Establishing Multinational Live, Virtual and Constructive Interoperability through Mission Partner Environments

Kevin Seavey, Emilie A. Reitz
Joint Staff J6 (Contactor support)
Alion Science and Technology, Norfolk, Va., USA
kevin.p.seavey.ctr@mail.mil; emilie.a.reitz.ctr@mail.mil

Major Jillian Klug
Telecommunications Systems Engineer (FA24)
Signal Corps, United States Army
jillian.m.klug.mil@mail.mil

ABSTRACT

As part of the U.S. Joint Staff's Bold Quest (BQ) coalition capability demonstration and assessment event, nations, Services and programs pool resources in a recurring cycle of capability development, demonstration and analysis. In the Live, Virtual and Constructive (LVC) domain, BQ provides a venue where participants can demonstrate integrated LVC environments, improve interoperability, and build and maintain joint fires proficiency. Due to the many policy, programmatic and technical issues that limit LVC interoperability, LVC environments are, in practice, almost never "plug and play." After many years of LVC development and effort, significant challenges still exist in creating and operating LVC systems as an integrated system of systems.

BQ 15.2 in October, 2015 provided the first opportunity to extend the LVC environment to partner nation simulator sites in France and Canada. BQ 16.1 in March 2016 used the U.S. Joint Training Environment Network (JTEN) to connect several new U.S. sites and, in the process, highlighted fundamental LVC interoperability issues, especially at the network level, that are widely recognized, persistent problems that stand as significant barriers to improving multi-Service and multinational LVC interoperability.

Significantly, BQ 15.2 provided the first opportunity to establish and operate a Mission Partner Environment (MPE). Designed to meet information exchange requirements among mission partners (twelve partner nations in the case of BQ 15.2), the MPE concept describes a shared information environment that leverages U.S. and mission partner information technology infrastructures. As demonstrated in 2015, the MPE has significant potential to improve operational and information technology interoperability across all participants. This paper discusses the application of the MPE concept to the LVC domain to help resolve some of the many long-standing LVC interoperability challenges. It offers long term, policy-based recommendations for using the MPE to improve joint and coalition LVC interoperability.

ABOUT THE AUTHORS

Kevin Seavey is a Military Analyst at Alion Science and Technology. He currently supports Joint Staff J6 Joint Fires Division in Norfolk, Virginia. In this capacity he leads Live, Virtual and Constructive (LVC) efforts for the Joint Staff's BQ capability demonstration and assessment event.

Emilie A. Reitz, M.A., is a Research Analyst at Alion Science and Technology. She currently supports the Joint Staff J6 Joint Fires Division in Norfolk, Virginia. In this capacity, she leads data collection and analysis efforts for the Joint Staff's BQ capability demonstration and assessment event. Her research focuses on integrating joint capabilities into modeling, simulation, and training, as a performance enabler.

Major Jillian Klug, is an active duty Army Signal Corps officer. She previously served in the Joint Staff J6 Joint Fires Division. During her tenure on the Joint Staff, she functioned as the BQ C4 Planner and Coalition Joint Task Force J6. In that capacity she was responsible for leading and overseeing the planning, engineering, and integration of a five nation Mission Partner Environment architecture that supported the full scope of Live, Virtual, and Constructive and Joint Fires mission threads.

Establishing Multinational Live, Virtual and Constructive Interoperability through Mission Partner Environments

Kevin Seavey, Emilie A. Reitz
Joint Staff J6 (Contactor support)
Alion Science and Technology, Norfolk, VA
kevin.p.seavey.ctr@mail.mil; emilie.a.reitz.ctr@mail.mil

Major Jillian Klug
Telecommunications Systems Engineer (FA24)
Signal Corps, United States Army
jillian.m.klug.mil@mail.mil

INTRODUCTION

Throughout the U.S. Department of Defense, there are interoperability efforts ongoing between the Training, Testing and Simulation communities, focused on creating live virtual and constructive (LVC). Every program office that deals with LVC has a hand in contributing to this work; due to the many policy, programmatic and technical issues that limit LVC interoperability, LVC environments are, in practice, almost never "plug and play." After many years of LVC development and effort, significant challenges still exist in creating and operating LVC systems as a coherent and integrated whole.

As part of the U.S. Joint Staff's Bold Quest (BQ) coalition capability demonstration and assessment event, nations, Services and program offices pool resources in a recurring cycle of capability development, demonstration and analysis. Since its inception in 2001, BQ has addressed a broad set of warfighter interoperability challenges in joint fires, to include Digitally-Aided Close Air Support, Friendly Force Tracking, and others. Since 2013, BQ has also provided a venue to demonstrate and assess methods to improve Live, Virtual and Constructive (LVC) interoperability in a structured manner.

BQ 15.2 in October, 2015 provided the first opportunity to extend this Bold Quest LVC environment to partner nation simulator sites in France and Canada. BQ 16.1 in March, 2016 used the U.S. Joint Training Environment Network (JTEN) to connect several new U.S. sites to the event and, in the process, highlighted fundamental, network level LVC interoperability issues, especially at the network level, that are widely recognized, persistent problems which stand as significant barriers to improving multi-Service and multinational LVC interoperability. Bold Quest BQ16.2, which will be conducted in October, 2016, will expand the number of U.S and partner nation participants and, in all likelihood, reveal new challenges in distributed LVC interoperability.

The 15 event also provided the first opportunity to establish and operate a Mission Partner Environment (MPE) in BQ. Building on the success of the Afghan Mission Network in integrating International Security Assistance Force (ISAF) operations in Afghanistan, the MPE is designed to meet information exchange requirements among mission partners (twelve partner nations in the case of 15.2). The MPE concept describes a shared information environment that leverages U.S. and mission partner information technology infrastructures, allowing them to all operate at a common classification level.

As demonstrated in 2015, the MPE has significant potential to improve operational and information technology interoperability across all participants. This paper discusses the application of the MPE concept to the LVC domain to help resolve long-standing LVC interoperability challenges. It offers a way ahead for using the MPE to improve joint and coalition LVC interoperability and describes initial steps toward that goal.

INTEROPERABILITY IN THE LVC DOMAIN

In a broad sense, interoperability is "the ability to operate in synergy in the execution of assigned tasks." (DoD, 2015) Interoperability in all areas is a primary requirement for building the future joint force. As the "Capstone Concept for Joint Operations: Joint Force 2020" states, the United States must:

> "Become pervasively interoperable both internally and externally. Interoperability is the critical attribute that will allow commanders to achieve the synergy from integrated operations this concept imagines. Interoperability refers not only to materiel but also to doctrine, organization, training, and leader development. Within Joint Forces, interoperability should be widespread and should exist at all echelons. *It should exist among Services and extend across domains and to partners*." (Dempsey, 2012 [italics added])

While there are many definitions of interoperability throughout the U.S. government and even within the U.S. Department of Defense (DoD), we are generally using the term in a broad sense meaning "the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces; and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together." (DoD, 2008) While discussions of LVC interoperability generally focus on technical issues, we are addressing interoperability in a broader sense that encompasses joint and coalition doctrine, tactics, techniques and procedures; national and Service information sharing and cybersecurity policies; LVC standards, protocols and systems; and personnel, to include organizational and cultural differences.

Historical Instances of Multinational LVC Interoperability

While we are using our recent experiences in BQ 15.2 and 16.1 as the basis for this discussion, BQ is certainly not the first multinational exercise or demonstration to face these problems. Many of the problems described in this paper are recurring problems in the LVC domain. As the cost of live training becomes more expensive and live ranges and platforms become scarcer, LVC capabilities become more critical to building and maintaining readiness. Subsequently the impact of non-interoperable LVC systems is no longer just a nuisance; it is now a warfighter readiness issue.

As a quick historical perspective, nearly every major joint and coalition LVC event over the last 15 years has experienced some level of LVC interoperability problems. The LVC environment for U.S. Joint Forces Command's (USJFCOM) exercise/experiment Millennium Challenge 2002 (MC02), the largest and most complex LVC event of its time, cost more than $250M and required multiple technical and operational tests over the course of a year to make sure it all worked. Despite the extended test and integration period, MC02 still witnessed numerous interoperability issues between simulations and with the interfaces between simulations and command and control (C2) systems (Myers, 2002). Efforts of this magnitude are certainly not typical LVC events, but still experience issues with interoperability.

Over the intervening years, the Joint Staff and Services have developed technical solutions that support interoperability for specific purposes. One of the most significant achievements was the creation of the Joint Training Enterprise Network (JTEN). JTEN is a persistent network that connects U.S. sites around the world, and serves as the framework for joint training among joint, Service, interagency and a limited number of partner nations (Greenyer, 2009). JTEN has greatly improved the ability to interconnect training sites in the U.S. However, as discussed below, there are barriers that still prevent the interconnection of JTEN to other U.S. training networks.

As another example, the Joint Staff J7's Joint Live, Virtual and Constructive (JLVC) federation of models and simulations provides a highly capable, integrated training environment that supports effective Combatant Command (CCMD), Joint Task Force and subordinate Component Command training. While JLVC has made substantial strides in providing a common training environment for U.S. CCMD and Service participants, it is nevertheless not fully interoperable with some Service training environments or with those of coalition partners beyond a small set of nations (USJFCOM, 2010).

In accordance with new DoD policy on information sharing, USJFCOM began work in 2006 to develop a secure interconnection between the JTEN and the Australian Defence Training and Experimentation Network (DTEN). In late 2006, the Defense Security Accreditation Working Group (DSAWG) approved interconnection of JTEN and DTEN for exercise Talisman Saber 2007 (Army Times, 2006). However, the U.S. Air Force (USAF) subsequently disapproved the interconnection of JTEN and its Distributed Mission Operations Network (DMON). Since then, USAF policy remains that routine JTEN and DMON interconnections are not authorized.

To overcome these issues, traditional approaches to interconnecting multinational networks typically focus on identifying specific solutions for connecting to specific nations or small groups of nations. For example, the JTEN was originally created to support U.S.-only operations. However, based on requirements to integrate certain coalition partners into joint exercises, JTEN developed a controlled interface to allow interconnection to Australian DTEN. While this interconnectivity supports valuable training and exercise support, the model is difficult to extend to other partner nations where different policies for information sharing exist. As a result, separate strategies must typically be developed to support connectivity between any particular set of partner nations.

BQ LVC OVERVIEW

The unique characteristic of the BQ LVC environment is its role in supporting coalition capability demonstration and assessment in the joint fires domain. Accordingly, LVC operations are high fidelity, multinational and multi-simulator events that are typically distributed globally via wide area networks.

During BQ15.2 (depicted below in Figure 1), French Air Force Joint Terminal Attack Controllers (JTACs) at the Air Ground Operations School at Nancy-Ochey Airbase, France conducted virtual close air support (CAS) missions with an AC-130 call for fire trainer at U.S. Special Operations Command's Joint Training Support Center (JTSC) at Hurlburt Field, Florida. Additionally, a Canadian infantry section at the Canadian Army Simulation Centre in Kingston, Ontario, Canada conducted distributed virtual missions with U.S., Canadian and Danish squads at Fort Bliss, Texas. Participating too were virtual UH-60 Blackhawk helicopters and a U.S. infantry squad located at Camp Atterbury, Indiana, and the JTSC AC-130 at Hurlburt Field.

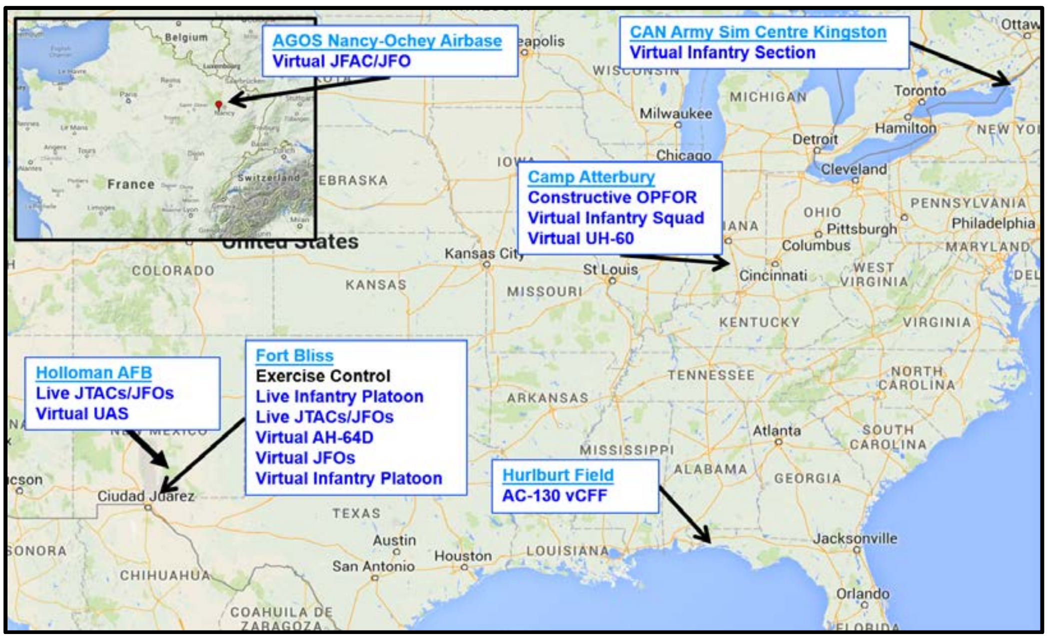

Figure 1 BQ15.2 Participating LVC Units / Sites

BQ 16.1 (depicted below in Figure 2) established an LVC environment that connected distributed simulator sites from the U.S Air Force, U.S. Army and Special Operations Command. This event allowed JTACs at the Air Force Research Lab (AFRL) in Ohio and at Muscatatuck Urban Training Center (MUTC) in Indiana to conduct virtual missions with CAS aircraft (AC-130U, A-10C and MQ-1) at distributed simulator sites. These missions included support from a new Air Support Operations Center trainer at AFRL and an intelligence team from a live Distributed Ground Station operating at Camp Atterbury with video feeds from simulated unmanned aerial systems and CAS aircraft targeting pods.

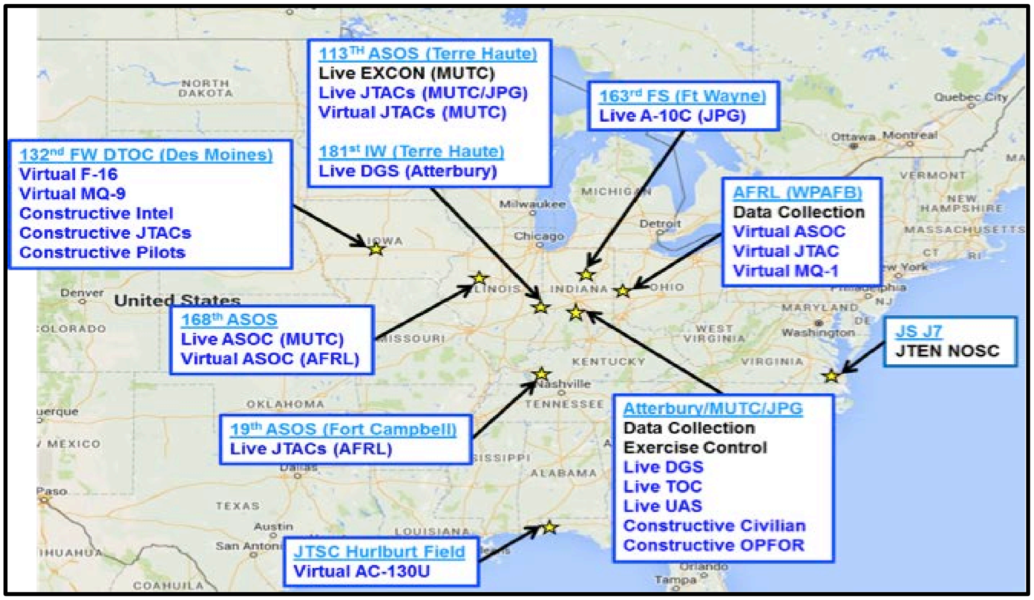

Figure 2 BQ 16.1 Participating Units / Sites

BQ 15.2 and 16.1 broke new ground in simulator interoperability and provided realistic training opportunities for all participants. These events also signal a trend toward increased distributed LVC operations in BQ, as France and other partner nations – Denmark, Great Britain and the Netherlands – will participate as distributed simulation sites in BQ 16.2 in October, 2016 (as depicted in Figure 3). BQ16.2 will expand the number of U.S and partner nation participants and, in all likelihood, reveal new challenges in distributed LVC interoperability.

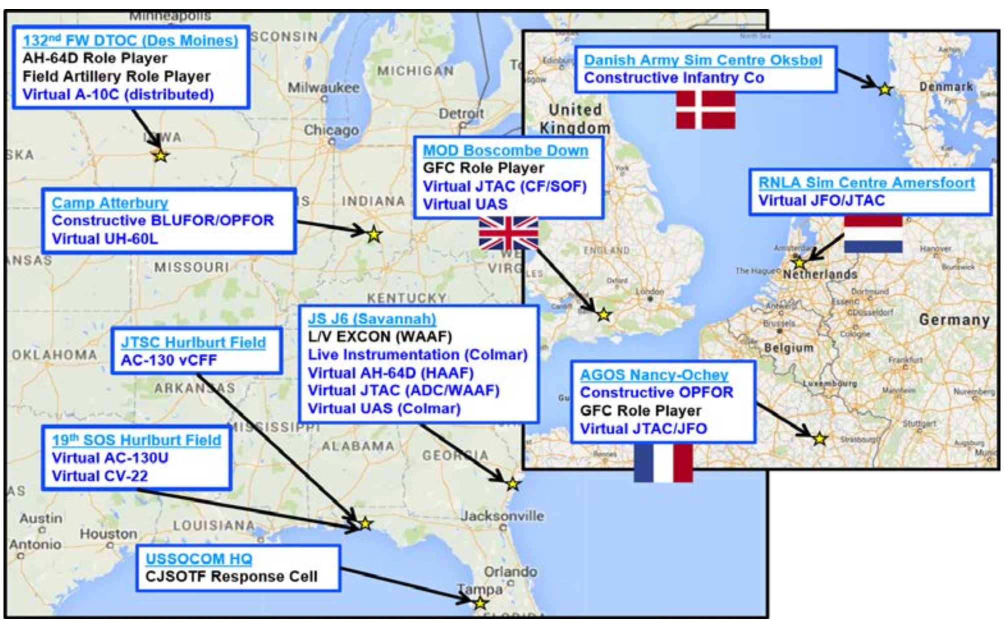

Figure 3 BQ 16.2 Projected LVC Units / Sites

LVC INTEROPERABILITY CHALLENGES

The promise of LVC is the ability to rapidly compose integrated and demanding environments where warfighters can come together from distributed locations to train and rehearse in realistic joint and coalition operations. This vision was perhaps best captured 12 years ago in the DoD's Training Transformation Implementation Plan that described an LVC environment whose purpose is to "prepare forces by providing units and command staffs with an integrated live, virtual, and constructive training environment that includes appropriate joint context, and allows global training and mission rehearsal in support of specific operational needs." (DoD, 2004). To fulfill this vision, LVC interoperability is a critical requirement.

As most practitioners of LVC well understand, LVC environments are almost never "plug and play." After many years of LVC development and effort, significant challenges still exist to rapidly compose LVC systems into a coherent and integrated whole. As we have previously asserted and described in some detail (Seavey, Reitz et al., 2016), these interoperability challenges apply to the broader LVC community and fall into three general categories:

1. Limitations in governing policies and guidance that promote interoperability (Policy)
2. Limitations in resources required to implement interoperability (Programmatic)
3. Limitations in technical standards or supporting technologies that enable interoperability (Technical)

We briefly outline these issues below. We have consistently found that policy and programmatic issues are often the larger and more intractable barriers to interoperability, and are generally harder to solve than technical problems. Policy issues, in particular, are a major barrier to interconnecting U.S. and partner nation networks to support distributed LVC operations.

Policy Issues.
Current policies for information sharing and release represent the largest barrier to joint and multinational LVC interoperability. These issues generally involve guidance and directives that limit the ability to interconnect LVC sites, systems and networks for the purpose of sharing information with U.S. and international partners. During recent events, we have encountered numerous examples of current policies that impose barriers to interoperability, especially in the ability to interconnect networks.

To illustrate this point, there are many wide area networks established within the U.S. for enabling distributed simulators to interconnect in support of training or testing. Some of the primary networks include the JTEN, DMON and the Air National Guard's Air Reserve Component Network (ARCNet). All of these networks are designed to enable distributed operations by connecting distributed simulators. Even though all are U.S. networks and operate primarily at the same classification level, with any connections to outside networks tightly controlled, interconnecting them to support cross-Service training or testing requires users to carefully navigate barriers imposed by policy. As one example, connecting a U.S. Air Force simulator site on the DMON to a U.S. Army site on JTEN to support joint training is generally prohibited without specific accreditation for a particular training event. Policies on how LVC sites can interconnect also hinder warfighter training by making routine training extremely difficult. Not surprisingly, the barriers imposed for connecting these U.S. networks to those of our partner nations are much higher; in fact, in most cases, they are currently insurmountable.

We experienced this problem firsthand during planning for BQ 16.1 when the 163rd Fighter Squadron at Fort Wayne, Indiana wanted to connect its A-10C simulator to the JTEN to conduct distributed missions. Because the simulator's only network connectivity was via ARCNet-1, it was not authorized to connect to JTEN, even though both networks were at the same classification level. The 163rd explored the option of moving its simulator to ARCNet-J, which is authorized to connect to JTEN, but the cost of new hardware and time required for re-accreditation were prohibitive. Even though we were not successful in integrating the 163rd's simulator, recent decisions by the National Guard Bureau may bring policy changes that should make connecting ARCNet-1 to the JTEN possible in the near future.

It should be noted here that we are not in any way arguing against maintaining the security of information at different levels of classification or the need to maintain the separation of systems and networks that carry sensitive information. Today's cyber threats demand careful consideration of any changes to cybersecurity policies. However, we are proposing that emerging DoD and NATO policies on information sharing, through constructs such as the Mission Partner Environment (MPE) and Federated Mission Network (FMN) concepts, should be applied to the LVC domain as well (DoD, 2014 and NATO, 2015). Taking this step could greatly improve our ability to rapidly compose interoperable LVC environments within larger policies familiar to all mission partners.

Programmatic Issues.
The way that nations, services, and program offices procure, field and maintain LVC systems represents another barrier to joint and multinational LVC interoperability. Acquisition of LVC systems is generally managed in

accordance with a nation's defense guidance**.** However, with rare exceptions, acquisition programs are initiated, funded and managed by the Services**.** Not surprisingly, primary interoperability requirements for each program tend to be Service-specific, focused on Service architectures and standards, with requirements for joint and coalition interoperability falling lower on the priority list.

Because many fielded training networks are not interoperable, the Joint Staff has historically created network connectivity itself to support BQ events. During BQ 15.2 the Joint Staff coordinated with the Joint Communications Support Element to provide a satellite terminal at Nancy-Ochey to support the necessary network transport. The satellite link met all requirements for the event, but was certainly a non-standard solution. Without persistent alternative network connectivity, the satellite link is unfortunately representative of the type of interoperability solutions required today. Programmatically, few groups establish consistent capabilities to connect Service LVC systems to joint and coalition systems.

Technical Issues.
An in-depth of discussion of LVC technical standards is beyond the scope of this paper. Despite the wide acceptance and use of international standards for simulation, making LVC systems interoperable is typically a protracted process involving coming to agreements on technical standards to be used, making changes to system baseline configurations (often requiring modifying simulator or interface application source code), and conducting lengthy rounds of testing and integration. The result of all this is that international standards for simulation promote interoperability, but do not guarantee it.

In response to this situation, many program offices, driven primarily by Service requirements, have developed particular interpretations of standards for providing interoperability among their own systems. These Service-centric guidelines generally work well for a particular simulation environment, but usually do not provide interoperability between LVC systems of other nations or Services. As a result, program offices generally field non-interoperable, Service- or program-specific LVC solutions. Therefore, whenever disparate simulators are integrated in an LVC environment, consensus must be reached on what standards – *and what specific interpretation of standards guidance* – will apply. Afterwards, lengthy cycles of development, integration testing, problem resolution and retesting are typically required to make it all work.

For further reading on the technical interoperability of systems, please refer to Wang, Tolk & Wang, 2009 or Bizub & Cutts, 2007; despite the years that have passed since their writing, the challenges and current technical solutions used to overcome the issues of interfacing differing standards or implementation of the same standards remains the same.

MISSION PARTNER ENVIRONMENTS AS AN INTEROPERABILITY ENABLER

How do we solve these problems in a cost-effective way that improves LVC interoperability without violating cybersecurity requirements of the various nations, Services and programs involved? Since we are arguing that policy barriers in the LVC domain are often the biggest hurdles to improved interoperability, we believe that technical solutions alone – new standards, systems or networks – will not solve the problem. Instead, aligning our efforts with broader DoD and multinational policy initiatives, like the MPE or FMN, which have significant traction already in the operational community, appears to be the best solution for driving change in the LVC domain.

The Chairman's *Capstone Concept for Joint Operations (CCJO): Joint Force 2020* (Dempsey, 2012) describes the Joint Information Environment (JIE) as a capability that will "increas[e] interoperability across the force …, facilitat[e] capabilities to address threats …, and encourag[e] flexibility and resilience in our information environment." As a foundational element of the JIE, MPE capabilities are the critical enabler for conducting operations with multinational partners. Based on lessons learned from over a decade of war, the MPE enables mission partners to plan and execute operations at a common security level via a common mission network with supporting tools and services. The MPE relies on the JIE for linking regionally-focused mission networks to the DoD network enterprise.

As demonstrated during BQ 15.2, a federated MPE can support effective operations among mission partners (Joint Staff, 2015). During this event, the Joint Staff led the implementation of an MPE that provided connectivity between the aligned events BQ 15.2 (with twelve participating nations), the U.S. Army's Network Integration Evaluation 16.1, and 1st Armored Division's Multinational Division Exercise. Denmark, France, Great Britain, Norway, the U.S. Army and the Joint Staff all agreed to federate their networks, core services and certain Command and Control (C2) systems as Network Contributing Mission Partners (NCMP). Other participants – Australia, Belgium, Canada, Finland, Germany, Italy, Netherlands, Poland and Sweden – did not bring their own networks, but connected their systems directly to and received services from an NCMP, thus participating as Hosted Mission Partners (HMP). As coordinator for all MPE operations, the Joint Staff led the collaborative development of Joining, Membership and Exit Instructions (JMEI) that ensured all mission partners understood how to operate as part of the mission network.

Much in the same way that it enabled C2 systems and core service interoperability in BQ 15.2, the MPE can be used as a model for improving LVC interoperability. Mission partners can join as NCMP or HMP and, following guidance provided in JMEI tailored to the LVC environment, conduct distributed operations via interconnected simulator systems. As with MPEs supporting operational C2, MPE capabilities offer the option of establishing an LVC mission network that is complementary to – not a replacement for – existing national, alliance or other multi-national networks.

To make this work for LVC systems, Cross Domain Solutions (CDS) may be required to allow fixed sites on persistent national networks (e.g., JTEN or ARCNet) to connect to episodic mission networks supporting LVC operations. CDS are a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains (CNSS, 2010). CDS offer tremendous potential to bridge networks and systems of different classifications. While CDS present their own challenges in terms of policy and timely accreditation and fielding, they can play a crucial role in improving joint and coalition simulator interoperability. We see CDS capabilities as an integral part of the MPE solution for the LVC domain.

WAY AHEAD FOR BQ LVC OPERATIONS

As we have experienced during BQ events, joint and coalition LVC interoperability is almost never easy. However, our experiences in implementing the MPE have highlighted promising opportunities to improve joint and coalition interoperability in the LVC domain.

During BQ 16.2, the Joint Staff J6 will again implement a mission network to connect all mission partners. Mission partners in BQ 16.2 will include 15 nations and NATO. As part of this effort, we will use the mission network for the first time to interconnect distributed simulators. In fact, BQ 16.2 will serve a proof-of-concept for using the BQ Mission Network as a way to improve LVC interoperability.

To support this proof-of-concept, we will develop detailed JMEIs defining the LVC "standard operating procedures" to be used, to include LVC standards, protocols and systems, as well as the supporting information sharing and cybersecurity policies to be employed. Since selection and interpretation of technical standards has often been a source of interoperability problems in the past, JMEIs will be the key to capturing the agreements and ground rules that facilitate joining and operating in the LVC environment.

We will also introduce additional CDS capabilities that support the interoperability of LVC networks of different classification. During BQ 16.2, we will demonstrate and assess a two-way, protected interface between JTEN and the BQ Mission Network, which will be releasable to all participating BQ nations. Joint Staff J6 will use this CDS as a critical component of an ambitious plan to link British JTACs in the United Kingdom operating in a JTAC simulator on the BQ Mission Network with the 19th Special Operations Squadron's AC-130U simulator at Hurlburt Field operating on the JTEN.

We recognize that adopting MPE capabilities to the LVC domain will require policy and cultural changes in the organizations that now support LVC development and fielding. These changes take time. The MPE concept is based on trust and peer-to-peer interaction; this trust can only be established by working through the policy and technical problems together with our mission partners. Practice and experience will increase trust among operators and cybersecurity staffs in each nation, as well as between mission partners. Beyond the mere technical interoperability we seek, experience in implementing MPE will strengthen personal and organizational ties with our mission partners that should eventually make it more efficient to establish MPE capabilities, ultimately resulting in better LVC interoperability that improves joint and coalition warfighter readiness.

ACKNOWLEDGEMENTS

This work was supported in part by the U.S. Joint Staff (Contract #W91247-11-D-0010-2B03). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Joint Staff or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes.

REFERENCES

Allied Command Transformation. (2015). *Federated Mission Networking.* North Atlantic Treaty Organization. http://www.act.nato.int/fmn, retrieved February 2016.

Army Times. (2006). USJFCOM Gets Approval to Connect U.S., Australian Networks. Army Times, https://www.army.mil/article/1065/usjfcom-gets-approval-to-connect-us-australian-networks, retrieved June 2016.

Bizub, W., & Cutts, D. (2007). Live Virtual Constructive (LVC) Architecture Interoperability Assessment. *In the proceedings of the International Training & Education Conference, 2007.*

Committee on National Security Systems (CNSS). (2010). Instruction 4009: National Information Assurance (IA) Glossary. Washington, DC, 26 April 2010.

Dempsey, M. E. (2012). *Capstone Concept for Joint Operations: Joint Force 2020.* 10 September 2012.

Dempsey, M. E. (2013). *Joint Information Environment White Paper*. 22 January 2013.

Department of Defense. (2004). *Department of Defense Training Transformation Implementation Plan*. Washington, DC: Office of the Under Secretary of Defense for Personnel and Readiness, 9 June 2004.

Department of Defense. (2007). *Department of Defense Information Sharing Strategy*. Washington, D.C.: Chief Information Officer, 4 May 2007.

Department of Defense (2008). *Information Sharing Environment Guidance (ISE-G) – Identity and Access Management Framework for the ISE Version 1.0*, 19 December 2008.

Department of Defense. (2013). *Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS).* Washington, DC: Deputy Chief Information Officer for Information Enterprise, Department of Defense; Chief Information Officer, Joint Staff; Chief Information Officer, U.S. Cyber Command, 25 January 2013.

Department of Defense. (2014). *Department of Defense Instruction 8110.01: Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD.* Washington, D.C. 25 November 2014.

Department of Defense. (2015). *JP 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington D.C. 8 November 2010 (as amended through 15 November 2015.

Greenyer, F. (2009) "Training Transformation – The Present and the Future." *MS&T Magazine,* Issue 4/2009

Joint Staff J6 (2015). Mission Partner Environment and Bold Quest, in proceedings of the Military Communications Conference (MILCOM) 2015, Armed Forces Communications and Electronics Association, 2015.

Myers, Grover E. (2002) Millennium Challenge 2002: Setting the Mark, in *Joint Force Quarterly*, Winter 2002-2003.

Seavey, K., Reitz, E. A., Lagrange, P.J., Gorham, W. B., Biran, H., & Whelan, D.. (2016) Bold Quest 15.2: A Case Study in Establishing Multinational Simulator Interoperability. In *Proceedings of MODSIM World 2016.*

U.S. Joint Forces Command (USJFCOM) (2010). Joint Live Virtual and Constructive (JLVC) Federation Integration Guide. USJFCOM, 13 January 2010 (retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a521311.pdf).

Wang, W., Tolk, A., & Wang, W. (2009). The levels of conceptual interoperability model: applying systems engineering principles to M&S. In *Proceedings of the 2009 Spring Simulation Multiconference* (p. 168). Society for Computer Simulation International.