

# Fighting Fast and Flat:

## *Use of 'Secure-but-Unclassified-Encrypted' Networks for C2 at the Squadron and Below*

MAJ MICHAEL R. NILSEN  
LTC PETE ERICKSON



*In the not-too-distant future, a Stryker squadron commander in the offense learns that the enemy has shot a Family of Scatterable Mines (FASCAM) obstacle, engulfing one of the squadron's troops while it attempted to breach the enemy's integrated defensive belt. It is a perilous moment. Momentum stalls, and friendly forces face significant risk of sustaining greater casualties. As the commander and leaders in the tactical command post (TAC) quickly think through options to continue the attack, only one stands out: reposition the squadron's attached North Macedonian company so that it can bring its dismounted anti-tank weapons to the fight. However, speed is essential; failure to accomplish this task quickly risks the success of the entire NATO multinational division headquarters.*

*Fortunately, the Stryker squadron has integrated with the North Macedonian company via a Secure-but-Unclassified-Encrypted (SBU-E) partner network, which enables interoperability alongside Integrated Tactical Network (ITN) equipment. Use of such a network enables the squadron to disseminate required fighting products quickly and securely, resulting in a high degree of shared understanding. Within two hours of notification, the North Macedonian company receives a fragmentary order and a concept sketch from the squadron, makes and disseminates its plan, and repositions itself at key terrain near the forward line of troops (FLOT). The squadron resumes the attack, and the North Macedonians destroy more than a company's worth of enemy BMPs and tanks.*

The scenario described above is not far-fetched. In fact, it describes what occurred to 3rd Squadron, 2nd Cavalry Regiment during the final day of Exercise Saber Junction 23, which occurred in September 2023 at the Joint Multinational Readiness Center.

As modern threats have evolved in recent years, Army units have recognized several imperatives, including trimming the size of command posts, maintaining connectivity in contested environments, and distributing useful fighting products that generate speed and shared understanding on the battlefield. This article describes one way that Army units at the squadron level and below can achieve the last two of these imperatives in cooperation with partner units. In most situations, Army tactical units can significantly increase their capabilities by exercising a SBU-E network rather than relying solely on their traditional classified networks. After framing the general need for a network that is widely accessible yet still secure, this article explains what a SBU-E network is and then highlights its major advantages, chief of which is the ability to better integrate and operate with our multinational partners.

## **The Need for a SBU-E Network**

Most leaders who have worked with multinational partners at some point during their careers would likely agree that our current U.S. security processes, caveats, and authorities — which are in place for understandable reasons — do not always facilitate seamless integration with our multinational partners. And yet, the exercise of command and control (C2) and the achievement of shared understanding are essential to achieving unity of effort and success on the battlefield.<sup>1</sup> In the modern European theater, the opportunities and challenges of working with multinational partners can be especially acute. Indeed, the chance for U.S. forces to operate alongside of multinational partners enables NATO to become stronger together, but our current security measures can sometimes seem a necessary but frustrating roadblock to effective integration with these same partners. When tactical units cannot talk to each other, nor access the same battlefield information (such as common graphics, operation orders, and other reports and data), the same units cannot fight as effectively as possible, and the whole operation can suffer. A SBU-E network can help overcome this important challenge.

### **What is SBU-E?**

Initially fielded as part of a new system that leverages technology known as the ITN, SBU-E is a cost-effective, secure-but-unclassified network that creates a flattened communications architecture across multiple types of electronic devices.<sup>2</sup> Using a level of encryption that is comparable to electronic banking, SBU-E provides a secure medium by leveraging advanced encryption protocols.<sup>3</sup> A primary feature of a SBU-E network is access to the Team Awareness Kit (TAK) software application, a flexible software suite that can be used in various operational environments. This common operating picture (COP) tool for squadrons/battalions down to the squad level is fielded as part of ITN to many infantry brigade combat teams (IBCTs); better yet, numerous civilian and partner militaries use TAK.

Across the world, the ability for U.S. forces to operate with and alongside our multinational partners is paramount. And yet, the U.S. military's use of classified networks such as the Secret Internet Protocol Router (SIPR) can at times be both an advantage and a hindrance. On one hand, SIPR networks work very well within the U.S. joint force, mainly because access to these networks is not an issue. On the other hand, use of classified networks hinders the ability for U.S. forces to share critical mission data with most allies and partners. Other networks besides SIPR, such as the Mission Partner Environment (MPE), sought to overcome this challenge, and to some degree, they have. However, ensuring reliable and secure access for our multinational partners remains an enduring issue. Tactical formations require a simple and easy way to connect and share vital battlefield data, such as friendly and enemy position location information (PLI). A SBU-E network provides a simpler and more effective solution that leverages a commercial off-the-shelf (COTS) hardware and software capability to solve tactical communication and interoperability challenges.

### **Advantages of SBU-E**

There are three main advantages that operating with a SBU-E network affords tactical military units. First, a SBU-E network is widely accessible yet secure. Users gain access by acquiring an internet connection, an end user device, and controlled-access permissions from the network administrator. Without significant classification caveats, allies and partners can use SBU-E to quickly integrate with U.S. units, greatly enabling shared understanding and decision-making. While U.S. classification caveats will always remain relevant and important, not every piece of warfighting data must be classified. Indeed, much of the intelligence that is most relevant to tactical-level units, such as enemy PLI, is highly perishable. Therefore, assigning a high level of classification to information that will be irrelevant or inaccurate in less than 24 hours inhibits battlefield coordination with multinational partners. Units can collaborate using a SBU-E network by sharing operation orders, full motion video, pictures, reports, and other data to help increase the speed and effectiveness of decision-making and fighting on the battlefield.

Second, a SBU-E network does not render legacy communication systems or higher-classified mediums obsolete. SBU-E can integrate with existing systems operating at higher classification levels when properly



**A Soldier in the 2nd Cavalry Regiment communicates using a Nett Warrior End User Device during Exercise Saber Junction on 9 September 2023 in Germany. (Photo by 1SG Michel Sauret)**

configured, thus ensuring security and preventing spillage. This allows innovation on SBU-E to continue concurrent with the use of existing capabilities.<sup>4</sup> By employing legacy networks and augmenting their use with SBU-E, commanders not only achieve the highest degree of intelligence prior to major operations or exercises, but they also position their commands to leverage the possibilities that data affords while warfighting — something that leaders have recognized as important moving into the future.<sup>5</sup>

Furthermore, the compatibility of SBU-E and networks such as SIPR and MPE means that command centers can track where units are on the battlefield, regardless of which network generates the data of a particular unit's location. For instance, during Exercise Saber Junction, the squadron TAC effectively led the squadron for more than 48 hours while dispersed and on the move using SBU-E. Ultimately, this compatibility enabled location data from sources such as smartphones and secret systems like the Joint Battle Command-Platform (JBC-P) to populate on a single common operating picture, greatly enabling the squadron TAC to make decisions and survive.

A final advantage is that a SBU-E is more cost-effective than previous legacy solutions.<sup>6</sup> SBU-E is a cloud-based system that avoids the expensive hardware and IT infrastructure that comprise traditional computer networks.<sup>7</sup> Thus, an ally or partner may pursue their own SBU-E network using various cloud-based commercial software solutions, such as Amazon Web Services, in a relatively simple manner.<sup>8</sup>

### **Balancing Operational Security with Operational Flexibility**

Anytime the military works with partners, leaders must responsibly ask themselves: How can we secure our own intelligence formation while sharing enough with our trusted partners to both accomplish the mission and not place anyone at greater risk than what is necessary? It is a question that oftentimes lacks an easy answer.

There may be situations in which a SBU-E network is not appropriate. For instance, although the Army is keen to embrace SBU-E, our joint partners are still evaluating its utility. But practically speaking, these situations constitute a small minority of overall operations for echelons that are generally higher than a brigade. The situation involving the North Macedonian company referenced in this article's introduction was dire. The North Macedonians could not and did not operate a legacy U.S. radio, such as an Advanced System Improvement Program (ASIP), due to U.S. disclosure laws. However, with access to a SBU-E network and new ITN equipment, the North Macedonians were able to communicate over TSM radios and on

devices such as the End User Device (EUD), a government-provided smartphone. Their ability to do so constituted a critical component to their successful operation.

For the near future, as technologies continue to rapidly improve and evolve, a limiting factor to achieving the flat communications and enhanced situational awareness described in this article will not be technology itself but rather the authorities and methods that govern how tactical Army formations implement their networks and communications equipment. We are emphatically not arguing for the wholesale or irresponsible shedding of these important authorities, processes, and caveats that safeguard our national interests. Yet, there is an opportunity, particularly as conflicts all over the world unfold, to wisely adapt. We as military professionals should therefore continue this discussion about how to best balance perfect operational security and flexibility based on the unique facets of each mission. No two partnered forces are the same, but the need for tactical U.S. Army units to share vital information in order to integrate on the battlefield will remain constant.

### Conclusion

This article emphasizes that tactical Army units, particularly at the squadron level and below, have much to gain by adopting and implementing a SBU-E network to share critical fighting products, such as operation orders and reports, and establish a COP. Compared to other networks of higher classification that the Army has previously used, a SBU-E network is easy to access and cost effective. Importantly, units can implement a SBU-E network in a manner that augments the capabilities provided by the Army's existing networks of higher classification. As Army and Department of Defense leaders have noted, our ability as a nation to implement strong deterrence against a variety of threats across the world requires U.S. military forces that can operate alongside our multinational partners.<sup>9</sup> Use of a SBU-E network in most situations helps achieve this important goal.

### Notes

<sup>1</sup> Allied Joint Publication 1-0, *Allied Joint Doctrine*, December 2022, 112.

<sup>2</sup> "Integrated Tactical Network," Program Executive Office Command Control Communication-Tactical, <https://peoc3t.army.mil/tr/itn.php>; MAJ Matthew S. Blumberg, "The Integrated Tactical Network, Pivoting



**A troop commander in 3rd Squadron, 2nd Cavalry Regiment provides a status update to his higher command using a radio and Nett Warrior system during a training exercise in Lithuania on 13 June 2018. (Photo by PFC James Crowley)**

Back to Communications Superiority," *Military Review* (May-June 2020), <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2020/Blumberg-Int-Tactical-Network/>.

<sup>3</sup> Sydney J. Freedberg Jr, "Keep Moving or Die: Army Will Overhaul Network for Rapid Maneuver in Big Wars," *Breaking Defense* (5 May 2023), <https://breakingdefense.com/2023/05/keep-moving-or-die-army-will-overhaul-network-for-rapid-maneuver-in-big-wars/>; Corinne Berstein, "Advanced Encryption Standard (AES)," TechTarget, <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>.

<sup>4</sup> "Integrated Tactical Network."

<sup>5</sup> Erik Davis, "The Need to Train Data Literate U.S. Army Commanders," *War on the Rocks* (17 October 2023), <https://warontherocks.com/2023/10/the-need-to-train-data-literate-u-s-army-commanders/>.

<sup>6</sup> Blumberg, "The Integrated Tactical Network."

<sup>7</sup> "Key Differences Between Cloud Computing vs. Traditional," AZTech IT, 7 September 2018, <https://www.aztechit.co.uk/blog/cloud-computing-vs-traditional>.

<sup>8</sup> 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](https://www.army.mil/article/267180/griffin_shock_23_strengthens_nato_readiness_through_cloud_enabled_applications); Defense Threat Reduction Agency's Chemical and Biological Technologies Department, video, "ATAK in the Field: Forging a Tactical Edge," 29 May 2020, <https://www.dvidshub.net/news/367459/atak-field-forging-tactical-edge>.

<sup>9</sup> David Vergun, "Austin Emphasizes Importance of Working with Partners in Center, South America," DoD News, 29 October 2021, <https://www.defense.gov/News/News-Stories/Article/Article/2826812/austin-emphasizes-importance-of-working-with-partners-in-central-south-america>.

**MAJ Michael R. Nilsen** currently serves as the operations officer for 3rd Squadron, 2nd Cavalry Regiment. Prior to the 2nd Cavalry Regiment, MAJ Nilsen served in the XVIII Airborne Corps and 2nd Security Force Assistance Brigade. For the last six years, he has helped spearhead SBU-E and other innovations for multiple U.S. Army units. Additionally, MAJ Nilsen is a U.S. Army Command and General Staff College (CGSC) Master Tactician, Level II Joint Qualified Officer, and Strategic Studies graduate. He holds a bachelor's degree from the U.S. Military Academy at West Point, NY, and a Master in Military Art and Science from CGSC.

**LTC Pete Erickson** currently serves as commander of 3rd Squadron, 2nd Cavalry Regiment. Prior to command, LTC Erickson served as the regimental operations officer for the 3rd Cavalry Regiment. He is an Andrew J. Goodpaster Fellow and holds a PhD in Political Science from the University of Wisconsin-Madison.