versus Reality," Commentary, *War on the Rocks*, December 9, 2015, https://www.rand.org/blog/2015/12/understanding-the-abrams-doctrine-myth-versus-reality.html.

[16] National Commission on the Future of the Army, Report to the President and the Congress of the United States, (Washington, DC, January 28,2016), page 49.

structure consisting of multi-component units. The readiness levels between active and reserve component forces vary based on size of units (Brigade Combat Teams to company-sized elements) and associated Mission Essential Task List (METL). The amount of training time required for a reserve unit to achieve validation of tasks is a fundamental factor for Army planners to consider when developing potential force structures. In addition, the cost to mobilize a reserve force to active duty status is also an important consideration. Funding for reserve components can become very expensive, mainly in personnel and operations and maintenance (O&M) areas. Although training time and financial requirements come with activation, the ability to accomplish the mission cannot be compromised. Today's reserve forces are utilizing their combat experience to keep pace with some of their active duty counterparts in areas of homeland defense, Cyber warfare, counterdrug programs, and missile defense. Air Force General Joseph L. Lengyel, National Guard Bureau Chief, stated in April 2018: "Your continued support allows us to leverage our years of combat experience to help confront current and future security challenges."[17] The reserve component soldiers are skilled soldiers. Their capabilities during force mix consideration discussion and planning cannot be overlooked. The experience of a civilian career meshed with a military occupation provide a valuable addition to the active force structure.

Over half of the Army force structure resides in the reserve forces. In particular some of the key critical capabilities such as: transportation, low density / high demand

[17] Terri, Moon Cronk. Bureau Chief Details National Guard's Contributions in Senate Hearing. Washington: Federal Information & News Dispatch, Inc, 2018. https://search.proquest.com/docview/2025958575?accountid=4444.

military occupational skills (MOS), and sustainment support units are in the reserve force. Every day these forces train, fight, and work for a common Army purpose to counter threats and protect the nation.[18] The active component executes daily U.S. military functions as their primary occupation, while the reserve components consist of soldiers performing military responsibilities part-time—and these reservists can be ordered to active duty when required. These skills make each element a valuable part of the whole Army Force. Former Secretary of Defense Ash Carter, August 2016, asserted: “The presence, skill and readiness of Citizen Warriors across the country give us the agility and flexibility to handle unexpected demands, both at home and abroad. It is an essential component of our total force, and a linchpin of our readiness.”[19] When reserve forces are activated, they enhance the capabilities of the Army. Take for example a National Guard soldier who is a structural engineer in his civilian job and an infantryman in his unit. The ability to utilize his structural engineer expertise when designing and building bases can be beneficial to all and enhance the capabilities of the Army unit. The Department of Defence (DoD) should catalog the expertise of the reserve force to call upon their service in fighting unforeseen demands similar to the national emergency associated with the COVID-19 virus.

[18] Jim Mattis, Summary of the 2018 National Defense Strategy of the United States of America (Washington, DC: US Department of Defense, 2018), 1-14, https://www.defense.gov/Portals/1/Documents/pubs/2018National-Defense-Strategy- Summary.pdf.

[19] The Reserve Forces Policy Board, *Improving the Total Force Using the National Guard and Reserves, to the Secretary of Defense as part of the Report to Transition of the New Admiration* (Falls Church, Virginia: Reserve Forces Policy Board, November 2016), 7.

The Army learned through previous wars and conflicts the importance of obtaining the right force mix.[20] From the Constitution through a series of strategic guidance documents describe the roles, responsibilities, missions, and types of forces the Army can construct to accomplish its assigned mission. Strategic documents listed above provide a starting point for force structure design to provide MDO capable forces.

The importance of the right composition and abilities within these force packages are evident in the comments of former TRADOC CG, General Steven Townsend: "Calibrated force posture combines position and the ability to maneuver across strategic distances…. Multi-domain formations possess the capacity, endurance, and capability to access and employ capabilities across all domains to pose multiple and compounding dilemmas on the adversary."[21] As the future requirements change, the force structure required to produce the effects required for MDO will probably also have to change. Some key capabilities from the reserve component will have to move to the active component to meet the training and availability requirements of the new operating environment. Balancing forces between the active and reserve component requires a determination of risk and potentially longer timelines for availability than may be optimal in resource unconstrained environment. However, the limitations of budgets and active component strength limit the Army to fewer forces on active duty than may be optimal to perform all required missions without increased risk. Many force structure models,

[20] Congressional Research Service, *Army Active Component (AC)/Reserve Component (RC) Force Mix: Considerations and Options for Congress, C*RS Report R43808, Andrew Fickert (Washington, DC, December 5, 2014), 3.

[21] Sean Kimmons, Army updates future operating concept", Army News Service, December 6,2018, https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1706332/army-updates-future-operating-concept/accessed on 26 Feb 20.

experiments, exercises, and wargames are utilized to develop and evaluate the appropriate force structure.

As part of a tabletop exercise conducted by Army Futures Command, professional military officers, senior leaders, and scholars, worked through the challenges of identifying a force structure to support the milestones and decisions required in a campaign for a scenario. The developed force packages at the strategic level (Theater and Field Army HQs) set the conditions during competition for the follow on forces and subsequent phases of the campaign. Continued development of theater headquarters capabilities also apply to MDO. The field armies, new formations of theater intelligence and chemical commands, as well as newly formed strategic space battalion formations will all provide enhanced capabilities that will assist in coordination of capabilities across domains. As these formations and headquarters structures mature, they should provide options to address expected challenges during the five phases of MDO, as well as ensuring resiliency through multiple enabled, integrated, and interoperable headquarters.

Despite the differences between the active and reserve forces, they both rely on experienced leaders and soldiers. Gen. J. Lawton Collins, former Chief of Staff of the Army, expressed: "The most precious commodity with which the Army deals is the individual Soldier who is the heart and soul of our combat forces."[22] In the absence of understanding the next battlefield or new concepts to wage war, one constant remains,

[22] Eric J. Carlson, Military Blogger, 07 November 2009, https://militaryjournalist.blogspot.com/2009/11/general-j-lawton-collins-vii-corps.html, accessed March 9, 2020.

the development of the human dimension. To better prepare for the uncertainty of future combat, the Army should invest in the leader development of the soldiers during the competition phase. During a recent MDO Integrated Research Project forum at the United States Army War College, LTG (ret) Paul T. Mikolashek, former Commanding General 3rd US Army, Army Forces Central Command and Coalition Land Forces Commander, emphasized "Leader development is critical at all times."[23] Whether it is fighting abroad or executing missions in the homeland, the development and continued education of soldiers is vital for success.

In the same fashion the Army uses the One Army School System (OASS) to ensure all components remain connected through a consistent education system. Army Regulation 350-1 described, "…the One Army School System is comprised of reserve and active component organizations that utilize the training resources to educate and train soldiers in the most efficient manner possible without regard to component."[24] Professional Military Education (PME) for both officers and enlisted soldier development should include an introduction to the Multi-Domain Operations concept.

Force design also has associated risk which impacts the force allocation between the active and reserve components and could result in a less than optimal force incapable of meeting the immediate demands imposed by an adversary. One of the criticisms of MDO comes from Major General (ret.) Robert Scales in a *War on the Rocks* article in which he contends, "…New technologies are inducing new battlefield

[23] LTG (R) Paul T. Mikolashek, Former Theater Army Commander Perspective, (lecture during Integrated Research Project Forum, Army War College, Carlisle, PA, 27 FEB 2020.

[24] National Commission on the Future of the Army, Report to the President and the Congress of the United States, (Washington, DC, January 28,2016), page 74.

imperatives and are forcing the nexus of ground warfare continually downward. Thus, the Army should pursue a parallel path of reform that builds from the bottom up as well as top down."[25] The MDO force package development must consider appropriate force mix levels at each echelon. General Scales appreciated the strategic and operational focus, but contended that the tactical level should not be overlooked and may drive changes to the MDO concept at the operational and strategic levels due to lessons learned at the tactical level. The people who develop future packages ought to include characteristics such as uniqueness, management, and culture when considering proposed solutions and future budget and resource constraints.[26] Tensions between active and reserve forces continue to this day with respect to readiness, capability, and overall performance as a result of the difference between training days available to the AC and RC. More importantly, a renewed focus demands the senior leaders at all levels focus on the total force required to win. This focus should examine the Notification of Stationing Memorandum, as a part of the mobilization and execution process for the reserve forces.

Mobilization and Execution Process

While not new to the mobilization process, the United States Army has significantly improved the mobilization and execution process since WWI, resulting in a more capable reserve force today. The modern mobilization process for WWII

[25] Robert H. Scales, "Tactical Art in Future Wars", Commentary, *War on the Rocks*, March 14, 2019, https://warontherocks.com/2019/03/tactical-art-in-future-wars/.

[26] David R. Graham et al., "Evolution of the Military's Current Active-Reserve Force Mix," Research and Publications, Institute for Defense Analyses, August 2017, https://www.ida.org/research-and-publications/publications/all/e/ev /evolution-of-the-military's-current-active reserve-force-mix accessed on 26 Feb 20.

experienced logistical issues from the activation of the National Guard in the summer of the early 1940s. In the 1950s the National Guard also experienced logistical issues, long training time, and manning issues. When finally up to deployable strength and acceptable readiness levels, the Korean War reached a stalemate. From the 1970s through the 1990s, the reserve forces experienced added issues with mobilization in the form of resources due to budget constraints, which contributed to longer training times affecting readiness. Moreover, with additional budget restrictions, manning and readiness levels came to the forefront and remain a constant concern for reserve and active component forces today.

The RAND Corporation, at the request of the Office of Secretary of Defense for Reserve Affairs, in 2019 published the study, *A Throughput-Based Analysis of Army Active Component / Reserve Component Mix for Major Contingency Surge Operations.*[27] The focus of their research centered on efforts to "maximize the number of ready forces from the reserve components available to support such a conflict. . . as Operation Desert Shield / Desert Storm-like event."[28] The study provided an in-depth focus on mobilization throughput, findings, and implications for the reserve forces.[29] Figure 3 below outlines the key elements of the study and implications for the force. Against a near peer competitor, one could assume that the enemy would not allow U.S. forces six months to a year to stage equipment, conduct training, mobilize, and integrate

[27] Michael E. Linick et al., A Throughput Based Analysis of Active Army Component/Reserve Component Mix for Major Contingency Surge Operations (Santa Monica, CA: RAND Corporation, 2019), 1. https://www.rand.org/pubs/research_reports/RR1516.html.

[28] Linick,1. https://www.rand.org/pubs/research_reports/RR1516.html.

[29] Linick, 1. https://www.rand.org/pubs/research_reports/RR1516.html.

essential combat capabilities. The study's in-depth findings identify valuable considerations and potential challenges for consideration when requesting reserve component forces associated with the mobilization process and readying of forces in support of significant operations. The mobilization decision and training time associated with this process requires detailed consideration by Army leaders in order to make informed decisions concerning risk and readiness. Figure three below reflects some of the findings of the Rand Mobilization Modeling study.

Mobilization decision	• Early mobilization has the largest effect on ability to meet demand with RC inventory • Early mobilization required credible warning and/or a decision to preemptively mobilize at least some units; this will not always be feasible or politically viable • Early mobilization allows both training and facility ramp-up to begin earlier
MFGI capacity	• Within the range examined here (based on reasonable ranges specified by subject matter experts), increasing the speed at which mobilization facilities ramp up capacity has a smaller effect than early mobilization
Training time	• Policies that reduce time required for postmobilization training improve RC's ability to meet demands but may come with higher cost and/or risk (e.g., resourcing/sustaining higher levels of pre-mobilization readiness, improving training, or accepting increased risk) • RC BCTs and CABs can be trained in time to meet a sudden demand above and beyond already planned deployments only if training time is reduced and/or they are mobilized early
Unit sequencing	• If MFGI capacity remains limited, allocation of RC postmobilization training facilities must be prioritized • Large, complex RC units can sometimes clog the training pipeline • RC most efficiently provides small, quicker-to-train units • RC contribution could focus on units well suited to rapid deployment • RC will not be able to meet demands in the first few weeks, with few exceptions

SOURCE: RAND analysis of mobilization modeling results.

RAND *RR1516-4.1*

Figure 3. RAND Key Findings[30]

The MDO competition phase incorporates the first three phases of the Mobilization and Execution Process in figure 4 below. The timing of requests for forces can either reduce or enhance the readiness levels of the units. To ensure critical timeliness of actions, leaders must be fully engaged in the decisions inherent in the first three phases of this process. Manning, training, and equipment shortages will likely occur early in the process and lengthen the training time in Phase IV.

[30] Michael E. Linick et al., A Throughput Based Analysis of Active Army Component/Reserve Component Mix for Major Contingency Surge Operations (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR1516.html, pg. 58.

Mobilization and Execution Process

MOBLIZATION PHASE	PHASE I Pre-Mob	PHASE II Alert	PHASE III Home Station	PHASE IV Mobilization Station (MS)	PHASE V Alert
PRIMARY ACTIVITY LOCATION	Home Station (Armory or USAR Center)	Home Station (Armory or USAR Center)	Home Station (Armory or USAR Center)	MS	Air or Sea Port
ACTIVITY DURATION (DAYS)	As Time Permits	3 to 7 Days	3 Days	10 to 180 Days	1 to 2 Days
PRIMARY ACTIVITY	• Mobilization Planning • Training • SRP	• Unit Recall • Mobilization Order Prep • Personnel Screening • Equip & Records Check	• Continue SRP • Inventory Equipment • Cross-level Personnel & Equipment • Load for Movement • ADVON to MS	• Move to PPP • Complete SRP • Conduct Training • Complete Cross-level • Complete Validation • Load for Movement	• Move to POE • Load Transport • Deploy
OUTCOME	Planning	Notification	Preparation	Validation	Deployment

ADVON: Advance Echelon
USAR: United States Army Reserve
POE: Point of Embarkation
PPP: Power Projection Platforms
SRP: Soldier Readiness Processing

Figure 4. Mobilization and Execution Process[31]

The activity and duration of the events depicted in the first row of the chart at the "primary location activity" are depicted as planning locations but may occur at another location because mobilization relies on a decentralized execution process. Identifying training support requirements for the reserve component is the responsibility of Forces Command (FORSCOM). First Army, FORSCOM enables the readiness and training requirements of the reserve forces. First Army (East and West), have the responsibility

[31] Douglas E. Waters, "Army Mobilization and Deployment", in *How the Army Runs* (reference material, Department of Command, Leadership and Management, U.S. Army War College, Carlisle Barracks, PA, 2018).

to “assess training and ensure units are ready before they can deploy.”[32] First Army remains a multi-component organization that partners with the reserve units throughout the mobilization process and readiness cycle to assist with scheduling and training with the reserve forces. First Army’s commitment to its partnership with the reserve forces is evident by comments from the First Army Commanding General, LTG Thomas James, Jr. at National Guard Green Tab Conference in Little Rock, Arkansas where he stated: “Your success is our mission . . . we are in this together, and at First Army we are solely focused on helping you generate warfighters to ensure you complete your missions.”[33] This type of commitment to total force readiness through training will serve the Army well for years to come.

The current 12-month training period includes not only all five phases of the Mobilization and Execution Process outlined in Figure 4 above, but also contains the post-deployment and demobilization periods. *The National Commission on the Future of the Army (NCFA)* report identifies and recommends the following solution to the current 12-month mobilization period that impacts the boots on the ground (BOG) time for reserve forces: “Recommendation 31: The Secretary of Defense should update the January 19, 2007, memo ‘Utilization of the Total Force’ to allow flexible involuntary mobilization periods in an effort to achieve common BOG periods for all components.”[34]

---

[32] National Commission on the Future of the Army, Report to the President and the Congress of the United States, (Washington, DC, January 28, 2016), 78.

[33] Aaron Berogan. “First Army Strengthens Partnership With National Guard Leaders, “Targeted News Service; Washington, DC [Washington, D.C] (January 8, 2019): https://search.proquest.com/docview/2166087915?pq-origsite=summon&accountid=4444 accessed 25 JAN 2020

[34] National Commission on the Future of the Army, 67.

This recommendation by the NCFA would not only make the reserve and active component deployment timelines equal within the Army, but would also require additional and intensive legislative work from the senior leaders of our Army and our civilian leadership to support the change. Such a move, however, would involve multiple changes within the Title 10 and Title 32 of U.S. Code and would increase cost requirements for the Department of Defense. The U.S. Department of Defense should consider the recommendation by NCFA and pursue potential changes to the law governing the total force if the nation is to be successful in future great power competition.

Conclusion

The Secretary of Defense, Honorable Mark T. Esper stated: “There will always be that need to have heavy armored forces and infantry soldiers to do what they need to do, but now that we are fighting in multi-domain operations we need to have the ability to fight by air, ground, sea, space, and cyberspace.”[35] The adaption of Multi-Domain Operations across the Army places its forces on an azimuth to counter the changing threats in the operational environment and secure the nation’s future as a global power. Senior leader efforts like those of: Secretary of Defense Esper, General McConville, Chief of Staff of the Army, and LTG Wesley, Army Futures Command, shape how the U.S. Army will train and will fight as part of the great power competition with MDO forces from all compositions.

[35] “United States: Army Secretary Visits Indiana Guard Cyber-Training Complex.” MENA Report (JUL 25, 2018). https://search.proquest.com/docview/2075904230?accountid=4444.

The threat of LSGCO is ever-present from the near peer competitors, China and Russia. As a result, the requirement to train, and be prepared, to fight together with the active force continues to place demands on the reserve forces as part of the total army. Consequently, the Department of Defense, and specifically the Army, must capture training and modernization requirements associated with the changes in the operational environment. Some of the changes discussed involve dispersal requirements, active and reserve force structure, development of MDO doctrine, and MDO concept inclusion in the PME system of all components. These challenges will affect our readiness as an Army, especially in the current active duty forces, but the forces can share this burden, when given enough time and resources, to rebalance the force for MDO requirements.

The scholars, planners, and leaders of the Army should reevaluate the requirements of the total Army as a part of the MDO concept. The continuous improvements in technology and capabilities available to the soldier require near constant concept development and force structure assessments. The inclusion of multi-composition forces, generations of new formations within the reserve component, and changes in force structure will impact the AC/RC mix for the future. As stated in the 2015 National Defense Authorization Act:

> …. [A]n evaluation and identification of force generation policies for the Army with respect to size and force mixture in order to fulfill current and anticipated mission requirements for the Army in a manner consistent with available resources and anticipated future resources… *2015 NDAA, Section 1703(a)(2)(B)*[36]

[36] House of Representatives, (2015, May 1), Rules Committee Print 11-14 Text of H.R. 1735, National Defense Authorization Act for Fiscal Year 2016, Title V, Subtitle C – Consolidation of Authorities to Order Member of Reserve Components to Perform Duty. Washington, D.C., U.S. House of Representatives Rules Committee.

Determining the right force mix is critical to the success of the Army to prepare for LSGCO and cannot be achieved in the active component alone.

The reserve force SFABs must be augmented to provide the training and force preparations needed to maintain readiness. The current mobilization and execution process utilized by the reserve forces limits their contributions because of their lower resourcing and readiness levels. The Combatant Commanders cannot provide additional training time or resources to improve readiness levels of reserve forces upon arrival to theater. The training and oversight responsibility lies with First Army and FORSCOM. Prior to LSGCO, the reserve force must train and validate readiness or face irrelevancy as the conflict terminates before they can arrive in theater. Time is not a renewable commodity and therefore maximizing each training hour in the day is a requirement.

The Chief of the National Guard Bureau General Joseph L. Lengyel said it best:

> Thirty-nine days a year' is no longer the standard for much of the National Guard. Today's force expects to be deployed. Predictable and rotational mobilizations, where our service members can utilize their training, will help keep the force relevant, ready, and integrated with our active components.[37]

The MDO concept focuses on how U.S. forces will deter and defeat near-peer competitors and adversaries. The Army can reduce military risk and risk to the force through updated policies, statutes, pre-mobilization training regulations and requirements. This would create a revised mobilization and execution process. By expanding the available period the reserve forces can serve on active duty, while also

[37] 2020 National Guard Bureau Posture Statement, *Implementing the National Defense Strategy*, (Washington DC, Jan 2020), 4, https://www.nationalguard.mil/Features/Posture-Statement/.

providing additional training time, would provide a more potent force for the Combatant Commander. Additional training time provides post-mobilization opportunities for specific elements and units, deployment, redeployment, and reintegration for the reserve forces. Understanding the additional deployment time may place burdens on the soldiers and their families, but the additional time should reduce risk to mission failure.

The MDO concept focuses on how U.S. forces will deter and defeat near-peer competitors and adversaries. The U.S. should implement these recommendations during the competition phase below the levels of armed conflict. Setting the right conditions, building and training the force across the total Army with a focus on the AC/RC balance will maintain America’s position as the most lethal Army on the planet and change the face of future warfare.

This Page Intentionally Left Blank

Information Operations and Information Warfare: Is the United States Prepared?

by

Colonel Michael R. West, United States Army

Information operations have tremendous impacts on the ways in which political goals are attained around the world. State and non-state actors are "frequently using similar techniques to influence the public and achieve political goals once only attainable through armed conflict."[1] Adversaries are conducting information operations on a different level, with different rules, than the United States. Our adversaries are fighting a street fight with no rules. The United States is responding as if it were fighting in an officiated match with strict adherence to a set of rules that limits U.S. actions and effectiveness.

This paper is unclassified, which limits addressing some aspects of the United States information operations program. However, this paper will assess information operations and information warfare, as well as other terms for these same activities, from the United States perspective and the adversaries' perspectives identified in the 2018 National Defense Strategy. It will also provide: examples of information operations and information warfare executed by our adversaries; a history of United States information operation organizations; ways in which the United States has historically

[1] Timur Chabuk and Adam Jones, "Understanding Russian Influence Operations," *Signal Magazine*, September 1, 2018, https://www.afcea.org/content/understanding-russian-information-operations (Accessed February 23, 2020).

countered the activities of our adversaries; and, a conclusion with recommendations for the future inclusion in the Multi-Domain Operations (MDO) concept.

United States Information Operations and the Information Environment

The United States Department of Defense views information operations as a "purely military activity involving a set of tactics or capabilities."[2] The Secretary of Defense's statement describes information operations as the "integrated employment, during military operations, of information-related capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" decision making processes and timelines.[3] IRCs traverse and interact with sections of military deception operations (MILDEC), operational security (OPSEC), military information support operations (MISO), and intelligence through specialized and non-specialized operations.[4] IRCs also conduct operations associated within electronic warfare, cyberspace operations, and influence operations.[5] The Department of Defense will ensure that military efforts made within information operations are coordinated and

[2] U.S. Library of Congress, Congressional Research Service, *Defense Primer: Information Operations*, by Catherine A. Theohary, IL10771 (Updated December 18, 2018), 1, https://fas.org/sgp/crs/natsec/IF10771.pdf (Accessed February 21, 2020).

[3] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (Washington, DC: Joint Chiefs of Staff, November 27, 2012, Incorporating Change 1 November 20, 2014), ix, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (Accessed February 23, 2020).

[4] Department of Defense, *Information Operations (IO)*, DoD Directive 3600.01 (Washington, DC: Department of Defense, May 2, 2013), 1, https://fas.org/irp/doddir/dod/d3600_01.pdf (Accessed February 23, 2020).

[5] Department of Defense, *Information Operations (IO)*, 1.

synchronized with other United States Government (USG) agencies.[6] The Department of Defense's will also integrate and coordinate with partners and allies, when feasible during military operations.[7] Since 2016, global information operations focused on foreign individual actors, groups, or countries and conducted outside of military operations are coordinated through the Global Engagement Center.[8]

The information environment is considered the sum of "individuals, organizations, and systems that collect, process, disseminate, or act on information."[9] According to Joint Publication 3-12, cyberspace is "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data."[10] There are three dimensions to the United States version of the information environment. These dimensions (physical, informational, and cognitive) constantly interact with the individuals, organizations, and systems. The MDO concept relies on a similar principle of convergence of capabilities from across Service or agency boundaries, and dimensions, to achieve our national objectives.

The physical dimension comprises leaders and decision makers, command and control systems and procedures, and supporting infrastructure that facilitate individuals,

---

[6] Department of Defense, *Information Operations (IO)*, 2.

[7] Department of Defense, *Information Operations (IO)*, 2.

[8] Executive Order Number 13721, 3 C.F.R. 13721(March 14, 2016), https://regulations.justia.com/regulations/fedreg/2016/03/17/2016-06250.html (Accessed March 11, 2020).

[9] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-1.

[10] Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, June 8, 2012), GL-4, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (Accessed February 23, 2020).

groups, or entire organizations to produce results.[11] This is the dimension that includes platforms and the communications systems that link them.[12] The physical dimension is interconnected and crosses economic, national, political, and geographic boundaries.[13] The informational dimension is data-centered and concentrates on the "where and how information is collected, processed, stored, disseminated, and protected."[14] This dimension is where commanders execute command and control of their formations and is the bridge between the physical and cognitive dimensions.[15] The cognitive dimension focuses on the:

> Minds of those who transmit, receive, and respond to or act on information and how their individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies influence the individuals' or groups' information processing, perception, judgement, and decision making.[16]

These dimensions (physical, informational, and cognitive) constantly interact with the individuals, organizations, and systems and utilize many types of information operations to achieve their national objectives.

[11] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-2.

[12] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-2.

[13] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-2.

[14] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-2, I-3.

[15] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-3.

[16] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, I-3.

Types of Information Operations

Information operations involve multiple categories of information that are used to influence populations (friendly, enemy, or neutral). This influence can motivate, scare, threaten, confuse, agitate, and/or demoralize all or parts of targeted populations. The MDO concept similarly requires information operations and other capabilities to be coordinated to achieve national objectives. The three primary categories of information operations include propaganda, misinformation, and disinformation.

Propaganda is "an idea or narrative that is intended to influence" an individual, organization, or country (similar to psychological or influence operations).[17] Information in this category tends to exaggerate the message in favor of the organization producing it. This type of information, sometimes called public diplomacy, can include true, mostly true, mostly false, and/or totally false data.[18] When utilized by a government or organization over extended periods of time, propaganda speeches, posters, advertising, and/or print, television, and radio content can influence key persons, organizations, or the entire population to respond within planned or expected behaviors.[19]

[17] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* by Catherine A. Theohary, R45142 (Updated March 5, 2018), 5, https://crsreports.congress.gov/product/pdf/R/R45142/5 (Accessed February 23, 2020).

[18] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

[19] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

Misinformation is the “spreading of unintentionally false information.”[20] This type of operation can happen across various modes of media, such as newspapers, magazines, news programs on television or radio, social media sites, and through word of mouth. This type of information spreads as false information or narratives and can get included into the public sector through news outlets. Many organizations do not hold the same regard for the truth or requirement to verify a story prior to reporting on the information available. Many news sources have different priorities and agendas. Some organizations are driven by a profit motive and need to be first with the news, rather than be always right. Other organizations have an agenda to publicize, or may be state sponsored, and fear reprisals from the state for speaking out. Many other factors influence the local politics or news cycles around the globe. However, the many different stories or information sow “divisiveness and chaos in a target society, as the truth becomes harder to discern.”[21]

Disinformation, on the other hand, is the spreading of intentionally false information.[22] This is accomplished through the planting of “deliberately false news stories in the media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release.”[23]

---

[20] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

[21] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

[22] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

[23] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 5.

Disinformation can quickly turn into misinformation if it is not identified early and prevented from spreading to and through the uninformed. All of these methods can take place throughout the information environment and within each of the previously described dimensions.

Hostile Social Manipulation

Hostile social manipulation is another method of information operations. Hostile social manipulation employs "targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, distribution of rumors and conspiracy theories, and other tools and approaches to cause damage to the target state."[24] This method is a combination of many successful forms of influence used in the past, such as propaganda, the Russian active measures, misinformation, disinformation, and political warfare and is usually combined with other lines of operations for greater impact or effect.[25] Adversaries utilizing human social manipulation "do not seek to attack their opponents physically but merely to destabilize them" by attacking their populations' social, economic, and political beliefs with the hope that the population will not distinguish between the fake and real information.[26] The idea that information is a weapon is a strange concept within many democratic countries. In democratic countries, freedom of information and the ability for all to receive it are inherent and seen as an

[24] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, RR 2713 (Santa Monica, CA: RAND, 2019), 2, https://www.rand.org/pubs/research_reports/RR2713.html (Accessed February 23, 2020).

[25] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 2.

[26] Hannes Grassegger and Mikael Krogerus, "Weaken From Within," *The New Republic*, November 2, 2017, https://newrepublic.com/article/145413/weaken-within-moscow-honing-information-age-art-war-how-free-societies-protect-themselves (Accessed February 23, 2020).

absolute right.[27] We must remember that nation states and non-nation states like Russia, China, Iran, North Korea, and Violent Extremist Organizations (VEOs) will utilize elements of human social manipulation, cyberwar, and electronic warfare as part of an integrated campaign that takes place continuously during cooperation, competition, and conflict.[28]

4+1 Adversary Information Operations and Information Warfare

Nation states and terrorist organizations are increasing their utilization of information operations to attain strategic level goals and objectives. The focus of this section is how Russia, China, Iran, North Korea, and VEOs (often referred to as the 4+1) view information operations and information warfare as part of their overall strategic level strategies. Each of these individual national strategies have incorporated and improved upon the use of information operations as a part of information warfare over the past several decades, while the United States has focused on other strategic operations, primarily counter insurgency (COIN) in Iraq and Afghanistan. Each national strategy is also unique, however, they share the use of all means available to divide and weaken their adversaries with information warfare without conducting armed conflict. The rules they are applying are utilitarian to achieve their goals.

Russia

The Ministry of Foreign Affairs of the Russian Federation defines information warfare as war between "two or more States in the information space with the goal of inflicting damage to information systems as well as carrying out mass psychological

[27] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 5.

[28] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 18.

campaigns against the population of a State in order to destabilize society and the government."[29] General Valery V. Gerasimov, the Chief of the Russian General Staff, highlights in his speeches, interviews, and military discussions this definition of information warfare and the Russian perspective that boundaries do not exist between stability and conflict in modern society.[30] This concept allows Russia to use all elements of a nation's power to achieve their national objectives at any time and against any entity.

Information warfare has developed into an essential facet of the Russian military strategy and is continuous and unrelenting.[31] Russia utilizes "propaganda, misinformation, and deliberately misleading or corrupted disinformation" via social media. They conduct data breaches of foreign industrial, governmental, and non-governmental agencies, and manipulates publicly accessible information available on its own operations within and outside of its borders.[32] Russia uses information warfare to initiate internal uncertainty and disbelief and to "confuse, distract, polarize, and demoralize" individuals, groups, and societies around the globe.[33]

---

[29] The Ministry of Foreign Affairs of the Russian Federations, Convention on International Information Security, September 22, 2011, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (Accessed February 28, 2020).

[30] Andrew E. Kramer, "Russian General Pitches 'Information' Operations as a Form of War," *New York Times*, March 2, 2019, https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html (Accessed February 23, 2020).

[31] Sophia Porotsky, "Analyzing Russian Information Warfare and Influence Operations," *Global Security Review*, February 8, 2018, https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/ (Accessed February 23, 2020).

[32] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 9.

[33] Sophia Porotsky, "Analyzing Russian Information Warfare and Influence Operations."

China

China utilizes a philosophy of unrestricted warfare that "combines elements of information operations, cyberspace operations, irregular warfare, lawfare, and foreign relations" executed continuously in peacetime and while at war.[34] China combines several elements into its information warfare strategy. For example, they utilize cyberspace operations to attain information superiority by conducting surveillance operations and espionage.[35] They also control the availability and content displayed on the internet within their borders overall and specifically within territorial regions.[36] This limits external global influence within the country, and enables the segregation of national information. Additionally, on a global scale, China influences intellectual think-tanks and academia around the world by providing funding with stipulations that research may not portray China negatively.[37]

China's use and understanding of historical concepts regarding the execution of modern-day warfare also pertain to information operations, information warfare, and the use of cyberspace. For example, they rely on the chronicled teachings from Sun Tzu's *Art of War* and their understanding of the *36 Stratagems*. These stratagems support the current Chinese strategy within information warfare that focuses on distracting, lying to,

[34] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 11.

[35] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 11.

[36] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 12.

[37] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 11-12.

and dominating the enemy.[38] Three particular stratagems relate to information operations:

1. "Besiege Wei to rescue Zhao" (don't attack a strong enemy directly, attack something the enemy holds dear and make them re-orient efforts to address multiple situations)[39]
2. "Replace the beams with rotten timbers" (change the way the enemy is used to operating and remove their support structure)[40]
3. "Let the enemy's spy sow discord in the enemy camp" (utilize the enemy's own spies against them and put your influence amongst the enemy)[41]

Each of these stratagems focus on the ability to impact an enemy's capability for cognition and to influence the substance, method, and focus of thinking of an enemy.[42]

North Korea

Since 1949, North Korea has conducted information warfare operations to promote its internal, regional, and global interests.[43] Currently, the dominant mode

[38] Davia Temin, "Ancient Wisdom for the New Year: The 36 Chinese Stratagems For Psychological Warfare," *Forbes*, January 2, 2017, https://www.forbes.com/sites/daviatemin/2017/01/02/ancient-wisdom-for-the-new-year-the-36-chinese-stratagems-for-psychological-warfare-in-business-politics-war/#5f9c664b2779 (Accessed February 29, 2020).

[39] Davia Temin, "Ancient Wisdom for the New Year: The 36 Chinese Stratagems For Psychological Warfare."

[40] Davia Temin, "Ancient Wisdom For The New Year: The 36 Chinese Stratagems For Psychological Warfare."

[41] Davia Temin, "Ancient Wisdom For The New Year: The 36 Chinese Stratagems For Psychological Warfare."

[42] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 11.

[43] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 13.

through which North Korea conducts information operations is cyber warfare. North Korea's focus is utilizing its "high capacity to conduct robust cyber operations aimed at collecting foreign intelligence, disrupting foreign computers, information and communication systems, networks and critical infrastructures, and stirring public discontent and disorder in the enemy state."[44] North Korea's current capability and capacity in cyber warfare has reached levels that threaten some of the world's preeminent, technologically advanced countries.[45] Examples of North Korean hostile cyber warfare activity includes stealing from foreign governmental and private sectors, outright destruction or damage to websites, and denial of service operations.[46] Other North Korean information operations include public relations messaging and campaigns to better position and improve the country's stance internationally.[47]

Iran

Iran utilizes information operations within its borders and abroad to further strategic objectives. Internally, while the country and its population have vastly improved access to the internet and other social media platforms, the government has also extended its control through censorship, monitoring, and manipulating access.[48]

---

[44] Alexandre Mansourov, Dr., Korea Economic Institute of America, *Academic Paper Series*, December 2, 2014,1, http://keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf (Accessed February 27, 2020).

[45] Alexandre Mansourov, Dr., *Academic Paper Series*, 1.

[46] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 14.

[47] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 14-15.

[48] Center for Human Rights in Iran, *Guards at the Gate: The Expanding State Control Over the Internet in Iran*, January 2018, 7, https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf (Accessed February 27, 2020).

Governmental control of the internet and social media is used to "target and discredit dissenters and adversaries" and in "limiting or prohibiting attempts by protesters to coordinate and organize."[49] This strategy is completed through intentionally slowing down or disrupting internet access and shutting down social media platforms within the country.[50] Iranian information operations capability and capacity has also increased within the global arena. Cyberattacks and cyber intrusion operations against foreign states are linked with information operations on social media platforms, providing a consolidated campaign across multiple domains to further Iranian objectives.[51]

Violent Extremist Organizations

Violent Extremist Organizations employ information operations similarly to nation-states. VEOs use information operations internally through "chat rooms, dedicated servers, websites, and social networking tools as propaganda machines, as a means of recruitment and organization, for training grounds, and for significant fund-raising through cybercrime."[52] Externally, VEOs conduct operations to create perceptions of weakness and vulnerability of enemy states. Examples of these operations include e-mail bombing of ideological enemies, data theft, denial of service attacks, defacement

[49] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 15.

[50] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 15.

[51] Jessica Guynn, "Facebook Information Warfare: Inside Iran's Shadowy Operations to Target You on Social Media," *USA Today*, January 11, 2020, https://www.usatoday.com/story/tech/2020/01/10/iran-influence-operations-target-americans-after-soleimani-killing/4422491002/ (Accessed February 29, 2020)

[52] U.S. Library of Congress, Congressional Research Service, *Terrorist Use of the Internet: Information Operations in Cyberspace,* by Catherine A. Theohary and John Rollins, R41674 (March 8, 2011), 5, https://fas.org/sgp/crs/terror/R41674.pdf (Accessed February 24, 2020).

and disabling of websites, and data breaches.[53] The intent of such activities include: "loss of integrity" (information is adjusted and no longer trustworthy), "loss of availability" (systems or information is no longer accessible by those in need), "loss of confidentiality" (essential information may be in the hands of the enemy), and "physical destruction" (use of imbedded commands to deliberately damage program capabilities or system functionality).[54] All of these strategies are designed to demonstrate capabilities and exert power over local and world-wide adversaries. They aim to use information to create or exploit vulnerabilities without the restrictions applied by the western media. The obstacles to entry to compete in the information realm are far less than competing militarily with international superpowers. Hence, Information warfare is an especially attractive means to compete with more powerful adversaries.

Near-Peer Adversary & VEO Usage Information Operations and Information Warfare

All members of the 4+1 utilize a version of information operations as part of a larger information warfare strategy. They do not apply the same terminology or techniques for their actions, but they attempt to utilize operations short of armed conflict to achieve their desired objectives. This is how information operations and information warfare are transitioning a key aspect of the modern battlefield into everyday life.

Russia

To understand the Russian Federation's use of information operations as part of information warfare, it is important to understand the efforts established and developed

[53] U.S. Library of Congress, Congressional Research Service, *Terrorist Use of the Internet: Information Operations in Cyberspace,* 4-5.

[54] U.S. Library of Congress, Congressional Research Service, *Terrorist Use of the Internet: Information Operations in Cyberspace,* 5.

by its predecessor, the Union of Soviet Socialist Republic (USSR). Starting as early as 1917, with the overthrow of the Tsarist regime, the new ruling power conducted its own "internal and external social manipulation efforts," consisting of propaganda designed to "discredit domestic and foreign adversaries and to foster support for the Communist ideology."[55] Internal to the Soviet Union, stringent censorship became the standard for all forms of media. The creation of the Komitet Gosudarstvennoy Bezopasnoti (KGB) in the 1950s drastically improved foreign Soviet social manipulation efforts through "expansion, institutionalization, and professionalization."[56] The importance of social manipulation as a means to assist in achieving strategic objectives continued to rise throughout the 1960s and 1970s within the Soviet government.[57] In the 1980s, the Soviets executed two notorious information operations against the United States. Operation Infektion was a disinformation campaign to "make people believe that the human immunodeficiency virus and acquired immunodeficiency below the level of syndrome (HIV/AIDS) was a result of American biological weapons experiments."[58] This operation was an example of the Soviet Union skillfully manipulating existing global stories, as an active misinformation campaign already existed and may have enabled easier public acceptance of these additional products.[59] Another 1980s era event

[55] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 33.

[56] Max Holland, "The Propagation of Power of Communist Security Services Dezinformatsiya," *International Journal of Intelligence and Counterintelligence*, vol. 19, no. 1 (Spring 2006): 5, https://www.tandfonline.com/doi/abs/10.1080/08850600500332342 (Accessed March 24, 2020).

[57] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 34-35.

[58] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 26.

[59] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 26.

involved the 1984 Olympic Games in Los Angeles, CA. The KGB sent "forged racist letters threatening Olympic athletes from 20 Asian and African nations in the name of the Ku Klux Klan" in an attempt to cause political and social discontent.[60] This instance coincided with the Soviet boycott of the Olympic Games that same year and was an attempt to devalue the Olympic spirit and meaning.

Russia currently employs decades worth of knowledge, experience, and expertise in information warfare across all means of communication and social media.[61] These operations include the use of cyber hacking groups that may or may not operate from within the country.[62] It is very difficult to confirm who comprises these groups, where they are working from, or who they are working for. The Russian's also utilize honeypots, which are fake or falsified social media profiles, to gain acceptance or trust of social media users.[63] Through this acceptance and trust, the Russian's spread propaganda, misinformation and disinformation, entrap people in unethical behavior, or gain access to systems through malicious code or malware.[64] Trolls and troll farms are another common Russian information warfare method. Trolls and troll farms, individuals and groups, are utilized to permeate social networking platforms with so much propaganda, misinformation, and disinformation that it becomes extremely difficult to

[60] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 25.

[61] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters," *Global Security Review*, January 11, 2018, https://globalsecurityreview.com/russia-manipulation-u-s-voters-social-media/ (Accessed February 23, 2020).

[62] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters."

[63] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters."

[64] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters."

identify fact from fiction.[65] This causes uncertainty and unrest within the target audience.[66]

Russia has increased the use of automated agents, called bots, to operate on social media platforms to create and distribute more content than is humanly possible.[67] Examples of these human and automated efforts include Russian intervention in the 2017 Catalan separation crisis in Spain, election interference throughout Europe, and election manipulation within the United States.[68] In January 2018, Twitter announced that it had identified over 50,000 Russian linked bots employed to influence the 2016 presidential election within the United States.[69] Content produced by these bots was directly followed, retweeted, or liked by 677,775 people and is assumed to have impacted perceptions.[70] Of note, that number does not include those that only saw the content through viewing other people's feeds.[71]

[65] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters."

[66] Sophia Porotsky, "Facebook, Compromised: How Russia Manipulated U.S. Voters."

[67] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 86.

[68] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 3-4.

[69] April Glaser, Slate, "Twitter Admits There Were More Than 50,000 Russian Bots Trying to Confuse American Voters Before the Election," January 19, 2018, https://slate.com/technology/2018/01/twitter-admits-there-were-more-than-50-000-russian-bots-confusing-u-s-voters-in-2016.html (Accessed March 19, 2020)

[70] April Glaser, Slate, "Twitter Admits There Were More Than 50,000 Russian Bots Trying to Confuse American Voters Before the Election."

[71] April Glaser, Slate, "Twitter Admits There Were More Than 50,000 Russian Bots Trying to Confuse American Voters Before the Election."

Russia also utilizes information operations to inflame existing social tensions within foreign nations to erode faith and trust in private and governmental institutions.[72] Within the United States, Russia emphasized and attempted to stretch the divide between the "Black Lives Matter" and the "Blue Lives Matter" movements through the use of social manipulation on Facebook by flooding the social media platform with pro and con messaging for both movements.[73] Within Spain, Russian and Venezuelan accounts swamped social media platforms with a pro-independence narrative in support of the 2017 Catalan separatist movement.[74]

China

China, like Russia, executes information operations within and outside its borders. Internally, China employs a rigorous combination of legal policies and the use of advanced information technology for censorship, monitoring, and tracking of malcontents who do not support the Chinese narrative.[75] China also segregates the availability and authorized content on the internet within the country by regions in an effort to maintain stability.[76] Externally, China is conducting information operations on multiple levels. China attempts to influence worldwide perception through public

[72] Timur Chabuk and Adam Jones, "Understanding Russian Influence Operations," *Signal* Magazine, September 1, 2018, https://www.afcea.org/content/understanding-russian-information-operations (Accessed February 23, 2020).

[73] Timur Chabuk and Adam Jones, "Understanding Russian Influence Operations."

[74] Michael J. Mazarr et al., Hostile Social Manipulation: Present Realities and Emerging Trends, 4.

[75] Simon Denyer, "China's Scary Lesson to the World: Internet Censorship Works," *Washington Post*, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.49ae25e59cbb (Accessed March 4, 2020).

[76] Rory Cellan-Jones, "China Internet: Xi Jinping Calls for 'Cyber Sovereignty,'" *BBC News*, December 16, 2015, https://www.bbc.com/news/world-asia-china-35109453 (Accessed March 4, 2020).

pronouncements of their peaceful pursuits of internal development and prosperity, and denying increased desire and effort toward international power and expansion.[77] This is an example of one of the methods China employs as part of a more robust national strategy to encourage contentment in current and potential adversaries.[78] Specifically, towards the United States, China has executed cyber related information operations to include computer network espionage, in an attempt to gain a competitive advantage.[79]

Two aviation related instances involve the United States F-35 Joint Strike Fighter and the C-17 military transport aircraft. In 2009, China is believed to have stolen F-35 design data from Lockheed Martin's computer network and those data-related aspects now appear on the Chinese J-31 fighter.[80] In 2016, a Chinese national living and working in the United States was arrested as part of a Chinese plot to steal military data related to military aircraft and capabilities in 2014.[81]

Additionally, China is conducting information operations with academia. China sponsors think tanks and Confucius Institutes, Chinese funded language, ethnic, and social centers, in over 100 colleges, universities and research institutes across America

---

[77] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 12.

[78] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 12.

[79] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 11.

[80] Marcus Weisgerber, "China's Copycat Jet Raises Questions About F-35," *Defense One*, September 23, 2015, https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859 (Accessed March 23, 2020).

[81] Department of Justice, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," March 23, 2016, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive (Accessed February 23, 2020).

and provides “strings-attached” funding to “deter research that casts…negative light” on China and Chinese activities.[82] China also strictly manages entry of academics into their country. Visas are frequently denied to academics that disparage the government or ongoing activities within the country, causing researchers to cautiously monitor and selectively publish findings and products to retain admittance into the country.[83]

North Korea

North Korea’s utilization of information operations and cyber warfare as part of its overall information warfare strategy focuses internally, regionally and globally. Internally, the regime controls all forms of media and has outlawed access to foreign material.[84] It strictly limits access of the internet and all activity is closely scrutinized.[85] The regime also severely restricts and monitors the limited tourist interaction with the populace.[86] Regionally, North Korea focuses manipulation efforts on building supportive followers in South Korea and Japan in attempts to sway South Korean and Japanese policies within the region.[87] In a more aggressive globally expansive manner, North Korea conducts cyber warfare attacks designed to steal from, damage, or manipulate governmental and

[82] Natalie Johnson, “CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions,” *The Washington Free Beacon*, March 7, 2018, https://freebeacon.com/national-security/cia-warns-extensive-chinese-operation-infiltrate-american-institutions (Accessed February 23, 2020).

[83] Natalie Johnson, “CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions.”

[84] Vishakha Sonawane, “Why is North Korea so Isolated? A Brief History of the Reclusive Country,” *International Business Times*, June 10, 2017, https://www.ibtimes.com/why-north-korea-so-isolated-brief-history-reclusive-country-2549981 (Accessed March 6, 2020).

[85] Vishakha Sonawane, “Why is North Korea so Isolated? A Brief History of the Reclusive Country.”

[86] Vishakha Sonawane, “Why is North Korea so Isolated? A Brief History of the Reclusive Country.”

[87] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 13.

private company websites, as well as denial of service attacks.[88] In 2014, The Federal Bureau of Investigation (FBI) concluded a cyber-attack against Sony Pictures Entertainment (SPE), that caused destruction of information systems and involved the theft of personal and commercial data, was sponsored by the North Korean government in an attempt to prevent SPE from releasing *The Interview*.[89] North Korea also utilizes global information campaigns designed to control international relations and establish advantages in negotiations with South Korea (peninsula centric) and the United States (nuclear).[90] Since 2012, North Korea and Iran have maintained a technology sharing treaty that focuses on cyber activities, to include tactics, techniques, and procedures.[91]

Iran

Iran executes information operations and cyber-attacks within a foreign (global) and domestic (internal) information warfare strategy. Globally, since 2017, primary social media enterprises (Facebook, Twitter, Instagram, etc.) have removed tens of thousands of fraudulent profiles, pages, organizations, and feeds connected with Iran and Russia alone.[92] Iran has focused foreign information operations into Asian,

[88] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 14.

[89] FBI National Press Office, "Update on Sony Investigation," December 19, 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (Accessed Mar 6, 2020).

[90] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 14-15.

[91] Claudia Rosett, "North Korea and Iran: Partners in Cyber Warfare?," Forbes, December 12, 2014, https://www.forbes.com/sites/claudiarosett/2014/12/12/north-korea-and-iran-partners-in-cyber-warfare/#21b0cd4859aa (Accessed March 05, 2020).

[92] Dorara Barojan, "Eight Takeaways From Iranian Information Operations," *Signal Magazine*, April 1, 2019, https://www.afcea.org/content/eight-takeaways-iranian-information-operations (Accessed March 6, 2020).

European, and North and South American countries to achieve political objectives and to discredit and manipulate foreign governments and populations.[93] Iran is more likely to utilize existing content and re-brand it as their own, which assists in smooth insertion into social media platforms and allows for quicker and more active engagement with target populations.[94] Additionally, Iran has utilized cyber-attacks against foreign countries. Specifically related to the United States, seven Iranians were indicted on charges for conducting a "coordinated cyber assault" against 46 banks and financial establishments from 2011 through 2013 and attempting to gain control of a dam in New York.[95]

While Iran does appear to have a global reach in information warfare, a significant amount of Iranian information operations is focused within its own country and used to control the population. In an effort to reduce coordination capabilities by internal malcontents, the Iranian government turned off access to social media platforms and interrupted internet connectivity in response to nationwide protests in 2018.[96] This activity highlighted the capability and capacity possessed within the country's information warfare division, and the extent to which the country was willing to go to maintain control over the population.

---

[93] Dorara Barojan, "Eight Takeaways From Iranian Information Operations."

[94] Dorara Barojan, "Eight Takeaways From Iranian Information Operations."

[95] Joseph Marks, "Indictment: Iranians Made 'Coordinated' Cyberattacks on U.S. Banks, Dam," *Politico Magazine*, March 24, 2016, https://www.politico.com/story/2016/03/us-indicts-iranians-in-cyber-attacks-on-dam-221196 (Accessed March 6, 2020).

[96] Cristina Maza, "Iran Protests: Government Took Control of the Internet to Silence Dissent, Report Says," *Newsweek*, January 10, 2018, https://www.newsweek.com/iran-protests-government-control-internet-dissent-776318 (Accessed March 19, 2020).

Violent Extremist Organizations

Violent Extremist Organizations conduct information operations over vast distances through access to various social media platforms around the world. Al Qaeda's utilization of social media includes the distribution of extremist ideological sermons, calls for action, attempts at radicalization of followers, and jihad.[97] An example of an offensive information operation against the United States was conducted by the Islamic State of Iraq and Syria (ISIS) in 2014. The Federal Bureau of Investigation and the Department of Homeland Security released a joint statement to United States military personnel concerning suspected ISIS social media data mining efforts in an attempt to gain sensitive, personal information on service members for future target lists and detection of possible followers for recruitment and indoctrination.[98] Other operations include taking control of Department of State and Department of Defense websites and rerouting normal operations to unwanted sites as a way to demonstrate superiority.[99] Internally, the VEOs use social media and information operations to conduct daily business, produce propaganda videos and messages for members, to aid in recruitment, and raise funds to keep the organization active, effective, and relevant.[100]

[97] U.S. Library of Congress, Congressional Research Service, *Terrorist Use of the Internet: Information Operations in Cyberspace,* 3.

[98] Brian Ross and James Meek, "ISIS Threat at Home: FBI Warns US Military About Social Media Vulnerabilities," *ABC News*, December 1, 2014, https://abcnews.go.com/International/isis-threat-home-fbi-warns-us-military-social/story?id=27270662 (Accessed March 23, 2020).

[99] U.S. Library of Congress, Congressional Research Service, *Information Warfare: Issues for Congress,* 13.

[100] U.S. Library of Congress, Congressional Research Service, *Terrorist Use of the Internet: Information Operations in Cyberspace,* 3-4.

United States Information Operations Organizations and Use

In an attempt to retain the gains made prior to the end of World War II in information operations, the United States Congress recognized the need for continued coordination and communication with foreign populations on a more permanent basis, during peacetime, and possible future war.[101] In 1953, the United States Information Agency was established, becoming an independent agency with the mandate to provide American public diplomacy (information operations).[102] The United States Information Agency's primary mission and focus became the Cold War and at its zenith of operations, it managed all United States governmental communications with over 150 international organizations and countries.[103] These efforts focused on countering Soviet disinformation about the United States, and expanding foreign understanding of United States' values, beliefs, national interests, policies, and citizens.[104] However, the United States Information Agency had a "de facto ban" against sharing any type of governmentally developed propaganda within the United States.[105] This ban was modified and updated several times over the years to emphasize the restrictions on domestic distribution. The Zorinsky or 1985 Amendment to the Smith-Mundt Act marked

[101] William M. Chodkowski, "Fact Sheet, The United States Information Agency," *American Security Project*, November 2012, 2, https://www.americansecurityproject.org/ASP%20Reports/Ref%200097%20-%20The%20United%20States%20Information%20Agency.pdf (Accessed March 9, 2020).

[102] William M. Chodkowski, "Fact Sheet, The United States Information Agency," 1.

[103] William M. Chodkowski, "Fact Sheet, The United States Information Agency," 1.

[104] William M. Chodkowski, "Fact Sheet, The United States Information Agency," 2.

[105] Weston R. Sager, "Apple Pie Propaganda? The Smith-Mundt Act Before and After the Repeal of the Domestic Dissemination Ban," (Northwestern University Law Review, vol. 109, no 2, 2015), 519, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1203&context=nulr (Accessed March 10, 2020).

the peak of restrictions on domestic distribution.[106] Over the next several years, restrictions on the availability of products produced by the United States Information Agency to the civilian population of America did increase, but the agency was abolished in 1999.[107]

Another organization established during the Cold War to specifically target Soviet disinformation operations around the world, especially those against the United States, was the Active Measures Working Group. President Reagan identified the necessity for the United States Government to stop pandering to the Soviet Union in the name of maintaining positive relations and to take an offensive approach to fight Soviet lies with American truth.[108] The Active Measures Working Group was established in 1981 as an interagency entity that included elements from the State Department, Department of Defense, Defense Intelligence Agency, Central Intelligence Agency, Department of Justice, Federal Bureau of Investigations, United States Information Agency, and the Arms, Control and Disarmament Agency.[109] The focus of the Active Measures Working

[106] Weston R. Sager, "Apple Pie Propaganda? The Smith-Mundt Act Before and After the Repeal of the Domestic Dissemination Ban," 524.

[107] William M. Chodkowski, "Fact Sheet, The United States Information Agency," 4.

[108] Katharine Cornell Gorka, "Re-engaging in the War of Ideas: Lessons from the Active Measures Working Group," (Westminster Institute, February 1, 2013) https://westminster-institute.org/articles/re-engaging-in-the-war-of-ideas-lessons-from-the-active-measures-working-group/ (Accessed March 10, 2020).

[109] Michael Dhunjishah, "Countering Propaganda and Disinformation: Bring Back the Active Measures Working Group?," War Room, United States War College, July 7, 2017, https://warroom.armywarcollege.edu/articles/countering-propaganda-disinformation-bring-back-active-measures-working-group/ (Accessed March 10, 2020)

Group was to "identify and expose Soviet disinformation" through the combined effort of all member organizations to expose lies and not ideology.[110]

Two key Soviet disinformation campaigns (mentioned in more detail previously in the section on Russian information operations) were debunked by the working group. First, the Soviet AIDS campaign that insisted the United States had developed the AIDS virus for use as a military weapon and actually utilized it in Africa.[111] Second, the KGB attempted to manufacture an international incident on the eve of the 1984 Olympic Games, being held in Los Angeles, by sending forged letters to African countries containing threatening language from the Ku Klux Klan.[112] The Active Measures Working Group utilized an approach that focused on accurate reporting, combined analyzation, and publicized results in unclassified documents to national and international media sources.[113] With the collapse of the Soviet Union, the Active Measures Working Group was destined to follow suit and was eliminated from the government structure in 1992.[114] However, in its' final report, the Active Measures Working Group warned of the potential for continued and newly developed active

[110] Michael Dhunjishah, "Countering Propaganda and Disinformation: Bring Back the Active Measures Working Group?."

[111] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," Institute for National Strategic Studies, National Defense University, June 2012, 6, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf (Accessed March 10, 2020)

[112] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 52-53.

[113] Michael Dhunjishah, "Countering Propaganda and Disinformation: Bring Back the Active Measures Working Group?."

[114] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 96.

measures by other anti-American countries and organizations.[115] They emphasized the need for an agency to remain in action to watch and examine activities, evaluate the implications, and thwart threats before they have lasting effects against the United States.[116]

In an effort to counter the ideologies and information operations of terrorist organizations and other violent extremists, President Obama established the Center for Strategic Counterterrorism Communications with Executive Order 13584.[117] This organization focused efforts to "coordinate, orient, and inform Government-wide public communications activities directed at audiences abroad and targeted against violent extremists and terrorist organizations."[118] The Center for Strategic Counterterrorism Communications almost immediately faced challenges from within the United States Government. Operations and products coming out of the organization appeared more like United States propaganda, as most content was openly identifiable as a product of the State Department.[119] This was highlighted in a United States Government produced anti-extremism video in 2015. The video, utilizing horrendous Islamic State propaganda

[115] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 96.

[116] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 96.

[117] Executive Order Number 13584, 3 C.F.R. 13584 (September 9, 2011), https://obamawhitehouse.archives.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c (Accessed March 10, 2020)

[118] Executive Order Number 13584.

[119] Guy Taylor, "State Department Global Engagement Center Targets Russian Propaganda, 'deep fakes,'" *The Washington Times*, December 12, 2018, https://apnews.com/9f7892a163582b5fd0297e2a81124c35 (Accessed March 9, 2020)

footage, went viral, and was believed to have unintentionally provided a boost to jihadist activities.[120]

In 2016, President Obama shut down the Center for Strategic Counterterrorism Communications and established the Global Engagement Center through Executive Order 13721.[121] The initial mandate for the Global Engagement Center emphasized an updated governmental strategy in which it would "lead the coordination, integration, and synchronization of Government-wide communications activities directed at foreign audiences abroad" targeted to "counter the messaging and diminish the influence of international terrorist organizations" and other violent extremists.[122] The Center concentrated on increasing partnership within a global system to employ local voices as delivery methods, and utilized data analytics to better understand the online methods used by terrorist organizations to recruit and radicalize vulnerable audiences.[123] It also developed partner and independent content to jointly message the anti-terrorism theme with cohort counter terrorism nations and partners, and through vigilant liaison within the United States Government, ensured coordination, cooperation, common understanding, and synchronization of interagency efforts.[124] In the early stages of President Trump's administration, drastic budget cuts throughout the government impacted operations, to

[120] Guy Taylor, "State Department Global Engagement Center Targets Russian Propaganda, 'deep fakes.'"

[121] Executive Order Number 13721.

[122] Executive Order Number 13721.

[123] United States Department of State, Archived Content (January 20, 2009 – January 20, 2017), "Global Engagement Center," https://2009-2017.state.gov/r/gec//index.htm (Accessed March 10, 2020)

[124] United States Department of State, "Global Engagement Center."

include those of the Global Engagement Center.[125] However, by 2018 additional mandates to the Global Engagement Center included countering the disinformation and propaganda of global actors, including Russia, China, and Iran.[126]

Conclusion and Recommendations

Information operations have existed as a part of warfare for centuries. The differences today from hundreds of years ago are the methods of dissemination and the speed at which disinformation, misinformation, propaganda, and cyber-attacks can reach intended audiences.[127] Additionally, due to the impact and effect information operations have towards strategic and political objectives, countries and organizations do not need to possess large military forces to fight high intensity conflicts. They can utilize specialized cyber warriors to execute operations below the level of armed conflict with surprising success.[128]

This paper identified some of the issues that impact the United States' efforts within information operations and information warfare. There is not a common understanding or set of universal definitions for all aspects involved in information operations or information warfare (internal to the United States Government or within the international system). Current United States governmental regulations restrict efforts to counter foreign information operations and their impacts on United States allies,

[125] Guy Taylor, "State Department Global Engagement Center Targets Russian Propaganda, 'deep fakes.'"

[126] Guy Taylor, "State Department Global Engagement Center Targets Russian Propaganda, 'deep fakes.'"

[127] Dorara Barojan, "Eight Takeaways From Iranian Information Operations."

[128] Dorara Barojan, "Eight Takeaways From Iranian Information Operations."

partners, and the United States population. Within the United States Government, continued improvement of operation, execution, and coordination is required as well as that with our allies and partners abroad during all stages of the conflict continuum (cooperation, competition, and conflict).

The United States Government must continue to emphasize the need for multinational interoperability and unity of effort between allies, partners, and trusted organizations. Key to this endeavor is information and technology sharing and partnership across all levels of information operations. This will include sharing and collaborating on tactics, techniques, and procedures to identify, analyze, and react to adversarial information operations across all forms of media (Facebook, Twitter, Tik Tok, other internet web pages and blogs, and print, radio, and television outlets). Likewise, it will require the same unity of effort against cyber activities designed to harass, deny services, manipulate site content, and steal data. We must work together as an international community to identify common terminology, pool resources and expertise, and develop capabilities and capacities to defeat our adversaries within the information operations realm during peacetime and while in conflict.

The current United States governmental lead agency for information operations is the Global Engagement Center. The center must improve upon its existing structure. In order for an interagency group to work effectively and produce on the national and global level. The center must have continued support from senior leaders from within all involved agencies, appropriate congressional oversite, and support to the operations

and organizations, and the required funding.[129] Information sharing across all agencies must become streamlined and integrated, as current threats are not being identified until after their desired affects are achieved. This is due to stove-piped reporting chains and lack of common understanding among and across all agencies. This situation requires legislative options to reduce current legal bottlenecks and restrictions that impact the actions of United States Governmental Agencies within the homeland and abroad. As stated in the Summary of the 2018 National Defense Strategy, the "homeland is no longer a sanctuary."[130] Our adversaries have foreign and domestic representatives operating within and outside our borders that must be addressed by a whole-of-government approach.

Even a whole of government approach may be insufficient when the individual user remains the weakest link in the chain that can be targeted and exploited by our adversaries. The ubiquitous presence of cell phones in society provides a means to enter other networks and exploit freedom of expression in the western world. Extremist views continue to divide societies and paralyze efforts to achieve a common goal through political action in a democracy. Discord becomes the political narrative and limits moderate efforts to achieve a greater good. Adversaries benefit from continued discord and information warfare provides the means to reinforce positions that create obstacles to unity of effort. Governments that continue to adhere to western rules of

[129] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," 107.

[130] Jim Mattis, Summary of the 2018 National Defense Strategy of The United States of America (Washington, DC: U.S. Department of Defense, January 2018), 3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (Accessed February 10, 2020).

conduct are being exploited by the 4+1 adversaries as they continue to steal our research and development. In essence, we are transferring wealth from the west to the east while we remain divided and vulnerable.

While this topic will continue to develop and require additional study, a final improvement needed within information operations internal to the United States requires improved relations between governmental agencies and domestic media. Current tensions between these entities cause mistrust and misunderstanding amongst the American population. Further, the assets best suited to counter information warfare maybe the commercial sector experts that have designed the internet service and associated software. Combining this situation with the efforts of our adversaries, it is becoming more and more difficult for the average person to discern fact from fiction. Our adversaries take full advantage of this vulnerability. People cite information posted on social media sites (Facebook, Twitter, Tik Tok, etc.) as if it was reported by the national media outlets or from a reputable print media source. Trust and confidence must be re-established between the media and the government for a combined effort to counter our adversaries' information operation campaigns.

In summary, this paper has shown many of the vulnerabilities the U.S. needs to address in order to be able to win in a 'street fight' operating environment that has evolved beyond U.S. capacity to control. General George S. Patton once said, "Successful generals make plans to fit circumstances, but do not try to create circumstances to fit plans."[131] The U.S. must make plans to fit the circumstances of the changing operating environment or expect the adversary will continue to exploit the

[131] George S. Patton Jr. https://quotefancy.com/quote/815542/George-S-Patton-Jr-Successful-generals-make-plans-to-fit-circumstances-but-do-not-try-to (Accessed April 14, 2020).

vulnerabilities that help achieve their national objectives at the continued expense of the U.S. and western world. One cannot expect the circumstances to change to match our plans.

Please send any comments or suggestions to

gregory.l.cantwell.civ@mail.mil

Gregory L. Cantwell

Center for Strategic Leadership

US Army War College

650 Wright Avenue

Carlisle Barracks, Pennsylvania 17013

THEATER ARMY ROLE IN MULTI-DOMAIN OPERATIONS INTEGRATED RESEARCH PROJECT

The Multi-Domain Operations (MDO) Concept aligns modernization efforts with future capabilities to provide a force structure that will be able to defeat a near peer competitor in large scale combat operations by the year 2035. The US Army War College study highlights student research on some of the challenges to the joint force of conducting MDO. It also presents some recommendations about future readiness for further consideration.

Gregory L. Cantwell, Ph.D.

Faculty Lead and Editor
Director, Joint Force Land Component Commander Course

STUDENTS

Darren Buss	**Colonel**	**U.S. Army**
Dan Harris	**Colonel**	**U.S. Air Force**
Michael Hays	**Lieutenant Colonel**	**U.S. Marine Corps**
Eric Jacobson	**Lieutenant Colonel**	**U.S. Army**
Brian Newill	**Lieutenant Colonel**	**U.S. Army**
Shawn Underwood	**Colonel**	**U.S. Army**
Michael West	**Colonel**	**U.S. Army**

UNITED STATES ARMY WAR COLLEGE CLASS OF 2020