

The V Corps Commanding General speaks with Soldiers assigned to the 3<sup>rd</sup> Armored Brigade Combat Team, 4<sup>th</sup> Infantry Division, at Drawsko Combat Training Center, Poland, October 29, 2024. (U.S. Army photo by 1LT Kimberly Blair)



## Introduction

During 2024, V Corps participated in two major exercises: Warfighter (WFX) 24-03 and Avenger Triad 24. WFX 24-03 was nested with theater exercise Austere Challenge 24 and led by U.S. European Command; Avenger Triad 24 was a multinational exercise led by U.S. Army Europe and Africa Command (USAREUR–AF) that involved six different North Atlantic Treaty Organization (NATO) and United States corps headquarters. Both exercises offered unique training opportunities that allowed V Corps to advance the Army’s understanding of multidomain operations while integrating host-nation, allied, and national capabilities. During Avenger Triad 24, V Corps validated its ability to achieve interoperability with NATO and USAREUR–AF using federated communications systems across all echelons of command with clearly defined common operational pictures (COPs) and mission command information systems (MCIS) by warfighting function.

WFX 24-03 and Avenger Triad 24 both presented challenges, but the V Corps G-2 came away with lessons learned and best practices to share with the greater intelligence community. Through the framework of the three interoperability dimensions (technical, procedural, and human), this article will describe how the V Corps G-2 integrated the Army’s MCIS with NATO allies to create a combined theater common intelligence picture (CIP), established intelligence synchronization procedures across the intelligence warfighting function, and leveraged the trust and rapport built through numerous previous engagements with multinational partners to overcome interoperability challenges.

## Technical Interoperability and Architecture

Although the most difficult of the three interoperability dimensions to achieve, technical interoperability is critical to enabling the procedural and human dimensions to create shared understanding across multinational forces. Coordination with

allied nations well ahead of an operation or exercise is crucial to achieving technical interoperability to accommodate U.S. forces and allies’ different systems and processes.

Before WFX 24-03, V Corps G-2 exercise planners scheduled frequent touchpoints with allies from Estonia and the United Kingdom, which resulted in an initial level of technical interoperability.<sup>1</sup> V Corps elements conducting distributed operations from Estonia, the United Kingdom, Poland, Romania, and Germany communicated effectively through email, chat, and distributed collaboration tools such as Cisco Media Server and Command Post Computing Environment. Additionally, V Corps and the multinational divisions could access each other’s sharing portals, enabling redundancy for sharing products if other communication platforms were degraded or disrupted.

From a technical interoperability standpoint, the WFX 24-03 intelligence architecture initially relied on the Warfighter Simulation Intelligence Module (WIM) to generate intelligence for the multinational exercise. However, due to network concerns, the WIM generated U.S. Message Text Format intelligence messages at the collateral Secret level, which precluded sharing with allied partners during the exercise. To overcome the issue, the Joint Multinational Simulation Center and Mission Command Training Program instituted the use of the Intelligence Electronic Warfare Tactical Proficiency Trainer (IEWTPT) on the lower-enclave Mission Partner Environment (MPE) network to generate U.S. Message Text Format intelligence messages with the Releasable to NATO Forces (REL NATO) dissemination marking.

Using the IEWTPT as the intelligence warfighting function simulator increased intelligence generated at the REL NATO level, which enabled a vast increase in intelligence sharing ability among allies. It also expanded the intelligence support to targeting supplied by U.S. personnel using the Intelligence

Fusion Server and by both U.S. and allied forces using the U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative. Intelligence messages generated from IEWTPT on the MPE network enabled timely high-payoff target list equipment targeting, as targeting information did not have to be transferred from the secured internet protocol router network (SIPRNET) to the MPE network where fires mission command systems resided.

The IEWTPT system resided and produced releasable intelligence reporting on the MPE network, but in a real-world environment, intelligence reporting from U.S. collection assets would occur over SIPRNET. The lack of a cross-domain solution at the tactical (corps and below) level hindered the ability to share intelligence with allies in a timely manner. To share intelligence among allies without a cross-domain solution requires a Soldier-in-the-loop to transfer data manually to the MPE network. This method is neither timely nor effective for quickly transferring large amounts of data. While producing intelligence on the MPE network is helpful in an exercise environment, it does not replicate real-world data flow or restrictions.

USAREUR-AF used the Global Command and Control System-Army (GCCS-A) to move the theater CIP from SIPRNET to MPE by transferring red track data through the Radiant Mercury cross-domain solution. The GCCS-A COP and CIP were both available to all personnel via web browser, allowing any user to visualize the battlefield quickly or query for specific units. The GCCS-A CIP also fed V Corps and subordinate unit Command Post Computing Environment mission command systems, which allowed for a comparison to the V Corps G-2 CIP while providing the authoritative top CIP to all training audiences.

United Kingdom intelligence analysts reported that this iteration of WFX was the first time they could use the MPE network to remain federated during planning and execution. For the duration of the operation, they tracked all battle damage assessments and participated in numerous V Corps battle rhythm events, all on sovereign United Kingdom systems.

One technical interoperability shortfall for the intelligence warfighting function was the lack of a Battlefield Information Collection and Exploitation System (BICES). The BICES can provide a direct link for intelligence between the United States and allied partners while delivering data to the NATO Intelligence Functional System used by tactical units. However, BICES does not communicate with mission command systems. With MPE now accredited to process NATO Secret intelligence, bridging the MPE and BICES networks is critical to ensuring technical interoperability between allied intelligence teams and allowing intelligence from all allies to reach the MPE mission command network.

The Maven Smart System is an emerging U.S. Army initiative that uses artificial intelligence and machine learning for geospatial visualization of data. Multinational interoperability must be considered when implementing the Maven Smart System as the authoritative COP for U.S. forces. If allied and partner nations can successfully navigate the technical requirements to integrate the Maven Smart System into their respective information systems, this will get us one step closer to true convergence.<sup>2</sup>

## **Procedural Interoperability**

As a tactical warfighting headquarters, it was essential for V Corps G-2 to create a shared understanding of the enemy scheme of maneuver across the battlespace, which is best achieved through synchronization with the V Corps subordinate divisions. V Corps held daily intelligence synchronization working groups (ISWGs) to accomplish this procedural interoperability: two with adjacent and downtrace units and two with higher echelons. This allowed V Corps and its subordinate elements to ensure each echelon had the same CIP of the enemy and the same understanding of what the enemy was likely to do in the next 48 to 96 hours. These ISWGs were essentially analytic conversations, and while V Corps and the subordinate divisions were not always in agreement about the enemy's next move, the units came out of these meetings with a logical, feasible, and, most importantly, synchronized assessment of the enemy scheme of maneuver.

Over time, the format for the ISWG adjusted to create and refine process efficiencies. At the beginning of WFX 24-03, the V Corps analysis and control element (ACE) briefed the overall enemy scheme of maneuver. The subordinate divisions then provided a detailed microanalysis of that enemy scheme of maneuver, a format that allowed the G-2 and subordinate divisions to remain synchronized on the current enemy situation. However, as time progressed, the G-2 and the ACE Chief realized that this format did not adequately provide the subordinate divisions with what they needed most: the corps-level assessment for the next 24 to 96 hours. The ISWG format was therefore adjusted to allow the divisions to brief first on the close fight. The Corps then closed with its assessment of the deep fight. This adjusted format was well received across the formations and provided the subordinate divisions with a more detailed assessment of how V Corps shaped the enemy.

In addition to the daily working groups, the Corps ACE ensured it had multiple conversations with its subordinate divisions outside of the ISWGs to ensure synchronization during the rapidly changing large-scale combat operations. These frequent conversations were especially important from a procedural interoperability standpoint, as allies from Estonia and the United Kingdom could not always access the same networks and tools as the United States intelligence entities.



Members of the V Corps staff and 2<sup>nd</sup> Corps, Polish Land Forces, staff synchronize their shaping efforts during a command post exercise at Grafenwöhr, Germany, October 26, 2023. (U.S. Army photo by SPC Devin Klecan)

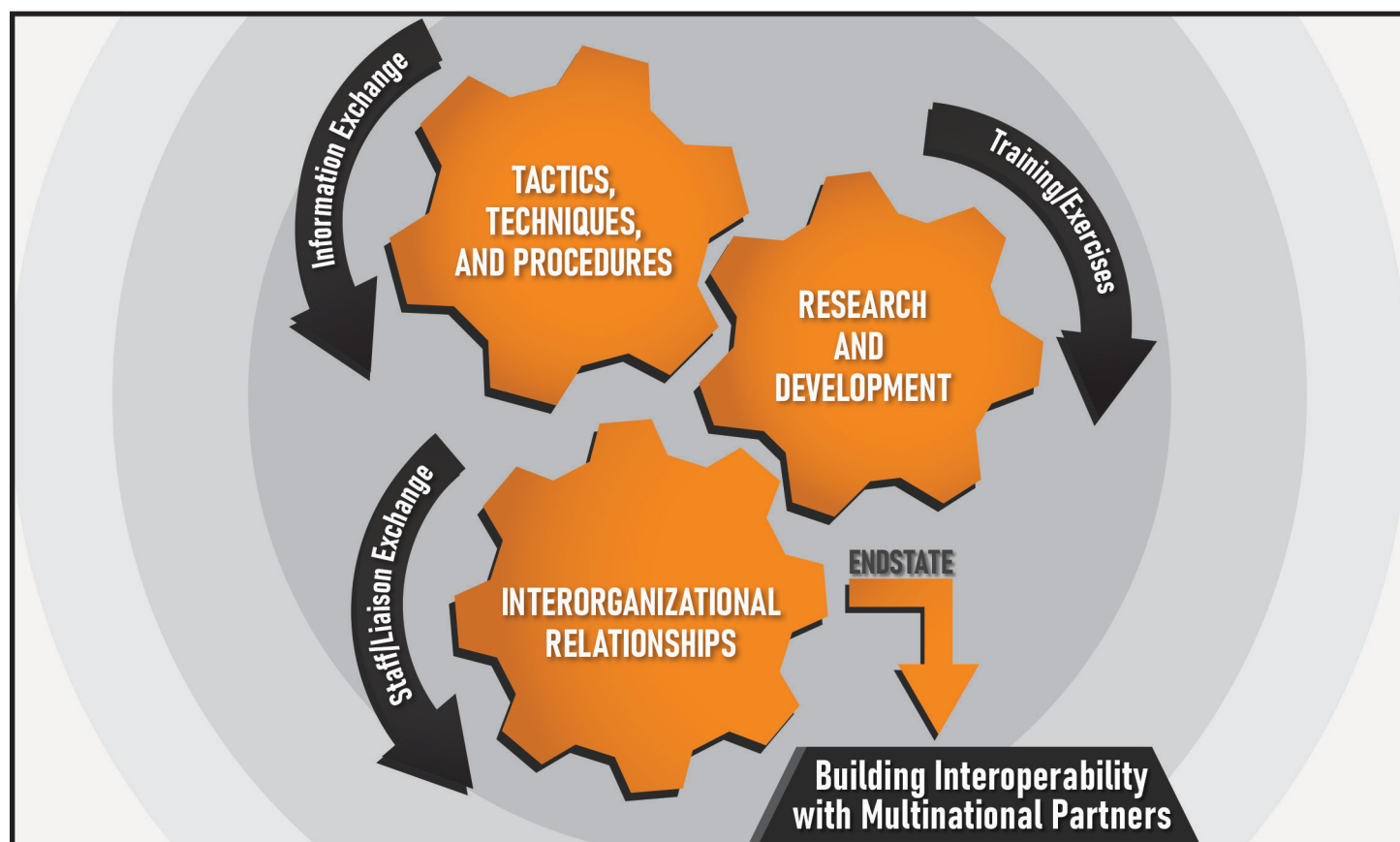


V Corps and subordinate units also passed near real-time information between formations and allies using TransVerse chat.<sup>3</sup> V Corps synchronized the intelligence warfighting function across echelons using chat rooms, each focused on a specific intelligence discipline or function, including targeting, battle damage assessments, general military intelligence, and intelligence operations. The United Kingdom accessed TransVerse through Joint Tactical Chat, NATO's secure, text-based chat system, allowing a seamless transfer of intelligence.

## Human Interoperability

V Corps leveraged trust and rapport built through numerous previous engagements with multinational partners to overcome interoperability challenges. Maintaining bi-weekly ISWGs and sharing all military decision-making process products early and often created an environment that deconflicted friction and facilitated a collective understanding across all formations. Following Avenger Triad 24, the V Corps G-2 has continued to build relationships with multinational partners by participating in staff-to-staff talks with adjacent corps headquarters and executing intelligence-focused tabletop exercises with adjacent corps G-2s.

WFX 24-03 and Avenger Triad 24 created challenges with downtrace allied divisions that could not participate in planning efforts and engagements before the exercises. U.S. divisions and separate brigades that only provided response cells hindered the ability of V Corps to build upon the human dimension before the WFX because of scheduling conflicts and competing requirements. Establishing sustained relationships with allied downtrace units to train and operate as a combined unit well before exercises or operations and leveraging liaison officers to fill gaps where the corps and divisions have not achieved full technical and procedural interoperability can lead to better human interoperability.




Building interoperability through key concepts<sup>4</sup>

There are also technical issues that the Army must address before future collaborations. During WFX 24-03 and Avenger Triad 24, the successful integration of allied partners into the intelligence warfighting function hinged on the support of personnel from digital liaison detachments and the 4<sup>th</sup> Security Force Assistance Brigade, who enabled access to the INSCOM Cloud Initiative on MPE and assisted with integration of CIP data with our allies. However, this is not a sustainable solution to the integration problem. In the future, the challenge of the mission command network interoperability will require a technical solution.

## Conclusion

Future interoperability efforts should include federation of allied mission command networks with the MPE network to enable full access to the GCCS—A COP and CIP web pages, the INSCOM Cloud Initiative, and other available tools to ensure full technical and procedural interoperability for the intelligence community. Additionally, technical interoperability between the MPE and the BICES would dramatically increase enhanced intelligence collaboration among allies and provide redundant procedural interoperability tools to ensure multiple means exist to collaborate and share intelligence data. IEWTPT use on the lower enclave at a releasable level should be sustained, as it increases situational understanding and targeting efforts for both the United States and partner nations in exercise environments. IEWTPT's ability to generate observation reports, electronic intelligence reports, and imagery reports was critical to the success of all training audiences in the exercise; however, this does not replicate

real-world collection efforts, and there remains a pressing need for a cross-domain solution from SIPRNET to MPE. While interoperability efforts continue to trend in a positive direction, we can take additional steps to innovate and improve our human, procedural, and technical domain goals. 

## Endnotes

1. Department of the Army, Center for Army Lessons Learned, *Commander and Staff Guide to Multinational Interoperability* (Fort Leavenworth, KS: Mission Command Center of Excellence, 2023), 57, <https://api.army.mil/e2/c/downloads/2023/01/31/3dadfaa2/20-12.pdf>.
2. Jon Harper, "Palantir Lands \$480M Army Contract for Maven Artificial Intelligence Tech," DefenseScoop, May 29, 2024, <https://defensescoop.com/2024/05/29/palantir-480-million-army-contract-maven-smart-system-artificial-intelligence/>; and Billy Mitchell, "NATO Inks Deal with Palantir for Maven AI System," DefenseScoop, April 14, 2025, <https://defensescoop.com/2025/04/14/nato-palantir-maven-smart-system-contract/>.
3. "Assured Collaboration Solutions Tactical Chat Server (TacChat) Data Sheet," OWL Cyber Defense Solutions, December, 10, 2021, <https://owlcyberdefense.com/wp-content/uploads/2020/12/20-OWL-0438-TacChat-V1.pdf>. TransVerse is an open-source chat client included with the Tactical Chat Server, used by the U.S. Department of Defense, NATO, and Coalition nations.
4. Figure adapted from Figure 2, Department of the Army, Center for Army Lessons Learned, *Commander and Staff Guide to Multinational Interoperability* (Fort Leavenworth, KS: Mission Command Center of Excellence, 2023), 7, <https://api.army.mil/e2/c/downloads/2023/01/31/3dadfaa2/20-12.pdf>; and information provided by the author.

*MAJ Robert Deitz currently serves as the G-2X for V Corps. His previous assignment was as the V Corps analysis and control element (ACE) chief. MAJ Deitz has also served as the theater ACE chief for U.S. Forces Korea as well as working in a wide variety of strategic, operational, and tactical intelligence positions.*