U.S. and Angolan airmen discuss unloading C-130J Super Hercules as part of African Partnership Flight with Angolan and Zambian air forces (U.S. Air Force/Benjamin Wilson)

Conducting Operations in a Mission Partner Environment

By Martin M. Westphal and Thomas C. Lang

We need innovation in how we operate—our ability to re-imagine the way we fight will determine if we succeed or fail.

—General Martin E. Dempsey
Chairman's Strategic Direction to the Joint Force

Martin M. Westphal is Vice Director of Command, Control, Communications, and Computers (C4)/Cyber, Joint Staff J6. Thomas C. Lang is Chief of the Interoperability and Integration Division, Joint Staff J6. This article is based on the Joint Staff J6, Director for C4/Cyber Future Mission Network 90-Day Study Report.

The joint force is undergoing a major cultural change. It is a fact that current and future operations will find the joint force organizationally and operationally integrated with allies, coalition members, interagency partners, intergovernmental and nongovernmental organizations, private volunteer groups, and private-sector partners. The days of each coalition member operating in defined areas and only on its respective national secret networks are over. Moving the coalition fight off of national secret networks to a tailored mission network in which all coalition members share and operate as equals is not only a major cultural shift but also a command and control (C2) force multiplier. Information-sharing bilateral agreements must transition to warfighting multilateral agreements on a single security domain allowing nations, including the United States, to bring their own equipment. To implement a Mission Partner Environment (MPE), the United States and its mission partners must repurpose materiel and nonmateriel capabilities used for training and operations today. MPE implementation increases combatant commander and component battlefield effectiveness and drives down costs through unity of effort.

The past decade of military operations has provided the Department of Defense (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. Furthermore, these operations were conducted with a diverse set of mission partners ranging from the familiar to the not so familiar. This multifaceted operational environment, coupled with the range of mission partners, demonstrates the need for commanders to possess a capability enabling unity of action.

Today's combatant commanders and their components require a warfighting capability that improves mission partner integration and interoperability and sets the conditions for integrated operations. Forged in the lessons learned from current operations, MPE is an operations-based construct providing the commander the agility to rapidly and decisively act, bringing to bear the unique capabilities and collective force of all to achieve mission success.

Past Is Prologue

In 2008, commanders noted that coalition forces in Afghanistan could not effectively communicate and share commander's guidance, mission information, and critical intelligence. Additionally, any networks that supported operations in Afghanistan tended to be nation-specific and not oriented to coalition data-sharing and enterprise mission execution. The net effect of these problems was increased risk to life, inefficient use of resources, and jeopardized mission accomplishment. From the U.S. perspective, many of these problems stemmed from the joint force standard: the requirement that American formations be led only by American commanders and the U.S. military propensity to use only the Secure Internet Protocol Router Network (SIPRNet) for warfighting operations. This operational framework resulted in a C2 structure that provided little to no ability for commanders to effectively combine U.S. and non-U.S. formations in the same battlespace or realize their full combat potential. Additionally, this arrangement prevented coalition battlespace owners from effectively leveraging key U.S. enablers that existed solely on SIPRNet, such as joint fires and intelligence, surveillance, and reconnaissance capabilities.

Prior to Afghanistan, operations with mission partners did not demand an open framework for greater information-sharing. For instance, operations in Iraq did not present a significant challenge for mission partner operations due to the relatively small number of partners, their assigned missions, and their familiarity with U.S. operations. Even at the peak of the surge in Operation *Iraqi Freedom* during 2007, the mission partner contribution was only 6 percent of the total personnel strength, and except for one specific area, all battlespace commanders were American. The one exception was in southern Iraq in the vicinity of Basra. The United Kingdom (UK) controlled this sector, and the unique military relationship between Washington and London helped to mitigate the friction caused by disparate C2 systems.[1] In this environment, the primary purpose for a mission partner network simply became a means for the United States to communicate with its mission partners but not a means to fight a true coalition fight. 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.

In Afghanistan, the mission partner dynamics dramatically changed. First, Afghanistan is a North Atlantic Treaty Organization (NATO) mission. Second, in comparison to the surge in *Iraqi Freedom*, the task organization for the coalition force for the 2010 Operation *Enduring Freedom* surge consisted of over 40 troop-contributing nations. The influx of coalition forces resulted in 27 percent of the total strength being non-American.[2] Third, many of the battlespace owners were not American. To realize the operational value of formations from the many contributing nations, commanders needed the flexibility to mix U.S. and non-U.S. formations down to the company level. These operational realities required a new way of thinking on how to share information and create the necessary unity of effort in theater. Simply put, the inability of commanders to speak with immediacy and share information equally with all mission partners inhibited the ability to rapidly direct U.S. and allied task forces. As the problem suggests, a single secure communication network became essential to the campaign objectives and priorities in Afghanistan. During 2008–2010, the Afghanistan Mission Network (AMN) became the International Security Assistance Force (ISAF) primary mission network. This network remains the primary C2 framework for mission partner operations in Afghanistan today.

Technically, the AMN is a federation of networks linked to a NATO core mission secret network, complying with Alliance security and information assurance policies. Information and data shared between AMN participants are organized to support agreed upon mission threads. AMN put all network users on a common mission network separate from its own national networks to achieve ISAF operational priorities and objectives. By May 2011, 48 NATO and partner nations were successfully operating in the AMN federation. The Chairman of the Joint Chiefs of Staff saw the need to ensure that the lessons learned from AMN are institutionalized as a future joint force capability. In August 2011 the Joint Staff J6 was assigned to "evolve the Future Mission Network."[3]

Culture Shock

General Stanley McChrystal once stated, "You don't give a senior leader a Blackberry or an iPhone and make [him] a digital leader."[4] While these advanced technological solutions can enable a user, the commander must have the vision and skill to create a shared understanding of mission and purpose with a diverse set of team members. This task is daunting enough within the U.S. forces with their rich histories, insular cultures, specific systems, and unique lexicons. When allies and perhaps governmental and nongovernmental organizations are included, the mission commander is faced with a full-blown information-sharing crisis. Complex partnered operations demand the ability to establish and maintain a common understanding of the operational environment through shared situational awareness. To achieve this aim, the mission commander must provide timely, reliable, interoperable, and secure information-sharing capabilities for planning, directing, and controlling the activities of all assigned forces. Significantly, the information environment is accelerated by the idea of interconnected, integrated joint forces and mission partners conducting dispersed operations around the globe.

From moving supplies in the wake of a hurricane, to ordering troops to the Pacific, to addressing mission partners on joint task force operations, the global dependence on integrated networks and shared information is stated in the Chairman's *Capstone Concept for Joint Operations: Joint Force 2020* (CCJO). With an emphasis on globally integrated operations, the CCJO outlines the need for the joint force to partner and to possess the ability to integrate with U.S. agencies, partner militaries, and indigenous and regional stakeholders—in short, with mission partners. Globally integrated operations will rely on a robust and secure information environment envisioned by the new DOD Joint Information Environment (JIE).

The JIE provides a shared information technology (IT) infrastructure, responsive set of enterprise services, and mission-integrated single security architecture. The JIE represents the IT capabilities and infrastructure that enable the joint force commander's ability to establish an MPE to support coalition operations. An MPE capability framework is inextricably linked to the JIE. Though IT and networks are critical elements of an MPE capability, these are merely the tools that allow the commander to visualize the battlespace, direct action in a timely manner, and establish trust with mission partners. An MPE capability framework is needed now to support the commander's ability to create unity of effort through the seamless exchange of information with mission partners.

The MPE framework is *commander-centric*, providing the means for commanders to effectively share their intent, communicate mission orders, and empower decentralized execution during mission partner operations. There are currently plans for building a standing coalition network for the United States to put in place quickly for future operations with mission partners. No one can argue against the need for such a capability, but a great deal of caution on the development of a persistent coalition network is warranted in the current fiscal environment. When faced with a new requirement, the U.S. military often defaults to the most comfortable solution, seeking a technological fix or building a new materiel system. As already established, the United States is executing MPE in Afghanistan today and has most of what is already needed to establish an information-sharing capability to launch the next MPE and meet the commander's next mission. By changing mindsets and simply adding some basic nonmateriel solutions, the joint force can apply current technologies and systems to meet warfighters' demands.

What the joint force needs now is a mission partner organizational framework to drive policy, IT transport, security, systems, and applications, along with concept of operations and standards. This mostly nonmaterial framework provides for a continual and dynamic process to inform improved information-sharing based on requirements and input from the combatant commanders and mission partners.

Describing the MPE

A Mission Partner Environment applies human and technical dimensions for sharing commander's intent, communicating mission orders, and empowering decentralized operations in keeping with the tenets of mission command.[5] The MPE capability framework is supported by a mission network in which partners plan, prepare, and execute operations at a single security classification level with a common language. The objective of the framework is to take the fight off SIPRNet, reduce the defended surface area, and leverage existing national networks. For instance, when the UK comes to fight alongside the United States, it does not have to drop what it has trained with and pick up an American product. The United States and its mission partners want to use familiar tools when it comes to a fight. The ultimate MPE vision is a framework of core services linked to authoritative data sources with the goal of allowing any partner to quickly join the network and receive specific services without major reconfigurations to their own national networks.

For success, MPE requires an overarching integrated approach that incorporates mission partners early in design, creation, and implementation. Early planning with partners builds a common basis for action, establishes the means and processes for mission partner integration, and identifies the methods to resolve knowledge management and interoperability challenges. Joint forces that effectively apply the principles of an MPE framework will have the tools to more rapidly form the collaborative networks (both IT-based and human) required for effective globally integrated operations with mission partners. MPE addresses the requirement for American forces to be able to lead a mission that includes partners and to operate a network separate and distinct from its national networks, specifically tailored to the mission and to the partners. Likewise, NATO has created a similar capability called Federated Mission Networking (FMN) to describe how Alliance forces will lead and operate a mission network. As expected, there are many conceptual and architectural similarities between the U.S. MPE and NATO FMN efforts. While this is a notable achievement, there is a need to implement the MPE and FMN concepts and architectures in a similar fashion and then train to them.

In keeping with the Chairman's Mission Command philosophy, the MPE capability framework provides strategic, operational, and tactical flexibility for all commanders to execute; it provides the means to clearly communicate commander's intent and achieves desired operational effects with all mission partners. MPE is a federated network concept supporting the connection of multiple networks through existing national systems with applications and tools to enable mission partner information-sharing within a single environment. Most important, the MPE is established within mission partner instructions where individual nations are resourced and equipped independently, each contributing its own equipment and resources to the mission network to achieve an optimal C2 environment. The MPE capability framework is not building or acquiring new systems; it addresses the need to shape and repurpose existing mission partner material and nonmateriel capabilities to address the commander's need for unity of effort and operational effectiveness based on the seamless exchange of information throughout an operation.

In Practice

From a U.S. perspective, joint forces currently deploy with two basic networks that support the C2 of forces via IT: SIPRNet and the Nonclassified Internet Protocol Router Network (NIPRNet). SIPRNet is used for sharing classified information among U.S. joint forces while NIPRNet is used for sharing unclassified information. The problem is that neither network can nor should communicate directly with a mission partner's network. Although there are other solutions via bilateral agreements and cross-domain technologies, the preferred near-term technique for sharing information with multiple partners for an assigned mission is the method employed in Afghanistan. The MPE framework builds and improves upon the federated network model of AMN. As with AMN, a theater agnostic framework requires American forces to repurpose existing equipment (for example, switches, routers, encryption devices, and so forth) or possess another "stack" of equipment to establish their mission network.

Sailor assigned to amphibious transport dock ship USS *Ponce* uses voice-recognition system to command virtual simulation of *Ponce* in Conning Officer Virtual Environment (U.S. Navy/Nathanael Miller)

Near-term emergent operations with mission partners require U.S. forces to deploy with SIPRNet, NIPRNet, and a mission network capability to connect with potential partners. The initial MPE capability is focused on six core services that provide basic human-to-human communications to support information-sharing in a mission partner operating environment:

- email with attachments
- text chat
- Web browsing
- video-teleconferencing
- voice over Internet protocol
- global address list sharing.

These services have been demonstrated within AMN and are essential to the implementation of an MPE framework. For today's fight, U.S. materiel and nonmateriel MPE capabilities will be whatever is "on the shelf"—it really is not new, but the environment in which these capabilities are employed and made secure will be new, as in a new concept of employment. As the American IT infrastructure of JIE evolves to cloud and virtualization technologies, so too must the MPE framework be able to adapt to improve the effectiveness and efficiencies associated with the establishment and operation of a mission partner network.

U.S. European Command's exercise Combined Endeavor 2013 (CE13) represented a significant paradigm shift from previous years. No longer was point-to-point technical interoperability the overarching focus with a cadre of observers to document, assess, and report results. Rather, CE13 focused

Marines set up command operation center to prepare for future squadron conditions in Germany (U.S. Marine Corps/Unique B. Roberts)

on implementing an MPE capability framework. The exercise provided the participating 40 nations and organizations a methodology for partners to plan, prepare, and execute a joint force mission on a single classification level with a common language. Employing core MPE precepts, CE13 provided the means to clearly communicate commander's intent for desired operational effects with all mission partners. Mission partner joining and exiting instructions created by the exercise community during the planning process represent the collective knowledge of the participating nations/organizations gained over 19 years, as well as lessons learned from 12 years in Afghanistan. These instructions matured the MPE concept, and the participants gained a clear understanding of how to operate within and share information in a coalition environment. Upcoming combatant commander exercises can only improve mission partner unity of effort using this framework.

"Harmony—Even Vicious Harmony . . . [Is] Based on Trust"[6]

The fundamental challenge of an MPE is changing the U.S. operational practice of relying on SIPRNet as the primary tool for information exchange during an operation. To that end, this current norm generates strategic, operational, and tactical limitations or restrictions to national leadership, as well as combatant and deployed commanders. As one general put it, "We must move the fight or operation off of SIPRNet to a new normal—a mission partnered environment including a mission network."[7] This network belongs to the mission commander. In the past, it was normal for the commander in theater to rely on traditional networks such as SIPRNet for operations. A national network (such as SIPRNet) must meet the needs of a diverse user base with many missions and is controlled by a national authority that usually exhibits considerable stasis. Without ownership, the mission commander cannot readily mold the environment to the specific needs of the mission and its information-sharing requirements. The commander must be able to bend and mold the environment. This shaping extends to adding and removing mission partners as membership changes during an operation. In this construct, at the mission commander's direction, information transmitted on the network must be releasable to all members, and all partners must be included on the network. Free flow of information to all mission partners is essential, so the use of firewalls or cross-domain solutions is eliminated in this environment.[8]

In cooperation with the combatant commander and U.S. Cyber Command, the mission commander must balance the need to share information with the need to protect. Mission partner trust cannot be surged; it must be established upfront through informed and inclusive information-sharing policies, training, and rehearsals. As stated in the Chairman's White Paper on Mission Command, "Building trust with subordinates and *partners* may be the most important action a commander will perform."[9] Coupled tightly with this element of trust is the commander's responsibility to balance the operational benefits of federating networks with the inherent risks that must be addressed through information assurance. Adjusting the attitudes and operational approaches of the U.S. military to support effective MPE employment requires changes to doctrine, education, and training. As relationships are forged with partners through training and exercises, so too is trust. With shared trust comes an understanding of the shared risks and the need to address cyber vulnerabilities before they become issues. But more important are the operational benefits and gains offered by the MPE.

Looking Ahead

Many of the principles and best practices for more effective and efficient mission partnered operations are being applied in Afghanistan and need to be codified and institutionalized. Specifically, an agreed-upon MPE organizational framework to drive policy, transport, systems/tools/applications, and agreed upon mission partner joining and exiting instructions (across nations and combatant commands) for coalition operations is necessary. This requires a persistent DOD-level process orchestrated by the Office of the Secretary of Defense and based on requirements and input from the combatant commands. Furthermore, combatant commanders should ensure there is an adequate governance structure in place to address their components' and coalition partners' requirements for an event that could happen tomorrow. Additionally, as forces draw down in Afghanistan, the Joint Staff needs to preserve the lessons learned by introducing MPE language into joint doctrinal publications and tactics, techniques, and procedures. Meanwhile, Service and joint schools should provide instruction on MPE while combatant commands explore and identify training exercises to introduce MPE precepts with mission partners. For the foreseeable future, Service components should remain equipped to support a mission network. This means forces deploy with SIPRNet, NIPRNet, and a third "stack." In many cases, this third stack can be realized through repurposing Combined Enterprise Regional Information Exchange System equipment.

The intent is to establish an MPE threshold capability in the near term (2014–2015) comprised of four recommended elements. First, each combatant command in coordination with its components should publish instructions for mission partners on how they can join and exit their theater mission networks. Additionally, these operationally focused instructions should be standardized across the regional combatant commands in recognition that mission partners often support more than one theater. Second, there should be Joint Staff activity focusing solely on finding and fixing mission partner interoperability issues before an operation occurs. For example, the Coalition Interoperability, Assurance, and Validation activity currently supporting operations in Afghanistan provides a viable model. It could be preserved and expanded. Third, the DOD Chief Information Officer could craft appropriate policy to specifically address rapid and efficient certification and accreditation processes for the establishment of mission networks and their associated systems and services. Finally, U.S. joint forces must begin practicing the principles and precepts of MPE in joint and coalition exercises. MPE needs a "if you can train to it and measure its readiness—it exists" mentality. Mission partner training and associated readiness metrics for an MPE capability framework would effect the necessary cultural changes to ensure joint forces are ready to operate on phase one/day one of any emergent operation. As experience and trust with mission partners grow, interoperability improves, and technological capabilities advance, the MPE framework could expand to include more complex information-sharing such as a digital common operational picture, targeting, fires, and seamless C2 among nontraditional mission partners. From a U.S. training and readiness perspective, the pace for MPE implementation falls on the combatant commanders and their components. They should set the education and training conditions during peacetime for the successful institutionalization of an MPE capability.

Conclusion

Globally integrated operations emphasize the need to partner, which requires the joint force to integrate with the full range of mission partners (interagency, intergovernmental, multinational, nongovernmental, private volunteer, and private sector). Moving the United States off SIPRNet for mission-partnered operations is more effective. MPE is a paradigm shift from information-sharing to coalition operations using a mission network for operations and warfighting with information-sharing as a byproduct of effective command and control. It is based on common standards, concepts of operations, and tactics, techniques, and procedures among nations, combatant commanders, and their components. An MPE capability is a critical enabling element of the Chairman's Mission Command operational objective of a "deeply interdependent" joint force. As such, its key attributes and enablers must be recognized, understood, and embedded in training and exercise objectives by combatant commanders and their components, likely mission partners, and warriors in the field. To achieve the Chairman's vision of a globally integrated force, the Armed Forces need to arrive on day one of the next crisis with a mission partner mindset ready to execute operations with allied, coalition, interagency, or intergovernmental mission partners. JFQ

Notes

[1] Brigadier General Brian Donahue, USA (Ret.), interview by author, The Pentagon, October 21, 2011.

[2] Ibid.

[3] Chairman of the Joint Chiefs of Staff, August 26, 2011. Document in authors' possession.

[4] Spencer Ackerman, "Stan McChrystal's Very Human Wired War," *Wired*, January 26, 2011, available at <www.wired.com/dangerroom/2011/01/stan-mcchrystals-very-human-wired-war/>.

[5] Lieutenant General Mark S. Bowman, USA, "Future Mission Network Study Report," December 17, 2012. Document in authors' possession.

[6] General James Mattis, USMC, Keynote Address, "Keeping the Edge: Revitalizing America's Military Officer Corps," Center for a New American Security, Washington, DC, February 18, 2010, available at <www.cnas.org/media-and-events/cnas-events/keeping-the-edge-revitalizing-americas-military-ffficer-corps#.U1gE3FxUGVk>.

[7] Donahue, interview.

[8] Gerald McGowan and Gregory Sisson, "Integration of Coalition Training into a Mission Network," Paper No. 11174, Interservice/Industry Training, Simulation, and Education Conference, U.S. Joint Forces Command, Suffolk, VA, 2011.

[9] Martin E. Dempsey, "Mission Command White Paper," April 3, 2012. Emphasis added. Both the Joint Information Environment and Mission Partner Environment have traceability to the Chairman's recent core strategic documents addressing joint capability.