U.S. Army photo by SGT Andres Chandler

M2A2 Bradley Infantry Fighting Vehicle crews assigned to 3rd Battalion, 67th Armored Regiment, 2nd Armored Brigade Combat Team, 3rd Infantry Division, conduct a river crossing with Polish Army Soldiers assigned to the 2nd and 5th Polish Engineer Brigade Battalion during exercise DEFENDER-Europe 20/Allied Spirit at Drawsko Pomorskie Training Area, Poland, June 10, 2020.

Setting the Theater:
Intelligence and Interoperability in DEFENDER-Europe 20

by Major Chad Lorenz

Introduction

Key lessons captured during DEFENDER-Europe 20 can significantly enhance the U.S. Army's efforts to train, build capability, and ensure readiness across the European theater. Phase I of the exercise culminated on 19 June 2020 at the Drawsko Pomorskie Training Area in Poland. The bilateral exercise included United States and Polish Soldiers operating under the control of the 1st Calvary Division (Forward) and featured both airborne operations and a United States-Polish division-size river crossing. Designed as a deployment and tactical exercise to build strategic readiness in support of the U.S. National Defense Strategy and North Atlantic Treaty Organization (NATO) deterrence objectives, DEFENDER-Europe 20 was downscaled because of the coronavirus disease 2019 (COVID-19) pandemic, yet the modified exercise design afforded participants the opportunity to test several important interoperability initiatives. Lessons in three areas stand out as especially significant from an intelligence interoperability perspective:

- Friendly collection and information operations.
- Transition to the Mission Partner Environment (MPE) information sharing capability.
- Provisioning of the U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative (ICI) web interface.

Background

In context, interoperability training opportunities are invaluable in a theater where the Army has a reduced force

posture in comparison to historical Cold War levels. In 1989, approximately 214,000 Soldiers covered a concentrated 175-mile frontage associated with the Fulda Gap. The Fulda Gap included several open passes northeast of Frankfurt, Germany, which was a likely invasion route for Soviet Bloc forces. Today, with the Warsaw Pact dissolved, 33,000 Soldiers supporting Operation Atlantic Resolve face a revanchist Russia across a much wider frontage spanning from Estonia to Bulgaria. To capably defend this terrain, Atlantic Resolve forces depend on allies and partners. In particular, across the Atlantic Resolve nations, this includes a multinational corps, three multinational divisions, and the Enhanced Forward Presence battlegroups in the Baltics and Poland. Additionally, Polish land forces include the Polish 11th, 12th, and 16th Divisions, all of which would play a vital role in stemming aggression in the event of a future military conflict.

Through dozens of exercises conducted annually, U.S. Army Europe hones its interoperability competencies with these elements as well as many other contributing military bodies. DEFENDER-Europe 20 was designed originally as an opportunity to do this at scale. Through the initial mobilization for the exercise, the Army tested force projection capability, coordinating large-scale movements from across multiple airbases and ports for onward movement to training areas in Germany and Poland. When the tactical portion of the exercise was changed to a modified division-level live exercise concept, the 1st Cavalry Division focused on drawing out key interoperability lessons realized in conjunction with elements from the Polish 12th Mechanized Division and the Polish 6th Airborne Brigade.

Friendly Collection and Information Operations

The first key lesson learned pertains to the unique capabilities and authorities our allies and partners possess. Successfully leveraging these competencies can significantly enhance friendly collection and information operations. The Polish 12th Mechanized Division brought two notable tactical capabilities to DEFENDER-Europe 20, both especially suited for European theater operations. The Drawsko Pomorskie Training Area featured dense foliage and numerous water obstacles, and the exercise took place during Poland's wet season. Polish personnel carriers (Rosomaks and BMPs) were equipped to ford large bodies of water and were able to conduct reconnaissance in portions of the training area that Bradley Fighting Vehicles could not access. Polish elements also employed a maneuverable quadcopter unmanned aircraft system that was able to fly underneath low ceilings and in conditions prohibitive to Shadow and Raven operations. The 2nd Brigade Combat Team, 3rd Infantry Division, which was the participating regionally aligned forces brigade combat team, received both capabilities through scenario cross-organizational decisions and proved especially adept at developing ground and aerial collection plans that leveraged them effectively.

The Polish also offered unique collection capabilities and authorities that they employed to protect the integrity of the DEFENDER-Europe 20 exercise in the face of real-world adversary propaganda efforts. Polish open-source intelligence cells constantly monitored the information environment in the period leading up to and during the exercise. Adversary messaging attempted to frame Poland and the United States as irresponsible for continuing the exercise in a COVID-19–threatened environment. When these narratives were published, early Polish open-source intelligence detections enabled timely and robust whole-of-government Polish messaging responses. Subsequently, other participating partners capitalized on this Polish competency to enhance similar narratives.

Overall, successfully incorporating Polish capabilities during DEFENDER-Europe 20 required deliberate arrangements planned and executed by the participating units. For example, the division (forward) G-2 officer in charge met with all unit S-2s during the military decision-making process to develop primary, alternate, contingency, and emergency communication plans and to discuss simulated intelligence collection constructs. During the exercise, the Polish airborne reconnaissance element provided an intelligence liaison officer to the division command post; and the 2nd Brigade Combat Team, 3rd Infantry Division's S-2 embedded an intelligence liaison officer in the Polish 2nd Mechanized Brigade, 12th Mechanized Division's command post with the Polish S-2. These arrangements ensured a common understanding of respective capabilities and the timely sharing of intelligence reporting.

Transition to the Mission Partner Environment

The second key interoperability lesson learned during DEFENDER-Europe 20 pertains to the Department of Defense and U.S. Army transition to the MPE information sharing capability. Incorporation of MPE was a keystone training objective for DEFENDER-Europe 20, with Polish forces accessing the network assisted by a regional signal support team. Network architecture planning enabled both Polish and United States elements to establish MPE network footprints, which capably facilitated the command and control of tactical operations in the Drawsko Pomorskie Training Area. However, although network access was robust, the operational environment information available for initial planning on the MPE network was minimal.

Thus, accessing and sharing items such as specialized maps, advanced terrain analysis, and timely imagery were difficult to accomplish during the exercise.

Capabilities of MPE

MPE will support an estimated 45,000 users with basic human-to-human services, such as chat, email with attachments, web, file-share, and other services, like command and control, weather, logistics, and planning. Specifically, it—

- Simplifies/standardizes information sharing through virtualization technologies.
- Eliminates costly and slow mission-specific build-outs.
- Operates at a variety of classification/releasability levels.
- Is comprised of [Department of Defense] DoD and mission partner-provided infrastructure, services, and agreed upon procedures.
- Allows the team to aggregate, reconfigure, and disaggregate as required.
- Is scalable and can support small enclave to major multination coalition operations.
- Frees planners to focus on unique mission capability needs by using a shared suite of utility-like services, such as email, chat, voice, or video teleconferencing (VTC).[1]

This issue in part hinged on the fact that MPE is not yet a mature network in theater, and therefore the tremendous amount of resources and theater databases currently available on the U.S. network are not yet accessible on MPE. For example, geospatial intelligence analysts and geospatial engineers participating in the exercise did not have access to the many terabytes of map data they would typically use to complete robust intelligence preparation of the battlefield planning. During DEFENDER-Europe 20, a cross domain solution was available at the U.S. Army Europe level. However, the cross domain solution process did not facilitate the transfer of items along a time horizon responsive to the real-time change of mission planning efforts.

Moving forward, in consideration of both future exercises and real-world operations, it is critical that the transfer of information and intelligence databases to MPE be prioritized at every echelon. This will require time and investment. Many products on the U.S. system are already classified at the SECRET//Releasable level and can be transferred to MPE without declassification or disclosure decisions. However, a significant number of other valuable products are overclassified and will require vetting by a foreign disclosure officer. This should happen both proactively, during the product creation phase, and retroactively, in terms of culling existing databases, identifying relevant items suitable for classification downgrade, and transferring those items to the MPE network. Although these solutions involve time-consuming processes, the availability of theater databases on MPE will allow for true interoperability during both exercises and real-world operations with our allies and partners.

Provisioning of the INSCOM Cloud Initiative Web Interface

The third intelligence interoperability takeaway from the DEFENDER-Europe 20 experience stands out as an area in which a training objective was not fully realized. The 1st Cavalry Division's G-2 and G-6 forward elements worked throughout the duration of the exercise to provision the ICI web interface to both United States and Polish counterparts but ultimately proved unsuccessful with Polish elements.

For context, ICI boasts numerous features that make it an ideal interoperability platform. INSCOM's design for the tool allows it to flexibly ingest data sources from across a range of organizations and sources, and users can view/manipulate that data through simple yet logical display tools. As a web interface, it bears some similarity to the Army's Command Post Computing Environment interface, but many features are tailored for intelligence consumers. Access to ICI is also generically afforded to other allies and partners because availability is not hamstrung by cumbersome licensing or software agreements.

At U.S. division and brigade echelons during DEFENDER-Europe 20, ICI worked as a key combat multiplier for intelligence and targeting operations. Using ICI as a common intelligence picture display, the 1st Cavalry Division G-2 was able to overlay operational graphics and develop separate user groups in ICI to ensure disciplined management of threat icons at echelon, in the brigade, division close, and division deep areas. Enemy icons were built and published in the Distributed Common Ground System-Army, and the 66th Military Intelligence Brigade's cross domain solution allowed those icons to appear on both the SECRET Internet Protocol Router and the MPE networks at multiple geographically distanced headquarters, including 1st Cavalry Division's main command post participating from Fort Hood, Texas. The exercise moving target indicator and full-motion video feeds were both readily available to all users with access to ICI. ICI also stood out as the only source of exercise intelligence on the MPE network. The G-2 targeting officer and collection manager used this intelligence to tip and cue simulated intelligence, surveillance, and reconnaissance assets such as Gray Eagle to confirm target locations and differentiate high-payoff targets from other less lucrative collects.

Ultimately, ICI was the only mechanism available to comprehensively share and manage situational awareness with Polish intelligence counterparts. However, despite significant troubleshooting, the Polish were unable to access ICI successfully during the 9-day live portion of the exercise. U.S. theater network technicians required additional approvals to add ICI to the common services hub within the demilitarized zone on the U.S.-owned portion of MPE. As such, Polish network technicians were not able to access ICI on MPE in the same way the United States units could.

NATO network interoperability, including access on MPE, is governed through the Federated Mission Networking initiative. According to NATO, the Federated Mission Networking was built to enable the "rapid instantiation of mission networks by federating NATO organizations, NATO Nations and Mission Partner capabilities, thereby enhancing interoperability and information sharing."[2] NATO accomplishes this through publishing spirals of the capability, or sets of network interoperability standards. Moving forward, key capabilities such as ICI will become even more necessary to enable interoperability as multinational collaboration opportunities increase. In this environment, intelligence leaders must understand network certification and access requirements in order to ensure intelligence equities are adequately postured for multinational operations.

Image courtesy of Allied Command Transformation Public Affairs Office

Conclusion

Overall, a modified DEFENDER-Europe 20 exercise allowed valuable perspective regarding intelligence interoperability initiatives. Future exercises, including the upcoming DEFENDER-Europe 21, offer additional opportunities to expand on the lessons learned and test additional initiatives. Meanwhile, leaders retain the responsibility to codify best practices, ensuring they are reinforced at echelon both in interoperability standard operating procedures and in governing documents such as the Federated Mission Networking spirals. If successful, U.S. forces will operate confidently in the face of adversary aggression, knowing the theater is set and allies and partners are poised to effectively leverage individual competencies toward the realization of multiplicative effects.

U.S. Army photo by SGT Andres Chandler

A U.S. Army first lieutenant assigned to Company C, 3rd Battalion, 67th Armored Regiment, calls out the description, distance, and direction of enemy opposing forces for his infantry dismounted fire team to lay suppressing sectors of fire during exercise DEFENDER-Europe 20/Allied Spirit at Buchierz Range, Drawsko Pomorskie Training Area, Poland, June 10, 2020.

Endnotes

1. "DoD's Mission Partner Environment – Information System (MPE-IS)," Chief Information Officer, U.S. Department of Defense website, accessed 26 August 2020, https://dodcio.defense.gov/In-the-News/MPE/; Department of Defense, Department of Defense Instruction 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD* (Washington, DC: U.S. Government Publishing Office, 25 November 2014), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811001p.pdf.

2. "Federated Mission Networking," NATO Allied Command Transformation website, accessed 26 August 2020, https://ww-.act.nato.int/activities/fmn.

MAJ Chad Lorenz is the S-2 for 1st Armored Brigade Combat Team (ABCT), 1st Cavalry Division, forward deployed to Europe as the regionally aligned forces ABCT. He most recently served as the 1st Calvary Division (Forward) G-2 in support of U.S. Army Europe and the Operation Atlantic Resolve mission. His previous assignments include three tours in Afghanistan and two rotations in the U.S. European Command area of responsibility. MAJ Lorenz is a 2007 graduate of the U.S. Military Academy and received his graduate degree in policy management from Georgetown University in 2017.