Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,Arroyo Center,1776 Main Street, PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**41**	

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

Research Report

Lessons Learned from the Afghan Mission Network

Developing a Coalition Contingency Network

Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, Bradley Lossing

RAND CORPORATION

Research Report

Lessons Learned from the Afghan Mission Network

Developing a Coalition Contingency Network

Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, Bradley Lossing

Prepared for the United States Army

ARROYO CENTER

The research described in this report was sponsored by the United States Army under Contract No. W74V8H-06-C-0001.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN 978-0-8330-8511-5

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA

CAMBRIDGE, UK • BRUSSELS, BE

www.rand.org

Preface

The objectives of this brief report are to describe the development and evolution of the Afghan Mission Network (AMN) and to discuss the challenges and opportunities that the U.S. military in general and the U.S. Army in particular (as the largest component of U.S. land forces) face as they pursue the creation of a deployable, tailored, and mission ready future coalition contingency network.[1] The history of AMN provides invaluable experiential data on the development of a mission-centric operational network. Perhaps more importantly, it also yields tactical, operational, and policy-relevant lessons that can inform future efforts—such as the Joint Staff's Mission Partner Environment (MPE) (formerly, Future Mission Network or FMN) initiative—to create a contingency network that is both effective across the range of military operations and useful to a host of military and nonmilitary partners.

The findings presented in this report are informed by a literature review, presentations, and briefings generated by the agencies involved in creating and maintaining the AMN, and information gleaned from interviews with numerous subject matter experts representing organizations involved in the development of the AMN. We identified three key takeaways from this study, with the second and third supporting the first: (1) a common mission network will likely be needed in every region where the United States conducts coalition operations, including each Geographic Combatant Command (GCC); (2) the Army should establish a persistent capacity for testing and validation of coalition network capabilities and equipment; and (3) appropriate requirements documents should reflect the information-sharing needs associated with ubiquitous coalition operations.

The research reported here was sponsored by the Army Chief Information Officer/G-6, and conducted within RAND Arroyo Center's Force Development and Technology Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center sponsored by the United States Army. Questions and comments regarding this research are welcome and should be directed to either the leaders of the research team, Isaac Porche (porche@rand.org) and Joel Predd (jpredd@rand.org), the lead author, Chad Serena (cserena@rand.org), or the director of the Force Development and Technology Program, Christopher Pernin (pernin@rand.org).

The Project Unique Identification Code (PUIC) for the project that produced this document is RAN116198.

[1] We use the term "coalition contingency network" to refer to any network developed to support coalition operations occurring during a contingency.

For more information on RAND Arroyo Center, contact the Director of Operations (telephone 310-393-0411, extension 6419; fax 310-451-6952; email marcy_agmon@rand.org), or visit Arroyo's website at http://www.rand.org/ard/.

Table of Contents

(This page is intentionally blank.)

Figures

(This page is intentionally blank.)

Tables

(This page is intentionally blank.)

Summary

This report discusses key lessons learned from the development and evolution of the Afghanistan Mission Network (AMN) and the lessons born of this effort that are of relevance to the development of future coalition contingency networks. Increasingly, U.S. military operations depend on the support of coalition partners and the networks, like the AMN, that link them. The AMN, a coalition (NATO) funded, sustained, and maintained initiative, was implemented in 2010 and was created as a common network from a collection of national and NATO networks. The AMN is now the primary Coalition, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C5ISR) network in the Afghanistan Combined Joint Operations Area (CJOA-A). By providing a common network[2] over which to share critical information, the AMN enabled a shift in information-sharing posture from "need to know" to "need to share," resulting in an increase in situational awareness (SA) among International Security Assistance Force (ISAF) partners. The end result of this effort has been greater situational understanding and serves as an object lesson in how to approach coalition networking. Although the AMN is not an end-state, it provides valuable concepts and processes for future similar efforts.

OEF, ISAF, and Timeline

The following timeline (Table S.1) shows the major events that shaped the evolution of the AMN. It is critical to analyze the AMN in the context of ISAF's progressively expanded mission. Our analysis fully takes this into account and evaluates the AMN from operational *and* technical perspectives. We determined that the AMN represents not only the physical communications network but also the operational context that drove network requirements and shaped the coalition's approach to developing the network. Each of these elements of the AMN's origin and evolution has important implications, discussed in subsequent chapters, on the development of future coalition networking efforts.

Methodology

The findings presented in this report are based upon the study team's literature review, multiple site visits (including visits to operations centers in Afghanistan), presentations and briefings generated by the agencies involved in creating and maintaining the AMN (including

[2] We define a "common mission network" as a federation of partially self-governing networks that share data and data storage and have agreed to follow pre-established interoperability standards allowing real-time exchanges of information supporting shared situational awareness.

Table S.1
OEF, ISAF, and AMN Timeline

Year	Key Operational Events	Key AMN Events
2001	• OEF commences • Taliban ousted • Republic of Afghanistan Established	
2003	• NATO assumes ISAF leadership • ISAF's mandate expanded beyond Kabul	
2004	• ISAF expands into Northern Afghanistan	
2006	• ISAF expands to Western Afghanistan • ISAF expands to Southern Afghanistan • ISAF expands to Eastern Afghanistan	• Mail exchange between US CENTRIXS GCTF and ISAF-S • UK Overtask interoperability initiative
2008	• GEN David McKiernan assumes ISAF leadership • U.S. forces increased by 4,500	• Genesis of federated AMN concept at Qatar NETOPS conference
2009	• U.S. forces increased by 17,000 • U.S. forces increased by 4,000 • GEN Stanley McChrystal assumes ISAF command • U.S. forces increased by 30,000	• GEN McKiernan endorses AMN concept
2010	• NATO launches Operation Moshtarek in Helmand	• GEN McChrystal orders coalition information sharing on single network • Stryker Brigade moved onto AMN prior to deployment • AMN Initial Operational Capability achieved • US CIAV receives USCENTCOM J2 funding
2011		• 48 NATO and Partner Nations operating on AMN

NOTE: This timeline is based upon information gleaned from various sources listed in Appendix A: OEF, ISAF, and AMN Timeline.

U.S. and NATO institutions), and information gleaned from interviews and discussions with numerous subject matter experts and organizations involved in the development of the AMN.

Overview of the Report

This report is divided into three chapters. Chapter One provides a short history of OEF (Afghanistan) and describes the formation of ISAF. Chapter Two provides a short history of and key milestones in the development of the AMN. Chapter Three presents our analysis of the evolution of the AMN and what we consider to be key takeaways when considering the development of future coalition contingency networks.

Acknowledgements

We are extremely appreciative of the support and encouragement provided by our sponsor COL Anthony Howard SAIS-AOB and other CIO/G-6 staff including Lew Saunders, Bob Landry, and the late Curt Hellenbrand.

Personnel at Fort Hood's Central Technical Support Facility (CTSF) were very helpful and spent many hours providing information to our research team and sharing their insights with us. They include: Deon Stanfield, Robert Boerjan, Don Kirby, Langston Carter, Mike Moore, Bill Durham, and others.

DISA JTIC personnel at Fort Indian Head were equally helpful. They are: Jeff Phipps, Todd Rissinger, John Peterson, and MAJ Kevin Neuman. All of them work as part of the CIAV. At DISA MNIS, we thank Susan Eaton, James Day, Burhan Adam, Michael Byrne. Martin Gross (DISA PEO C3) also shared some insights with members of our team.

At PEO-C3T, we thank Jennifer Zbozny for her insight and input. At PEO-IEWS, we thank Dr. Richard Wittstruck. At NATO, we thank Cdr Howard Tweedie, Friedrich Gernot, and Torsten Graeber (NATO C3 Agency). They exchanged many email messages and phone calls with us. We also thank Rajeev Parekh (USDI BICES).

We are particularly grateful for the many subject matter experts in Kabul who gave freely of their time and candidly shared their observations and insights and supported our visit to Afghanistan. At USFOR-A J6, we thank COL Charles "Rusty" Baumgardner, LTC Charles D. Robinett, and MSG Alan Stanford. At Task Force 236, we thank CPT David Anderson, Paul Cralley, Juan Toves, and Larry Good. At ISAF HQ, we thank LTC Schonberg, MAJ Mitch Jackson, LCDR Andy Dittmer, and Jim Valentine. At IJC CJ6, we thank COL Vernon, LTC (U.K.) Gary Mason, Wing Cdr (U.K.) Ian Allen, MAJ Dan Zander, and CW2 Ada. At RC(E) CJ6, we thank LTC Kilgore and MAJ Schaefer. At RC(S) CJ6, we thank John Conniff. At RC(SW) CJ6, we thank LTC Baker, MAJ Wenn, and CPT Malone. At NTM-A CJ6, we thank COL William Gerhard. Last but not least, we thank the RAND and USFOR-A staff who helped with visit logistics ranging from taking care of the initial paperwork to providing lodging, transportation, and protection in theater: Patrice Lester, Natalie Ziegler, Maria Falvo, COL Charles Baumgardner, LTC Charles D. Robinette, MGySgt Norman, TSgt Steenwyk, and Sgt Haley.

Others providing insights included Dan Bradley (NSA), LTC (Ret.) Mark V. Hoyt, Jeremy Brady, Peter Morosoff, and LTC David Wills.

We thank our RAND colleagues who contributed their insights at various stages of our analysis. Specifically, we thank Chris Pernin, Ryan Brown, Myron Hura, and Paul Emslie. We also thank Michelle McMullen, who helped edit many versions of this document and provided administrative assistance in its preparation.

Finally, we would also like to thank our internal and external reviewers for their careful examination of our report and for their helpful recommendations.

Abbreviations

AMN	Afghan Mission Network
ANSF	Afghan National Security Forces
ATA	Afghan Transitional Authority
BCT	Brigade Combat Team
C2IEDM	Command and Control Information Exchange Data Model
C2IS	Command and Control Information Systems
C5ISR	Coalition, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCER	CENTRIXS Cross Enclave Requirement
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBLNet	Combined Federal Battle Laboratories Network
CIAV	Coalition Interoperability Assurance and Validation
C-IED	Counter-Improvised Explosive Device
CJOA-A	Combined Joint Operations Area (Afghanistan)
CCMD	Combatant Command
COIN	Counterinsurgency (Operations)
COP	Common Operational Picture
COSMOS-ACTD	Coalition Secure Management and Operations System-Advanced Concept Technology Demonstration
CTE2	Coalition Test and Evaluation Environment
CTSF	Central Technical Support Facility
DISA	Defense Information Systems Agency
FMN	Future Mission Network
GCC	Geographic Combatant Command
GCTF	Global Counter Terrorism Force
HADR	Humanitarian Assistance/Disaster Relief (Operations)
IA	Information Assurance
IOC	Initial Operational Capability
ISAF	International Security Assistance Force
ISAF-S	International Security Assistance Force Secret (Network Designation)

ISR	Intelligence, Surveillance, Reconnaissance
J3IEDM	Joint Command, Control, and Communications Information Exchange Data Model
JITC	Joint Interoperability Test Command
JMETC	Joint Mission Environment Test Capability
LC2IEDM	Land Command and Control Information Exchange Data Model
MEDEVAC	Medical Evacuation
MIP	Multinational Interoperability Programme
MPE	Mission Partner Environment
NATO	North Atlantic Treaty Organization
NATO CIS	NATO Communications and Information Services
NC3A	NATO Consultation, Command, and Control Agency
NCSA	NATO CIS Support Agency
NETOPS	Network Operations
NGO	Non-Governmental Organization
NIRIS	Networked Interoperable Real-Time Information Services
NSA	National Security Agency
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
RC	Regional Command
SA	Situational Awareness
SIGACT	Significant Activity
SIPRNet	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure
SVTC	Secure Video Teleconference (or –Conferencing)
TTP	Tactics, Techniques, and Procedures
UNAMA	United Nations Assistance Mission Afghanistan
UNSCR	United Nations Security Council Resolution
USAFRICOM	United States Africa Command
USCENTCOM	United States Central Command
USPACOM	United States Pacific Command
VOIP	Voice Over Internet Protocol

1. Operation Enduring Freedom (OEF) and the International Security Assistance Force (ISAF)

Operation Enduring Freedom (OEF) (Afghanistan) began in October 2001 and was initially conducted by a relatively small coalition of United States, United Kingdom, Australian, and Afghan (Northern Alliance) forces. Although OEF was broadly supported internationally and by the United Nations (UN), it did not receive its first international sanction until the December 2001 passage of UN Security Council Resolution 1386 (UNSCR 1386) at what has become known as the Bonn Conference. UNSCR 1386 gave the combined forces operating in Afghanistan international approval by authorizing a six-month deployment of what was termed the International Security Assistance Force for Afghanistan or ISAF.

ISAF's initial mission was relatively limited and included providing security for Kabul and its surrounding areas. But as the conflict in Afghanistan continued and as more nations and nongovernmental organizations (NGOs) began various assistance efforts in Afghanistan, ISAF's mission was expanded. UNSCR 1510 (2003) broadened ISAF's mandate to the entirety of Afghanistan. Per this and other relevant UNSCRs, ISAF was charged with assisting the Afghan government in establishing a safe and stable environment in urban centers and areas beyond Kabul. ISAF was also made responsible for supporting reconstruction and development projects designed to help the Afghan government cultivate institutions for good governance and in support of the rule of law.

To reflect its expanded role, the North Atlantic Treaty Organization (NATO) assumed leadership of ISAF in August 2003. Between 2003 and 2006, ISAF expanded its bases of operation throughout Afghanistan—first to the north, then to the west and south, and finally to the east. As ISAF's geographical footprint expanded and as it added more and more members and partnered with more and more organizations, its operations became radically more complex. Initially, ISAF consisted of roughly 5,000 troops and focused on operations in and near Kabul. By 2010, ISAF consisted of well over 100,000 troops representing 48 countries (including all 28 NATO countries) and interacted with innumerable NGOs and Afghan partner institutions throughout the whole of Afghanistan.[3]

Since its inception, ISAF has been led by 15 different commanders from seven different countries and has conducted missions across the range of military operations including, but not limited to, humanitarian assistance, stability operations, counterinsurgency operations, and combat operations. Presently, ISAF's mission is focused on conducting a number of military and nonmilitary missions in support of the Afghan government:

[3] This discussion of ISAF's role in Afghanistan is based in part on NATO's history of ISAF, as recounted at http://www.isaf.nato.int/history.html.

In support of the Government of the Islamic Republic of Afghanistan, ISAF conducts operations in Afghanistan to reduce the capability and will of the insurgency, support the growth in capacity and capability of the Afghan National Security Forces (ANSF), and facilitate improvements in governance and socio-economic development in order to provide a secure environment for sustainable stability that is observable to the population.[4]

[4] ISAF's mission is available at http://www.isaf.nato.int/mission.html.

2. The Afghan Mission Network (AMN)

As ISAF's mission, geography, operations, and partners expanded, so too did its networking and network support needs. Although never simple, the architecture, equipment, personnel, governance, and data-sharing and integration requirements necessary to effectively support ISAF's diverse operations became much more complex as ISAF added partners and took on additional responsibilities commensurate with its expanded mission.

Prior to the 2005–2006 period—the time that ISAF's mission was expanded to cover all of Afghanistan—few concerted efforts were made to integrate all or even a large portion of ISAF's partner nation networks on one coherent and accessible Coalition, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C5ISR) network. Despite its ostensible utility, a common mission network for ISAF forces did not emerge. This was due to three intertwined factors: (1) individual countries' information and data-sharing practices remained relatively stovepiped; (2) traditional and long-standing security concerns trumped operational necessity; and (3) the difficulties associated with connecting disparate national and functional systems.[5]

In 2005 and 2006, ISAF's operational needs (chiefly the needs of the United States and the United Kingdom) took precedence over many of these factors and spurred an effort to establish shared services on a common network. This effort manifested in the United States instituting an email exchange service with other NATO nations and the UK creating a connection mechanism within the ISAF-Secret or ISAF-S network ensuring the interoperability of UK and NATO forces on a common core network. These initiatives demonstrated the feasibility and potential utility of establishing a common federated network that could enable information sharing for all of ISAF's partners.

Despite accelerating operational requirements for information sharing and some efforts toward enhanced data-sharing among a growing (and changing) coalition, a true coalition network did not begin to emerge until the 2008–2010 timeframe.[6] The first major step in the development of a network to fully support ISAF's expanded operational scope occurred in 2008 at a USCENTCOM Network Operations (NETOPS) conference held in Qatar. It was at this

[5] Prior to the advent of the AMN, the regional commands, or RCs, and mission partners were using four primary networks: the Secret Internet Protocol Router Network (SIPRNet); Combined Enterprise Regional Information Exchange System–Global Counterterrorism Force (CENTRIXS-GCTF); ISAF-Secret; and NATO-Secret. Using these various networks resulted in fragmented mission command. CENTRIXS-GCTF was an early means of limited data-sharing (via email and voice over internet protocol or VOIP). According to Wills (2012), the initial realization of the AMN was born from an isolated version of CENTRIXS-GCTF, with non-OEF partners like Russia "pruned" from the resulting network.

[6] Of particular import was the intelligence-driven nature of the COIN fight, which necessitated, both operationally and technically, more than just "core network services."

conference that a number of participants acknowledged the mission-related and network-related challenges that ISAF faced and proposed the AMN concept as the solution. This meeting produced the following critical observation:

> If you need to do your mission with unstructured data, running it through guards will break your sharing AND doesn't even make for effective risk mitigation. Don't use guards if you want robust sharing with NATO. [Instead] turn GCTF in Afghanistan into CENTRIXS-ISAF[7] so the CENTRIXS-to-NATO ISAF boundary is no longer a cross-domain boundary. Make CENTRIXS-ISAF the primary mission network and try to move U.S. users onto that network for the Afghanistan mission.[8]

In early 2009, GEN David McKiernan, then the commander of ISAF, concurred with the conference's findings and approved the process that led to the development of the AMN.[9]

The second major step in the development of the AMN corresponded with GEN Stanley McChrystal's assumption of ISAF command. Expanded and more complex operations, coupled with the increased rotation of U.S. forces, prompted GEN McChrystal to establish an ISAF-wide requirement for each partner nation to share data on the AMN. GEN McChrystal—and many others—had noted that as ISAF's mission evolved, information-sharing limitations were having a significant effect on operational efficacy and force protection.[10]

Accordingly, policies and procedures that reinforced a "need-to-know" culture needed to be replaced with policies and procedures emphasizing a "need-to-share," so that ISAF could collectively leverage disparate coalition data and populate common operational pictures (COPs) in a timely fashion. In other words, ISAF needed a network that was premised on common mission requirements. Operational necessity combined with guidance provided by McKiernan and McChrystal led to the full implementation of the AMN.

The AMN began as a network for facilitating fairly commonplace human-to-human exchanges and included the following basic services:

- Chat
- Voice over internet protocol (VOIP) telephone connectivity
- Email
- Web browsing
- Secure video teleconferencing (SVTC)

---

[7] CENTRIXS is the Combined Enterprise Regional Information Exchange System.

[8] This observation, which reflects a consensus of a number of key conference participants that the study team had the opportunity to speak with, marked the conceptual origin of a federated network operating on a single-classification level.

[9] Memorandum to Commander (2009).

[10] GEN David Petraeus emphasized similar points. He recognized that mission data were not being shared as efficiently or effectively as required. In response, he recommended a paradigm change, focusing on net-enabled and command-centric data delivery.

Over time, it evolved to become the primary C5ISR system in Afghanistan, consisting of the ISAF-S core and each of the participating nations' national extensions (e.g., CENTRIXS-ISAF—US; CAESAR—Italy; OVERTASK—UK; LCSS—Canada; and so forth). Other battlespace awareness features, like the sharing of significant activity reports or SIGACTS and friendly force tracking exchanges across COPs, have been added over time.

The AMN is now a federated network. It provides connectivity and allows for information sharing among all participating ISAF countries over a common secret network. Data are organized around agreed upon "mission threads"[11] that individually and collectively comprise the types of missions conducted throughout Afghanistan. ISAF employs eight of these mission threads in Afghanistan and on the AMN: Battlespace Awareness, Joint Fires, Joint ISR, MEDEVAC, C-IED, Freedom of Movement, Force Protection, and Service Management.

Although the framework and capabilities that comprise the AMN were implemented in a relatively short period (between 2008 and 2010), standing up the AMN has not been without its challenges, including:

- **Policies, procedures, and governance.** Establishing common policies, procedures and governance for information sharing among a 40-plus country coalition within the context of an already functioning network of systems.[12]
- **Manifold interoperability challenges.** One of the challenges faced in developing the AMN affects the development of all coalition networks: layers of interoperability. Layers of interoperability range from the organizational to the technical domains. Interoperability spans political objectives, harmonized strategy/doctrines, aligned operations, aligned procedures, knowledge/awareness, information interoperability, data- or object-model interoperability, protocol interoperability, and physical interoperability.[13] This challenge was fully exposed during the development of the AMN as operations and intelligence interoperability needs clashed with the network's preexisting constructs and physical interoperability requirements. The Coalition Secure Management and Operations System (COSMOS) Advanced Concept Technology Demonstration (ACTD) was one of many efforts that attempted to reduce the information-sharing and interoperability difficulties faced in Afghanistan. Although not ultimately successful in

[11] Mission threads are also referred to as mission areas. The concept of mission threads, in addition to providing foci for data structuring, represent communities that are readily understood and accepted by coalition participants. A mission thread is defined as an "operational description of end-to-end activities that accomplish the execution of a mission. Mission Types and Tasks provide the Operational Mission Area context for the development of complete end-to-end Mission Thread architectures that will also describe the Information Products, User Applications and Technical Services required to successfully execute a Mission Thread from end-to-end." (NATO, 2012, p. 17) Sharing with others within a mission thread is a good intermediate step between need-to-know and need-to-share—sharing still occurs but is defined by mission considerations as opposed to nation or service.

[12] CENTRIXS-GCTF was used to develop the AMN (Wills, 2012).

[13] Tolk and Muguira (2003).

this regard, experiences with COSMOS ACTD helped inform the concept of the AMN and influenced its evolution.[14]

- **Integration.** COP integration challenges posed by data that were expressed in multiple languages, intended for particular echelons of command, or were of differing levels of classification.[15]
- **Standardization.** Standardization, protocol, and formatting challenges to operational and incident reporting and visualization.[16]

How the AMN evolved and the challenges that were overcome in its establishment demonstrate that developing a coalition mission network is truly much more than a technical or materiel problem, and that doctrine, leadership, training, and planning processes all have bearing on how a network should be constructed and on how it actually operates.

No fewer than 48 coalition partners demonstrated interest and willingness in developing the AMN, and through their concerted efforts many long-standing policy barriers militating against the establishment of a coalition network were broken down.[17] Despite, or perhaps because of, the

---

[14] For a discussion of COSMOS ACTD, see Slaybaugh (2009), pp. 10–12.

[15] One effort to bridge the gaps between the various domains in the ISAF network involved the use of cross domain solution or CDS systems. This was problematic. Although effective when rule sets for data formatting and structure are established and recognized, CDS have limited utility when data or information is unstructured. But data-sharing in a collaborative environment, particularly data which lends itself to better situational awareness (SA), tends to leverage unstructured data/information that is contextually rich (e.g., PDF and Microsoft Word files, which are not filtered properly by CDS despite being formats widely used for information-sharing purposes). Given the almost infinite ways of structuring data and various means of transmitting data in a coalition environment, CDS are currently and will likely in the future be effective only for limited applications. Past efforts by DISA to use CDS to enable seamless cross enclave sharing include the Coalition Cross Enclave Requirement effort (CCER). This initiative sought to collapse coalition networks into a single network, starting with CENTRIXS-GCTF and CENTRIXS-MCFI. The progress/success of this initiative remains unclear. Corrin (2010) reports that the "Centrixs Cross-Enclave Requirement contract for replacement of the Trusted Network Environment is on hold pending analysis." Quoting DISA and USPACOM (2011): "Based on FY2011 Congressional budget cut, ASD/NII, DISA, Joint Staff J6 and USPACOM J6 decided to terminate CCER Phase I operation by 15 February 2011(ref f) and declared strategic pause for CCER Phase II. Direction included terminating Phase I early…"

[16] This led to the development and modification of tools like Networked Interoperable Real-time Information Services (NIRIS) and the evolution of the Multinational Interoperability Programme (MIP). NIRIS was initially a solution to strategic-level commanders' requests to view air track data in the Bosnia theater of operations in 1994 but has evolved into a more nuanced system providing, principally, air track data feeds to the ISAF COP. See, Bayer (2005), p. 52. The MIP was established by the project managers of the Army Command and Control Information Systems (C2IS) of Canada, France, Germany, Italy, the United Kingdom, and the United States in 1998. The aim of the MIP was and is to achieve interoperability of C2IS at all echelons of command. MIP "solutions" include specifications and standard operating procedures (SOP) that enable information exchange among coalition partners. Progressively, the MIP baseline has evolved from the Land C2 Information Exchange Data Model (LC2IEDM), through the C2 Information Exchange Data Model (C2IEDM), and into the Joint C3 Information Exchange Data Model (JC3IEDM). See discussion in NATO (2007), pp. xxiii–xxv.

[17] It is important to note that the collaboration that took place in the development of the AMN and afterward was in many ways a product of the trust engendered by long-standing working relationships. Trust and collaboration mutually reinforce one another. In terms of the AMN, each is reflected in the development of shared tactics, techniques, and procedures (TTP), in the development of shared protocols, policies, and procedures, and in the actual sharing of data and information.

challenges faced in developing the AMN, a number of important opportunities were revealed, each of which is instructive for establishing future coalition contingency networks. ISAF established commonly accepted mission threads that can guide future operational planning and execution and can help facilitate horizontal and vertical data exchange among coalition partners. Additionally, NATO, the UN, and U.S. Combatant Commands (CCMDs) beyond USCENTCOM witnessed the value and potential of coalition networking. Lessons were learned that hopefully will not have to be relearned in future efforts. Even if the AMN does not provide a comprehensive or necessarily specific roadmap for the establishment of a future coalition contingency network, many of the countries involved in its genesis and evolution undoubtedly now share a common understanding of the value of creating such a network. The evolution of the AMN not only yields important lessons in this regard, it also serves as an experiential reference point that will likely shape future efforts, understandings, and expectations.

(This page is intentionally blank.)

3. Toward a Coalition Contingency Network

Our examination of the AMN yields three valuable observations. First, enhancing collaboration among partner nations and enabling interoperability on the AMN required relaxing various security constraints that slowed the transfer and/or accessibility of mutually beneficial data and precluded sharing of SA-related information. ISAF participating nations had to ease prevailing "need-to-know" restrictions in order to substantiate a "need-to-share" culture. In other words, achieving mission assurance required higher levels of collaboration, which in turn required changing information assurance (IA) standards. The inherent tradeoff between collaboration and information assurance is captured in Figure 3.1. The relationship between collaboration and mission assurance is captured in Figure 3.2.

This problem is not unique to Afghanistan or the AMN. Indeed, it pervades many collaborative information-sharing efforts, particularly those where IA *or* collaboration is at a premium, such as during humanitarian assistance and disaster relief (HADR) efforts.[18] It stands to reason that this kind of tradeoff will be encountered in the development of future coalition contingency networks. This should be acknowledged and, if possible, mitigated through pre-established policies and conventions for IA and collaboration in future coalition networks.

The second observation is that the utility of the AMN must be understood within the context of commonly agreed upon, developed, and tested mission threads.[19] Mission threads provided the baseline for the data organization, sharing, and analysis at the center of the AMN.[20] These, and other commonly defined and understood mission threads, should be used to guide the development of future coalition data-sharing enterprises.

The third observation is that extra-theater testing, assurance, and validation efforts like those conducted by the Joint Interoperability Test Command's (JITC) Coalition Interoperability Assurance and Validation (CIAV) program enable controlled network experimentation and testing pursuant to network solutions that can later be replicated in theater. CIAV's initial task was to help enable mission-based operational information dissemination and interoperability within the AMN construct. Its mission-based execution process provided for a rapid mission-based assurance and validation methodology for immediately addressing identified war-fighting gaps. This process was eventually shared with USCENTCOM. This set the foundation for subsequent assessments of war-fighting technologies prior to their introduction and operational fielding into the AMN enterprise. CIAV presently reviews all technology upgrades and

[18] See the discussion of IA and collaboration during post-Hurricane Katrina operations in Porche et al. (2008).

[19] Much of this process was conducted at Fort Indian Head, Maryland and at Fort Hood, Texas.

[20] For an extended discussion of the process of technology transition and change management, see Rissinger (2009).

Figure 3.1
Inherent Tradeoffs in Information Sharing

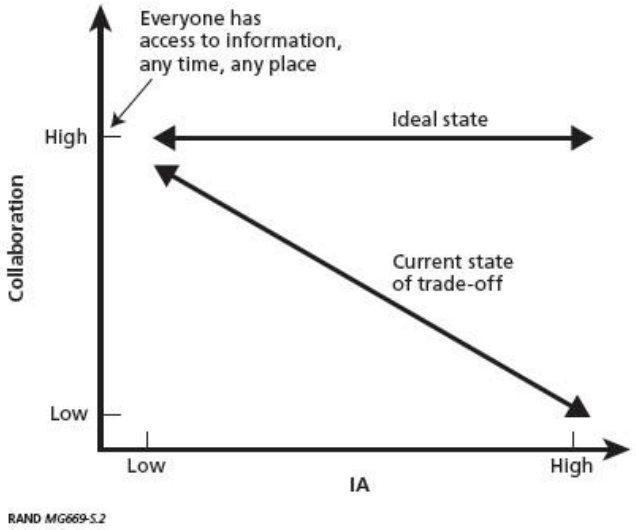
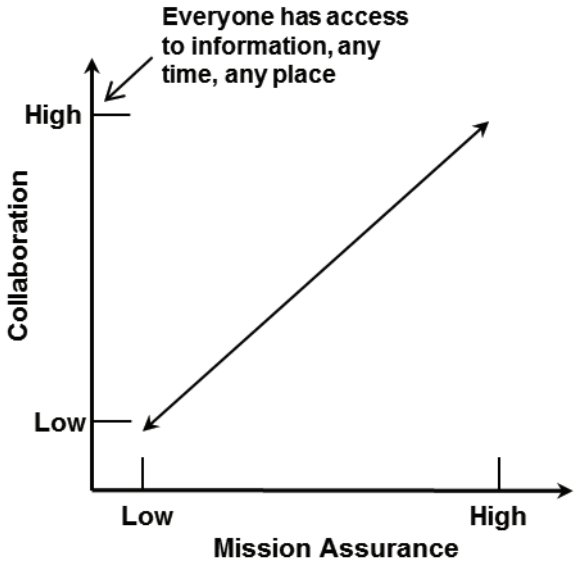


Figure 3.2
Collaboration and Mission Assurance



integration efforts prior to their fielding into the AMN.[21] A turning point in the functional development of the AMN occurred after the creation of a cooperative theater-laboratory engagement process. This cooperation had two substantial and notable effects: (1) it freed warfighters to continue with the conduct of their various missions; and (2) it leveraged expertise and systems that might not necessarily be available in theater. Leveraging laboratories—like CIAV—prior to, during, and after the construction of coalition contingency networks can substantially reduce the time, resources, and energy devoted to developing and managing the network "in-theater." Such strategic engagement can help to ensure that those personnel involved in administering the functions and/or operation of the network can be freed to focus on more pressing mission-essential tasks.

Key Takeaways

From our analysis, we suggest three key takeaways for the development of future coalition contingency networks (the second and third are subordinate to and support the first one). Each is premised on the principal lessons of the AMN that can be abstracted to similar efforts.

A common mission network will likely be needed in every region where the United States conducts coalition operations.

The emerging regionally aligned force concept will pair Brigade Combat Teams (BCTs) with each of the six GCCs, such as U.S. Africa Command (USAFRICOM) or U.S. Pacific Command (USPACOM). Each BCT will be responsible for, among other things, establishing new and/or deepening existing relationships with coalition partners. One of the principal lessons learned from OEF (Afghanistan) and other recent experiences[22] is that a common mission network is vital to successful mission-oriented collaboration and coordination. Establishing this kind of network can be challenging and time-consuming. Therefore, planning for future mission networks within each GCC should begin as soon as possible—i.e., in advance of any future contingency or conflict. This planning must consider the history of and lessons learned from the formation of the AMN, both of which are detailed in this report.

In each of the GCCs, a single common mission-centric network should be created. A single common mission-centric network will not only reduce costs, it will also alleviate many of the

[21] This includes the efforts of other laboratories and testing networks such as the Combined Federal Battle Laboratories Network (CFBLNet), CTE2 (Coalition Test and Evaluation Environment), the Joint Mission Environment Test Capability (JMETC), and the Army's Central Technical Support Facility (CTSF), among others.

[22] Recent exercises in Jordan—dubbed Eager Light—highlight the utility of establishing coalition mission networks. This joint-partnered exercise in Amman, Jordan is an annual event that brings together the U.S. and Jordanian militaries. At the 2012 event, the U.S. 1st Armored Division, the Combined Joint Task Force, and the Jordanian Armed Forces shared a COP of the ground situation, which included tracking refugee flows. Independent of this exercise, a number of U.S. troops, to include U.S. Army special operations forces, are in Jordan today as a result of ongoing events in Syria. This exercise and the actual deployment of forces are narrow but instructive examples of how and why common mission networks should be developed. See Associated Press (2012); Cutohin (2012), p. 9; and Baldor and Jelinek (2012).

technical and operational data-sharing problems that initially plagued ISAF's operations in Afghanistan and that are inherent to all coalition networks. Regardless of the contingency, mission, or coalition assembled, coalition partners will arrive "as they are," meaning that the equipment they possess and security protocols they follow will differ from those of the U.S. military and/or other potential partners. The history of the AMN suggests that in order to quickly develop a single mission-centric network, participating nations will, at a minimum, have to establish the joining instructions, governance, and standards necessary for the network's functioning prior to its operationalization.[23]

A challenge for a future mission network will be to design a one-size-fits-all system for all theaters or GCCs. This is due to the likelihood that each theater or GCC may present its own unique partners and information exchange requirements.[24] However, this challenge could be ameliorated by the study's second takeaway.

The Army should establish a persistent capacity for testing and validation of coalition network capabilities and equipment.

CIAV and other similar organizations' experience in the development of the AMN are instructive in this regard: any dynamic coalition network (i.e., one whose mission will evolve and one whose partnerships will change) will require continuous and progressive testing and validation with joint/coalition partners throughout the life of the coalition and/or its mission. This will likely require standing as well as ad hoc organizations that can work intra- and extra-theater to preempt or solve problems in parallel to operations and in synchronization with operational needs.

Appropriate requirements documents should reflect the information-sharing needs associated with ubiquitous coalition operations.

Regardless of the contingency, it is very unlikely that the U.S. military will engage in future missions absent a coalition of partners. It follows that U.S. network needs will also be coalition network needs. No future coalition network can be established in isolation and instead will require close collaboration and interoperability with mission partners—a fact not addressed in legacy or forthcoming Army requirements documents. The study team recommends that future requirements documents duly recognize these needs.

Conclusion

Prior to the AMN, USCENTCOM operated on four different mission networks in Afghanistan.[25] Now, USCENTCOM operates on one federated network in Afghanistan, the

[23] This will help to facilitate collaboration and trust among potential and actual partners.

[24] Wills (2012).

[25] U.S. SIPRNet, CENTRIXS-GCTF, ISAF-Secret, NATO Secret.

AMN. Although operations in Afghanistan will be pared substantially in the near future, the lessons learned by ISAF and through the development of the AMN will be enduring. And while future contingencies and the coalition partners participating in these contingencies cannot be effectively predicted, the types of networking challenges they will face most certainly can. The solutions to these challenges, many of which were engendered throughout the course of the AMN's maturation, should be no less than a partial prologue to the development of any future coalition contingency network.

(This page is intentionally blank.)

Appendix A: OEF, ISAF, and AMN Timeline

The following timeline highlights key events in the progression of OEF, the development and expansion of ISAF, and the evolution of the AMN. This timeline substantiates the timeline presented in the report summary.

2001

- The United States (US), United Kingdom (UK), Australia, and Afghan Northern Alliance launch OEF with the goals of removing the Taliban regime, destroying al-Qaeda and its operational capacity in Afghanistan, and creating a democracy.
- Passage of UNSCR 1386. ISAF is created (a three-way partnership between the Afghan Transitional Authority (ATA), the United Nations Assistance Mission Afghanistan (UNAMA), and ISAF) through the Bonn Conference and begins operations in and near Kabul, Afghanistan (International Security Force Afghanistan, undated (a)).
- Taliban is ousted in the weeks following the initial invasion.
- Islamic Republic of Afghanistan is created and an interim government established (BBC News, 2012).

2003

- NATO assumes leadership of the ISAF mission and forces.
- UN Security Council Resolution 1510 (UNSCR 1510) expands ISAF's mandate to the entirety of Afghanistan (United Nations Security Council, 2003).

2003–2004

- ISAF expands the mission into the northern areas of Afghanistan (International Security Force Afghanistan, undated (a)).

2005–2006

- ISAF expands the mission into the western and southern areas of Afghanistan (International Security Force Afghanistan, undated (a)).
- ISAF expands the mission into the eastern areas of Afghanistan and effectively to the entire country (International Security Force Afghanistan, undated (a)).
- Creation of mail exchange between CENTRIXS GCTF (US) and ISAF-S (C4I Technology News, 2011).

- OVERTASK (UK) interoperability initiative in Regional Command (RC) South and Helmand Province (C4I Technology News, 2011).

2008

- General David McKiernan assumes command of ISAF forces.
- U.S. forces increased by 4,500 (BBC News, 2012).
- NATO funded effort to provide voice, chat, and Web access over OVERTASK (UK) (C4I Technology News, 2011).
- Participants in the Qatar NETOPS Conference propose to USCENTCOM J6 a network architecture in Afghanistan with permissive sharing policies in a common mission environment on a common mission network.

2009

- U.S. forces increased by 17,000 (BBC News, 2012).
- U.S. forces increased again by 4,000 (BBC News, 2012).
- General Stanley McChrystal assumes command of ISAF forces.
- U.S. forces increased by 30,000 (BBC News, 2012).
- Increase in U.S. force rotation to Afghanistan (BBC News, 2012).
- McKiernan endorses AMN concept (Memorandum to Commander, 2009).
- Gaps identified and specified in information sharing of partner nations.
- AMN begins to emerge as CENTRIXS is connected to ISAF-S (Collins, 2010).
- U.S. CIAV receives U.S. Central Command (USCENTCOM) J2 Funding (CIAV Management Group, 2012).

2010

- NATO launches Operation Moshtarak in Southern Helmand Province (BBC News, 2012).
- McChrystal requires each coalition nation to share information on a single information infrastructure (Miles, 2011).
- Coordinated and independent efforts by ISAF; NATO CIS Support Agency (NCSA); NATO Consultation, Command, and Control Agency (NC3A); USCENTCOM; U.S. Defense Information Systems Agency (DISA); and others take place to support McChrystal's mandate (NATO, undated).
- Stryker brigade moved onto network prior to deployment (STAND-TO!, 2010).

- Governance for structures and framework of standards for introducing C5ISR systems (NATO, undated).
- AMN Initial Operational Capability (IOC) achieved (Kenyon, 2012).

2011

- 48 NATO and partner nations operating on AMN (Seffers, 2011).

(This page is intentionally blank.)

References

Associated Press, "US Sends Troops to Jordan to Help Deal with Syria Crisis," *The Guardian*, October 10, 2012. As of January 15, 2013: http://www.guardian.co.uk/world/2012/oct/10/us-troops-jordan-syria-crisis

Baldor, Lolita C., and Pauline Jelinek, "SecDef: U.S. Sends Troops to Jordan, *The Army Times*, October 10, 2012. As of January 15, 2013: http://www.armytimes.com/news/2012/10/ap-panetta-says-us-forces-sent-to-jordan-101012/

Bayer, Matthew E., *Analysis of Binary XML Suitability for NATO Tactical Messaging*, thesis, Monterey, Calif.: Naval Postgraduate School, September 2005.

BBC News, *Afghanistan Profile*, May 29, 2012. As of May 29, 2012: http://www.bbc.co.uk/news/world-south-asia-12024253

C4I Technology News, *Project Review: The Afghan Mission Network*, November 30, 2011. As of May 8, 2012: http://www.c4i-technology-news.blogspot.com/2011/11/project-review-afghan-mission-network.html

CIAV Management Group, "Coalition Interoperability Assurance & Validation (CIAV)," briefing slides, March 1, 2012.

Collins, Patricia S., "Coalition Network Reports for Duty," *Signal Online*, June 2, 2010. As of May 24, 2012: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2313&zoneid=296

Corrin, Amber, *DISA Moves to Eliminate Contract Redundancies*, December 13, 2010. As of May 30, 2012: http://defensesystems.com/Articles/2010/12/10/Montemarano-DISA-contract-news.aspx?Page=1

Cutohin, Ryan (Major), "'Warrior Diplomats' Participate in Exercise Eager Light," *The Frontline*, December 6, 2012. As of January 15, 2013: http://www.fortstewartfrontline.com/currentFrontLine/FLCurrentNews.pdf

Defense Information Systems Agency (DISA) and U.S. Pacific Command (USPACOM), "MNIS CCER Lessons Learned Version 1.5," April 13, 2011.

Hoyt, Mark, telephone communication with the author, May 22, 2012.

International Security Force Afghanistan, *About ISAF, History,* undated (a). As of May 3, 2012: http://www.isaf.nato.int/history.html

International Security Force Afghanistan, *About ISAF, Mission*, undated (b). As of May 3, 2012: http://www.isaf.nato.int/mission.html

Kenyon, Henry S., "NATO Focuses on the Bottom Line to Support Warfighters," *Signal Online*, September 2010. As of May 24, 2012: http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2378&zoneid=47

Memorandum to Commander, USCENTCOM*, AMN Requirements,* January 20, 2009.

Miles, Donna, *New Afghan Network Supports Coalition Sharing*, March 9, 2011. As of May 24, 2012: http://www.defense.gov/news/newsarticle.aspx?id=63080

NATO, *The Joint C3 Information Exchange Data Model (JC3IEDM Main)*, Greding, Germany: NATO, December 2007.

NATO, Headquarters Allied Command Ramstein, *The Afghanistan Mission Network*, undated. As of May 24, 2012: http://www.airn.nato.int/focus_areas/mjo/articles/mjo0310.htm

NATO, *C3 Classification Taxonomy*, May 1, 2012. As of February 3, 2013: http://www.ncia.nato.int/Opportunities/Documents/C3_Classification_Taxonomy_V0.95_Report.pdf

Porche, Isaac R. III, Elliot Axelband, Jeff Rothenberg, Joshua S. Caplan, and Bradley Wilson, *Extending the Army's Reach: Collaboration and Information Sharing in Diverse Environments,* Santa Monica, Calif.: RAND Corporation, MG-669-A, 2008. Not available to the general public.

Rissinger, Todd K., "Transforming the Process of Technology Transition: Standardizing Mission Focused; Capability Based Performance and Acquisition Strategies," September 2009.

Seffers, George I., "France Joins Afghan Mission Network," *Signal Online*, May 13, 2011. As of May 14, 2012: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2616&zoneid=316

Slaybaugh, Paul J., *A Business Case Analysis (BCA) of the One Box-One Wire (OB1) Joint Combined Technology Demonstration (JCTD)*, thesis, Monterey, Calif.: Naval Postgraduate School, March 2009.

STAND-TO!, May 14, 2010. As of May 24, 2012:
http://www.army.mil/standto/archive/2010/05/14/print.html

Tolk, Andreas, and James Muguira, "The Levels of Conceptual Interoperability Model," paper presented at Fall Simulation Interoperability Workshop, Orlando, Fla., September 2003.

United Nations Security Council, *UNSC Resolution 1510 (2003)*, October 13, 2003.

Wills, David, personal communication with the author, May 29, 2012.

Recent and likely future U.S. military operations depend on coalitions of foreign military and nonmilitary partners, and a coalition mission network is necessary to support those operations. The Afghan Mission Network (AMN) is the primary network for the International Security Assistance Force (ISAF) in Afghanistan, allowing the United States and its coalition partners to share information and data across a common Secret system. Many view the AMN as a successful enabler of coalition information sharing. It is thus critical that the Army understand the principal lessons of the development of this network as it plans to develop future coalition contingency networks. To this end, the Army Chief Information Officer/G-6 asked RAND Arroyo Center to provide an independent review and assessment of the operational and technical history of the AMN and to identify lessons learned for future coalition networks. The history of the AMN provides an example of how to develop information systems to support operational missions, but perhaps more important, it also yields tactical, operational, and policy-relevant lessons that can inform future efforts to create contingency networks that are both effective across the range of military operations and useful to a host of military and nonmilitary partners. This report presents findings drawn from interviews with key AMN developers and maintainers and the documentation they produced during the network's development.

ARROYO CENTER

www.rand.org

$14.95

ISBN-10 0-8330-8511-5
ISBN-13 978-0-8330-8511-5

RR-302-A