Mission Partner Kit:

Advancing Multinational Interoperability with NATO Allies

COL DONALD R. NEAL JR.
MAJ AZIZ ATAKUZI

The war in Ukraine has demonstrated how commercial technologies can reshape the battlefield, becoming essential tools in a modern military's arsenals. Technologies such as Starlink satellite terminals have provided decentralized, resilient communication networks, enabling Ukrainian forces to maintain real-time situational awareness under cyber and kinetic attacks. Similarly, off-the-shelf drones like DJI quadcopters have been repurposed for reconnaissance and offensive operations, outpacing the deployment speed of traditional military systems. Ukraine has quickly adopted the use of commercial technologies during conflict, demonstrating the importance of agility and innovation in modern warfare for U.S. and NATO forces.

Informed by these lessons, the 2nd Cavalry Regiment (CR) developed and tested the Mission Partner Kit (MPK) to improve multinational interoperability.[1] Enabled by trained liaison officers (LNOs), the kit provides a cutting-edge commercial off-the-shelf (COTS) command and control (C2) software-centric solution. This capability transforms the ability of conventional U.S. and NATO forces to establish technical interoperability at the tactical level. The capability can be scaled to and adapted by any geographic combatant command. It can be easily scaled by any Army unit because the system relies on secure commercial technologies to bridge critical gaps in information sharing between U.S. and allied forces, enabling unity of effort and creating cohesive multinational units.

Interoperability Challenges in Multinational Operations

Army Regulation 34-1, *Interoperability*, outlines the principles and guidelines for achieving multinational force interoperability (MFI). It defines MFI as the ability of forces from different nations to train, exercise, and operate effectively together to achieve shared objectives. The regulation emphasizes the importance of standardization, common procedures, and compatible equipment to ensure seamless collaboration between allied forces. Interoperability spans across all warfighting functions and includes three domains — human, procedural and technical.[2] The human factors include language, terminology, and training; procedural factors include doctrine and procedures; and technical factors include hardware and systems.

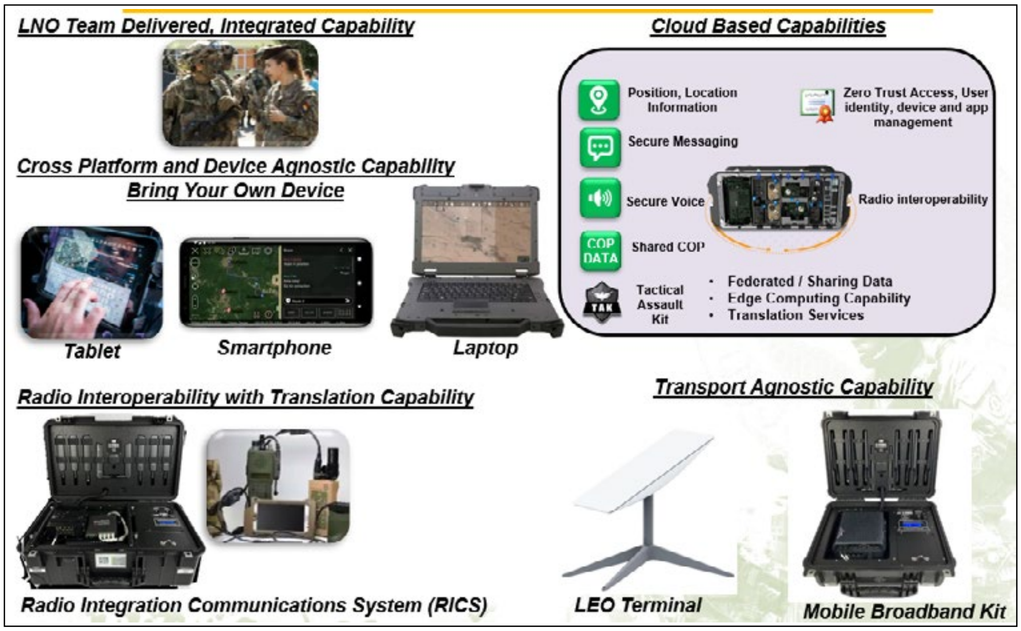
To accurately assess the level of interoperability between partners, NATO and the U.S. Army have implemented a standardized system from level zero to level three. Level three is the desired end state for multinational operations. The levels are defined as:

- **Level 0:** Not Interoperable. Partners at this level lack the necessary capabilities to operate together. They must maintain independent operations, as their C2 systems are incompatible and could potentially interfere with each other.

- **Level 1:** Deconflicted. Partners at this level can coexist in the same operational area without causing significant interference; however, they do not interact or coordinate their activities. To achieve this level, partners must align their capabilities and procedures to establish common operational norms.

- **Level 2:** Compatible: Partners at this level can interact and cooperate with each other in pursuit of shared objectives. They possess similar or complementary capabilities and processes, enabling them to operate effectively together.

Figure 1 — Mission Partner Kit


LNO Team Delivered, Integrated Capability
Cloud Based Capabilities
Position, Location Information
Zero Trust Access, User identity, device and app management
Secure Messaging
Secure Voice
Radio interoperability
COP DATA
Shared COP
TAK
Tactical Assault Kit
Federated / Sharing Data
Edge Computing Capability
Translation Services
Cross Platform and Device Agnostic Capability
Bring Your Own Device
Tablet
Smartphone
Laptop
Radio Interoperability with Translation Capability
Transport Agnostic Capability
Radio Integration Communications System (RICS)
LEO Terminal
Mobile Broadband Kit

A German soldier speaks into a radio attached to a Radio Integration Communications Suite (RICS) during Saber Strike 24 on 18 April 2024. (Photo by SPC Andrew Clark)

- **Level 3:** Integrated: Partners at this level can seamlessly integrate with each other upon arrival in a theater of operations. They have robust network-enabled interoperability, allowing them to participate in the full range of military operations. Partners can routinely establish networks and operate effectively with or as part of U.S. Army formations.

2CR experienced some challenges with achieving fully integrated interoperability in February 2022 when it deployed to NATO's eastern flank following Russia's invasion of Ukraine to reassure allies. It was difficult for 2CR squadrons to digitally integrate with units from Romania, Hungary, and Slovakia because of the distributed nature of multiple units and lack of interoperable systems. The lack of interoperable systems delayed information sharing and joint decision-making — critical requirements in multinational operations.

Challenges ranged from differences in communication networks to issues with data classification and secure information-sharing protocols. For example, it was challenging to integrate tactical partner units into 2CR's common operating picture (COP) because of incompatibility of partner radio networks and the need to share operational graphics and reports. This incompatibility caused delays increasing risk to mission accomplishment.

The Mission Partner Kit: A Game Changer

To address interoperability challenges, 2CR developed the MPK capability, which allows U.S. and NATO tactical units at brigade and below level to quickly establish network-enabled interoperability.[3] It provides tactical formations a scalable, mobile, and platform-agnostic system designed to simplify and improve information-sharing between NATO forces at the sensitive but unclassified level.[4] Built on the foundation of the Army's Nett Warrior system, MPK leverages COTS hardware and software to deliver a fast, secure, and cost-effective solution to improve C2 with multinational partners.[5,6] The kit provides four core services: situational awareness by displaying friendly and partner force's location on COP, secure chat, voice, and collaboration tools. What makes the kit mobile is all the applications are hosted in the government-approved commercial cloud. Partners can easily access applications from any mobile device with an internet connection or download the apps with a quick response (QR) code, because each application is publicly accessible and does not require special installations or downloads.

The security of applications and data is ensured through requiring all users to authenticate with their own credentials, reinforcing zero-trust cybersecurity principles. If partners do not have mobile devices, the U.S. unit can issue a device such as smartphone or a laptop with the application preinstalled for the partner force to use. This approach eliminates system incompatibilities because partners are onboarded into a common network and use the same applications, enabling faster decision-making and coordinated mission execution. This simple approach and design bridge disparate systems and networks, allowing coalition forces to exchange critical information quickly and efficiently using common applications without requesting access to connect to a special network. Most importantly, leveraging software-based encryption protocols eliminates the requirement to have special hardware encryption devices, which reduces the complexity and burden of current hardware-based solutions.

Commanders from different NATO nations can C2 as a unified force using common apps which increases real-time collaboration. This minimizes risks of miscommunication, significantly enhancing the effectiveness of joint operations. Additionally, the software enables real-time sharing of intelligence, surveillance, and reconnaissance (ISR) data, providing a COP for all coalition forces. The MPK is also suitable for a broad range of military operations, from humanitarian missions to high-intensity conflicts. Its portability and scalability to onboard many multinational users at once ensures multinational forces can respond effectively to any emerging threats.

Case Study: 2CR and NATO Joint Exercises

2CR has demonstrated the transformative potential of the MPK during major NATO exercises, including Griffin Shock 23, Saber Junction 23, Saber Strike 24, and Saber Junction 24.[7,8,9,10] These exercises underscored how simple commercial solutions can enable seamless communication across multinational forces, integrating battalions from France, Italy, and Spain into a unified operational framework. Having a shared COP with secure voice and chat capabilities enabled multinational commanders to synchronize efforts and accelerate decision-making.

During the Saber Strike 24 exercise in Poland, 2CR used a secure messaging application to establish chat rooms between its headquarters and the German Army battalion tasked with augmenting the regiment. German Army battalion leaders used the application to report crossing checkpoints and issues in real time during a tactical road march. To facilitate this, 2CR issued MPK smartphones with the application to German Army users, enabling secure and instant communication. This allowed 2CR to track the German convoy in real time, enhancing situational awareness during the critical tactical movement from Germany to Poland. This use of secure messaging demonstrates how MPK can easily overcome technical interoperability barriers with widely available commercial applications. Without this application, training exercises or tactical road marches would have faced significant delays and reduced multinational cohesion due to incompatible communication systems.

Lessons for Warfighting and Interoperability

The conflict in Ukraine has demonstrated that the rapid adoption of commercial technologies can quickly increase U.S. Army and NATO warfighting capabilities. However, significant interoperability challenges remain, especially in encouraging the adoption and implementation of commercial software solutions. To address these gaps, the U.S. Army can champion secure architecture that facilitates real-time collaboration with allies. Drawing from Ukraine's experience, the Army can also explore how emerging technologies, such as artificial intelligence (AI) and 5G networks, can be leveraged to enhance situational awareness and decision-making while operating alongside our allies and partners.

Success requires deliberate investment in commercial solutions and a commitment to standardizing interoperability frameworks. By leveraging commercial technologies and fostering a culture of innovation, the Army can transform multinational interoperability and ensure that NATO remains prepared to meet the demands of future conflicts.

The Future of Multinational Interoperability

The Mission Partner Kit is more than a solution to interoperability challenges — it is a game changer for increasing interoperability during multinational operations. By enabling seamless communication, secure data-sharing, and real-time collaboration, MPK ensures that the U.S. Army along with our NATO allies can operate as a unified force, even in the most challenging environments. As the U.S. Army continues to champion innovation and adaptability, the MPK capability represents a path forward for multinational interoperability. Its success highlights the significance of using commercial technologies to ensure NATO allies and partners remain prepared to defend the alliance and respond to the evolving threats of future battlefields.

Soldiers with the 2nd Cavalry Regiment participate in a distinguished visitors event as part of Griffin Shock 23 in Poland on 19 May 2023. (Photo by SSG Agustín Montañez)

Notes

[1] Austin Roberston, "Saber Strike: An Exercise in Foundational Partnership," Army News Service, 26 April 2024, https://www.army.mil/article/275706/saber_strike_an_exercise_in_foundational_partnership.

[2] Duane Gamble and Michelle Letcher, "The Three Dimensions of Interoperability for Multinational Training at the JMRC," Army News Service, 14 October 2016, https://www.army.mil/article/173432/the_three_dimensions_of_interoperability_for_multinational_training_at_the_jmrc.

[3] Enterprise Cloud Management Agency Public Affairs, "Griffin Shock 23 Strengthens NATO Readiness through Cloud-Enabled Applications," Army News Service, 1 June 2023, https://www.army.mil/article/267180/griffin_shock_23_strengthens_nato_readiness_through_cloud_enabled_applications.

[4] Gabe Camarillo and Randy George, "Command and Control in a Digital Age: The U.S. Army's Blueprint for the Future Battlefield," AUSA, 24 May 2023, https://www.ausa.org/articles/command-and-control-digital-age.

[5] Kathryn Bailey, "'Stryking' towards Networked Battlefield Communications," Army News Service, 23 February 2023, https://www.army.mil/article/264225/stryking_towards_networked_battlefield_communications.

[6] Sean Carberry, "NATO Allies Get on Same Page During Biggest Exercise," NTSA, 27 June 2024, https://www.ntsa.org/news-and-archives/2024/6/27/nato-allies-get-on-same-page-during-biggest-exercise.

[7] Enterprise Cloud Management Agency Public Affairs, "Griffin Shock."

[8] Shane Killen, "Multinational Forces Unify to Fight at Sabre Junction 23," Army News Service, 20 September 2023, https://www.army.mil/article/270072/multinational_forces_unify_to_fight_at_saber_junction_23#:~:text=Moving%20into%20their%20fighting%20positions,in%20a%20relentless%20training%20environment.

[9] Roberston, "Saber Strike."

[10] Danielle Rayon, "Sabre Junction 24 Strengthens Ties between NATO Allies and Partner Nations," Army News Service, 17 September 2024, https://www.army.mil/article/279611/saber_junction_24_strengthens_ties_between_nato_allies_and_partner_nations.

COL Donald R. Neal Jr. currently serves as the commander of the 2nd Cavalry Regiment.

MAJ Aziz Atakuzi currently serves as the regimental cyber electronic warfare officer for the 2nd Cavalry Regiment.