NEWSLETTER

19-03

DEC 2018

MULTINATIONAL JOINT FORCIBLE ENTRY OPERATIONS BLUE FLAG/ JOINT WARFIGHTING ASSESSMENT 2018

BLUE FLAG | JOINT WARFIGHTING ASSESSMENT

Multinational
Joint Forcible Entry Operations

Blue Flag/Joint
Warfighting Assessment 2018

DIGITAL VERSION AVAILABLE

A digital version of this CALL publication is available to view or download from the CALL website:

https://call.army.mil

FOLLOW CALL ON SOCIAL MEDIA

https://twitter.com/USArmy_CALL
https://www.facebook.com/CenterforArmyLessonsLearned

Foreword

The Joint Modernization Command and the Center for Army Lessons Learned partnered in the production of this newsletter to provide the force an overview and selected best practices for multinational interoperability, multi-domain operations, common operating picture, and large-scale combat operations. Each of these are essential in accomplishing military objectives against near-peer competition and conflict.

Observations in this newsletter are from the Joint Warfighting Assessment 18 and Blue Flag 18 exercises. U.S. Air Forces Europe, U.S. Army Europe, Third Fleet, and U.S. Army Special Operations Command participated in these events.

Forces provided for this multinational exercise employed Joint Force Component Command: 1 Infantry Division Headquarters; three U.S. brigade combat teams in sustainment, armor, and infantry (2CR SBCT, 2/1 ABCT, and 173rd IBCT); and four multinational brigades from the United Kingdom, Canada, Germany, and France in both live and simulated environments. More than 7,000 personnel participated from 19 APR to 9 MAY 2018.

The primary focus of the exercises was to assess multi-domain and multinational interoperability in Field Manual 3-0, *Operations*.

Joint Warfighting Assessment 18 and Blue Flag 18 incorporated experimentation, interoperability, and exercises providing an excellent opportunity for the U.S. Army, the Joint team, and key multinational partners to develop an enduring mutual trust and shared understanding to enhance our ability to fight and win together against a near-peer advisory in high-intensity conflict.

Fight Tonight!

Michael J. Lawson
COL, FA
Director, Center for Army Lessons Learned

Multinational Joint Forcible Entry Operations
Blue Flag 18 and Joint Warfighting Assessment 18

Table of Contents

Center for Army Lessons Learned	
Director	**COL Michael J. Lawson**
CALL Analysts	**Mr. Craig G. Hayes**
Joint Modernization Command	**JMC Staff**

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, ADRPs, ADPs, ATPs, FMs, TMs, etc., must be obtained through your pinpoint distribution system.

Introduction

U.S. Army Joint Modernization Command, Joint Warfighting Assessment 18 Overview

MAJ Rich Marsh, Joint Modernization Command Strategic Plans

From 12 APR to 9 MAY 2018, 7,000 personnel from 162 organizations representing the militaries of the United States and nine North Atlantic Treaty Organization partners converged on five training sites in southern Germany as part of the U.S. Army's first Joint Warfighting Assessment (JWA). Their common goal was to advance their collective ability to overcome aggression from a near-peer competitor in Europe. In pursuit of this goal, they trained to fight as a single, cohesive, and multinational division against a near-peer adversary. This training produced numerous lessons, many of which are detailed throughout this Center for Army Lessons Learned publication, about how to foster interoperability and about which concepts and capabilities will enable multi-domain operations (MDO). JWA 18 was thus an important step forward for the Army as it seeks to adapt the force to the demands of a rapidly changing and complex world.

Two movements within the U.S. Army converged to produce JWA 18: the effort to assess the value of new concepts and capabilities and the effort to train the Army to fight on a large scale as part of a joint and multinational force. JWA 18 evolved from the Army Warfighting Assessment (AWA), which the Army Chief of Staff inaugurated in 2015 and which the U.S. Army Joint Modernization Command (JMC) first executed in 2017. The AWA assessed concepts and capabilities with the realism afforded by a corps-level exercise to provide new insights into the operational value of those concepts and capabilities. JWA continued as an operations-focused assessment but expanded its scope beyond U.S. forces to include forces from the Navy, Air Force, and nine partner nations. This produced the opportunity to assess concepts and capabilities that had the potential to improve the ability of the United States and its partners to fight together and accomplish their collective mission.

The joint and multinational scope of JWA emerged from the recognition among leaders from the United States and its partner nations that the collective group would need to fight as a unified body to succeed in stopping the aggression of rising revisionist powers. The U.S. Army, for its part, sought to align itself accordingly with the Army Operating Concept, which argues that, "To win in a complex world, Army forces must provide the joint force with multiple options, integrate the efforts of multiple partners, operate across multiple domains, and present our enemies and adversaries with multiple dilemmas." Subsequently, U.S. and allied leaders determined that they needed a venue where they could collectively train to improve their ability to fight as a unified team. This multi-partner, multi-domain, and multi-dilemma foundation for winning was what JMC achieved for the first time in JWA 18.

JMC provided JWA 18's unprecedented venue for operational assessment by integrating two formerly distinct exercises into the base JWA 18 scenario. Blue Flag 18, the Air Force's annual operational-level training exercise, and Combined Resolve X, the 2nd Brigade of the 1st Infantry Division's (1 ID's) regionally aligned force certification exercise. These exercises merged with the multinational division scenario of JWA 18 to provide opportunities for assessments at echelons through the level of coalition forces land component command (CFLCC). By also incorporating the staffs of partner nation militaries, the exercise provided a space to

develop innovations in multinational as well as joint interoperability. JMC summarizes the value of the JWA venue as a "triple payoff" that enhances training readiness for Soldiers at all echelons, enables joint and multinational interoperability, and informs the force for future force development (see Figure 1).

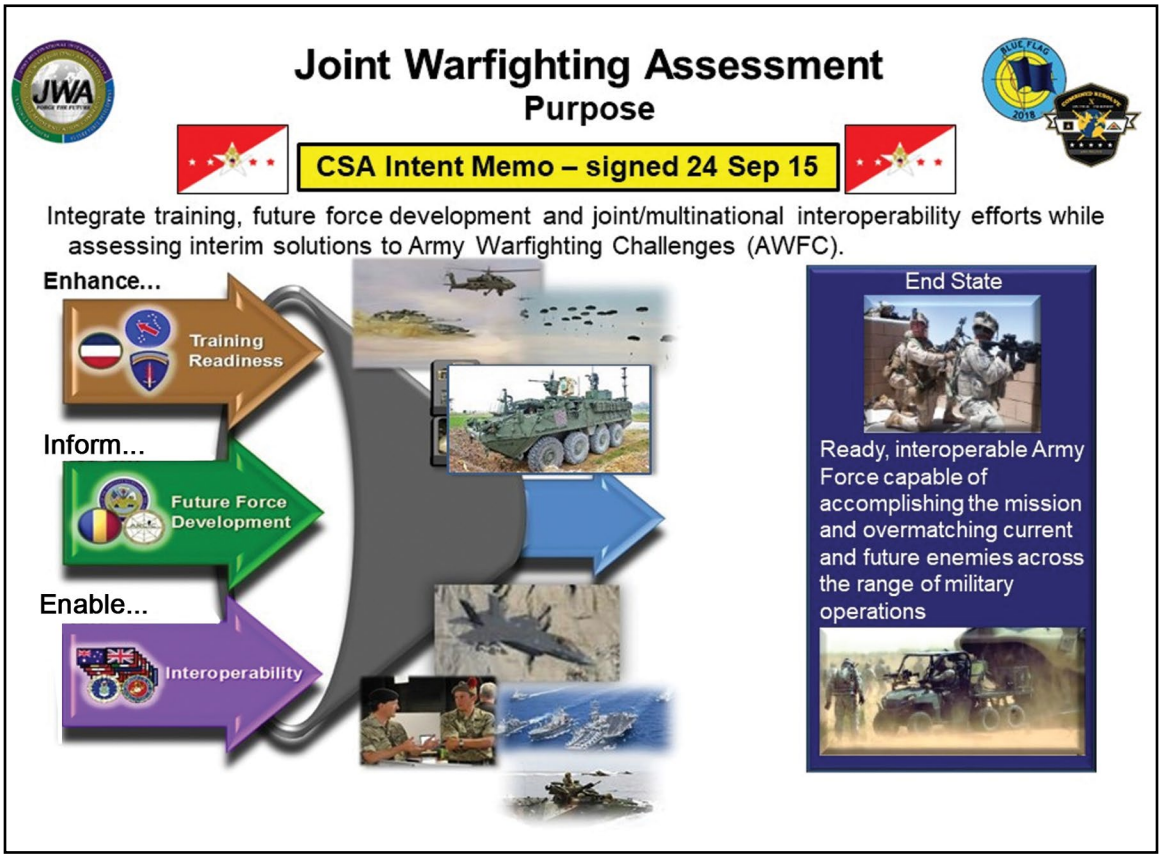


Figure 1. The three integrated exercises of JWA 18 facilitated a triple payoff in force modernization.

In the JWA 18 scenario, the joint and multinational partners came together as part of a combined joint task force (CJTF) with a mission to liberate a friendly nation that had recently been invaded and occupied by a near-peer enemy. U.S. Army Europe served as the CFLCC for the task force. By way of Blue Flag 18, staff elements from U.S. Air Forces in Europe served as the coalition forces air component command for the CJTF and the staff of the Navy's Third Fleet served as the coalition forces maritime component command. Completing the task force was a response cell from Special Operations Command, which emulated the actions of a coalition forces special operations component command. The live presence of these joint partners was indispensable in enabling JWA 18 to gain insight into the viability of concepts and capabilities under assessment.

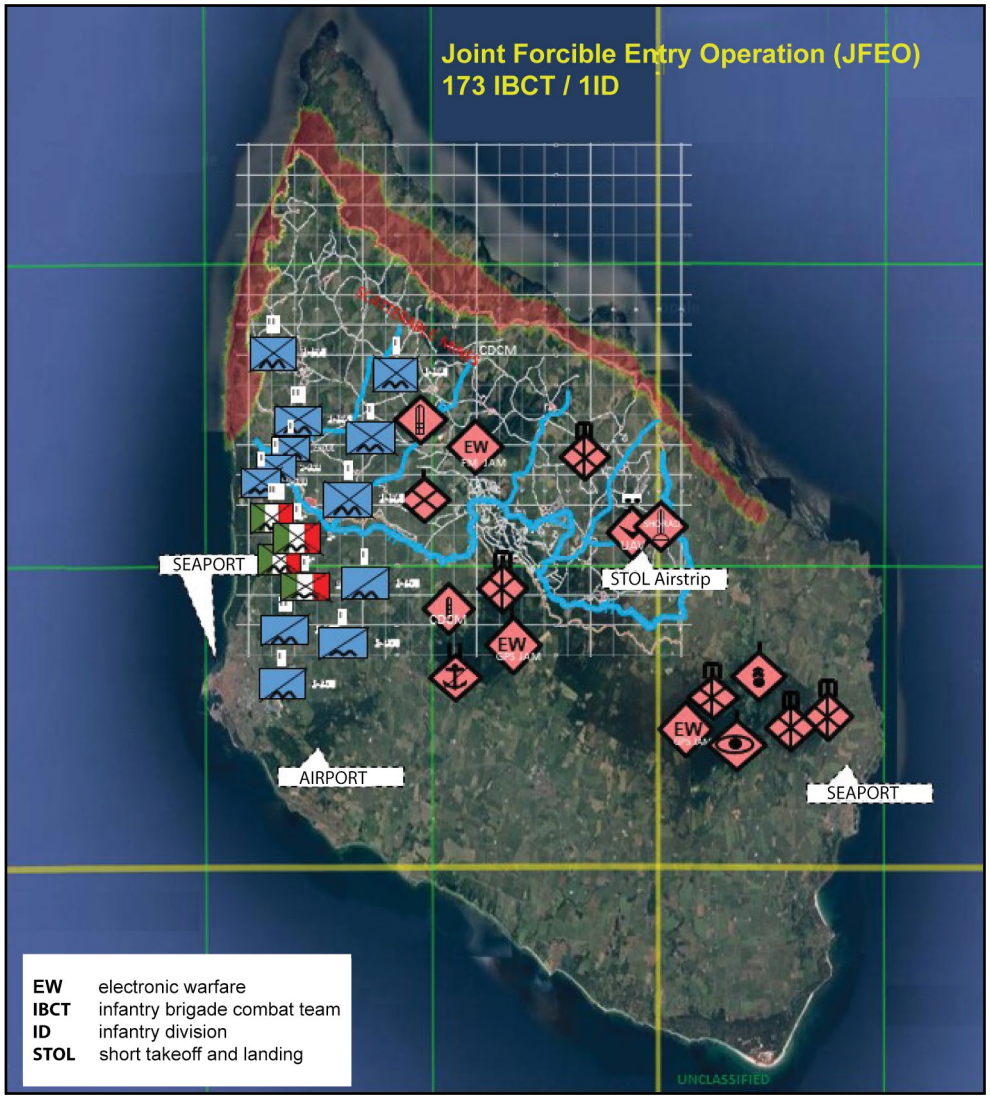


Figure 2. Joint forcible entry operations scenario map.

This multi-echelon approach provided opportunities to assess cutting edge concepts and capabilities that seek to reestablish the United States and its allies' overmatch versus near-peer competitors. Foremost among these is the concept of MDO. MDO enables Army leaders to maximize the agility of the joint force. In the future, leaders will exploit windows of advantage to achieve decisive action against a near-peer enemy. In order to exploit windows of advantage, the joint force must be interoperable. The component commands have to have access to one another's capabilities on the battlefield when and where it is most advantageous. They must be able to engage precisely from any domain (land, air, space, cyberspace, and maritime) into any other domain. Each component must be able to communicate the effects of its engagements with every other component in real time in order to make MDO possible. The opportunity to assess joint force interoperability was one of the most important products of the integration of Blue Flag 18 with JWA 18.

Within the CFLCC, the 1st ID Headquarters commanded a multinational division composed of U.S., French, German, British, and Canadian brigades. The 1st ID established its tactical operations center at Grafenwöhr Training Area in Germany. Staff elements from each of these brigade combat teams also established command posts at Grafenwöhr. The U.S. 1-503rd Airborne Infantry Battalion operated out of Hohenfels Training Area as a fully manned live force as did 2nd Brigade, 1st ID (2/1 ID), which was the rapid assistance force brigade combat team participating in Combined Resolve X.

This multinational division allowed JMC to assess concepts and capabilities that enabled interoperability with multinational partners. Perhaps the most important capability under assessment that addressed the multinational interoperability gap was the mission partner environment (MPE). MPE is a third computer enclave beyond secure Internet protocol router (SIPR) and non-secure Internet protocol router (NIPR) that allows existing U.S. digital systems to securely connect to multinational partners with tools that facilitate information sharing. It takes the joint and multinational force off of separate national networks and places this force on a common network, while allowing multinational partners to retain their existing digital warfighting systems. The MPE proved to be the most significant technological facilitator of interoperability for the multinational division as it engaged the enemy in JWA 18.

While the MPE improved the technical dimension of interoperability, another capability, the digital liaison detachment (DLD), enhanced the human dimension of interoperability. DLDs are U.S. liaison teams attached to the headquarters of partner nation brigades. They enabled digital coordination between the brigades and the 1 ID headquarters to facilitate mission command by clarifying orders, interpreting the commander's intent, and resolving issues with the goal of ensuring communication, mutual understanding, and unity of purpose. The DLDs helped produce a digital common operating picture that incorporated all relevant data from U.S. forces and our multinational partners.

The live forces of the multinational division, particularly 1-503rd IN, 2/1 ID, and 5-5 Air Defense Artillery provided the opportunity to assess concepts and capabilities at the tactical level under rigorous environmental conditions while confronted by a creative and adaptive live opposing force at the Joint Multinational Readiness Center at Hohenfels. Troops from these units assessed 16 concepts and capabilities in these conditions. Among them were: Stryker Directed Energy, Maneuver-Stinger, Division and Below Short Range Air Defense, and the Mounted Maneuver Concept, which addressed gaps and needs in the joint force's ability to execute responsive fires across domain and rapidly exploit windows of opportunity on the fast and lethal modern battlefield.

JWA 18's joint and multinational scope provided unprecedented insight into the value of the concepts and capabilities necessary to maintain the joint force's overmatch against near-peer adversaries. It was a step forward in the Army's effort to operationalize the multi-domain operations concept, and improve the interoperability of the joint and multinational force. In doing so JWA 18 adapted the force to the demands of a rapidly changing and complex world. This publication tells that story in detail.

Chapter 1

U.S. Army Joint Modernization Command, Joint Warfighting Assessment 18

Initial Insights Report

> "We have worked hard to increase our readiness, now we must modernize our concepts and capabilities. We must turn ideas into actions through continuous experimentation and prototyping, integrating technology and new ideas with Soldiers earlier to inform requirements, ensure allied interoperability, reform acquisition, and improve training for high-density conflict."
>
> – U.S. Army Modernization Strategy (AMS) Report to Congress, 30 APR 2018

The Army used Blue Flag (BF)/Joint Warfighting Assessment (JWA) 18 as an opportunity to practice what the AMS describes. Three significant takeaways are: (1) Multinational (MN) interoperability at division and below has improved significantly; however, more work needs to be conducted with joint partners; (2) Readiness training and capability assessments can be compatible, aligning readiness training and experimentation was challenging; (3) The Army can equip the future force with some better concepts and capabilities now, but the "operationalization" of multi-domain operations requires a more deliberate approach with a focused organization conducting a "campaign of operational experimentation."

Background and Purpose

> "JWA has been an excellent petri dish for modernization, helping to develop our warfighting edge in a "safe to fail" learning environment. We have made significant interoperability gains and have had a great chance to look at how we command and fight in the near future within a divisional context against a peer opponent. Critically it has shown us where our gaps lie and where renewed and sustained focus is required."
>
> – Brigadier Zac Stenning, 1 Armored Infantry Brigade Commander, UK

BF/JWA 18 evolved from the Army Warfighting Assessment (AWA), established by the Army Chief of Staff in 2015 and first executed in 2017 at Fort Bliss, TX. The AWA was the first assessment by Joint Modernization Command (JMC) of concepts and capabilities in a corps-level exercise incorporating a division headquarters (HQ) and three heavy multinational brigades. It provided breakthroughs in interoperable networks and was a venue for concept and capability assessments, though it gave little understanding of the near-future environment or the emerging multi-domain battle (MDB) concept. The AWA was not "joint" beyond the participation of Army-aligned United States Air Force (USAF) support elements and sorties by air assets stationed nearby.

BF/JWA 18 was expanded in its scope, scale, focus, and horizon. The JMC's engagement with multiple service components, doctrine and concept writers, and most importantly the U.S. Army Europe (USAREUR), resulted in a multi-service event of more than 7,000 personnel and aligned the JWA with U.S. Air Forces Europe's (USAFE) Title X BF 18. The JMC's engagement also incorporated the U.S. Navy 3rd Fleet's Maritime Operations Center certification exercise and the USAREUR's Combined Resolve X (CbR X). As a result, JWA was added to the Chairman's Joint

Exercise Program list for 2018. Using a framework of innovate-practice-learn, the exercise's purpose was to enable joint and multinational interoperability, enhance readiness training, and inform the future force (i.e., the "triple payoff").

Set in an aspirational near future with a 2-to-10 year horizon, BF/JWA 18 was conducted 17 APR to 09 MAY and assessed 30 concepts and capabilities (C&Cs). Among the concepts and capabilities were three big C concepts: Field Manual (FM) 3-0, *Operations*, tenets in Europe; the approved MDB concept; and interoperability activities with joint and multinational (MN) partners. The combined exercise leveraged a joint operational architecture simulating theater component structures. The exercise had a contracted "V Corps" HQ with experienced retired officers (and a retired Army LTG as senior mentor/corps commander). The 1 ID served as a MN division (MND) HQ. There were three U.S. brigade combat teams (BCTs) of the 173rd Infantry BCT, 2nd Armored BCT/1 ID, and a response cell from 2nd Stryker Cavalry Regiment. Also included were four MN brigade HQs: 1st Armored Infantry BDE (UK), which also participated in AWA 17.1; 1st Canadian Mechanized BDE Group (CMBG); 7th French Armored BDE; and 23rd German Mountain Infantry BDE. Events were in both live and constructive environments and included conducting a joint forcible entry operation (JFEO) and unified land operations. Ground forces operated in a robust and successful mission partner environment (MPE) supporting the integration of mission command, intelligence, joint fires, and sustainment. During CbR X (1-9 MAY), JMC placed 17 of the C&Cs in the hands of 2/1 ID Soldiers (working for 12th Polish Mechanized Division) to provide candid feedback to stakeholders.

Combining exercises requires common understanding of terms and objectives. BF 18 and CbR X were readiness training exercises, whereas JWA 18 was an experimentation exercise. As used in this chapter, "capabilities" generally refer to lower tactical level materiel solutions while "concept" describes a problem to be solved, assumptions, the expected environment, and components of the solution. The JMC uses "concepts" to describe both higher (division and above) and lower (BDE and below) concepts. MDB refers to the multi-domain battle concept published in DEC 2017. The term multi-domain operations (MDO) is used to describe the larger institutional effort to change the Army's orientation to a new way of fighting.

This chapter highlights initial insights derived from observations, direct Soldier feedback, and preliminary analysis by a diverse integrated assessment team, distinguished visitors, and subject matter experts. A more complete understanding of lessons learned and recommendations from JWA 18 is available in the Joint Exercise Report.

Triple Payoff through the Multinational Lens

> "JWA and CbR X provide hundreds of challenges and thousands of opportunities."
>
> – MG Rajmund Andrzecjak, Commander, 12th Polish Division

MN partners expressed that JWA 18 allowed them to validate their respective warfighting capabilities. It served as a "forcing mechanism" to validate progress in all aspects of interoperability as each MN BDE worked hard to achieve its primary objectives of operational connectivity and planning under a U.S. division HQ. They also used JWA 18 for future force assessments: the 1st UK BDE capped two years of experimentation with its "Strike" concept, the 1st CMBG and the 23rd Mountain BDE looked at command posts (CPs), and the 7th Armored BDE integrated its national mission command systems. All strongly expressed the intent of their

nations to continue to participate. Thirty-two senior officers ranking from COL and above from 12 nations, visited the exercise including the UK's Deputy Chief of General Staff, the United Arab Emirates' Commander of Ground Forces, and the French Deputy Chief of Land Forces. JWA 18 allowed these leaders to assess their own acquisition priorities which will prove useful in future staff talks and coordination.

Enabling Interoperability Insights

> "JWA is actually integrating with our partners. Because they [partners] are using their own systems to tie into the mission partner network, this allows us to move forward with common goals."
>
> – LTC Nicole Vinson, 86th Expeditionary Signal Battalion Commander, Coalition Network Operations and Security Center Director

Mission Partner Environment

The MPE was the centerpiece of JWA. Its size, scale, and scope were greater than in previous exercises. The network was built in a series of local and distributed risk reduction events which were considered a best practice by MN partners. The MPE stimulated the simulation and connected U.S. forces with eight multinational partners. It enabled experimentation with several materiel capabilities and concepts using both North Atlantic Treaty Organization (NATO) Federated Mission Networking and American, British, Canadian, Australian, and New Zealand (ABCANZ) standards as the framework. A brief review of each follows.

The enterprise services provider (ESP) was the hub of the MPE network and is ready now as a "fight tonight" capability. The ESP was built from repurposed Army mission command equipment and can serve as an initial capability for Army units joining or hosting training or operational MPE networks now. It was both the central network interconnection point for all MN partners and the bridging for the MPE and European Command's (EUCOM's) strategic MPE network. The ESP enabled the sharing of collaborative enterprise services (email, voice, chat, video teleconferencing, web/file sharing, etc.) and provided the path to integrate U.S. and MN mission command systems and applications across warfighting functions.

The Commercial Coalition Equipment (CCE) Internet protocol voice bridging and cross-banding capabilities are very promising even though they require continued risk management and policy decisions to use with mixed communications security algorithms. The CCE was employed by 1 ID and all MN BDE command posts (CPs) to extend tactical radio signals throughout dispersed areas of operations. It enabled the interoperability of disparate tactical radios while allowing MN BDE commanders the ability to communicate with the division CP from their CPs using their organic national equipment.

Coalition Network Operations and Security Center (CNOSC). The CNOSC operated, maintained, and defended the network under the direction of the 86th Expeditionary Signal Battalion with augmented manpower from all MN partners.

The "COP shop." The common operating picture (COP) at BF/JWA 18 was a significant improvement over AWA 17. It was comprised of U.S. and MN partners with their respective mission command systems to ensure data passed in a timely manner and adequately populated

the disparate national systems. This innovation ensured commanders had confidence in the shared digital COP derived from multiple national systems. The COP shop is a best practice now.

Network developmental operations. This approach helps speed the acquisition and fielding of new technologies by providing direct user feedback to developers in real time. Three COP-related capabilities were employed during JWA 18. The CP Computing Environment capability (based on SitaWare software and formerly known as Mission Command Information System) was easy to use with an average of four hours to learn the system. It was immediately adopted by 1 ID and all four MN brigades as the primary means to collaborate for daily updates in the COP. The Program Manager-Mission Command was able to take operator feedback in real time, update coding by developers in the U.S., and make immediate changes to deliver enhanced functionality. The Army Coalition Interoperability Solution (ACIS) was the nucleus of COP data exchange with five MN partners. ACIS is a significant improvement over the previous Army COP gateway. Additionally, U.S. Army Special Operations Command elements employed the Automated Information Discovery Environment platform in the MPE to assess interoperability between special operations forces (SOF), conventional Army units, and MN partners.

Assessing Interoperability

> "Interoperability [multinational] has grown leaps and bounds since AWA 17.1."
>
> – Fires Battalion Commander, 1 CMBG

People, processes, and technology are the key components of successful interoperability. Liaison officers remain a vital asset and require extra consideration when working with MN and joint partners. JWA 18 provided an opportunity to observe and stimulate intra-Army, joint, and MN interoperability.

Intra-Army Interoperability

The 1 ID's tactical command post served as the controlling HQ over 173rd Infantry BCT's Airborne (A) JFEO and under a combined force land component command (CFLCC) cell provided by USAREUR. Common processes and the MPE allowed successful interoperability between these Army elements.

Multinational Interoperability

The most obvious success in the exercise was found in MN interoperability. Additional tools are necessary to capture, measure, and understand this success. One of these tools was the Center for Army Analysis's Communications Interoperability Capability Appraisal Table pilot that enabled assessment of the fires warfighting function (WfF) against standardized tasks. This program should be implemented in all interoperability exercises to refine its utility across all WfFs. Another tool is found in Army Exercise Order 293-17, establishing four priority focus areas (PFA) for MN interoperability. Following is a brief assessment of each:

- **PFA#1: Network Command Information Systems (CIS)/information management.** Linked to the MPE, CIS, and COP, this information management was perceived as very successful by participants. The speed of the JWA 18 MPE compounded challenges to many routine mission command procedures. For example, unlike U.S. units' procedure to transfer routine information via a "publish/subscribe" methodology and have it

pulled by other users, many MN partners require relevant information to be pushed. The use of chat rooms in our tactical CPs has increasingly taken primacy over voice as the preferred means to disseminate information. However, much may be misinterpreted when English is not a native language. Without established procedures, critical information can be lost.

- **PFA #2: Intelligence.** 1 ID established a MN intelligence fusion cell (IFC) to synchronize a common intelligence picture. The IFC was incorporated directly into the assistant chief of staff for intelligence for the Allied Command Europe. Mixed national teams successfully used Distributed Common Ground System-Army to develop fused intelligence and sharing through the use of the U.S. Army Intelligence and Security Command Cloud Initiative, accessible on the MPE via web services. Intelligence fusion made significant progress in a MN environment and must have continued focus to enhance national-level intelligence sharing to the lowest tactical levels.

- **PFA#3: Digital fires.** The division targeting board is a critical element of a battle rhythm enabling a high-tempo fight. The network necessary for fires was successfully built at Bold Quest (Joint Staff J-7 [Deployable Training and Simulations team] innovation venue) and Dynamic Front (USAREUR fires integration exercise). The division and brigades demonstrated responsive fires with some elements even firing across boundaries in support of each other.

- **PFA#4: Sustainment.** Sustainment interoperability was not modeled or measured in detail during BF/JWA 18. Human and procedural interoperability are currently used to overcome technical incompatibility. The Logistics Functional Area Service System and Joint Operations Planning and Execution System interoperability were demonstrated; however, these were not implemented during BF/JWA 18. Logistics systems should be a priority in future interoperability exercises with NATO partners.

Joint Interoperability

JWA confirmed the observation from a recent article in Breaking Defense, that air operations centers (AOC) are "set up to handle requests for air support coming from the Army's top echelons, not from lots of widely dispersed and fast-moving brigades." Deliberate lethal targeting was adequate, though dynamic lethal fires and non-lethal effects in both deliberate and dynamic situations were not. However, small corps and CFLCC cells may have been limited in their ability to provide responsive fires.

This challenge was exacerbated because air and maritime components did not fully join or had inadequate MPE resources. As BF 18 was a training certification event, there was a concern that joining the MPE might impede execution, or was unnecessary.

The USAFE provided a Joint Air Component Coordination Element under a USAF brigadier general; the 19th Battlefield Coordination Detachment worked within the AOC. Both greatly contributed to developing procedures between components; however, both were hampered by "swivel chair" dynamics. The MN participation (intelligence, surveillance, and reconnaissance video) within the AOC was limited by classification constraints. The secret releasable (SEC-REL) MPE allowed for information exchange with MN partners. The USAFE identified that joining MPE could be beneficial in future exercises in providing more responsive joint fires and enabling MN participation.

The absence of standing joint structures outside of NATO hinders continuous training and experimentation. The combined force air component commander initiated a joint targeting effects cell (JTEC) to address these issues, It is worth developing and assessing the JTEC's utility in future events.

Enhancing Readiness Training Insights

"JWA provided us the opportunity to invest additional resources to conduct a full BCT command post exercise with all subordinate battalion CPs live at Hohenfels. This was the first time we were able to exercise at this scope and scale in my time in command. This live and constructive exercise provided a good ramp up for our follow-on USAREUR Saber Strike exercise."

– COL Jay Bartholomees, Commander, 173rd IBCT (A)

The BF/JWA 18 exercises fulfilled the Chief of Staff of the Army's (CSA) 2015 charge to "build unit readiness" by embedding assessments into high-quality training at both the higher and lower tactical organizations. Leveraging this training yielded many insights.

Interoperability is an Additive Dimension of Readiness

The operations plans depend on working with MN partners, making interoperability readiness critical. The 1 ID was the perfect choice to serve as the MND HQ. Its recent operational and training experience put it at a peak level of readiness. JWA 18 imposed the unique conditions of an OPLAN-informed European scenario with multiple subordinate MN brigades supported by U.S. functional units. This exercise allowed 1 ID to enhance its readiness with proficiency in MN interoperability.

Readiness Training and Assessments Were Compatible, Developing Capabilities can be Complementary

Embedding assessments into training allowed compatability and capabilities development of these to achieve their purpose. The JMC conducts concept and capability assessments (CCAs) to observe, analyze, and recommend solutions on the performance of specified processes and equipment available for integration in the near term. JWA 18 enabled the 173rd commander to conduct his first BCT-level command post exercise and provided training objective readiness standards for 1-503rd priorities of intelligence requirements. A combat training center rotation exercise (CbR X) produced optimal conditions for candid Soldier feedback and the JMC Operations Group achieved its primary objective of building a ready unit.

Success of the MPE in both Warfighter (WfX) 18-04 and BF/JWA 18 shows that these two events were complementary in the development of specified capabilities. As the current FM 3-0 transitions into MDO doctrine, both exercises can serve as "incubators" of processes and organizational refinement by introducing aspects of the emerging operational environment and updated concepts. The Army must synchronize WfXs and JWAs closely because of shared resources (such as Mission Command Training Program teams) and proximity of execution.

Aligning Readiness Training and Experimentation is Challenging

The USAFE and 3rd Fleet accomplished their BF training objectives. However, the experimentation by 1 ID in MDO was not fully aligned with the certification requirements for these other components. This challenge was heightened by a lack of developed procedures and a small "combined joint task force" (CJTF) HQ provided by the 505th Combat Training Squadron (led by a USAF LTC, with two retired USAF general officers as senior mentors). JWA 18 was a "marriage of convenience" with multiple elements taking advantage of one of the few integrated joint training and Army experimentation exercise opportunities. Participants must agree on similar approaches to enable experimentation on a wide scale with new concepts, processes, and organizations to realize the greatest benefit. The USAFE participants acknowledged that future exercises need emphasis on all component training and experimentation objectives during planning.

Simulation Challenges

The training environment for assessing combined, joint, and multi-echelon operations requires a platform that is scalable, robust, and adaptable to the always-changing dimensions applicable to replicating future warfare. BF/JWA 18 stretched the Joint Multinational Simulations Center system beyond its capacity, despite extraordinary efforts to make it work. Three simulations: Air Warfare Simulation Model for USAFE, Joint Semi-Automated Forces for 3rd Fleet, and Joint Conflict and Tactical Simulation (JCATS) for Army units were federated across two enclaves (secure Internet protocol router [SIPR] and MPE) with approximately 127,000 individual entities (in Phase III, decisive operations) to enable a high fidelity of tactical play.

The system accommodated training during the largely U.S.-only Phase II (JFEO). During the larger decisive operation in Phase III, the training audience did not have the opportunity for automated game play against a near-peer competitor. A classified opposing force database ensured the integrity of classified threat performance data; however, it created additional complexity in simulation architecture and likely contributed to instability in JCATS. Entity-based ground simulation provided fidelity at the smaller unit levels, although it contributed to the latency of gameplay. Consolidation of entities up to battalion level did not alleviate these challenges. The 1 ID solved the problem of stimulating mission command systems by modifying its war-gaming technique, using proven quantitative tables to enable the movement of elements within the simulation.

The factors of joint, multinational, and multi-echelon organizations and multiple enclaves drive the development of the synthetic training environment (STE). For current simulation systems, the Army should examine the use of unclassified threat databases or cross-domain solutions to enable unified action at all echelons, from all of our Joint and MN partners, and be robust enough to incorporate all forms of data regardless of classification. The USAREUR's 7th Army Training Command (7ATC) has submitted an operational needs statement for a SEC-REL simulations network to complement a similar mission command network for future exercises.

Informing the Future Force Insights

> "The joint and combined training taking place through the cooperation of BF and the Joint Warfighting Assessment improves our ability to communicate, to cooperate, and to bring real strategic effects to bear in the complex unpredictable environment of tomorrow's battlefield."
>
> – Maj. Gen. Jon T. Thomas, USAFE A-3

The JMC derived insights to inform the future force at higher and lower tactical levels. At the lower level, the Hohenfels Assessment Team (HAT) with JMC personnel and external support (e.g., subject matter experts from Centers of Excellence) conducted CCAs in Phase II, driving the scenario for the 173rd during CbR X while embedding assessments into a standing training rotation.

Concepts and Capabilities, "Best in Show"

The JMC's most valuable data input is candid feedback from Soldiers, who often modify capability employment to create a desired effect. This results in one of four outcomes: (1) A C&C is assessed as ready now; (2) C&C shows promise but it does require further development; (3) C&Cs need much more development before going to the operational force for assessment; (4) A C&C does not meet the operational needs of Soldiers and leaders. The HAT assessed 18 C&Cs.

Cyber-electronic warfare intelligence (CEWI) platoon. Similar to a concept developed by the Intelligence Center of Excellence and Cyber Center of Excellence, 173rd IBCT consolidated its electronic warfare (EW) and signals intelligence teams into a single platoon to leverage the Rapid Capabilities Office EW package provided for the exercise. Combining intelligence with electronic attack allowed the BDE to use the electromagnetic spectrum to engage targets. The CEWI platoon, attached to A/1-91 Cavalry (attached to 1-503rd PIR), assisted in delivering effective fires on the opposing force. The EW capabilities assessed are ready now to provide immediate benefit to operational units; however, they require continued refinement to fully integrate into mission command systems.

The Robotic Complex Breach Concept (RCBC) showed promise in successful manned-unmanned teaming with prototypes and surrogate platforms. The engineer battalion breached a complex obstacle with less risk to personnel while maintaining an acceptable operational tempo. During the final iteration, the unit synchronized all elements and completed the breach significantly faster than previous iterations. The engineer battalion commander observed that, "The RCBC allows my unit to move forward, at times that they would have been delayed, to ensure full suppression of the enemy."

Mounted maneuver concept (MMC). The MMC, also known as the IBCT light fleet concept (LFC), will bring three new combat vehicles into the IBCT: ground mobility vehicle, light reconnaissance vehicle (LRV), and mobile protected firepower. The LFC provided A/1-91 CAV with the 30-millimeter-equipped LRV surrogate. This additional firepower and mobility enabled the squadron to win the reconnaissance fight in the disruption zone, facilitating the maneuver of U.S. main body forces. Although showing promise, two areas need to be studied further: (1) The concept extends the distance from the main body necessitating a more powerful communications capability; (2) LFC strains the organic logistical capability of the IBCT. The dispersed and long-distance movements envisioned by the LFC require dedicated and well-thought-out sustainment assets. As in Network Integration Evaluation 16.1 and AWA 17.1, this concept was practiced with surrogate platforms; future assessment should include prototypes.

Rapid fabrication via additive manufacturing on the battlefield is a capability allowing units to print the parts of end items three-dimensionally, permitting rapid battlefield repairs of critical equipment now. Among the more than 50 parts printed, one was a replacement part on a Long-Range Advanced Scout Surveillance System mount, returning it to service within a day and saving approximately $30,000 and the waiting time for a replacement through the supply system.

Fire support team cross-domain directed energy. This system and crew performed well as a combined fire support and counter-unmanned aerial system (C-UAS) capability. It detected, tracked, and defeated Class I low, slow, and small UAS. The four-Soldier crew successfully tracked a Class I UAS for 10 minutes while conducting calls for fire. The promise of these systems to provide enhanced fire support ability paired with a C-UAS capability are indications that the paired capabilities will have a positive operational impact for maneuver forces.

Location and Azimuth Determining System (LADS). The LADS was overwhelmingly acclaimed by users in the 13B military occupational specialty of cannon crewmember. It delivered precise location and azimuth of fire to artillery units in a global positioning system (GPS)-degraded environment. One observation from a gunnery SSG was, "Even when we've been awake for 52 hours straight, the LADS software is easy to use and makes it hard to screw up." The Army should fix the identified training limitations, LADS-GPS integration, and then field LADS to the force.

Tactical decontamination concept. This on-site immediate decontamination method proved its operational utility following two iterations of simulated persistent nerve agent attacks during CbR X. Crews mitigated contamination to their Bradley Fighting Vehicles in less than two hours, minimizing a simulated chemical attack's impact. This effort simultaneously met the Second of the 1 ID training objectives, enabled observations, and allowed on-the-spot improvement to the capability (the Chemical School commandant replaced the TYVEK suits with Soldier's Joint Service Lightweight Integrated Suit Technology). Tactical decontamination was quicker and required less water than current decontamination procedures performed by dedicated chemical, biological, radiological, and nuclear units.

Application of FM 3-0 and Multi-Domain Battle Concept

Insights at the higher-tactical level came from division operations in JWA 18 Phase III at Grafenwöhr, Germany. To prepare for this phase, 1 ID, MN BDE leadership, Training and Doctrine Command (TRADOC), and Army cyber developers gathered in February at Fort Riley, KS, in an academics session to prepare for JWA. Grounded in 1 ID's recent Warfighter experience, this group developed innovative tools that helped visualize convergence of effects in MDO.

Army and Air Force processes required for MDO. Current air tasking, joint targeting, and collection management cycles constrain opportunities to exploit windows of advantage and must adapt to the tempo and flexibility anticipated in MDO. The air tasking order (ATO), produced by the joint targeting cycle, proved useful only for deliberate operations. Dynamic re-tasking was not agile enough to take advantage of the opportunity of convergence windows. The AOC placed standby close air support within each ATO for emerging ground requirements; however, 1 ID was not aware of these assets. As the 1 ID air liaison officer stated, "Any effects on the enemy's integrated air defense system are welcome, but the Air Force will not necessarily launch assets based on a dynamic window of opportunity."

Timely battle damage assessment (BDA) was not consistently available at all echelons to identify or create windows of advantage. Air assets and processing, exploitation, and dissemination platforms are not usually tasked for BDA in support of dynamic targeting. This ultimately resulted in redundant targeting, the misdirection of resources, and the inability to identify windows of advantage or loss of a window to enemy success. The fusion of sensors will assist in more awareness of shared capabilities.

Integration of cyber/EW remains a significant challenge. Nonlethal effects generally do not follow a 96-hour cycle, they require longer planning cycles and differing approval processes. This is a significant impediment to the execution of MDO. Many of the tools needed have not been developed or require theater or higher authority, approval, and allocation. The 1 ID's chief of staff was in a challenging position, "Converge multi-domain capabilities from the national to tactical level for a three-hour window of advantage 96 hours before I need them. When the battle doesn't play out the way I predicted, I can't shift all those assets quickly enough." Understanding how commanders intend to fight informs developers of which tools with preapproved authorities are needed. The USAFE leaders understand these challenges and innovations, such as the JTEC assisting in integrating domain effects.

Consolidation of area operations. MDO requires attention to the lessons of the past 17 years of war, specifically stability and consolidation tasks. For battlefield architecture, the designation of a consolidation area and support area CP is critical to counter the enemy's use of SOF and information operations to shape their deep operations. In BF/JWA 18, 1 ID tasked 2nd Stryker Regiment to conduct wide-area security which, in conjunction with friendly SOF conducting counter-SOF operations, limited the enemy's ability to observe targets for long-range kinetic systems. However, having five maneuver brigades may be more than other divisions will have on future battlefields. Consolidation of areas of operations must continue to be stressed in experimentation.

A More Focused Approach to "Operationalizing in the Multi-Domain"

Practical application of FM 3-0 with multinational partners in a European OPLAN-informed scenario provided many lessons. It also formed a potential path to operationalize MDO by 2028. Changing the cognitive approach to the future environment, maturing MDO concepts into doctrine, training leaders and units to employ this doctrine, and integrating capabilities into the force requires a more deliberate effort that is described below.

"Operationalize MDO" should be the primary task for the Army Futures Command (AFC) Futures and Concepts (F&C) Division. This effort synchronizes "development of operational concepts to drive capability development and provide the basis for modernization" (Army Modernization Strategy [AMS] Report, page 3). F&C can harness the efforts of other entities: cross functional teams (until integration into AFC), Capability Development and Integration Directorates (CDIDs), TRADOC's Combined Arms Center, the operational force (i.e., Forces Command [FORSCOM] and Army Service Component Commands), exercise development and assessment teams, and even joint (e.g., J-7), and MN partners.

F&C should develop a plan that encompasses events of varying scope and scale with defined metrics and waypoints. MDO requires training and experimentation scenarios for multiple exercises at varying echelons and from different organizations to provide an understanding of the complexity of the environment and the tools necessary for Army forces to fight and win. These experiments and exercises should be conducted in conditions aligned with those near, mid,

and far horizons established on page 8 of the AMS Report. These conditions should incorporate "real-world" scenarios in the closer horizons, such as those found in combatant command OPLANs. Critical to this effort are constructive environments that replicate weapons and other environmental factors for each horizon that are "good enough" to change the cognitive approach needed for MDO. Upgrades in current simulations are necessary until the STE matures.

In the near-to-mid future, the Army should use operational units to experiment with MDO. Units provide a "crucible of practicality" to assess utility of concepts. Units will adapt to win. The integrated team must develop tools, including "playbooks," to educate leaders and Soldiers and then allow the unit to experiment with those tools. Trained units provide immediate feedback on concepts and tools by developing their own concepts and tools or refining those given to them.

Finally, there must be a governance structure of senior Army leaders, informed by a running estimate, to implement what has been learned. These efforts will help foster a "culture of innovation, discipline, and accountability" that "integrates the Warfighter" (AMS Report, page 4).

Return on Investment, Initial Assessment

A consideration for the future of JWA and its place in modernization is return on investment. The Army allocated $30 million for JWA 18, with separate operations tempo (OPTEMPO) funding for CbR X. The JWA funding was provided directly to FORSCOM in November 2017 and managed by a "gatekeeper" construct with representatives from FORSCOM, TRADOC, and USAREUR. The estimated cost of JWA 18 was $20.3 million; $16.5 million of it was for OPTEMPO from JWA funding, not including CbR X OPTEMPO. This paid for the movement of personnel from 18 units and 2,100 pieces of equipment as well as other support costs.

We anticipate a rich output that will resonate throughout the joint force and across MN partners. Multiple units conducted mission-focused training, COEs observed their sponsored capabilities in action, and more than 100 senior U.S. and MN leaders saw firsthand the progress made in all areas. The JMC is preparing an Army Capabilities Integration brief to the Vice CSA and the Joint Exercise Report for Army-wide distribution. There are several other products pending publication including a Center for Army Lessons Learned collection prepared by participants on various aspects of the exercise, a report from the ABCANZ Program Office, and a paper on the design and execution of JWA by the Institute for Defense Analyses.

A Way Ahead

> "We need a campaign of development or experimentation versus islands of getting it done."
>
> – LTG Chris Cavoli, USAREUR Commanding General

The BF/JWA 18 exercises demonstrated a way to conduct operational experimentation. As a large-scale exercise incorporating training and experimentation objectives with CCAs, BF/JWA 18 suggests a potential way ahead for MDO. To tap the full potential of operational experimentation, the Army should link a series of exercises to constitute a campaign of operational experimentation producing immediately actionable outcomes, cumulative learning, and understanding of long-term implications.

This campaign could increase the scope, scale, and tempo of modernization. Operational commands can purposely link exercises and provide the opportunity to collectively experiment with concepts, organizations, and processes and provide a venue to assess capabilities like those being developed by contract field teams and CDIDs. Adding joint and MN elements provides opportunities to develop these concepts into practices, further fostering a culture of interoperability. Units could adopt C&Cs early by keeping what works, maintaining what works in theater for immediate use, and providing additional feedback to sponsors.

The JWA 19 features I Corps as a CJTF, with 7 ID at Joint Base Lewis-McChord, WA, in a constructive environment and serving as an MND. It will incorporate 2nd Sustainment BCT/2 ID's Bayonet Focus exercise (pre-combat training at Yakima, WA) and at least three MN brigades (from the UK, Canada, Australia, and New Zealand). Notably, it is also part of the U.S. Army Pacific's Multi-Domain Task Force pilot exercise program with 17th Field Artillery BDE. There is no confirmed joint participation for JWA 19, although the Marines and USAF may provide response cell HQs.

The year 2020 provides a tremendous opportunity to execute a campaign of operational experimentation focused on USAREUR. The USAREUR has been charged by EUCOM to develop its capacity to serve as a CFLCC in the first critical days of a transition from competition to conflict. This gives the command the opportunity to apply the reality of the European theater to MDO in a series of exercises. At the very least, Dynamic Front Division Exercise 20 and JWA 20 should be linked to address multiple objectives: practicing theater army and CFLCC responsibilities; employing high-end tactical formations (possibly a MN or U.S. corps HQ); conducting reception, staging, onward movement, and integration procedures on a large scale; and assessing available lower-level concepts and capabilities. Importantly, it may also develop a MN theater surface fires command, a proposed operational fires command structure, to establish joint fires linkage from tactical to theater level while permitting experimentation with future force capability.

The JWA proved itself as an exercise that can be shaped to support multiple modernization, training, and interoperability objectives. It provided an opportunity for our joint and MN partners to work together in a rigorous environment and made progress in many areas. As the Army Modernization Strategy and Army Futures Command drive the operationalization of multi-domain operations, JWA can play a key role in executing that effort.

Chapter 2

Future Operating Environment-Europe Command Crisis: Internally Displaced Persons Impacts to Maneuver from the Multi-Domain Battle Inspired Threat Information Operations

Chris Rogness, Program Manager, Joint Modernization Command, Assistant Chief of Staff for Intelligence (G-2) Support

LTC Albert Roach, G-2, Joint Modernization Command

European Operating Environment Observations

Exercise design efforts of Joint Warfighting Assessment (JWA) 18 endeavored to create a European operating environment (OE) that U.S. and coalition forces are likely to encounter five to 10 years in the future. With multi-domain operations as one of the big three concepts under assessment, significant emphasis was placed on designing a threat that focused on maintaining standoff from U.S. forces and their multinational partners (MNP), while mounting a persistent information operations campaign to delegitimize coalition responses to the regional crisis. The opposing force was equipped with Tier 1 anti-access/area denial capabilities consisting of layered and integrated air defense (strategic to tactical) as well as the most capable of coastal defense cruise missiles and tactical ballistic missiles, making the deployment of forces to theater and their protection once in aerial and seaports of entry a significant challenge.

With movement of internally displaced persons (IDPs) like those depicted in JWA 18 scenario (Donbass News Agency), peer adversaries have adapted to separate and defeat U.S. Joint forces and partners through:

Competition:

- Destabilizing partners and allies
- Separating U.S. and alliances politically
- Penetrating and reconnoitering friendly systems
- Supporting and enabling information warfare (IW) with unconventional warfare (UW)
- Reinforcing UW and IW and set conditions for “fait accompli” campaign with conventional capabilities

Armed Conflict:

- Separating the joint force strategically across distances with intelligence, surveillance, and reconnaissance (ISR)-strike; UW; IW; and cyber warfare
- Separating the joint force operationally in time and space with ISR-strike, UW, cyber warfare, and integrated air defense (IAD)

- Separating the joint force tactically by isolating and defeating forces with ISR-strike, electronic warfare, and IAD
- Achieving strategic objectives rapidly before the joint force can respond effectively
- Consolidating gains, setting defenses, and requiring the joint force to attack at very high cost

Return to Competition:

- Reaching negotiated settlements on favorable terms
- Destabilizing partners
- Occupying and defending occupied territories
- Fomenting insurgencies and reinforcing them with UW systems and operations
- Extending regional influence and separating the U.S. and its allies politically

When coalition forces reached forward staging bases and tactical assembly areas, the problem sets became no less challenging. Precision and massed long-range fires, in the form of theater ballistic missiles and multiple rocket launchers, ensured that no headquarters or command posts within a region of conflict were out of the enemy's range. Additionally, our reliance on computer networks and the electromagnetic spectrum to synchronize operations proved tenuous when considering the enemy's ability to employ offensive cyber and electronic warfare capabilities.

The following is stated in the Peer Adversary Objectives White Paper, "Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040," (Army Capabilities Integration Center):

In Ukraine, Russian-language print, internet, and television media had fairly heavy saturation prior to 2014, particularly in Crimea and in the east. Their narrative, aimed at both Russians and Ukrainians, was meant to convince audiences that the European Union (EU) association would lead to political chaos and economic collapse. Social media activism amplified these messages.

It is important to note the use of cyber electronics in the conflict in Ukraine. Early in the conflict, these attacks took the form of distributed denial of service and defacement attacks. More debilitating was a December 2015 attack on Ukraine's power grid, which shut down electricity to hundreds of thousands of people.

The Justice Department claimed Iran had attacked U.S. infrastructure online, by infiltrating the computerized controls of a small dam 25 miles north of New York City, heralding a new way of war on American soil. "We can tell the world that hackers affiliated with the Iranian government attacked U.S. systems and we seek to bring them to justice for their crimes" Assistant Attorney General John P. Carlin said, unveiling charges against seven Iranians for cyber attacks. The hackers, members of the Iran's Islamic Revolutionary Guard Corps, also targeted several financial institutions, the New York Stock Exchange and AT&T telecommunications with barrages of incoming emails designed to slow or shut down some of their computers, according to the indictment.

Officials in the Indian government have alleged that attacks on Indian government networks, such as that of the Indian National Security Council, have originated in China. According to the government, Chinese hackers are experts in operating robot networks. Several instances have been reported about Chinese cyber attacks against India.

None of the challenges mentioned above came as a surprise to the training audience in JWA 18. Throughout a week of JWA academics, the 1 ID staff consistently demonstrated the ability to incorporate these problem sets into their military decisionmaking process. Great strides were made in our collective understanding of our deficiencies and abilities to counter and overcome deficiencies through multi-domain operations. Doctrine and capability developers have been provided vital data to inform them of the best way to confront these challenges.

There is one dynamic of the OE that may be difficult to counter with innovative doctrine and material solutions. This is the dynamic presented by the ever-present concern of civilians on or near the battlefield. Nearly 75 years have passed since the type of conflict demonstrated in JWA 18 has occurred in Europe. In those 75 years, all of Europe has seen a significant demographic shift from rural to urban populations. Eastern Europe in particular, has seen a 132 percent increase in its urban population since 1950, while its rural population has decreased by 33 percent in the same amount of time (United Nations, World Urbanization Prospects). With Eastern Europe's population projected to be overwhelmingly urban by 2020 (203 million urban to 87.5 million rural) the implications are far reaching for any U.S. or partner-nation commander forced to respond to conflict in the region.

The refugee crisis, a result of the conflict in Donbass, had both tactical and strategic impacts on the Ukrainian government. According to a United Nation's report in March 2016, 1.6 million people were registered as internally displaced by the Ukrainian government with 800,000 to one million of them having lived within Ukrainian government-controlled areas.

Conditions Established During the Exercise

As discussed, the difficulties presented by the threat's standoff capabilities going into the exercise were well understood and considered. As a result, the exercise leadership determined that the Phase III portion of the exercise should start with the corps led by the U.S. already having closed most of the gap between staging areas and the enemy's forward line of own troops. This approach would ensure adequate time to assess the multinational division's ability to create and exploit windows of advantage while employing multi-domain battle concepts and still achieve MNP training objectives. This meant that ground coalition forces were nearly in direct fire range of the enemy as Phase III began.

The maneuver defense concept for the opposing forces (OPFOR) was to displace from initial battle positions under the cover of massed rocket and howitzer artillery fire just before becoming decisively engaged. This would allow the enemy to heavily attrite coalition forces, as it maintained combat power to continue the occupation of seized territory (primary strategic threat objective), and thereby force the coalition to negotiate and relent the disputed land. As part of the OPFOR plan to disrupt 1 ID's push into the contested territory, OPFOR scenario designers implemented a storyline in which the threat would foment civil unrest in cities, forcing IDPs to move toward the coalition's ground forces advance.

These conditions were established by scripting a scenario in which private military contractors (PMCs), working in conjunction with criminal elements backed by the threat, would create unrest in major population centers near the border of the contested area. At key moments when coalition forces appeared to be achieving success, the threat would initiate a false information campaign to make the displaced local population believe coalition forces were prepared to provide for their needs. This messaging resulted in mass flows of IDPs moving toward coalition positions, largely along key lines of communications, and ultimately delayed the advance toward secondary OPFOR battle positions and key terrain. The subsequent effects undoubtedly impacted 1 ID and its subordinate multinational brigades' abilities to reach objectives on planned timelines. The pace of one brigade in particular, which was in sector of the largest population center, was significantly hindered by the existence of these IDP flows. Due to limitations in simulation for replicating these types of events, it was often difficult to assess what effect response efforts had on countering this threat initiative. However, what is certain is that

commanders would have been forced to respond in some measure in order to continue operations in support of tactical and operational objectives.

The concept of taking advantage of refugees and other humanitarian crises to achieve political goals is not a new one. Professor Kelly M. Greenhill of Tufts University has written extensively on real-world examples in her article, "Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion" (Strategic Insights, 2010). Fidel Castro's use of migrant flows to Florida to force U.S. policy concessions in the 1970s and 1980s and Muammar Kaddafi's threats to flood Europe with North African migrants to lift EU sanctions against Libya both stand out as examples of the effect potential humanitarian crises can have, especially on Western liberal democracies (Greenhill, 2010). What is less understood however, is the full impact similar smaller scale conditions would have on combat operations at a tactical and operational level. Could, or should, an adversary's threat to initiate humanitarian crises impact a commander's objectives or scheme of maneuver? If a humanitarian crisis is encountered, are division and brigade commanders and staffs resourced to deal with it? Will other governmental and nongovernmental organizations be provided access to support crisis response in the midst of a high intensity warzone? These, and many other unanswered questions, tell us of the importance to continue to evaluate these challenges in future exercises.

Although the entirety of IDP considerations could not be replicated within the confines of the JWA 18 scenario, these conditions did create a baseline for assessment and a place to build from in future JWAs. The IDP scenario was supported well with intelligence reporting of the PMC activity in population centers as well as a slowly building threat IO campaign through social media and traditional media source replication. However, as mentioned, it was not always clear as to what was causing movement disruption within the simulation. Further, effectiveness of Blue Force for responses were often difficult to measure. Additionally, more data could have been incorporated from regional experts and sources from the humanitarian response community to add to realism. Moving forward, JWA threat scenario developers must work with the modelling and simulation community, as well as regional subject matter experts, to develop solutions that add fidelity and increase overall value for these types of scenario events.

Chapter 3

Joint and Multinational Impacts of Multi-Domain Operations in Europe

CPT Shannon M. Killian

Blue Flag/Joint Warfighting Assessment 18 (BF/JWA 18) served as a capstone exercise during which the U.S. Army explored the operations of multi-domain operations (MDO) within a joint and multinational context. The concept of MDO is predicated upon both joint and multinational operations through a cohesive massing of capabilities to deter conflict and when necessary, decisively defeat a peer threat. By combining the U.S. Air Force Europe BF 18 with U.S. Army Europe and JWA 18, the Joint Modernization Command hosted an exercise that replicated operational-level and large-scale warfighting conditions for a collective 7,000 participants. Hosting the exercise in Europe provided a relevant and realistic backdrop in which the training audience was forced to address tactical, operational, strategic, and political constraints.

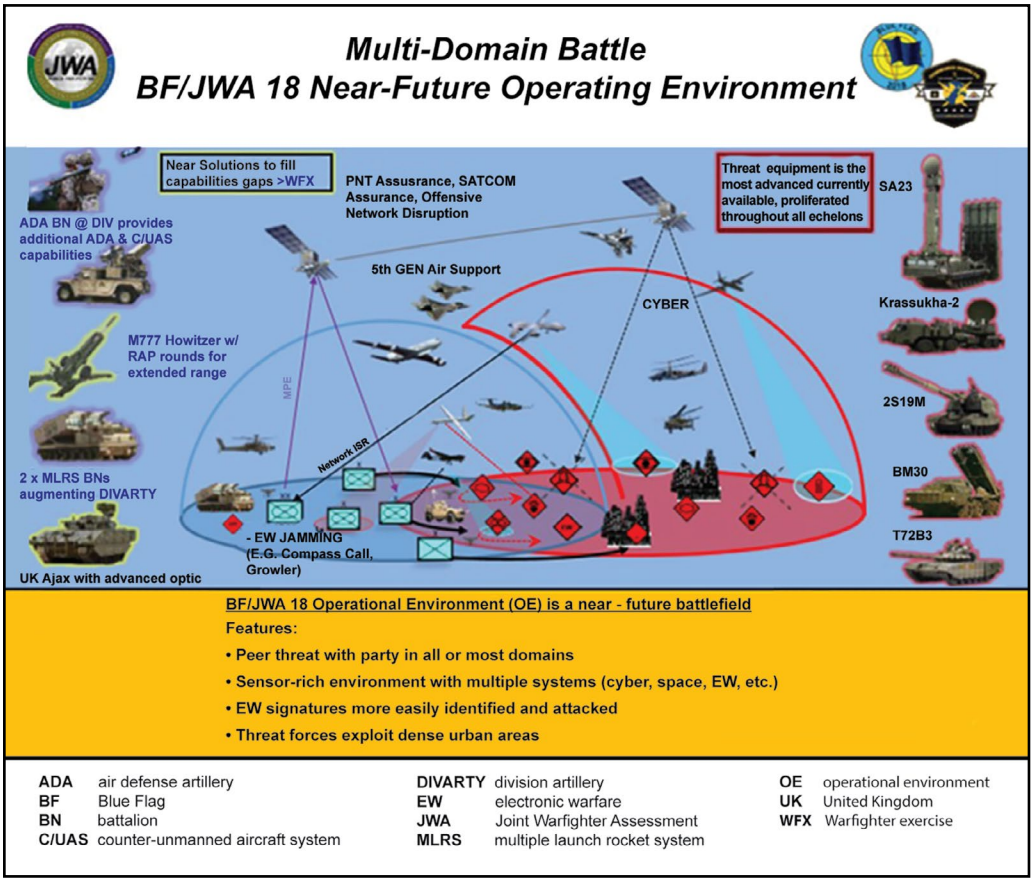


Figure 3-1. Multi-domain battle BF/JWA 18 near-future operating environment.

BF/JWA 18 provided the complex environment necessary to train and identify strengths and weaknesses across a joint and coalition force particularly within the scope of MDO. Increasingly sophisticated peer adversaries demand the joint force organize, practice, and employ capabilities and methods across domains, environments, and functions over time and physical space through efficient and effective interoperability. BF/JWA 18 provided the opportunity to assess numerous

challenges to the operationalization of MDO including command and control, resourcing shortfalls, and technological disparities.

Command and control of joint and multinational formations and processes are complicated and are further convoluted by ill-defined responsibilities at echelon. Realistic and mature relationships with higher echelons (corps, combined force land component command, combined force air component commander, etc.) are necessary for tactical units to synchronize and prioritize independent targeting requirements. At any time over the continuum of competition through armed conflict, national assets will be applied against a peer adversary; tactical echelons must understand the shaping efforts of higher and neighboring entities. Responsibilities at echelon for shaping an expansive battlefield and contributing to temporary and enduring windows of advantage were undefined during JWA 18. Loosely defined command and support relationships ultimately led to redundant targeting, misallocation of resources, and unsynchronized and untimely actions on the battlefield.

The potential latency in delivering effects when higher echelons control assets can have an adverse operational impact when facing an agile peer threat. The joint planning cycle to include the targeting cycle, collection management cycle, and joint air tasking cycle, serves to highlight both the rigidity of necessary authorities and permissions in addition to resourcing shortfalls. The joint planning cycle results in production of the joint integrated prioritized target list, joint integrated prioritized collection list, and air tasking order which ultimately supports the prerogative of a combatant or joint task force commander and is deliberate and does not afford tactical commanders flexibility against an incredibly dynamic threat. The overall cycle time associated with nonlethal effects, compounded by a 72-to-96 hour joint planning cycle, exacerbates the dilemma that tactical commanders must confront against a threat that enables lower-level formations with capabilities across all domains. Permissive nonlethal coordination must be accessible to a tactical commander through a flexible tasking cycle. Divisions must be empowered through direct relationships with proponent agencies responsible for the execution of effects requiring external support.

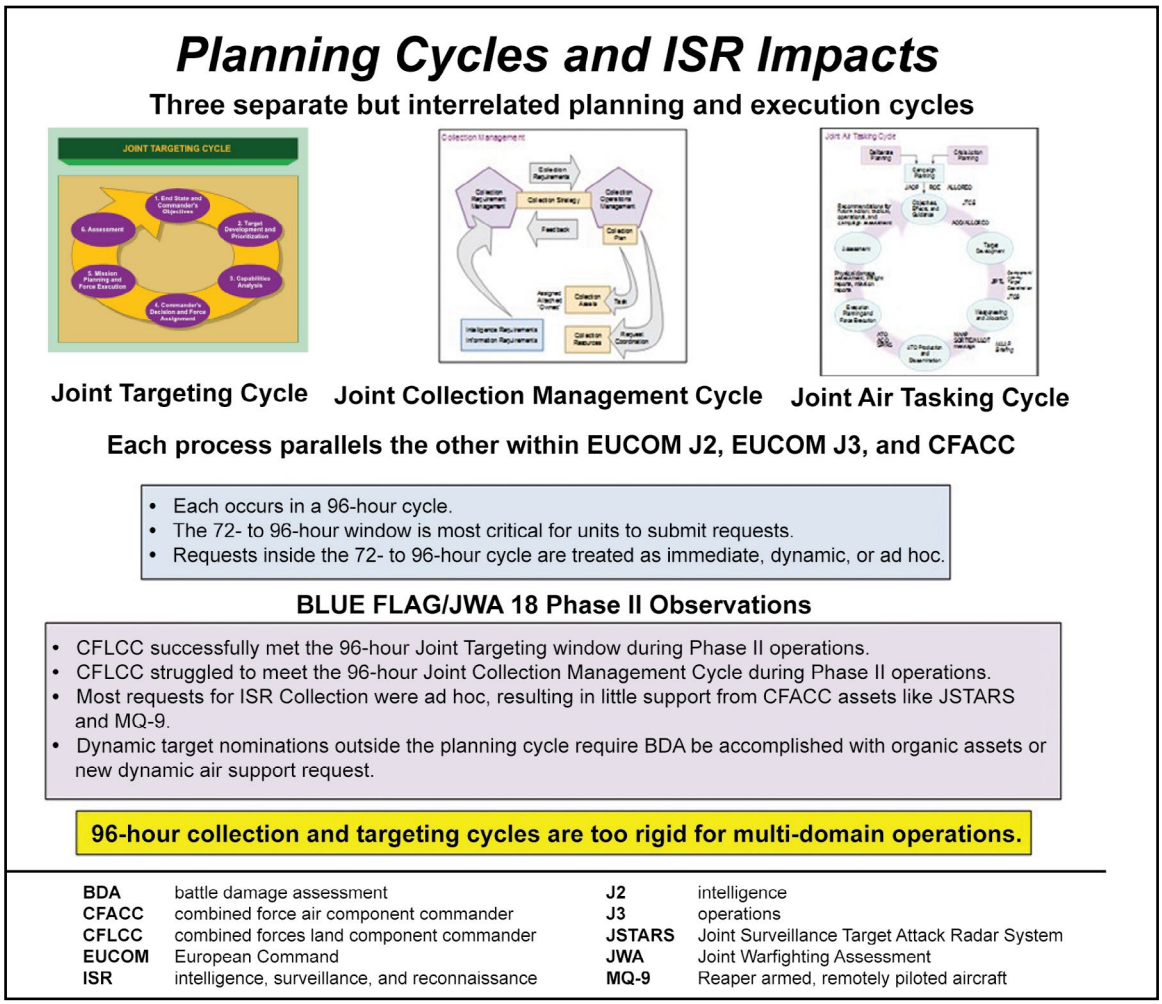


Figure 3-2. In the joint planning cycle, multi-domain operations require dynamic targeting that is responsive to all echelons of command.

The execution of MDO at the tactical level was further complicated by classification restrictions, national caveats, and inhibited understanding due to technological incompatibilities across the joint and multinational forces. Although the mission partner environment proved successful in fulfilling technical objectives, the inability to sufficiently staff work stations and a lack of common experience with digital mission command information systems amongst subordinate units ultimately continued to sow misunderstanding between nations. In a compressed decision-making cycle, commanders at all levels must exercise disciplined initiative in order to maintain an increased operational tempo. Any incompatibility across systems severely degrades intelligence fusion and the ability to maintain command and control across subordinate organizations. Challenges with battle damage assessments, intelligence reporting, and information management led to an inconsistent understanding of the enemy and vulnerabilities across maneuver formations throughout the exercise.

Despite the many challenges faced by the joint and multinational effort during JWA 18, the lessons learned from the exercise will accelerate force modernization through the evolution of organizational concepts and materiel capabilities to improve the combat effectiveness of U.S. and partner forces. Whether in Europe or any other region, coalition forces will face a threat that operates by any means necessary to inhibit friendly objectives. MDO allow commanders at all levels, under any variety of circumstances, and facing any threat, to leverage all available assets and capabilities to seize the initiative and achieve overmatch. Exercises such as BF/JWA 18 will allow U.S. forces to maintain momentum toward a modernized force capable of achieving decisive victory against any variety of threat. The underlying and first-order principles of MDO are integral to the success of a campaign in any theater. The ability to conduct joint and multinational exercises with a focus on massing capabilities proves critical to a genuine understanding of and ability to plan for future operations.

Chapter 4

Division-Level Joint Forcible Entry Operations

LTC Gregory A. Wallsten, Joint Modernization Command
Assistant Chief of Staff for Operations and Training,
Current Operations Chief

The Joint Warfighting Assessment (JWA) 18 scenario was founded on the fact that the anti-access/area denial (A2/AD) capabilities of near-peer enemies require the joint force to conduct a joint forcible entry operation (JFEO) to gain entry to a contested theater. Planners recognized that the joint entry force must converge assets from all five domains (air, maritime, land, space, and cyberspace) to be successful in a JFEO.[1]

It is essential to understand that successful operations now require planners to fully integrate multiple domains while including our unified action partners so that all available resources are effectively employed in time and space to achieve decisive results. Given these constraints, the JWA 18 exercise scenario assessed a JFEO to examine the multi-domain operations concept in the European Command (EUCOM) theater.

The JFEO, because of its applicability to near-peer scenarios that confront the United States, provided particularly relevant lessons about how to operationalize the multi-domain operations (MDO) concept. The outcome of the JWA 18 scenario demonstrated that for a JFEO to be successful, the joint and multinational force must converge all domains at the point of penetration of the A2/AD system. In the exercise, joint operations converged domains to steadily degrade enemy A2/AD systems. This first allowed the U.S. Air Force to safely deliver U.S. Army paratroopers to their objectives and then enabled the expansion of the lodgment to set the conditions for the follow-on operations that defeated the enemy. This chapter will describe how the combined joint task force converged all five domains to successfully penetrate the enemy's A2/AD umbrella and gain entry to the contested theater.[2]

In the maritime domain, the U.S. Navy's 3rd Fleet conducted operations in the North Sea and Norwegian Sea to achieve maritime superiority 500 miles beyond the capability of the enemy's fleet forces. This ensured the protection of sea lines of communications (SLOCs) and air lines of communications (ALOCs). Without the success of 3rd Fleet's mission to secure SLOCs and ALOCs, enemy forces could have interdicted friendly forces with a variety of modern weapons systems. The 3rd Fleet's actions prevented the enemy navy from employing either air, surface, or subsurface support including non-kinetic assets. This left the isolated enemy forces trapped on the island without support. With the maritime domain secure, 3rd Fleet shifted its focus. It began providing support to the combined forces land component command, which further increased coalition combat power against the weakening enemy.

This ability to shift assets as conditions get set strengthened the coalition actions and produced more problems for the enemy. Additionally, at the start of the JFEO assault, 3rd Fleet supported 1st Infantry Division (1 ID) operations with an expeditionary mobile base (EMB) ship that utilized multiple helicopter landing pads and forward arming and refueling point services. This allowed Army helicopters to stage at sea and prepare to provide close combat attack, air assault options, and "on call" sustainment deliveries. In MDO, by supporting other services, additional synergies and capabilities are provided. The Navy was able to create additional support to the

land component with the contributions 3rd Fleet made toward 1 ID military objectives on the island with electronic warfare (EW) assets, Tomahawk Land Attack Missiles (TLAMs), aerial interdiction of enemy strike aircraft, and supporting vessels like the EMB.

The joint force covered the cyber domain with a number of different assets. The Navy initiated electromagnetic spectrum operations that supported the JFEO. An hour prior to the Rangers' air assault, a Navy Prowler flying near the island conducted an EW attack that paralyzed the enemy's communications systems. Due to previous shaping operations with special operations forces (SOF), maritime elements, and air elements, the enemy had no significant EW assets remaining on the island. The joint force was able to dominate the electromagnetic spectrum at the most critical time in the operation, that of the assault. They had spectrum control a few hours prior to the beginning of the JFEO which remained for the duration of Phase II. Local maritime and air superiority was critical in the joint force's ability to dominate the electromagnetic spectrum. It provided further evidence that the joint force must coordinate across all domains to successfully gain control of the electromagnetic spectrum.

1 ID converged all the other domains into the land domain to create a window of advantage that allowed the insertion of airborne forces on the island. 1 ID conducted mission command of U.S. and multinational land forces for the JFEO and coordinated with SOF teams and U.S. Army Rangers to achieve mission objectives prior to the combat jump of the 173rd Infantry Brigade Combat Team (IBCT). The lodgment in this exercise was an airfield which was needed for following forces. The SOF land forces conducted intelligence, surveillance, and reconnaissance (ISR) and targeting of air and sea missile defense systems. Four SOF teams infiltrated the island approximately two weeks prior to the JFEO assault as the initial ground elements. They were dual-purposed between providing intelligence for the joint force and providing training to the local resistance forces in preparation for the JFEO.

Prior to the airborne drop, one of the SOF teams destroyed an enemy coastal defense cruise missile battery in a direct action which was a high-value target. This action was the final condition needed to receive the "go" decision from the 173rd IBCT commander to launch the JFEO. Destruction of the cruise missile batteries allowed support ships to approach the island. At approximately 2100 hours on 23 APR, a Ranger company air assaulted onto the island to disrupt enemy positions in support of the attack on the airfield by the 173rd. The SOF and conventional Army coordination had been ongoing for days with a SOF liaison working inside the 1 ID tactical command post (TAC) to ensure all critical details were synchronized.

The airborne operation in JWA 18 required a large commitment of planning and sustainment resources. For 1 ID, this was a major event that required joint coordination across multiple domains and included the nonorganic 173rd IBCT. The 1 ID staff rose to the challenge. At 2302 hours on 23 APR, the 173rd IBCT conducted their airborne operation to seize the lodgment and set the conditions for follow-on forces to rapidly seize the island over the next 72 hours. Within eight hours of the first landing, 173rd forces had seized 50 percent of the island plus the airfield itself. The 1 ID TAC continued to conduct mission command as they continued with Phase III: domination of the operation. Seventy-two hours after the it assault began, the island was being transferred to the local forces as the last remnants of the enemy surrendered, as prescribed by Phase IV: introduction of follow-on forces.

In the air domain, the multinational air forces (U.S. Air Force along with U.S. Navy, Danish, United Kingdom, and French Air Forces) was able to support 1 ID by isolating the enemy prior to the commencement of the JFEO assault. In 36 hours prior to the JFEO assault, the multinational air forces had gained localized air superiority over and around the island. Air superiority was essential and was the highest priority. The multinational air forces gained it through the suppression of enemy air defenses and the prevention of enemy air interdiction. After this air force gained localized air superiority and effectively isolated the lodgment from enemy air support, they began conducting shaping operations in preparation for Phase III: domination, which was a ground attack. These actions kept the enemy on the defensive and unable to influence actions in the 1 ID operational environment. The resupply of SOF/1 ID land forces and the evacuation of casualties was possible through the synergies created with localized air superiority around the island. Additionally, the multinational air forces continued providing air strikes, EW jamming, and ISR to facilitate ground operations by dominating the air domain throughout the operation.

An important takeaway from JWA 18 is that expert staff work at multiple echelons was required to synchronize multiple domains. JFEO Phase 1: preparation and deployment, required coordination at the national level to get critical assets in place. Fully integrating and coordinating for MDO went beyond the capacity of a joint task force (JTF) air tasking order process. The national approval process for some assets, such as naval strike assets, required more than 72 hours. Once a domain gained localized superiority, joint assets were temporarily massed for greater effects. For these reasons, setting up an MDO working group at JTF headquarters that concentrates on domain convergence would produce superior results overall. Multiple echelons from JTF to EUCOM to national assets need to be included with the critical coordination to synchronize all domains toward the senior command's objectives.

In conclusion, the JWA 18 exercise provided the opportunity to conduct JFEO within the challenging geography of an island setting that was influenced by enemy maritime, air, land, space, and cyberspace spectrum domains. The 1 ID's effort to use MDO concepts, coordinate all elements, plan an airborne attack, and leverage SOF elements facilitated the JTF's success at the tactical and operational level. The 1 ID's joint forcible entry operation allowed assessment teams to collect data and identify additional MDO concepts that still require further testing.

Endnotes

1. There are five phases to a JFEO, Phase I: preparation and deployment, Phase II: assault, Phase III: stabilization of the lodgment, Phase IV: introduction of the follow on forces, and Phase V: termination of transition operations. The JWA 18 exercise focused on critical tasks in Phase II through Phase V. One of the critical conditions of JFEO prior to assault is to isolate the lodgment. 1 ID coordinated with special operations forces and other services to use all five domains to isolate the island.

2. The U.S. Navy's 3rd Fleet provided maritime, air, and electromagnetic spectrum support. The U.S. Air Force's 603rd Air Operations Center (AOC) provided air, space, and cyber support to the exercise.

Chapter 5

Running a Division with Multinational Forces in Europe

LTC Gregory Wallsten, Assistant Chief of Staff for Operations and Training
Joint Modernization Command

In Joint Warfighting Assessment (JWA) 18, Joint Modernization Command (JMC) assessed the multi-domain operations (MDO) concept through a robust combination of live field training and constructive (simulation) events. The audience for this training was a multinational division (MND) composed of the U.S. 1st Infantry Division (1 ID) headquarters and subordinate brigades (BDEs) from four partner nations. Multinational (MN) interoperability is an MND enabler that is critical for MDO, especially when confronting a near-peer enemy in the European theater. JWA 18 provided a unique opportunity for the 1 ID headquarters to exercise its mission command (MC) systems connected to a dedicated MN interoperability network with four partner nations nested and with live troops conducting competitive operations in the field.

To conduct an exercise that supports MN interoperability, planners must establish the technical, procedural, and human foundations for interoperability. Headquarters, Department of the Army, has identified four levels of interoperability which begin at Level 0 – not interoperable. The next level is Level 1, deconflicted, which is when the U.S. Army can coexist with MN forces but cannot interact together. Level 2, compatible, is when the U.S. Army is able to interact with key allies and partners in the same geographical area in pursuit of a common goal (e.g., the MN force can communicate securely by radio or phone but not over a network). Level 3, integrated interoperability, is when the MN partners have a network-enabled architecture that allows the sharing of all forms of data. Level 3, interoperability, means U.S. and MN partners are networked to conduct MC that is synchronized for joint and MN operations. Based on current and future threats, having Level 3 integrated interoperability is the only viable way to conduct effective MN MC during large-scale competitive operations against a near-peer adversary.

During planning, 1 ID along with JMC's Network Integration Division, designed the mission partner environment (MPE) network that would allow for continuous and real-time MC capabilities with Level 3 integrated interoperability in most cases. The MPE provided the network for Level 3, full interoperability with our coalition partners while the UK, France, Germany, and Canada set up live BDE command posts (CPs) at Grafenwöhr, Germany. The live CPs provided training opportunities for the entire staff across all warfighting functions (WfF) with the focus on MDO. The network common core services of email, voice over Internet protocol (VoIP), chat, and video and file transfers, improved operational maneuver, intelligence collection/dissemination, digital joint fires, and sustainment communications. Inherently, the most advantageous service provided was the common operational picture (COP) shared with all coalition exercise partners.

The MND COP was visible in all CPs, which enhanced fires and maneuver options allowing commanders to achieve mission objectives. The 1 ID MC COP displayed the position locator indicator (PLI) icons that commanders and staffs viewed on the battlefield in real-time allowing them to visualize the fight. The PLI for the JWA 18 was transmitted from Joint Conflict and Tactical Simulation Enhancements simulation databases securely through the network to the CP screens. Live unit PLI was transmitted over Blue Force Tracker, which could be integrated into the COP as required. As it would be in actual combat, the coalition could only see friendly icons

until intelligence, surveillance, and reconnaissance assets or units in contact reported enemy locations that were identified. The known enemy locations were then added to the COP, which presented opportunities for coalition targeting and updated intelligence assessments.

As the MND COP was transmitted over the MPE, all warfighting functions (WfF) were included to fully synchronize friendly operations. The MPE network was the means by which JMC established interoperability among four MN partners: Germany, Canada, France, and the UK. It created the MN COP through a program called Army Coalition Interoperability Solution (ACIS). ACIS has been going through a series of upgrades that have steadily improved the software solution. The benefit of ACIS is that select MN MC systems can actively join the network, which eliminates the need to train MN partners (MNP) to operate U.S. systems like Advanced Field Artillery Tactical Data System (AFATD) or Distributed Common Ground System-Army. Importantly, MPE through ACIS allowed each partner to use their country's specific MC equipment to transfer information across a common network in real time. The MPE network is Secret/releasable to those MN partners who have joined with the joint task force. This protects digital information while enabling unified action partners to synchronize joint and MN operations while each partner maintains their nation's Secret network for internal communications.

Building the MPE network allowed MC systems to communicate COP information to all MN partners and provided all networked CPs the ability to use common services like email, VoIP, portal/share drives, video, and chat. Orders were posted on the portal for easy access and email allowed for quick distribution to large groups. The MPE VoIP phones allowed for Secret point-to-point conversations when needed. Video conferencing and video feeds required the most bandwidth of all the services provided but were critical at times for leader visualization of the battlefield with the need to quickly share information. Full-motion video feeds from unmanned aircraft vehicles and MPE Secret video teleconferences could link commanders together for operations orders, backbriefs, and any other distance meetings as required to improve clarity and accuracy. The use of chat rooms was extensive throughout the exercise to the point that standard operating procedures were developed to control information flow similar to how frequency modulation radio nets are managed by commanders. These chat rooms rapidly linked together specific WfF for continuous information flow both vertically up and down the chain of command and laterally between BDE CPs.

A few nation-specific systems could not join the MPE network. As an intermediate solution, compliant systems were able to fill the gap. For example, the Canadian fires system was not compatible with the MPE. The Canadians overcame this problem by using an Australian AFATD supplemented with U.S. operators. This gave them a networked fires capability on the MPE and thereby solved the technical shortfall keeping them at interoperability Level 3. As more exercises occur, these interoperability integration problems will be addressed until each nation can use the issued equipment of its own military. For now, bridging the gaps with U.S. systems allows our MNPs to conduct operations at interoperability level 3, which is the ultimate goal for joint and MN interoperability.

The U.S. Army's digital liaison detachment (DLD) concept was also employed and assessed during JWA 18. The DLD provided U.S. mission command systems and operators who integrated into the German BDE CP. This facilitated the German's ability to rapidly integrate into the MPE network; however, it was a U.S. solution to a MN problem. The DLD does not solve the root cause of cultural and organizational differences between the allies. These differences compartmentalize military equipment purchase decisions. This is even with the knowledge that it is highly probable these nations will go to war as coalition partners critically needing Level 3

interoperability. With that understood, the DLD is a powerful and relatively quick solution that allows MNPs to join the MPE network, thus receiving the myriad of MC advantages gained from a fully networked fighting force.

During the exercise, all fighting BDEs encountered an aggressive and professionally equipped enemy force that employed assets across all domains. Only the maritime domain had a minimal role when the battle moved into the interior of a large land mass. As the forces clashed, each unit brought its military strength into the action. As the coalition achieved its objectives, the MND COP provided the live picture the commanders needed to control the tempo, set conditions, and then defeat the enemy in multiple domains. Having all MNPs on the same network fighting together produced the results that could not have been achieved with independent actions connected by phone calls or messengers driving to and from CPs.

JWA 18 provided a unique opportunity for 1 ID to conduct MC with MN partners through the ACIS on the MPE. Employing a MN division with networked BDE CPs in the field is the best way to replicate how an MND will conduct MC during large-scale combat operations against a peer adversary. JWA 18 provided a robust training scenario that allowed 1 ID and our MNPs to train their staffs, develop their procedures, and evaluate their interoperability status to guide future improvements. These improvements are critical to maintaining MNP overmatch against our peer adversaries.

Chapter 6

Interoperability from the United Kingdom Perspective:

1st Armored Infantry Brigade at Joint Warfighting Assessment 18

Brigadier Z. R. Stenning, Order of the British Empire

the UK 1st Armored Infantry Brigade operated as a strike brigade under a U.S. division in Joint Warfighting Assessment 18 (JWA 18). This was a valuable learning experience and a good test of our interoperability.

Different in size, structure, and outputs to a Warfighter exercise (WFX), JWA 18 was focused on fighting in the near future against a peer opponent. Set within a 2025 timeframe, the complex operational scenario, coupled with a "safe to fail culture," enabled us to draw valuable lessons. The scale of the exercise was more ambitious than Army Warfighting Assessment (AWA) 17 with France, Germany, and Canada all providing brigade headquarters operating under the U.S. Army's 1st Infantry division (1 ID). The 1 ID is involved with Atlantic Resolve and it was exceptionally helpful to work within a headquarters that is focused on current operational challenges in Europe. In addition, a large number of joint assets were integrated at various levels to emulate a multi-domain focus. The exercise organizer, Joint Modernization Command, aimed to deliver a triple payoff for participating brigades: interoperability, force development, and training. From a UK perspective, we added additional objectives, including developing strike tactics and trying agile command in a multinational (MN) environment.

JWA 18 provided an opportunity to learn the extent to which 1st Armored Infantry Brigade's interoperability with the U.S. has progressed since our last experience on AWA in 2017. The JWA assessment revealed that the common operating picture (COP), digital fires and intelligence, surveillance, and target acquisition fusion have all improved. We were far better connected than we were two years ago, using radio communications under canvas. In 2017, we used fiber inside the Fort Bliss Mission Training Center to connect. The next logical step is to test the COP, digital fires, and J-2 connectivity in a more robust environment, ideally where at least one of the headquarters is maneuvering. Participation on WFX 18-4 and Dynamic Front have been the key accelerants to these tests. Findings from this JWA experience are tempered with one caveat in that a major glitch in the simulation software (Joint Combat and Tactical Simulation [JCATS]) prevented us from fully stress-testing our interoperability procedures and systems. Exercise control recovered well and the manual/digital wargame replacement still allowed us to get at most of our objectives, albeit at reduced tempo.

Interoperability

Our primary focus on the exercise was to deepen the technical ability for a British brigade to operate within a U.S. division. The key interoperability focal areas were:

- **Network command information systems (CIS)/information management**. The 21st Signals Regiment worked hard, drawing on lessons from WFX 18-4, to deliver a systems network that delivered the required functionality. From connecting to the U.S. mission partner environment (MPE) network via fiber on AWA 17, progression this year was made in connecting the UK and U.S. networks via military communications. All core services worked well.

- **COP.** The MN COP was a success. The picture remained stable and latency was low.

- **Digital fires**. Digital fires continue to improve. It was fortunate to have deployed the Fire Control Battlefield Information System Application midlife upgrade capability demonstrator, which has been used on Dynamic Front and WFX. Although not stress-tested on this exercise, it is improving the call for fires. There should be an aim for less than three minutes when fighting peer opponents. MG Dyess noted during his visit that the next step for interoperability should be better sensor integration.

- **Intelligence, surveillance, and reconnaissance fusion/processing, exploitation, and dissemination cycle**. Intelligence fusion, which is the synchronization of intelligence from multiple sources, was enabled through the introduction of U. S. Army Intelligence and Security Command Cloud lnitiative 7, accessed from UK operations CIS in the brigade command post via a web service into the U.S. MPE. This application enabled browsing the Distributed Common Ground System-Army, which in turn informed participants' understanding and decision making.

- **Sustainment**. Combat sustainment support interoperability was not modelled or measured in detail on JWA and this must be addressed in future MN experimentation. Human interoperability is currently used to overcome technical and procedural incompatibility. Timely tracking and reporting on the Logistics Functional Area Service System would enhance logistic interoperability.

- **Humans**. A key observation during the exercise was the importance of a strong liaison/embedded staff officer footprint. A U.S. division primarily operates on an "information pull" approach with high degrees of connectivity enabling lower formations to swiftly access critical information digitally, thereby enabling superior decision making and tempo. The MN brigades with lower levels of connectivity tend to operate on a culture of "information push" down to subordinate units, utilizing voice and data to sustain decision making and tempo. The grease between the two approaches on JWA 18 was liaisons and embedded staff officers. Throughout, they facilitated common understanding and accessed critical information and communicated battle winning direction. Regardless of whether achieving full connectivity in the future, there is still a central need for human liaison in the MN fight and updating our brigade into U.S. division staging and onward movement with the latest recommendations for the optimal liaison/embed footprint.

- **Strike tactics.** JWA was an excellent opportunity to experiment with strike tactics, with the caveat that the simulation did not allow a full stress test of the strike tactics. Nonetheless, a free-playing enemy commander and a rules-based wargame enabling identification of a number of positive insights. Dispersed infiltration through a large battlespace was successful with relatively low casualties, especially in complex wooded terrain.

Conclusion

JWA has been an excellent petri dish for modernization, helping to develop our warfighting edge in a "safe to fail and learn" environment. Boosted considerably by three UK divisions' experiences on WFX 18.4, significant interoperability gains have been made and there is a great chance to look at how to command and fight in the near future within a divisional context against a near-peer opponent. Critically, it has shown us where our gaps lie and where renewed and sustained focus is required.

Chapter 7

The Mission Partner Environment Network: The Technical Road to Achieve Interoperability

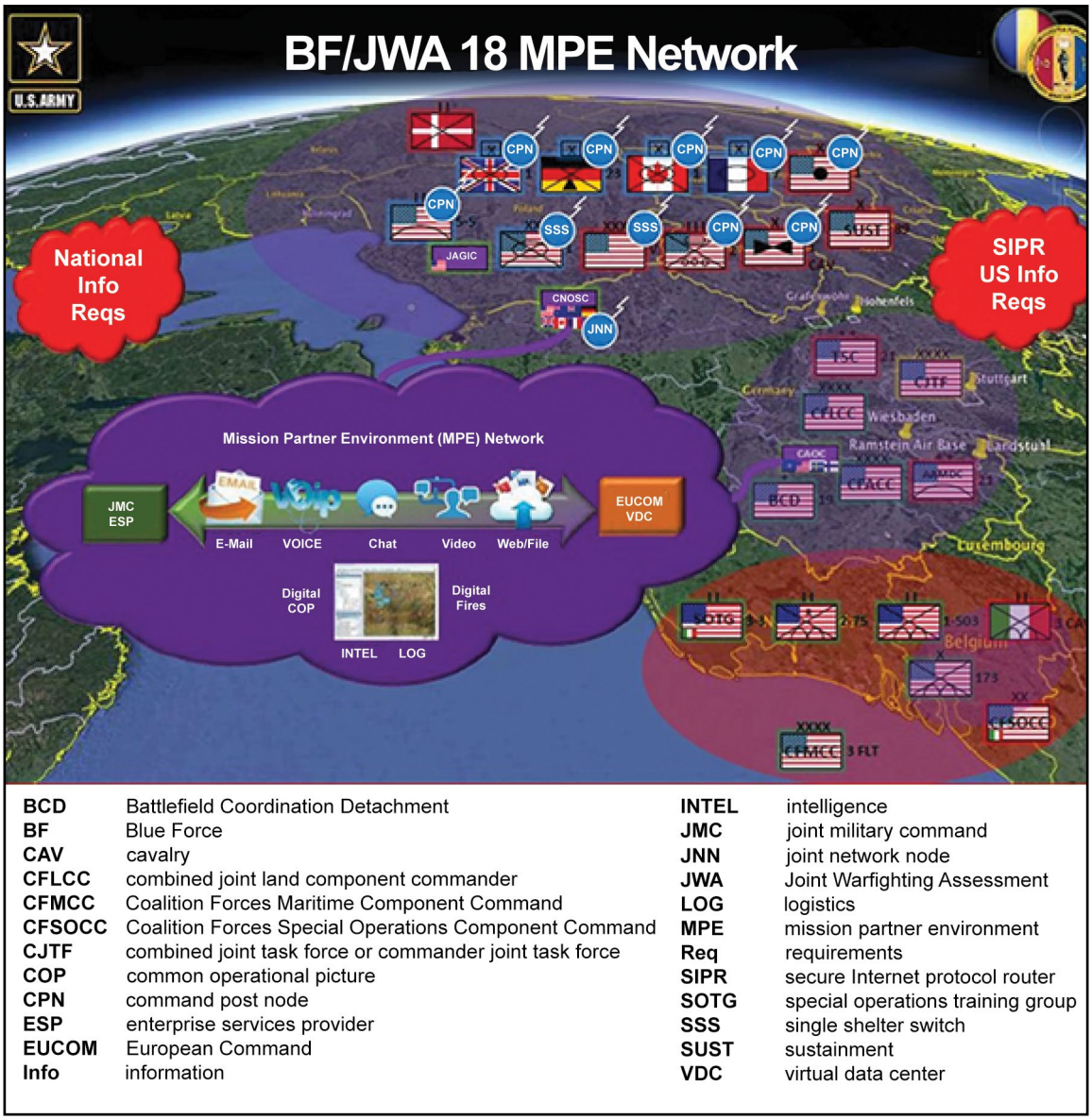
COL Eulys "Bert" Shell II
Chief, Network Integration Division
U.S. Army Joint Modernization Command

The U.S. Army will not fight future conflicts alone and therefore must achieve enhanced interoperability readiness levels with Joint, inter-organizational, and multinational (JIM) unified action partners to meet the demands of executing unified land and multi-domain operations. Interoperability with allies and strengthening partnerships are key components of the Army Campaign Plan (ACP) and the National Defense Strategy to obtain military and political goals.

Interoperability is defined as the ability to routinely act together coherently, effectively, and efficiently to achieve mutual objectives. These objectives are met through the establishment of a mission partner environment (MPE) between the Army and JIM partners, where the need to share information in the preparation and execution of military operations is fundamental. The ACP outlines four interoperability priority focus areas to maximize information sharing between the Army and multinational partners: (1) communications and information systems/information management, (2) intelligence, (3) fires, and (4) sustainment.

Paramount to achieving enhanced levels of interoperability across these priority focus areas and Joint and Army warfighting functions is the MPE Network, which provides the technical road that interconnects the Army with JIM partners. During Joint Warfighting Assessment (JWA) 18.1, conducted in Germany from April to May 2018, the U.S. Army Joint Modernization Command (JMC) led the employment of several innovative concepts and capabilities that were successful in delivering an effective MPE Network that enabled commanders and staffs at all levels to communicate securely and share critical warfighting information largely using organic national systems to fight a near-peer adversary in a realistic operational environment.

The JWA 18.1 MPE Network (JMN) was the centerpiece of the exercise spanning from the operational headquarters of U.S. European Command (EUCOM), U.S. Air Forces Europe, and U.S. Army Europe (USAREUR) to the tactical edge comprised of the U.S. V Corps, U.S. 1st Infantry Division as well as multiple brigades, battalions, and enablers from the U.S., UK (1st Armored Infantry Brigade), France (7th Armored Brigade), Canada (1st Armored Brigade), Germany (23rd Mountain Infantry Brigade), Denmark (2nd Battalion Royal Life Guards), Italy (Folgore Battalion), Australia, and New Zealand. The size, scale, and scope of the JMN were greater than in previous exercises and built in a collaborative effort between the Army and JIM partners using the Department of Defense and Federated Mission Networking along with American, British, Canadian, Australian, and New Zealand Armies Program standards.



BCD	Battlefield Coordination Detachment	**INTEL**	intelligence
BF	Blue Force	**JMC**	joint military command
CAV	cavalry	**JNN**	joint network node
CFLCC	combined joint land component commander	**JWA**	Joint Warfighting Assessment
CFMCC	Coalition Forces Maritime Component Command	**LOG**	logistics
CFSOCC	Coalition Forces Special Operations Component Command	**MPE**	mission partner environment
CJTF	combined joint task force or commander joint task force	**Req**	requirements
COP	common operational picture	**SIPR**	secure Internet protocol router
CPN	command post node	**SOTG**	special operations training group
ESP	enterprise services provider	**SSS**	single shelter switch
EUCOM	European Command	**SUST**	sustainment
Info	information	**VDC**	virtual data center

Figure 7-1. Mission Partner Environment Network.

The JMC designed and built an innovative Army MPE Network gateway capability from repurposed Army mission command equipment that served as the core infrastructure of the JMN. This MPE Network gateway, termed the enterprise services provider (ESP) capability, served as the central interconnection point for all multinational partners and bridged the tactical JMN to EUCOM's strategic MPE capability. This tactical-to-strategic connectivity demonstrated the Army's ability to integrate into a combatant commander's MPE infrastructure while providing tactical commanders with the flexibility to host or participate in an MPE Network.

Both tactical and strategic transport assets were employed during JWA 18.1 for the JMN, particularly leveraging Program Executive Office Command Control Communications-Tactical Global Agile Integrated Transport infrastructure in combination with the Defense Information Service Agency and the Network Enterprise Technology Command strategic in the EUCOM theater infrastructure. Tactical communications means were employed for tactical forces to replicate a disconnected, intermittent, and limited bandwidth environment that military formations will experience against a near-peer adversary. The JMN's architecture provided the Army with a more effective cybersecurity posture while simplifying MPE Network management following U.S. and North Atlantic Treaty Organization doctrine for communications support.

At the tactical level, the ESP enabled the sharing of human-to-human enterprise services (email, voice, chat, video teleconference, and web/file sharing) and provided the technical road map to integrate U.S. and multinational functional mission command systems and applications. The ESP is ready now as a "fight tonight" MPE Network Gateway capability and JMC recommends fielding of the ESP as an initial MPE Network Gateway capability to all Army Service component commands, corps, divisions, and signal brigades. The JMC left the ESP with USAREUR at the completion of JWA 18.1 to augment their Atlantic Resolve MPE network exercise capability.

Through the JMN and the Warfighter 18-4 MPE Network, the Army was successful in achieving an integrated level of interoperability with the UK, Canada, and France for enterprise services and enabled compatible and integrated levels of functional services supporting the Army's interoperability priority focus areas. Secure tactical voice, shared digital common operational picture, and digital fires were all accomplishments during JWA 18.1 via the JMN.

The JMC and the Army will continue to pursue future MPE Network and interoperability concepts and capabilities as part of a campaign of learning and operational experimentation. JMC will extend the JMN technical road to the Indian Ocean and Asia/Pacific area during JWA 19 during April and May 2019 and strive to achieve an integrated level of interoperability across the Army's interoperability priority focus areas.

Chapter 8

The Common Operational Picture Shop

LTC Curtis Hill
Joint Modernization Command

Enhanced levels of interoperability between the U.S. forces, interagency, inter-organizational, and multinational (MN) unified action partners is essential to meet the demands of the multi-domain and unified land operations. Trust and reliability in a digital common operating picture (COP) were identified as major underlying issues in Army Warfighting Assessment 17.1. In preparation for Joint Warfighting Assessment (JWA) 18, the Joint Modernization Command (JMC) established the concept of the digital "COP shop" to enhance the common situational awareness of the battle for ground forces. This innovation ensured commanders had confidence in the shared COP by projecting a dynamic, accurate, and shareable digital COP in order to set interoperability conditions in support of multi-domain operations.

The COP shop was composed of U.S. and MN partners with their respective mission command (MC) systems to ensure data passed in a timely manner and adequately populated the disparate national systems. The COP shop increases proficiency in achieving core interoperability objectives of ensuring secure tactical voice, a shared digital COP, and enhancing digital fire with joint and MN partners. Network Integration Evaluation (NIE) 17.1 established COP connections using military intelligence program (MIP) translation protocols, whereas JWA 18 established connections utilizing both MIP and the North Atlantic Treaty Organization (NATO) friendly force information (NFFI) protocols. MIP alone could not handle the capacity of data exchange between national MC systems and as a result, systems experienced several crashes in NIE 17.1 and commanders reverted back to analog warfighting practices, thus hindering their decisionmaking process.

JWA 18 was the first successful implementation of the COP shop. As a conceptual idea at the time, the COP shop was composed of MC system experts and operators from JMC, Program Manager-MC, the UK, Canada, France, Australia, and New Zealand. As for U.S. personnel within the COP shop, the recommendation is to include operators in the ranks of SPC to SSG under the direction and guidance of a master gunner for MC systems. The military occupational specialties assigned to the COP shop are most likely immaterial but personnel with an understanding of MC and previous user experience with operations at the battalion level or higher and the respective systems would be best suited.

COP architecture leveraged command post computing environment (CPCE) as the primary viewer for both air and ground tracks. The use of the U.S. Army Coalition Interoperability Solution (CPCE SitaWare software), in accordance with the NFFI standards and coupled with COP shop procedures, enabled an integrated joint and MN COP. A division headquarters would need to be equipped with a CPCE and conduct a troop-to-task analysis to determine the number of personnel additions required in order to manage current and new tasks associated with this tested and proven system.

For the first iteration of JWA 18, the COP shop was co-located with the Coalition Network Operations and Security Center (CNOSC), ensuring one location for all technical SMEs on hand. The establishment of this "center of gravity" along with persistent interaction resulted in faster

resolution of issues and a better understanding of coalition needs. For example, as mentioned earlier, the COP shop connections were utilized through MIP and NFFI translation protocols. This required that those specific protocols be implemented on all national MC systems. The COP shop was another instance where the joining, membership, and exiting instructions, commensurate with American, British, Canadian, Australian, New Zealand, and NATO standards, established a framework as a foundation and reference point to manage changes**.**

During the exercise execution, the COP shop provided the technical one-stop place for all COP users, managers, and technical experts to discuss COP-related issues, concerns, and trends in an effort to be proactive to operations as needed. This concept facilitated the cross pollination of knowledge of subject matter experts from the U.S. and MN partners, resulting in faster resolution of issues and a better understanding of coalition needs.

The COP shop at JWA 18 is assessed to be the current "best practice" and the recommendation is that U.S. Army and MN forces adopt this digital COP for all future operations. The COP shop monitored the following command and control categories: MC, fires, airspace, air defense, and intelligence. Initially, plans were for logistical systems to be integrated; however, the use of the logistics functional area service system to observe and analyze logistic interoperability was not thoroughly resourced and therefore was not implemented. This should be taken into consideration for future experimentation. Also, JMC established the COP shop with the CNOSC to align it with network management resources for additional support and assistance. However, once familiarity with systems is established, the initial consideration foresees the COP shop as an addition to the division's assistant chief of staff for operations and training section with equipment and dedicated personnel for management.

Chapter 9

86th Expeditionary Signal Battalion Builds a Coalition Team to Take on the Joint Warfighting Assessment 18 and Blue Flag 18

One Team – One Voice!

86th Expeditionary Signal Battalion

One of the main challenges for the Army today is how to create and extend a coalition network that supports a multitude of requirements from each theater of operation. Is the best option fielding a third set of equipment and placing additional burden on corps, divisions, or brigades or is rolling out a software partitioning solution the best option? A current gap exists in our ability to integrate quickly with coalition partners. Using an expeditionary signal battalion (ESB) may serve as an interim solution by providing supported units with the necessary flexibility to leverage their organic warfighting capacity, especially during high-operational tempo.

With slight modifications, the ESB may provide the initial forward presence of a coalition network enabling corps, divisions, or brigades to transition into an area of operations focusing on the mission rather than working on specific details and intricacies of bringing together a diverse coalition network that varies with each mission. As a proof of concept, the 86th ESB established a Coalition Network Operations and Security Center (CNOSC) and provided tactical signal support to extend the mission partner environment (MPE) network to the U.S.-led multinational division, four multinational brigade combat teams, 10th Army Air and Missile Defense Command, and the corps and combined force land component commander during Joint Warfighting Assessment (JWA) 18. The CNOSC concept delivered a resilient MPE Network to all participants and there were several key lessons learned that could assist in the design of the future ESB.

Training and Readiness

The current mission of an ESB is to provide command and control (C2) and oversee the engineering, installation, operation, and maintenance (EIOM) of nodal and extension communications in support of Army units, combatant commanders, Army Service component commanders, or joint task force/joint land force component commands. During JWA 18.1, the 86th ESB joined forces with the Joint Modernization Command (JMC) to EIOM the MPE Network. This training opportunity allowed the battalion to train all required battalion mission essential tasks, maintain readiness, and expand capability as they established the first CNOSC in support of an exercise of this scale.

Coalition Integration

The CNOSC provided a central location for partners to gather and solve networking issues. The 86th ESB's assistant chief of staff for operations and training (S-3) section served as the core CNOSC structure. Coalition partners and JMC embedded key personnel into the CNOSC to round out shortages with specific technical personnel that an ESB's current structure lacks. This includes additional network engineers, server technicians, battle captains, and directors. The added skill sets provided by our multinational partners as well as the human, technical, and procedural interaction in building the signal/communications and information systems all

proved invaluable. As the coalition partners embedded into the CNOSC, working side by side on "one network," a cohesive team emerged creating trust among the coalition. This integrated staff facilitated quick responses to network outages or concerns and the fusion of multinational partners in the CNOSC led to success.

Providing Flexibility

The CNOSC set up and established the MPE Network transport using Warfighter Information Network-Tactical line-of-sight, fiber, and satellite communications to the 1st Infantry Division (1 ID) and all coalition partners. Having the network available prior to their arrival, allowed each unit to establish connections rapidly and to begin mission planning rather than focusing on the overall network connection. The 86th ESB provided 1 ID with additional flexibility as they were able to manage the network, troubleshoot external links, coordinate communications security requirements with coalition partners, troubleshoot firewall issues, assist with technical issues with brigades, and facilitate the federation of coalition partners to the enterprise services provider (ESP) capability. The 86th ESB sent a (penetration) team to Italy to facilitate the connection of an Italian battalion while also working directly with the German brigade to not only connect into the MPE Network but to also use the core services. The help desk provided training to both units ensuring the fullest possible integration. The battalion sent a team to the 173rd Armored Brigade Combat Team to assist in the connection to MPE as well as to support the installation of its secure, mobile, anti-jam, reliable, tactical terminal into the network. The capacity to flex teams where needed is another key capability of the ESB. Rather than the division conducting network management, the CNOSC took on this role for MPE.

The CNOSC monitored all traffic across the MPE, providing not just the U.S. but also all coalition partners with analysis of the usage across the network. The CNOSC used the monitoring traffic to conduct detailed analysis of the network and services and then shared this analysis and recommendations with the 1 ID and the coalition partners. This allowed each element to make modifications to their internal networks or request changes through the standardized change board, which was in turn a part of the technical exchange working group. This level of analysis reduced the overhead required by the division to capture and track this level of information while at the same time, the analysts enabled critical decision making on the network and implementation of the digital rules of engagement. By the end of the exercise, coalition partners were able to troubleshoot at their own level by viewing the information provided by the CNOSC, further increasing efficiency in troubleshooting and overall network performance.

Recommendations:

- Continue leveraging the ESB to provide CNOSC operations and train specified mission essential tasks (METs) while expanding the ESB companies and platoons to provide additional capacity to coalition integration.

- Update the already fielded third stack in the single shelter switch to provide forward presence of the MPE.

- Deploying ESBs to the tactical edge to provide flexibility and integration to division and corps assistant chiefs of staff for information operations (G-6s), while providing additional Soldier technical subject matter experts, prevents duplication of effort and confusion.

- The ESB does not have the depth in engineer and service technicians required to EIOM a CNOSC and MPE Network for a large JWA. Increased manning can be resourced at ESB headquarters to include additional engineers, network technicians, and server administrators with coalition partners through an exchange program.

- Field the ESB with ESP and mission command stacks and modify mission and METs to include services as part of the mission set.

- Continue to incorporate exercises requiring codified multinational standards and defined network expectations to integrate ESBs, division/corps G-6s, and coalition partners to gain synergy and momentum with coalition network integration.

- Create a culture where all communicators (U.S., joint, and multinational), regardless of whether ESB or division and below, focus on the same skill sets to achieve synergy throughout the signal community.

Conclusion

The 86th ESB established the foundation of the CNOSC and transportation connection to several coalition partners during the JWA 18.1. This allowed 1 ID additional flexibility as it transitioned to the JWA MPE. The use of the ESB in concert with JMC and coalition partners demonstrated that an ESB provides added capacity to establish a coalition network at the tactical edge for divisions and brigade combat teams.

Chapter 10

Constructive Chaos: Key Challenges To Consider When Replicating the Future in Large-Scale Joint Multinational Simulation Supported Environments

MAJ Jim Teters, Medical Service Corps Officer

The modeling and simulation (M&S) support requirements for Joint Warfighting Assessment (JWA) 18 were the first of their kind. They were the first to require replication of future platforms in a contemporary simulation (Joint Conflict and Tactical Simulation [JCATS]). They were the first to require a simulation that could join a Title X exercise (Blue Flag 18) with a joint, multinational, multi-echelon (J/M/ME) constructive simulation and they were the first to require a simulation that could replicate all battlefield domains. This chapter will sketch out the complexities and hindrances that emerged from requirements as cutting edge as those of JWA 18. These complexities prohibit the Army's current M&S capabilities from delivering a simulation that is adaptable, predictable, and suitable and therefore capable of fully supporting JWA 18 training objectives.

The overarching M&S challenge of JWA 18 was the modeling of warfare as conceived by the multi-domain operations framework. The Army Chief of Staff has indicated that multi-domain operations are the framework for future warfare. Therefore, the M&S requirements of JWA 18 should be the minimum requirements of all future exercises, and going forward, these requirements should guide the developers of training environments. The solutions to the problems posed will produce more agile, predictable, and suitable simulations.

Adaptability

The replication of future platforms (two to 10 years out) was one of the primary exercise objectives of JWA 18 and also the source of important challenges. Planners assumed that future platforms would have increased capabilities than the platforms that JCATS currently replicates. Although the modelers were able to change the parameters of a gun's ability to shoot farther and an unmanned aircraft system (UAS) to fly longer in JCATS, it was only until a week or so prior to the start of exercise of JWA 18 that the multinational partners were able to validate their "new" platforms in the simulation database due to the limited availability of the database at the primary U.S. simulation center. This last-minute validation produced platforms with unrealistic parameters, which lowered the fidelity of the simulation.

JWA 18 M&S planners chose JCATS as the simulation model because the North Atlantic Treaty Organization and other multinational partners were familiar with it and the Joint Multinational Simulation Center was experienced with it. JCATS functioned as a centralized planning tool for the exercise; however, it was not optimal for this purpose. Therefore, for future simulations, the Army should develop a centralized planning tool that works on any U.S.-releasable network and allows for the U.S. and its multinational partners to update the database model anytime throughout the Joint Event Life Cycle (JELC). This would allow for up-to-date changes and configurations to the experimental platforms in the exercise and mitigate the risks of implementing a platform with unrealistic parameters.

Predictability

In simulation-supported training exercises, whether it be a platoon conducting convoy operations using Virtual Battlespace 3 to a corps-level exercise fighting a multi-echelon fight using war simulation, one cannot escape the reality that in order to set conditions for a predictable and stable training solution, it is prudent to utilize a risk-reduction strategy that involves standing up the tactical and simulation network and integrating the networks throughout the JELC. This will create opportunities to run all of the critical threads such as sensor-to-shooter (also known as fires thread) early and often enough to minimize the potential for negative training effects caused by unrealistic results in the models. Due to constraints outside of the simulation center's control, the ability to stand up a full mockup of the training environment was not possible until very late in the risk reduction timeline. One of the constraints was that the U.S. Air Force had to replicate the air fight on a classified training domain. This necessitated the creation of two JCATS games within the simulation construct, allowing for more complexity and opportunity for risk.

Furthermore, it is possible that because the simulation community was not able to stand up the simulation network in a timely manner, this may have caused the inability to observe the anomalies in JCATS such as "ghosting" of units within the simulation (a unit would appear and suddenly disappear on the simulation). These "ghosting" anomalies had an adverse effect on the ability for the simulation operators to accurately replicate effects of direct and indirect fire between friendly and opposing forces. The JCATS platform would also freeze numerous times during runtime, making the simulation almost all but impossible to replicate from a simulation operator's perspective. The exercise director at one point discontinued competitive play within JCATS and instead utilized an operations research and systems analyst to adjudicate the fight manually. Thus, JCATS was no longer dependable as a stable ground maneuver model that could replicate the ground fight as required. It cannot be stressed enough that the earlier you are able to fully replicate the models and test the simulation and their interactions, the better you will be able to fully grasp the complexities associated with integrating models and simulations together and create predictability for both you and the commander.

Suitability

As the character of warfare changes, so do the requirements to replicate all domains virtually on the battlefield and at all echelons. Therefore, replicating warfare in all domains (land, sea, air, space, and cyberspace) was another primary exercise objective for JWA 18. The challenge existed in that during the time of execution, there was no model that was immediately available for the simulation operators to use in order to replicate cyber and space effects at any echelon.

In the past, the effects on the space domain and (more exclusively) the cyber domain have been approximated during simulation supported exercises. For example, if the enemy jams friendly force radios, the exercise control element enters the Blue Force's area and turns off the simulation operator's screen for a specified number of minutes to replicate the jamming of communication systems. Although this is a solution, it is not the most realistic and efficient solution from an exercise design perspective. Therefore, developers of our future simulated training environments must replicate cyber and space effects at all echelons regardless of classification of the exercise. This will allow the Soldiers and commanders to understand the complexities and challenges that are associated with accurate and realistic cyber effects.

The U.S. Army simulation developers have made progress toward this goal. They are working on a program called Cyber Operations Battlefield Web Services (COBWebS) that has the potential to be integrated in the U.S. Army's primary home-station training ground-maneuver simulation platform. Currently, the Joint Modernization Command anticipates that COBWebS will be demonstrated at Network Integration Evaluation 18.2. Although commanders often perceive approximated cyber effects to be a distraction from the real business of warfighting, they perceive cyber effects that are integrated into the digital simulation to be a natural part of the battlefield. Consequently, the best way to train commanders and staffs on how to respond to cyber effects is to build a digital simulation that is capable of accounting for them. The Army should then continue the development of non-kinetic models such as COBWebS and integrate them into home-station training simulation solutions.

Conclusion

JWA 18 has taught us to consider a number of factors when planning and developing solutions for a successful joint, multinational, multi-echelon simulation-supported environment as required for all J/M/ME exercises. The simulations and models utilized must be able to adapt to the changing parameters such as probability of kill ratio, duration of flight (UAS), or new caliber of munition. The M&S professional must advocate and stress the importance of a robust and integrated risk reduction event timeline to minimize the potential for catastrophic effects such as the inability to replicate basic blue-on-red effects during runtime. Lastly, the M&S community must innovate and create practical and feasible simulation solutions that will replicate effects down to the platoon level for exercises as demanding as JWA.

Glossary

A2/AD	anti-access/area denial
AAMDC	Army Air and Missile Defense Command
ABCANZ	American, British, Canadian, Australian, and New Zealand
ACE	Allied Command Europe
ACIS	Army Coalition Interoperability Solution
ACP	Army Campaign Plan
AFATDS	Advanced Field Artillery Tactical Data System
AFC	Army Futures Command
AIDE	automated information discovery environment
ALOC	air line of communications
AMS	Army Modernization Strategy
AOC	air operations centers
APOD	aerial port of debarkation
ARCIC	Army Capabilities Integration Center
ASCC	army service component commander
ATO	air tasking order
AWA	Army Warfighting Assessment
AWSIM	Air Warfare Simulation Model
BCD	battlefield coordination detachment
BCT	brigade combat team
BDA	battle damage assessment
BF	Blue Flag Exercise
BFT	Blue Force Tracker
C2	command and control
C&C	concepts and capabilities
CbR X	Combined Resolve 10
CBRN	chemical, biological, radiological, and nuclear
CCA	concept and capability assessments or close combat attack

CCE	commercial coalition equipment
CCMD	combatant command
CCOE	Cyber Center of Excellence
CDCM	coastal defense cruise missiles
CDID	Capability Development and Integration Directorate
CEWI	combat electronic warfare intelligence
CFACC	combined force air component commander
CFLCC	combined force land component commander
CFMCC	coalition forces maritime component command
CFSOCC	coalition forces special operations component command
CFT	contract field teams
CIS	command information systems
CJTF	combined joint task force
CMBG	Canadian Mechanized Brigade Group
CNOSC	Coalition Network Operations and Security Center
COBWeBS	Cyber Operations Battlefield Web Service
COE	center of excellence
COMSEC	communications security
COP	common operational picture
CP	command post
CPCE	command post computing environment
CPN	command post node
CPX	command post exercise
CSA	Chief of Staff of the Army
CSS	combat sustainment support
C-UAS	counter-unmanned aircraft system
CUOPS	current operations
DCGS-A	Distributed Common Ground System-Army
DLD	digital liaison detachment

EIOM	engineering, installation, operation, and maintenance
EMB	expeditionary mobile base
ESB	expeditionary signal battalion
ESP	enterprise services provider
EUCOM	European Command
EW	electronic warfare
EXCON	exercise control
F&C	Futures and Concepts Division
FARP	forward arming and refueling point
FIST-X DE	Fire Support Team-Cross Domain Directed Energy
FLOT	forward line of own troops
FM	frequency modulation
FORSCOM	U.S. Army Forces Command
GAIT	Global Agile Integrated Transport
GPS	Global Positioning System
HAT	Hohenfels Assessment Team
HQ	headquarters
IAD	integrated air defense
IBCT	infantry brigade combat team
ICI	U.S. Army Intelligence and Security Command Cloud Initiative
ICoE	Intelligence Center of Excellence
IDA	Institute for Defense Analyses
IDP	internally displaced person
IFC	intelligence fusion cell
IM	information management
INSCOM	U.S. Army Intelligence and Security Command
IO	information operations
IP	Internet protocol
ISR	intelligence, surveillance, and reconnaissance

ISTAR	intelligence, surveillance, and target acquisition
IW	information warfare
JACCE	Joint Air Component Coordination Element
JCATS	joint conflict and tactical simulation
JELC	joint event life cycle
JER	joint exercise report
JFEO	joint forcible entry operation
JFLCC	joint force land component command
JIPCL	joint integrated prioritized collection list
JIPTL	joint integrated prioritized target list
JMC	Joint Modernization Command
JMEI	joining, membership, and exiting instructions
JMME	joint, multinational, multi-echelon
JMNI	joint and multinational interoperability
JMRC	Joint Multinational Readiness Center
JMSC	Joint Multinational Simulations Center
JNN	joint network node
JOPES	Joint Operations Planning and Execution System
JSAF	joint semi-automated forces
JSLIST	Joint Service Lightweight Integrated Suit Technology
JTEC	joint targeting effects cell
JTF	joint task force
JWA	Joint Warfighting Assessment
LADS	Location and Azimuth Determining System
LFC	light fleet concept
LOC	line of communication
LOGFAS	Logistics Functional Area Service System
LOS	line of sight
LRAS	Long Range Advanced Scout Surveillance System

LRV	light reconnaissance vehicle
LSS	low, slow, small
M/UM-T	manned-unmanned teaming
M&S	modelling and simulation
MCIS	mission command information system
MDB	multi-domain battle
MDMP	military decisionmaking process
MDO	multi-domain operations
MDTF	multi-domain task force
MIP	military intelligence program
MMC	mounted maneuver concept
MN	multinational
MND	multinational division
MNP	multinational partners
MOC	Maritime Operations Center
MPE	mission partner environment
MPF	mobile protected firepower
MRL	multiple rocket launcher
NATO	North Atlantic Treaty Organization
NETCOM	Network Enterprise Technology Command
NFFI	North Atlantic Treaty Organization friendly force information
NID	network integration division
NIE	network integration evaluation
OBJ-T	objective training
OE	operating environment
ONS	operational needs statement
OPFOR	opposing force
OPLAN	operation plan
OPTEMPO	operating tempo

ORSA	operations research and systems analysis
PED	processing, exploitation, and dissemination
PEO-C3T	Program Executive Office, Command Control Communications-Tactical
PFA	priority focus area
PIR	parachute infantry regiment, or priority information requirement
PLI	position locator indicator
PMC	private military contractor
PM-MC	Program Manager-Mission Command
RAF	rapid assistance force
RCBC	robotic complex breach concept
RCO	Rapid Capabilities Office
RFAB	rapid fabrication via additive manufacturing on the battlefield
SACP	support area command post
SCR	Stryker cavalry regiment
SEAD	suppression of enemy air defenses
SHORAD	short range air defense
SIGINT	signals intelligence
SIPR	secret Internet protocol router network
SLOC	sea line of communications
SMART-T	Secure, Mobile, Anti-jam, Reliable, Tactical-Terminal
SME	subject matter expert
SOCOM	Special Operations Command
SOF	special operations forces
SOI	staging, onward, movement, and integration
SOP	standard operating procedure
SOTG	Special Operations Training Group
SPOD	seaport of debarkation
SSS	single shelter switch
STARTEX	start of exercise

STE	synthetic training environment
TAC	tactical command post
TBM	theater ballistic missile
TEWG	Technical Exchange Working Group
TRADOC	U.S. Army Training and Doctrine Command
TSFC	Theater Surface Fires Command
UAP	unified action partner
USAF	U.S. Air Force
USAFE	U.S. Air Forces Europe
USAREUR	U.S. Army Europe
USASOC	U.S. Army Special Operations Command
UW	unconventional warfare
VBS3	Virtual Battlespace 3
VCSA	Vice Chief of Staff of the Army
VDC	virtual data center
VoIP	voice over Internet protocol
VTC	video teleconferencing
WARSIM	Warfighter simulation
WfF	warfighting function
WFX	Warfighter exercise
WIN-T	Warfighter Information Network-Tactical

SUBMIT INFORMATION OR REQUEST PUBLICATIONS

To help you access information efficiently, the Center for Army Lessons Learned (CALL) posts publications and other useful products available for download on the CALL website:

https://call.army.mil

PROVIDE LESSONS AND BEST PRACTICES OR SUBMIT AN AFTER ACTION REPORT (AAR)

If your unit has identified lessons or best practices or would like to submit an AAR or a request for information (RFI), please contact CALL using the following information:

Telephone: DSN 552-9533; Commercial 913-684-9533

Fax: DSN 552-4387; Commercial 913-684-4387

Mailing Address: **Center for Army Lessons Learned**
ATTN: Chief, Analysis Division
10 Meade Ave., Bldg. 50
Fort Leavenworth, KS 66027-1350

REQUEST COPIES OF CALL PUBLICATIONS

If you would like copies of this publication, please submit your request on the CALL restricted website (CAC login required):

https://call2.army.mil

Click on "Request for Publications." Please fill in all the information, including your unit name and street address. Please include building number and street for military posts.

NOTE: Some CALL publications are no longer available in print. Digital publications are available by clicking on "Publications by Type" under the "Resources" tab on the CALL restricted website, where you can access and download information. CALL also offers Web-based access to the CALL archives.

CALL produces the following publications on a variety of subjects:

- **Handbooks**
- **Bulletins, Newsletters, and Observation Reports**
- **Special Studies**
- ***News From the Front***
- **Training Lessons and Best Practices**
- **Initial Impressions Reports**

FOLLOW CALL ON SOCIAL MEDIA

https://twitter.com/USArmy_CALL
https://www.facebook.com/CenterforArmyLessonsLearned

COMBINED ARMS CENTER (CAC)
Additional Publications and Resources

The CAC home page address is: **https://usacac.army.mil**

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) or the Central Army Registry (formerly known as the Reimer Digital Library).

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas.

Capability Development Integration Directorate (CDID)

CDID conducts analysis, experimentation, and integration to identify future requirements and manage current capabilities that enable the Army, as part of the Joint Force, to exercise Mission Command and to operationalize the Human Dimension.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

CENTER FOR ARMY LESSONS LEARNED
10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350
https://call.army.mil

U.S. ARMY COMBINED ARMS CENTER
https://usacac.army.mil