AIR WAR COLLEGE

AIR UNIVERSITY

THE MISSION PARTNER ENVIRONMENT:

CHALLENGES TO MULTINATIONAL INFORMATION SHARING

by

Robert B. Sims, Colonel, U.S. Army

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Group Captain Shaun Harvey, Royal Air Force

15 February 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Robert (Bob) Sims is assigned to the Air War College, Air University, Maxwell AFB, AL. Colonel Sims has over 22 years of service in the U.S. Army, initially as an Infantry officer and subsequently as an Information Systems Manager. His experience includes assignments at the tactical, operational, and strategic levels, while living over 12 years abroad while working with both joint and multinational partners. Colonel Sims participated in operational missions to Afghanistan, Bosnia and Herzegovina, Kosovo, Japan, South Korea, and other locations within Europe, the Middle East, and the Pacific Rim.

Abstract

The need for U.S. forces, and the Army in particular, to conduct operations in complex environments integrated with multinational partners is well founded both in contemporary experiences and strategic guidance. In order to synchronize with these mission partners, U.S. forces must be willing and able to share digital information at operational and tactical levels with trusted coalition forces. In spite of this widely recognized requirement, the U.S. Army still has no single interoperable allied mission network available for rapid deployment. As a result, Army organizations are unable to realize the full potential of the Regionally Aligned Forces (RAF) initiative or mission command doctrine. The lack of a sustainable coalition network, or Mission Partner Environment (MPE), further prevents Army units from rapidly integrating or maintaining command and control with multinational partners as required by combatant commanders. This study reviews the history of these shortcomings and explores the Afghanistan experience to support specific recommendations for the emerging MPE. The relative success of the Afghan Mission Network (AMN) makes the case for the using common operational priorities ("mission threads") as the basis for network security architecture. This examination will show the MPE must be included and prioritized within Army network programs of record and that policy must shift to allow more flexible risk assessment with respect to information sharing in support of current and future multinational operations.

Introduction

In February 2015, the deputy commanders of five major U.S. combatant commands sent a mutually signed memo to Department of Defense (DoD) officials requesting the accelerated fielding of a warfighting network to enable information sharing between multinational coalition partners. This powerful document became known as the "15-star memo", as it was signed by five three star general officers: the deputy commanders of the Special Operations Command and four regional commands (Africa Command, Central Command, European Command, and Pacific Command). On behalf of their powerful 4-star combatant commanders, the deputies asked the Pentagon for financial and technical support to build a common multinational information network. They urged the DoD's chief information officer to complete initial deployment of this proposed Mission Partner Environment (MPE) no later than the end of fiscal year 2016. The MPE aims to provide a contingency communications network that is both effective across the range of military operations and useful to both U.S. and non-U.S. coalition military and nonmilitary partners.

This broad expression of unity between multiple senior officers reflected the latest high-water mark by a rising tide borne of both the opportunities and frustrations of a changing operational environment. "The past decade of military operations has provided the DoD with many enduring lessons that must be applied to the current and future joint force. From major combat operations to humanitarian relief efforts, the United States has encountered a challenging and complex operational environment including asymmetric threats and an array of actors."[1]

Thesis

This study will demonstrate that in spite of tremendous progress towards developing technical solutions for multinational information sharing at the joint and strategic levels

(particularly in Afghanistan), this progress has not translated adequately into sustainable solutions required by U.S. Army formations to support combatant commanders. As a result, this shortcoming constrains Army commanders' ability to fight effectively as Regionally Aligned Forces (RAFs) within a joint, multinational, and interagency environment. Furthermore, the continued lack of a common MPE solution inhibits Army forces from realizing the full potential of their "Mission Command" leadership philosophy. Taken together, these deficiencies will prevent Army forces from effectively planning, synchronizing, and fighting within the certain multinational environment of the joint force. This study will draw lessons from these findings that should inform future development of the MPE.[2]

Background

As evidenced by a broadening and increasingly complex range of current and anticipated worldwide operations, to include conflict areas such as Iraq, Afghanistan, Libya, and Syria, commanders understand that joint forces must be prepared to conduct missions both operationally and organizationally integrated at the lowest levels with allies, coalition members, interagency partners, non-governmental organizations, volunteer groups, and others. These complex regional conflicts may include operations involving irregular warfare, counterinsurgency, nation building, counter-narcotics, and cross-border sanctuaries. These operations require information sharing of a broad array of digital information, including: operational force disposition, intelligence information, mission requirements for coordination of coalition forces, theater ballistic missile defense, chemical, biological, radiological and nuclear (CBRN) threat warning, regional military and civil air movement scheduling, and more.[3] With coalition entities each becoming increasingly dependent on data networks for all aspects of operations, cooperation and communication across organizational boundaries means

interoperability, or the ability to exchange useful data between systems and applications. Joint operations conducted in close cooperation with coalition partners in the face of complex threats can no longer afford to rely on separate national secret networks within carefully partitioned physical spaces.[4]

The increasing importance of interoperability in multinational operations is well founded in contemporary strategic guidance issued by both the DoD and the Army. Following multinational experiences in Kosovo, the 2001 Quadrennial Defense Review (QDR) identified "information technology and innovative concepts to develop interoperable Joint [command and control]" as one of six key operational goals to receive DoD investment resources for the purpose of "deterring conflict and conducting military operations."[5] The document further details the need for "high-capacity, interoperable communications systems that can rapidly transmit information over secure, jam-resistant datalinks to support joint forces."[6] It recognized that future operations would not only be joint, but would also include reserve components, civilian specialist, interagency partners, and coalition forces. Interestingly, even this early document recognized that "the effectiveness of these operations will depend upon the ability of DoD to share information and collaborate externally as well as internally."[7]

A few years later, following substantial U.S. and coalition interventions into Iraq and Afghanistan, the DoD continued to emphasize interoperable multinational operations as a key operational capability. One of the eight operational capabilities identified as a focus of defense transformation in the 2005 National Defense Strategy was "increasing capabilities of partners (international and domestic) [through]... combined concept development and experimentation; information sharing; and combined command and control."[8] The next year's QDR also directed the development of "an information-sharing strategy to guide operations with federal, state, local

and coalition partners"[9] and identified additional priorities such as "strengthening interagency operations" and "working with international allies and partners"[10].

Early efforts to provide the shared networks required to support these strategic data sharing requirements generally took the form of a specially protected shared network, or enclave, with an architecture customized for specific multinational operations or requirements. In this approach, a coalition lead nation (typically the U.S.) would provide shared access to a secret ("classified") network using common software applications, mutually negotiated cost-sharing agreements, and shared technical support. The U.S. developed tailored agreements to provide physically isolated networks shared between the U.S. and a second country (bilateral) or with additional partners (multilateral). This family of shared network enclaves would be known collectively as the Combined Enterprise Regional Information Exchange System (CENTRIXS). In practice, there was no interconnection between the various partner networks, so operators would refer to each CENTRIXS "flavor" separately relative to the particular network partner. In almost all cases, the lead nation (U.S.) would retain final authority over the network infrastructure, connections to other networks or data feeds, security controls, and (most critically) the network encryption. While the shared enclave solution allowed the lead nation to share its investments and tested solutions, it necessarily limited the other participants to client status with little vote in how or when they would share information.

Limitations of the Lead Nation Solution

As other nations developed and deployed their own national mission networks integrated across their internal command and control (frequently in parallel to CENTRIXS participation), their reliance on CENTRIXS would become problematic. As CENTRIXS was largely lead nation developed, designed, and controlled, it did not always meet the specific requirements or

needs of the non-U.S. mission partner. Simple interface issues such as English-only software or keyboards and limited prioritization of English-only support desk staff became significant hurdles to widespread adoption. Limited partner acceptance of U.S.-provided shared enclaves resulted in poorly coordinated planning, movements, and responses between partner forces.[11] More significantly, partner nation forces found it difficult to trust an information sharing system over which they had no authority or security controls. Depending almost wholly on a lead nation for the encryption, security, network management, and support meant the partner nation did not share full ownership of the network, and thus was unable to fully share trust as well.

Because multinational networks were regional in nature and generally considered unique to each command's area of responsibility, the planning and implementation for each network remained a transaction between the CCMD, the participating nations, and the U.S. DoD's Assistant Secretary of Defense (ASD) for Networks and Information Integration (NII).[12] While this arrangement attempted to broker agreements, policy, and technical solutions for the limited sharing required at the CCMD headquarters' level, it did not field multinational information systems throughout the service-specific formations serving as components for CCMD missions. Accordingly, the services remained dependent on U.S.-only information sharing policy and networks. A British Navy captain lamented that coalition operation with U.S. forces created an artificially degraded communications environment. "Citing examples in exercises, he noted that U.S. and British ships have no problem sharing information through CENTRIXS, which is designed to provide interoperability between close allies. However, as soon as combat began, U.S. ships would revert to using the SIPRNet, which would leave only the British ships using CENTRIXS. As a result, neither fleet could alert each other to threats or other key situational awareness changes."[13]

Within the U.S. Army, network service providers, information security policy, and communications fielding programs remained responsible and resourced (funded) only for U.S.-only networks. As a result, deployed Army organizations continued to rely primarily on SIPRNet systems for command and control. "These early efforts at mission partner coordination were marked by heavy use of liaison officers and the manual (air gap) data transfers among American, allied, and coalition networks. This information sharing process is slow and subject to errors, and it does not achieve the intended unity of effort or speed of command to deliver the required operational effects."[14] Both commanders and staff routinely complained of having to use multiple computer terminals for each classified network and the difficulty to move even unclassified information between those networks.[15]

Afghanistan Experiences

In Afghanistan, the operational dynamics would force International Security Assistance Force (ISAF) leadership to seek a more coherent and enduring approach to information sharing. As ISAF expanded operations throughout the country, it added more members and partnering organizations. By 2010, ISAF represented more than 48 countries (including all 28 NATO members) and interacted with many non-governmental organizations (NGOs) and Afghan partner institutions. Significantly, nearly a third of the total coalition strength consisted of non-U.S. troops, with non-U.S. commanders in charge of vast areas of inhospitable geography. The enormous size and scope of this mission created incredibly complex information sharing requirements between multinational forces at the division level and below, with forces conducting a broad range of activities, to include humanitarian assistance, stability operations, counterinsurgency operations, and combat operations.[16]

To gain full advantage of the coalition against this diverse set of missions, "commanders

needed the flexibility to mix U.S. and non-U.S. formations down to the company level."[17] In spite of this, ISAF did not have a common, shared mission network prior to 2006. This was due mostly to three interrelated reasons: individual nations' information and network sharing practices remained isolated ("stovepiped'); ingrained and centralized security concerns took precedence over operational urgency; and the difficulties with creating rigidly controlled connections ("guards") between different national networks, protocols, and mission command systems.[18] Nevertheless, Afghanistan's difficult operational requirements provided fresh urgency to determine new ways to create unity of effort and improve coalition information sharing. The inability of commanders and staff to communicate equally, accurately, and urgently with all partners constrained ISAF's ability to direct forces, created fragmented mission command, and created unacceptable levels of risk to mission accomplishment. A commonly shared, secure coalition network became an operational necessity required to accomplish ISAF's campaign objectives in Afghanistan.[19]

This shared network concept would grow into the Afghan Mission Network (AMN), originally beginning in 2008 by connecting an existing U.S. multilateral CENTRIXS network with a multilateral NATO network. The AMN grew due to recognition amongst senior staff that the existing data sharing methods (guards) across multiple networks were unreliable and did not support the dynamic, synchronous exchange of unstructured data (such as text chat or voice). These senior staff officers found that the use of rigid guards between isolated networks neither enabled effective information sharing nor provided information security. This finding was more about policy than technical solution, and the realization that the security-centric policy was not providing security or enabling operational success. Subsequent ISAF commanders would endorse this key understanding at the staff level, eventually requiring all partner nations to share

ISAF operational information through the AMN by connecting their own national ISAF-specific network enclaves.[20]

The AMN marked the first widespread and large-scale use of a common federation of networks instead of the previous shared enclave method. As the mission lead, NATO provided and operated the core network while the members connected through national network extensions owned and governed by those nations within the overarching operational security, network security, and network operations governance established by NATO ISAF. This federation framework provided a significant advantage over the shared enclave approach, in that each national extension within the AMN is provisioned and operated with the resources and equipment that each participating nation provides. Critically, unlike the shared enclave approach, nations retained ownership and sovereignty over the networks they managed and the information protected within their respective national networks. The AMN federation approach gave the participating national partners ownership of their portion of the network, building trust in its utility and overcoming reservations associated with simply operating as clients on an extension from a shared enclave wholly controlled and administered by a lead nation.[21]

This federation approach to information sharing, and the control it allowed participants, first required solving problems that were primarily non-technical in nature. For example, the participating nations agreed on common functional areas, or "mission threads", requiring mutual information sharing. Mission threads included Joint Fires, Force Protection, Counter-Improvised Explosive Device, and more. These agreements on shared operational taxonomy and priorities are significant because they forced alignment of the network architecture to support the specific mission threads. While the different troop contributing nations might use separate information sharing processes and applications within these mission threads, participation in the AMN

required the common harmonization, or interoperability, of protocols between partner forces. These interoperability challenges included aligning political considerations, operational procedures, and information formats, along with technical protocols. Resolving differences was not trivial, as it required establishing common information sharing policies, procedures, and governance within a coalition of more than 40 countries within the context of existing national and multilateral networks of systems.[22] General consensus on mission threads and governance was essential to the technical solutions that followed, allowing human-to-human interaction at all levels of command by means of AMN's core capabilities: interactive web browsing, email exchange (with attachments), text chat, voice-over-IP (VoIP), video teleconference (VTC), and shared address directory.[23]

Achieving this consensus meant that each mission partner had to overcome the tension between information security (need to know) and the requirement to collaborate (need to share). For the U.S., this problem is not unique to Afghanistan or the AMN. In fact, several other regional CCMDs have invested significant resources and staff effort in developing similar multilateral sharing networks in efforts to achieve multinational information sharing in accordance with national guidance. The AMN demonstrates that commands must recognize the tradeoff between need to know and need to share, and should be prepared to ease restrictions with the former in order to achieve higher degrees of the later. Furthermore, the AMN concept of mission threads provides the baseline for common data organization, sharing, and analysis at the core of any partner mission network. The dual lessons of accepting prudent risk and developing common operational priorities (mission threads) should guide the development of future mission partner information sharing initiatives.[24] Unfortunately, because of the continued theater-specific

approach to multinational information sharing, much of the AMN's design and success would remain exclusive to the Afghanistan mission and theater.

AMN Lesson Unrealized

While the AMN shares common policy lessons and mission requirements with similar information sharing efforts outside of Afghanistan, its actual implementation and execution remains unique to the ISAF mission. In fact, a few short years after the establishment of the AMN, there would be nothing comparable for U.S. partners in the Operation Inherent Resolve campaign operating in northern Iraq and Syria. The J6 of the U.S. regional command overseeing the operation observed, "Every time we stood up a new coalition for a new crisis, it has required establishment of additional hardware and additional points of presence, to create a new network depending on the makeup and composition of the coalition... With no standard infrastructure in place to handle 'secret releasable' coalition data, commanders have to rely on customized systems."[25] This frustration expressed by the senior communications officer of a U.S. regional combatant command stood in sharp contrast to recurring strategic guidance, which since 2001, consistently identified multinational operations and information sharing as strategic priorities. This disconnect indicates a gap between the requirement for multinational operations as recognized by U.S. national leadership and the tools services provide to commanders to effect these operations.

This discrepancy between requirements and capability is rooted in the DoD's strategy of enabling the regional commands to develop their own coalition networks with relative independence. While this approach allows regional commands to tailor solutions specific to their own policy and sharing requirements, it does so at the cost of sustainability over time and interchangeability between operations and partners. The lack of a common solution prevents

U.S. service components from developing or fielding their own mission partner networks and interfaces to provide for the CCMD's information sharing requirements. In short, this prevents a service component (such as an Army unit) from deploying ready to fight into a regional command's area of responsibility. In spite of over a decade's worth of DoD strategic guidance directing multinational information sharing, and notwithstanding the operational experiences with the AMN, the U.S. Army's Director of Army Enterprise Architecture still recognized this shortcoming as capability gap in 2014. He wrote, "Currently, there is no single interoperable allied mission network that is available for immediate deployment."[26]

The Army further documents it limitations in fielding and sustaining a mission partner network in Army Regulation (AR) 25-2, "Information Assurance," its fundamental cybersecurity policy publication. Reflecting the lack of common architecture or funding for a common interoperable multinational network environment, which the regulation terms as joint interagency multinational (JIM) networks, the document explicitly formalizes strict limitations on Army enterprise support for coalition networks. It is significant because it specifies what the Army *will not* provide regarding mission partner networks, as opposed to what it will. Specifically, the document directs that JIM networks will not "require Army network and systems management, systems administration, or maintenance and repair support... [or] require Army to provide security oversight, management, or services... [or] receive Army funding for implementation at the location."[27] Curiously, the regulation does not specify what entity would be responsible for providing these types of resources or governance for mission partner networks. Based on this language, as well as the previously identified roles and practices within the DoD, a commander reasonably assumes that the Army enterprise considers the provisioning of a mission partner environment to be a matter of negotiation between CCMDs and their assigned Army units. This

negotiation, along with the subsequent provisioning of a bespoke and ad-hoc information sharing network, robs the commander and his forces of valuable preparation and planning time, and prevents the commander and his staff from synchronizing their operations with their coalition counterparts.

Army Shift To Regionally Aligned Forces

Unfortunately, the continued primary reliance on U.S.-only networks and the lack of a common MPE solution fail to meet the information sharing needs of the tactical commanders, especially as the Army transitions to a model of Regionally Aligned Forces (RAF) by assigning units to specific CCMDs for the purposes of planning, exercises, and training for specific regional operations and contingencies.[28] The RAF initiative by the Secretary of the Army seeks to provide the CCMDs with mission-tailored, pre-assigned units "to support operational missions, bilateral and multilateral military exercises, and theater security cooperation activities."[29] One senior division commander proposed "the regionally aligned headquarters can be the consistent face of the U.S. military for the members of the partner nation's military and can establish long-term relationships to aid in building the capacity of our key allies."[30] Inherent in this concept, with its explicit mission "to assist our joint, interagency, intergovernmental and multinational partners in building a stronger global security environment"[31] and to "establish long term relationships"[32] between people and organizations separated by wide geography is the requirement for a persistent and durable means for multinational communication and collaboration. This division commander sought to use a persistent multinational network in order to create daily interactions, staff repetition, and routine familiarity to increase trust and understanding with their multinational counterparts. Additionally, the commander sought for his unit to remain persistently connected in order to develop "a staff that has at least a basic

understanding of the operating environment" and ease the learning curve associated with deploying into a foreign conflict zone.[33]

The RAF approach is, in part, an extension of the Army's command philosophy known as *mission command*. The foundations of mission command are outlined in the Army Doctrine Publication "Mission Command" which explicitly directs commanders and their staffs to build cohesive teams through mutual trust and shared understanding.[34] The publication further includes multinational partners as part of a holistic team building effort by stating, "Effective commanders build teams within their own organizations and with *unified action partners* [emphasis added]... Unified action partners are those military forces [and] governmental and nongovernmental organizations... with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations..."[35] Implicit in this directive is the requirement to build trust with these partners through sharing information: "Uniting all the diverse capabilities necessary to achieve success in operations requires collaborative and cooperative efforts that focus those capabilities toward a common goal."[36] The doctrine even captures the shifting balance away from the need to know to a need to share, stating bluntly, "The traditional view of communication within military organizations is that subordinates send commanders information, and commanders provide subordinates with decisions and instructions. Mission command requires interactive communications characterized by continuous vertical and horizontal feedback. Feedback provides the means to improve and confirm situational understanding."[37]

In spite of the previously mentioned division commander's well-founded intent to fulfill both mission command doctrine and the Army chief of staff's direction, he found his efforts limited with respect to the mission partner environment. First, he noted "regional alignment should grant units access to forward networks from home station, but bureaucracy at multiple

levels (Army service component command, and CCMD) makes this a slow process and prevents an easy and seamless connection..."[38] Secondly, he found additional constraints in long-established policy and practices governing information sharing, finding "that the protocols for sharing information with coalition partners are neither fully established nor sourced. Issues here include an ingrained Army habit of over-classifying products and an associated foreign disclosure process that prevents the timely sharing of information with partners; both practices inhibit information sharing."[39] The Army's established ad hoc, limited approach to the mission partner environment proved insufficient.

These findings should present no surprise. In spite of the RAF concept, the proven utility of the AMN, and more than a decade of strategic guidance pertaining to multinational operations and information sharing, Army information technology providers continue to develop and invest deeply in the SIPRNet as the Army's primary warfighting network at the expense of multinational information sharing. This is evidenced by mandated deployments of distributed network services and data tightly coupled to SIPRNet connectivity. For example, the Army mandates that units maintain SIPRNet connectivity to their tactical network systems through the Installation as a Docking Station (IADS) program, maintaining tightly coupled, persistent linkages to enterprise-managed intrusion detection and vulnerability reporting systems.[40] These requirements effectively prevent Army units from re-purposing their primary deployable network equipment and resources for the mission partner environment. Furthermore, the lack of Army enterprise operations on and support to mission partner networks, as explicitly outlined in AR 25-2, prevents those same mandated intrusion detection and other enterprise services from existing on multinational networks. This results in degraded functionality on multinational networks relative to the heavily supported U.S.-only counterparts. Finally, the traditional design

of Army tactical networks, with computing power tied tightly to domain-specific storage mediums from the servers down to client computers, makes repurposing any equipment a labor-intensive, process-intensive, and non-trivial task akin to rebuilding a network from scratch. Considered in total, these policy, support, and material limitations "stack the deck" against any Army unit operating in a mission partner environment, resulting in units that are unable to rapidly coordinate or cooperate in operations with their multinational partners.

Assessing Shortcomings and Opportunities

There are several lessons drawn from this study to reinforce the actions requested by the "15-star memo" cited as introduction. First off, the requested action in the memo for the DoD CIO to "assign and align MPE capabilities to various established programs of record" is perhaps the most important and traditionally overlooked in terms of delivering a sustainable multinational network capability to Army units. As the DoD has not specifically tasked or funded the Army to deploy, operate, or maintain a specific mission partner environment network capability, the Army continues to misplace its efforts by developing and investing in the SIPRNet as the primary operational network. Accordingly, the supporting programs of record that provide network service, security, data, and equipment remain nearly exclusive to the SIPRNet. As current policy and design inhibits the flexible transfer of unit network equipment or data from the SIPRNet to a multinational network, units cannot meet the intent of the RAF concept or deploy to a CCMD area of responsibility fully ready to fight, as the unit would need further preparation to operate on the CCMD's designated mission partner environment.

Secondly, the Army must begin implementing specific changes in policy and technical authorities in anticipation of a common mission partner environment network and more appropriately aligned with the Army's mission command precepts. In accordance with the

strategic guidance documents cited in this study, Army network authorities and service providers must provide for units to conduct future operations primarily in the mission partner environment, with SIPRNet being the exception. Operational experiences in Bosnia, Iraq, Afghanistan, and elsewhere further underscore this urgent need. Specifically, the Army must shift away from its reliance on automated network guards and rigid foreign disclosure policy as means to limit and control the sharing of information. These controls, while well intended, neither allows for effective mission command nor provide for effective information security. Instead, the Army should consider user-based enforcement (UBE) that delegates both the responsibility and authority for information sharing to trained and trusted staff members. Additionally, operational Army headquarters at the appropriate level (such as the Army service component or a Corps headquarters) or comparable network service providers (such as a Regional Cyber Center or theater network service provider) should be empowered and resourced to provide a minimal level of enterprise services for intrusion detection and vulnerability reporting within the mission partner environment, much as currently exists on SIPRNet as Army enterprise-provided services. These changes will allow the Army to align its information sharing and network management policies with four of its mission command principals: build cohesive teams through mutual trust, create shared understanding, exercise disciplined initiative, and accept prudent risk.

Finally, the Army must engage with the DoD CIO to ensure integration of Army tactical networks and mission command systems (specialized Army systems) as part of the emerging mission partner environment network implementation. The Army should especially consider technical advances in virtualization and diskless computing solutions that separate computing resources from specific hardware or domain-specific data storage. This technology has the potential to allow significant re-use of network hardware components by Army units across

multiple enclaves, limiting requirements for additional equipment and software. This could yield size and labor advantages across both multinational and SIPRNet networks, as it could allow multiple enclaves to share common hardware, or allow units to rapidly repurpose or reconfigure hardware as required to meet new mission needs. At least two CCMDs have already prototyped this type of environment.[41]

There are also some broader conclusions to draw from this study. The AMN presents a compelling case for network federation as the future model for the mission partner network, as opposed to the monolithic shared enclave with lead nation ownership and rigid technical guards. The federation gives each participant nation a vote of ownership over the network, allowing the participant to decide what information is shared and how it operates and secures its respective portion of the network. In recognition of the value the federation principle provides to its partners, NATO is preserving the AMN concept for future operations at the Future Mission Network (FMN). As requested in the 15-star memo, the DoD should ensure its own mission partner environment is closely aligned with that of its largest alliance in order to ensure future operational interoperability with NATO partners, even at the tactical level.

While the 15-star memo provides fresh urgency for determining a common mission partner environment, it represents another milestone along the DoD's long road towards determining the best approach to digital multinational information sharing. While significant, the stated requirement is neither new nor unprecedented. The Army's RAF initiative provides further need for a persistent, enduring mission partner environment. Both the DoD and the Army have long recognized this requirement, with the AMN representing the most significant achievement through the implementation of a command-driven federation that overcame many of the shortcomings inherent in the previous shared enclaves, with their strict technical guards and strict

limitations on sharing of unstructured data. In order to achieve the multinational sharing requirements of regionally aligned forces and future coalition operations, the DoD should direct and resource the Army, along with other component forces, to develop technology that promotes a common mission partner environment in order to support CCMD's mission requirements. Without a sustainable solution fully embraced by the Army (and other services), the mission partner environment will otherwise remain an ad hoc and low priority effort, impeding the RAF initiative and similar efforts to operate and fight with multinational partners as part of the joint force.

Notes

[1] Thomas C. Lang and Martin M. Westphal, "Conducting Operations in a Mission Partner Environment," Joint Force Quarterly, no 74 (July 2014): 45.

[2] This study assumes the operational importance of multinational information sharing through communication and collaboration is implicit within the conduct of multinational military operations, much as effective communications is critical to the command and control of unilateral military operations. While there is certainly a case to be made that the effectiveness of multinational information sharing (or lack thereof) directly impacts the successful conduct of coalition operations, this study instead will focus primarily on the "how" by assuming the "why" to be self-evident – that U.S. forces, operating primarily alongside multinational partners, require the means to effectively communicate with their counterpart multinational echelons in order to achieve mutual operational objectives.

[3] Jill L. Boardman and Donald W. Shuey, "Combined Enterprise Regional Information Exchange System (CENTRIXS): Supporting Coalition Warfare World-Wide," Air War College Gateway to the Internet, last modified April 2004, accessed December 8, 2015, http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf.

[4] Ibid., 44-45.

[5] Donald H. Rumsfeld, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, 2001), 41-45, quoted in David R. Wills, *Mission Networks: An Evolution in Information Sharing* (Carlisle, PA: U.S. Army War College, 2012), 2-3.

[6] Ibid., 45.

[7] Ibid., 46.

[8] Donald H. Rumsfeld, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, 2005), 19.

[9] Donald H. Rumsfeld, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, 2006), 59.

[10] Ibid., 84-87.

[11] Author's observations through assignments and exercise participation as a U.S. military officer working with non-English speaking partners during exercises and operations in Southwest Asia (2005-2006) and East Asia (2013-2015).

[12] Ibid.

[13] Robert K. Ackerman, "Perils to Asia-Pacific Networks Lie Within," AFCEA Signal (blog), entry posted November 19, 2015, accessed December 8, 2015, http://www.afcea.org/content/?q=Article-perils-asia-pacific-networks-lie-within.

[14] Lang and Westphal, "Conducting Operations in a Mission," 45.

[15] Christina Hicks, Ernest Jenkins, and Dave Waller, "Viewpoint: The Network of the Future Is Needed Now." AFCEA Signal (blog), entry posted December 1, 2015, accessed

December 8, 2015, http://www.afcea.org/content/?q=Article-viewpoint-network-future-needed-now.

[16] Lang and Westphal, "Conducting Operations in a Mission," 45; Chad C. Serena et al., *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network* (Santa Monica, CA: RAND, 2014), 3.

[17] Lang and Westphal, "Conducting Operations in a Mission," 45.

[18] Serena et al., *Lessons Learned from the Afghan*, 3.

[19] Lang and Westphal, "Conducting Operations in a Mission," 45.

[20] Serena et al., *Lessons Learned from the Afghan*, 4.

[21] Lieutenant General Mark S. Bowman, *Future Mission Network Study Report* (Norfolk, VA: U.S. Department of Defense Joint Staff J6, 2012), 16.

[22] Serena et al., *Lessons Learned from the Afghan*, 5.

[23] Lieutenant General Mark S. Bowman, *Future Mission Network Study*, 16.

[24] Serena et al., *Lessons Learned from the Afghan*, 9.

[25] Sandra I. Erwin, "U.S. Central Command Leads Push to Connect Allies in Common Network," National Defense, September 2015, 21.

[26] Gary W. Blohm, *U.S. Army Network Operations Reference Architecture* (Washington, DC: U.S. Army CIO/G6, 2014), 16.

[27] Army Regulation (AR) 25-2, *Information Assurance*, 23 March 2009, 39.

[28] Ray Odierno, "Regionally Aligned Forces: A New Model for Building Partnerships," Army Live (blog), entry posted March 22, 2012, accessed December 22, 2015, http://armylive.dodlive.mil/index.php/2012/03/aligned-forces/.

[29] "TODAY'S FOCUS: Regionally Aligned Forces," STAND-TO! (blog), entry posted December 20, 2012, accessed December 22, 2015, http://www.army.mil/standto/archive/issue.php?issue=2012-12-20.

[30] Wayne W. Grigsby, Jr. et al., "Mission Command in the Regionally Aligned Division Headquarters," Military Review 93, no. 6 (November/December 2013): 6.

[31] Odierno, "Regionally Aligned Forces: A New Model," Army Live (blog).

[32] Grigsby et al., "Mission Command in the Regionally," 6.

[33] Ibid., 5.

[34] Army Doctrine Publication (ADP) 6-0, Mission Command, 17 May 2012, 2-3. This document clearly reflects the Army's substantial combat experience in Iraq and Afghanistan, where commanders were routinely and independently responsible for wide geography and uncertain missions well outside of the doctrinal scope of their units. ADP 6-0 directly aims to build operational flexibility by tasking commanders to build trust and assume prudent risk at all levels: "Effective commanders understand that their leadership guides the development of teams and helps to establish mutual trust and shared understanding

throughout the force. Commanders allocate resources and provide a clear intent that guides subordinates' actions while promoting freedom of action and initiative. Subordinates, by understanding the commander's intent and the overall common objective, *are then able to adapt to rapidly changing situations and exploit fleeting opportunities* [emphasis added]." (page 2).

[35] Ibid., 3.

[36] Ibid.

[37] Ibid., 9.

[38] Grigsby et al., "Mission Command in the Regionally," 7.

[39] Ibid.

[40] Author's own experience while implementing Installation as a Docking Station (IADS), Host Based Security System (HBSS), and Assured Compliance Assessment Solution (ACAS) on U.S.-only networks under U.S. Army mandate from 2013-2015 at I Corps Headquarters. See also Blohm, *U.S. Army Network Operations*, 14-15.

[41] George L. Seffers, "Information Flows at Pacific Command's Synchronization Hub," AFCEA Signal (blog), entry posted November 1, 2015, accessed December 22, 2015, http://www.afcea.org/content/?q=Article-information-flows-pacific-command%E2%80%99s-synchronization-hub.

Bibliography

Ackerman, Robert K. "Perils to Asia-Pacific Networks Lie Within." AFCEA Signal (blog). Entry posted November 19, 2015. Accessed December 8, 2015. http://www.afcea.org/content/?q=Article-perils-asia-pacific-networks-lie-within.

Army Doctrine Publication (ADP) 6-0, *Mission Command*, 17 May 2012.

Army Regulation (AR) 25-2, *Information Assurance*, 23 March 2009.

Blohm, Gary W. *U.S. Army Network Operations Reference Architecture*. Washington, DC: U.S. Army CIO/G6, 2014.

Boardman, Jill L., and Donald W. Shuey. "Combined Enterprise Regional Information Exchange System (CENTRIXS): Supporting Coalition Warfare World-Wide." Air War College Gateway to the Internet. Last modified April 2004. Accessed December 8, 2015. http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf.

Bowman, Mark S. (Lieutenant General, U.S. Army) Future Mission Network Study Report. Norfolk, VA: U.S. Department of Defense Joint Staff J6, 2012. Report in author's possession.

Erwin, Sandra I. "U.S. Central Command Leads Push to Connect Allies in Common Network." National Defense, September 2015, 20-21.

Grigsby, Wayne W., Jr., Patrick Matlock, Christopher R. Norrie, and Karen Radka. "Mission Command in the Regionally Aligned Division Headquarters." Military Review 93, no. 6 (November/December 2013): 3-9.

Hicks, Christina, Ernest Jenkins, and Dave Waller. "Viewpoint: The Network of the Future Is Needed Now." AFCEA Signal (blog). Entry posted December 1, 2015. Accessed December 8, 2015. http://www.afcea.org/content/?q=Article-viewpoint-network-future-needed-now.

Lang, Thomas C., and Martin M. Westphal. "Conducting Operations in a Mission Partner Environment." Joint Force Quarterly, no. 74 (July 2014): 44-49.

Odierno, Ray. "Regionally Aligned Forces: A New Model for Building Partnerships." Army Live (blog). Entry posted March 22, 2012. Accessed December 22, 2015. http://armylive.dodlive.mil/index.php/2012/03/aligned-forces/.

Rumsfeld, Donald H. *Quadrennial Defense Review*. Washington, DC: U.S. Department of Defense, 2001.

Rumsfeld, Donald H. *National Defense Strategy*. Washington, DC: U.S. Department of Defense, 2005.

Rumsfeld, Donald H. *Quadrennial Defense Review*. Washington, DC: U.S. Department of Defense, 2006.

Seffers, George L. "Information Flows at Pacific Command's Synchronization Hub." AFCEA Signal (blog). Entry posted November 1, 2015. Accessed December 22, 2015. http://www.afcea.org/content/?q=Article-information-flows-pacific-command%E2%80%99s-synchronization-hub.

"TODAY'S FOCUS: Regionally Aligned Forces." STAND-TO! (blog). Entry posted December 20, 2012. Accessed December 22, 2015. http://www.army.mil/standto/archive/issue.php?issue=2012-12-20.

Wills, David R. *Mission Networks: An Evolution in Information Sharing*. Carlisle, PA: U.S. Army War College, 2012.