A field artillery officer with the Multifunctional Strike Troop, 2nd Armored Brigade Combat Team, 1st Cavalry Division, uses an Android Tactical Assault Kit (ATAK) at National Training Center Rotation 26-02, November 2, 2025. (U.S. Army photo by 1LT Tyler Williams)

# The Swivel Chair War: How Disconnected Systems are Failing the Modern Soldier

by Major Eric S. Killian and Staff Sergeant Joshua S. Griggs

## A Communications Challenge

Over the last four years, the U.S. Army has been collecting and learning from observations gathered during the war in Ukraine, resulting in the Transformation in Contact (TiC) initiative's efforts to innovate, learn, refine, and develop solutions faster. Specific lines of effort include improving command post survivability and exploiting a transparent battlefield. The push to reduce physical and electronic footprints across echelons has led to changes in command and control, both in architecture and in mission command systems. However, in our haste to streamline communications and reduce our footprint, we may increase the risk to our ability to communicate intelligence across echelons.

This article discusses the communications challenge between a brigade that relies primarily on sensitive but unclassified mission command systems and a division that collects and disseminates intelligence over the Secret Internet Protocol Router Network (SIPRNET). It offers recommendations to ensure brigades can receive intelligence while still taking advantage of the capabilities on sensitive but unclassified systems.

During National Training Center (NTC) Rotation 26-02, the 1st Cavalry Division (1CD) employed a multidiscipline analysis team–situational understanding (MDAT-SU) to support a brigade combat team (BCT) as part of continued implementation experiments for the intelligence and electronic warfare battalion-next force design update. This rotation also served as the TiC 2.0 rotation, during which the BCT experimented with a wide array of new mission command system equipment, such as the Android Team Awareness Kit. Because all of these systems resided on the Nonclassified Internet Protocol Router (NIPRNET), the BCT was forced to rely on NIPRNET communications both internally and up to 1CD. The BCT's reliance on NIPRNET communications was exacerbated by frequent displacement—an action that was significantly more disruptive to SIPRNET than to NIPRNET. This degraded the 1CD's ability to pass intelligence to, and receive combat information from, the BCT.

To address this issue, the MDAT-SU "swivel-chaired" selected intelligence from the Army Intelligence Data Platform (AIDP) on SIPRNET to the Maven Smart System (MSS) on NIPRNET, where the BCT could access it. However, this manual workaround complicated the MDAT-SU's mission of delivering situational understanding, introduced opportunities for error, reduced timeliness, and raised policy concerns related to classification management.

One of the MDAT-SU's primary tasks was creating and maintaining the BCT common intelligence picture (CIP). A vast stream of reporting from national technical means, the division's organic collection assets, and analysis by signals intelligence and geospatial intelligence analysts within the MDAT-SU was used to build the CIP. To make sense of the reporting, analysts employed a SIPRNET AIDP-generated map displaying the data generated from the reports. Significant, high-confidence reporting was then manually transferred to the NIPRNET CIP on MSS. The NIPRNET CIP was maintained at a granular level, depicting detailed individual weapon systems and pieces of equipment. Responsibility for maintaining both the analytical map and the CIP, and for making sense of the intelligence to understand the enemy's composition, disposition, and intent, fell to one or two MDAT-SU Soldiers per shift.

The "swivel chair" process was entirely manual: when updates for the CIP came in, the receiving Soldier had to refer to the corresponding report and then build an icon on the CIP, adding location, unit type and size, and other corresponding variables. This is a simple process, but when supporting an armored brigade on the attack, maintaining the CIP becomes a nonstop activity in which mistakes, delays, and oversights have serious consequences.

Spillage concerns further complicated the process. Reporting arrived with numerous classifications and caveats, and analysts were neither trained nor authorized to downgrade classification levels. Instead, they had to determine which aspects of reports were classified and could not be represented on the NIPRNET CIP, and which were safe to depict. While this issue was fairly easy to manage in the simulated exercise environment, in real-world operations, it would result in a far less informative and accurate CIP. The necessity of working with a NIPRNET CIP hinders BCT and battalion

leadership's ability to make informed decisions. Between details being omitted to avoid spillage and delays from analysts manually transferring intelligence from SIPRNET to NIPRNET, the BCT receives a less specific product that takes longer to produce. The all-source analyst dedicated to maintaining the CIP has considerably less time to conduct analysis, develop assessments, and deliver completed products to the BCT. Furthermore, any time the analyst is pulled away from CIP maintenance, the product begins to lose relevance, risking becoming a source of confusion.

## Potential Solutions

There are three potential solutions to this communications problem: implementing a cross-domain solution (CDS); rehearsing and refining swivel-chair processes; and prioritizing SIPRNET for BCTs. However, only one of these will work in practice.

**Implementing a cross-domain solution.** A CDS would automatically filter data and pass the appropriate information to the NIPRNET-based mission command system. For this filter to work, every iota of information in every report would need to be properly classified. Because each report's overall classification must match the highest level of any single element of the report, the CDS could not simply reference the overall classification and move on. Instead, it would need to reference each element of the report and pass along only the unclassified portions, resulting in less detailed but potentially still useful information. In real-world operations, however, the most meaningful elements of any report will be classified, thereby diminishing the value of the CDS. This approach may work if the theater issues a more permissive security classification guide and reports include portion markings enabling the CDS filter to pass more information.

**Refining and rehearsing swivel-chair processes.** Improved processes may enhance analysts' ability to quickly digest, analyze, and transcribe information from SIPRNET to NIPRNET, but the extent of this improvement is uncertain. It is still not a highly efficient manual process. In contrast, when a SIPRNET-based AIDP CIP is paired with a SIPRNET-based MSS, the customer can see it within seconds. Because no additional work is required, the analyst is free to interpret and refine the intelligence, buying time for production, discussion, briefings, and improved analysis. It is a combat multiplier. In the controlled environment provided by NTC, the data processed by the MDAT-SU was merely a fraction of what would be processed during large-scale combat operations. Likewise, the enemy formation was relatively small, and the array of sensors feeding the MDAT-SU produced only a fraction of what would be available from real-world national collection. Swivel-chair data transfer delays would be magnified, likely leading to a decision to transfer only data related to key units and equipment. This would defeat the purpose of the MDAT-SU, upon whom the brigade relies for detailed analysis. There is no amount of refined and rehearsed swivel-chair activity that can compete with eliminating the swivel-chair process entirely.

**Prioritize SIPRNET.** If a BCT wants to "fight the enemy, not the plan," it must prioritize SIPRNET. This is the only solution that effectively addresses the swivel chair dilemma. BCTs have fought at NTC on SIPRNET for decades. TiC 2.0 solutions that prevent BCTs from fighting on SIPRNET are not solutions at all. At a minimum, the BCT S-2 section must have a method to maintain a stable SIPRNET connection. Even if the BCT fights internally on NIPRNET, the S-2 should receive timely intelligence from the MDAT-SU on SIPRNET and manually transfer (swivel chair) key elements of that intelligence to NIPRNET. If a BCT absolutely cannot establish SIPRNET and must transition to the Joint Battle Command Platform and analog operations, the MDAT-SU can still provide the information at the proper classification level to enable that fight. However, the BCT must adjust expectations, knowing it will not encounter a fully transparent battlefield.

## Connecting the Echelons

The data transfer challenges experienced during NTC Rotation 26-02 highlight a critical military modernization lesson: introducing new technology without adapting doctrine, training, and communication protocols creates inefficiency and increases operational risk. The "swivel chair" scenario forced upon the MDAT-SU, caught between the division's SIPRNET-based AIDP and the BCT's NIPRNET-based MSS, significantly increased workload, delayed intelligence delivery, and created a dangerous potential for information loss. To resolve this challenge and prevent future occurrences, BCTs must have assured, steady SIPRNET connectivity between the S-2 and the MDAT-SU. By doing so, the Army can ensure that technological modernization initiatives truly enhance, rather than hinder, the warfighting function.

*MAJ Eric Killian is the Analysis and Control Element Chief for the 1st Cavalry Division (1CD) at Fort Hood, TX. A graduate from Texas State University, he assumed this role in late 2024 following assignments as the 1CD Sustainment Brigade S-2 and the III Armored Corps Fusion Officer in Charge. MAJ Killian's command experience includes serving as the Headquarters and Headquarters Company commander for the 1st Armored Division/U.S. Forces-Army during a deployment to Bagram, Afghanistan. His earlier commands include the 1st Armored Division SIS Company and a recruiting company. Earlier in his career, he was the S-2 for the 40th Brigade Engineer Battalion, deploying to Kuwait for Operation Spartan Shield.*

*SSG Joshua Griggs is a Fusion Team Leader in the 1CD Analysis and Control Element. Since joining 1CD in Poland, he has taken part in Operation Combined Resolve 25-01 and supported multiple Pegasus Forge exercises and two National Training Center rotations. Before that he served as a battalion S-2 noncommissioned officer in charge and brigade intelligence support element squad leader with the 25th Infantry Division. He began his career at the National Training Center where he was a Blackhorse intelligence analyst and Puma Team Leader.*