34th Infantry Division Soldier cools the expandable van temporary sensitive compartmented information facility environmental control unit using a commercial off-the-shelf water gun. (U.S. Army Photo by SPC Tyler Becker)

NEAR-TERM COMMAND POST SURVIVABILITY: LESSONS LEARNED FOR THE INTELLIGENCE COMMUNITY

BY CAPTAIN AUSTIN LIND

Introduction

Division G-2's must evolve to maintain survivability during large scale combat operations. Command post (CP) survivability is a critical aspect of military operations during large-scale combat; however, the traditional CP configuration, with electronic emitters, dozens of generators and vehicles, and extensive support requirements, is easily targeted and destroyed by an ever-expanding array of threat sensors and shooters. The 2023 *Military Review* article, "The Graveyard of Command Posts," addresses the vulnerability of traditional CPs.[1] Near-term solutions for more survivable CPs require an assessment of tactics, techniques, and procedures (TTPs) focused on survivability using existing equipment. To increase survivability, division intelligence elements must operate in the rear and increase the mobility of forward elements. At the same time, the intelligence warfighting function must consider security requirements when planning distributed operations.

Division intelligence staff require access to sensitive compartmented information (SCI) to conduct operations and inform the commander's decision making. SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which must be managed within formal access control systems established by the Director of National Intelligence.[2] SCI may only be processed in a secure, enclosed area designed for processing and handling SCI, known as a sensitive compartmented information facility (SCIF).

34th Infantry Division's temporary sensitive compartmented information facility while conducting dispersed operations in the U.S. Central Command area of responsibility. (U.S. Army Photo by SPC Tyler Becker)

While deployed to the U.S. Central Command area of responsibility, the 34th Infantry Division fielded the Integrated Tactical Network (ITN) as part of the Army 2030 and Transformation in Contact initiatives. Concurrently, the 34th Infantry Division was tasked with conducting distributed CP operations to provide feedback to the Army on CP survivability. The goal was for the division to train on the new ITN equipment, conduct a CP survivability assessment using the ITN equipment, and support mission requirements for Operation Spartan Shield while distributed. To accommodate this requirement, the 34th Infantry Division G-2 used a distributed mobile temporary SCIF, or T-SCIF, capable of all-source intelligence operations.

Lessons Learned for the Intelligence Community

The 34th Infantry Division G-2 incorporated five principles of near-term CP survivability drawn from the March 2023 U.S. Combined Arms Center white paper, *Near-Term Command Post Survivability*,[3] into the planning process, which culminated in a successful command post exercise in August 2024. (The article addresses integrating the five principles in a later section.) The G-2's experience with distributed SCIF operations and the ITN equipment offers valuable insights and lessons into near-term CP survivability and ways ahead for the intelligence warfighting function when conducting distributed operations.

The special security officer is integral to distributed command post intelligence operations. The special security officer (SSO) is responsible for overseeing the physical and technical security measures that protect SCI. In a distributed environment where intelligence activities are conducted across multiple locations, the SSO must ensure security measures are applied consistently and effectively across all locations. This may involve working with other SSOs, special security representatives (SSRs), and security managers. Accreditation documentation for SCIFs must be completed by an SSO who should be an E-7 or above and appointed by the senior intelligence officer.[4] SSRs are physically located at distributed sites, where they assist with implementing the SCI Security Program and managing SCIF operations under the direction of the SSO. SSRs can be E-5s and above and are appointed by the senior intelligence officer.[5] The SSO and SSRs must have in-depth knowledge of both Army Regulation 380-28, *Army Sensitive Compartmented Information Security Program*, and Intelligence Community Directive 705, *Sensitive Compartmented Information Facilities*, before conducting distributed operations.[6]

SCIFs must be mobile in large-scale combat environments. A fixed SCIF does not offer the mobility necessary for survival in large-scale combat operations. A T-SCIF is the ideal type of facility for distributed intelligence operations.

> ***T-SCIFs are used . . . for a limited time where physical security construction standards associated with permanent facilities are not possible. They may include hardened structures (buildings and bunkers for example, truck-mounted or towed military shelters, tents, prefabricated modular trailers or buildings, and areas used on aircraft and surface and subsurface vessels).***[7]

Flexibility, adaptability, and mobility are necessary for CP survivability. The 34th Infantry Division G-2 found that using an M1087A1 Expandable Van in conjunction with military intelligence (MI) systems provided the best mobility and met the most operational requirements for large-scale combat operations. An expandable van offers a large workspace that can accommodate up to 10 soldiers at one time alongside the necessary MI systems. This provided the division G-2 with a tactical mobile CP that enabled all the intelligence functions to operate within a single controlled space.

Utilizing an expandable van as a mobile T-SCIF also offers several security advantages because this type of mobile T-SCIF conforms better to SCIF regulations than an existing permanent building in a combat operations environment. Intelligence

Community Directive 705 states that any proposed T-SCIF structure previously occupied by a non-U.S. element must undergo a technical surveillance countermeasures (TSCM) inspection to prevent or detect the interception of sensitive or classified information. Therefore, any permanent type hardened structure in a deployment area would require a TSCM inspection.[8] However, division headquarters do not have the organic capability to conduct a sweep for surveillance devices, and coordinating a TSCM inspection is time-consuming and not feasible during large-scale combat operations. The Accrediting Official can avoid the risk posed by surveillance threats during large-scale combat if units use this mobile T-SCIF concept. Other security benefits include acoustic protection for a classified discussion area and an easily controlled single point of access to prevent surreptitious or forced entry. The mobile T-SCIF offers demonstrable benefits; however, division G-2s are not organically equipped with expandable vans. This is a capability gap that the Army should consider. Division intelligence must be allocated expandable vans or similar vehicles or find an alternative means of making a mobile T-SCIF when planning for large-scale combat operations.

Establishing a T-SCIF takes extensive planning and preparation and requires multiple steps. Establishing a T-SCIF is a complex undertaking vital for maintaining secure communications and intelligence operations, particularly in rapidly evolving environments. While established procedures exist, practical experience reveals critical nuances in successful T-SCIF deployment and sustained operation. This section covers key areas such as site selection, security protocols, personnel management, and accreditation. This analysis provides valuable insights for personnel responsible for establishing and maintaining secure intelligence capabilities in dynamic operational environments.

Site Selection. The location should be secure, free of counter-surveillance threats, and have adequate space for intelligence equipment and personnel. The SSO, SSRs, and military intelligence systems maintainers should utilize pre-deployment site surveys whenever possible to ensure the site is protected against surreptitious or forced entry.

Design and Construction. T-SCIFs have strict construction and security requirements, including establishing layers of physical security, access control, and manning requirements.

Equipment and Manning. Conduct pre-combat checks and inspections on vehicles and equipment, including workstations and MI systems. Mobile T-SCIFs contain sensitive equipment but are not equipped with an intrusion detection system. Therefore, they require adequate manning by SCI-indoctrinated personnel to accommodate 24-hour operations in a large-scale combat environment.

Personnel Security. All personnel must meet clearance requirements. The SSO or SSR should post a security clearance access roster at the single, controlled entrance for access control and verification of personnel.

Training. All T-SCIF personnel must train in proper handling of SCI information and sensitive equipment; they must also be grounded in T-SCIF procedures, including rehearsals of the standard operating procedures and emergency action plan.

Accreditation. The accreditation process involves a thorough review of the facility's physical and technical security measures, as well as its personnel, policies, and procedures. While the Accrediting Official determines what documentation is necessary for accreditation, it is the SSO who creates those documents with assistance as needed from SSRs.

Post Accreditation. Once the Accrediting Official approves the T-SCIF, the SSO or SSRs handle providing updates relating to the current locations and status of T-SCIFs under their control as directed by the combatant command SSO.[9]

Intelligence systems maintainers are instrumental in enabling distributed CP intelligence operations. Network access requests, communications security requests, and network testing of MI systems are complex, often unpredictable processes and should be factored into planning well before a division conducts distributed operations. MI systems maintainers are essential to these processes.

Establish competencies in convoy operations and plan for the wear and tear of intelligence equipment. While the mobile nature of the T-SCIF offered undeniable advantages, it also presented some unanticipated challenges. For example, when conducting dispersed operations, the expandable van's environmental control unit (ECU) could not compensate for both the outside temperature and the communication equipment's interior heat generation. To combat this, the 34th Infantry Division G-2 shaded the ECU with camouflage netting and used a water sprayer to cool the unit to prevent it from overheating.

Intelligence equipment in permanent structures, like those used during counterinsurgency operations, rarely moved and thus did not require regular recalibration. However, because of the jarring and vibration resulting from displacing the 34th Infantry Division G-2 T-SCIF, the equipment often required recalibration. Going forward, the Army may need to re-examine the design of intelligence equipment for better durability in mobile operations.

Establish clear classification guidance for the Integrated Tactical Network. The ITN is comprised of radios operating on the tactical scalable mobile ad-hoc networking waveform, which allows them to work in secret and sensitive but unclassified-encrypted (SBU–E) enclaves. These radios provide line-of-sight voice, data, and near real time friendly force position, location, and identification (PLI). Any equipment providing near real time PLI in the U.S. Central Command (CENTCOM) area of responsibility should be classified at the secret level,

The 34th Infantry Division expandable van temporary sensitive compartmented information facility environmental control unit. (U.S. Army Photo by SPC Tyler Becker)

depending on the mission; however, CENTCOM's classification guidance did not address SBU–E equipment, and there was no clear guidance on individual PLI data. CENTCOM is working with both the Joint Staff and Army Program Executive Office to address this emerging technology, but end-user organizations must continue to push for updated guidance.

Integrating Near-Term Survivability Principles[10]

The evolving threat landscape demands a re-evaluation of traditional CP security measures. Modern adversaries possess increasingly sophisticated capabilities to detect, target, and disrupt command and control nodes. Consequently, near-term survivability principles—encompassing dispersion, sub-surface cover and concealment considerations, signal management, and nodal movement—are paramount. This section explores the practical application of these principles, drawing on recent intelligence operations observations and offering recommendations for bolstering CP resilience in a contested environment.

Rearward functional echelonment. Most intelligence capabilities will remain in the rear. Divisions must assess the allocation of MI forces among distributed CPs in the large-scale combat environment.

Dispersion. The distributed CP concept requires dispersion of the division staff elements. Nodes must be broken down into sub-nodes, or "micro CPs," each with two mobile T-SCIFs providing top secret capability not only for intelligence personnel, but also for other division staff elements such as the G-31 (Training, Readiness, and Exercise Division) space and cyberspace electromagnetic activities personnel. Two mobile T-SCIFs provide redundancy to support intelligence operations in the event of a micro CP loss. The dispersed operations conducted by the 34th Infantry Division G-2 had two vehicles within its pod, mitigating the possibility of visual detection and targeting by indirect fire.

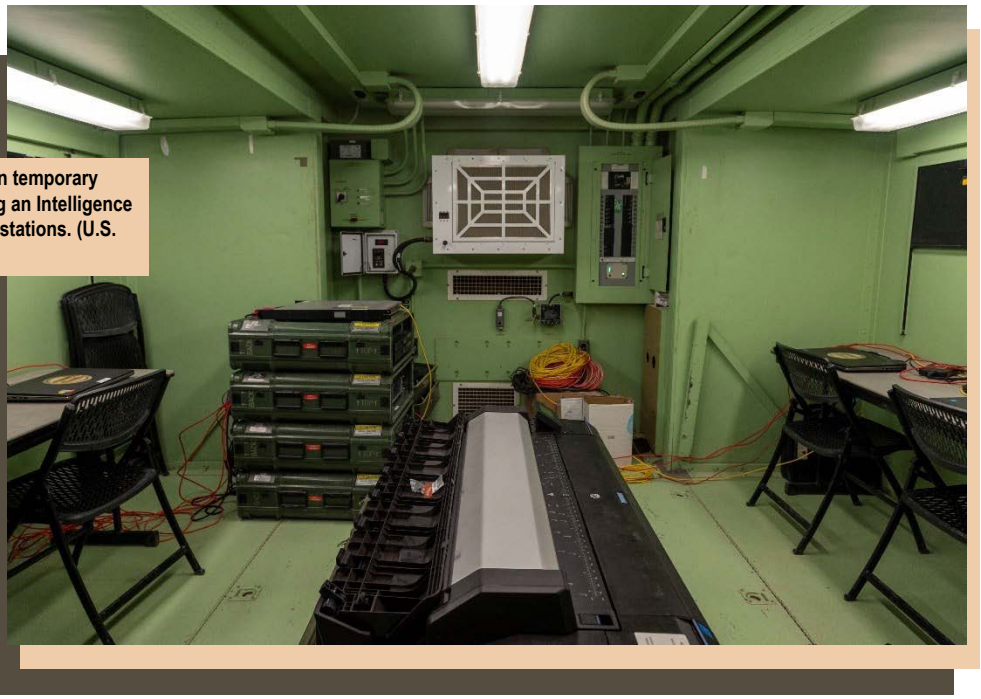
Sub-surface cover and concealment. We previously addressed the security risk of using permanent-type hardened structures in a large-scale combat environment. This includes sub-surface structures. While these structures can certainly provide cover and concealment for a T-SCIF, they nevertheless pose a surveillance security risk for SCIF operations and limit the CP's mobility. Additional planning is necessary to ensure the site is suitable for T-SCIF emplacement and MI system connectivity. Using hardened or sub-surface structures will require expanded TTPs to ensure intelligence elements have the flexibility, adaptability, and mobility necessary for CP survival.

Signal management. MI systems have a pronounced, identifiable signature, making them easier to target. Additionally, while ITN radios do not have distinct signatures when operating en masse, using them enhances the electromagnetic signature. The 34th Infantry Division G-2 attempted to gather baseline readings of electromagnetic activity and bandwidth usage for dispersed MI systems; however, the request did not have a high enough priority to receive collection. Use of MI systems in distributed operations nevertheless requires additional analysis to determine how they can "swim" within the electromagnetic spectrum, especially in austere environments.

Nodal movement. The 34th Infantry Division G-2 designed its mobile T-SCIF to pack up and jump to a new location within 24 hours, mitigating the risk of accurate, targetable detection by threats. By using two distributed mobile T-SCIFs, the division G-2 could alternate survivability bounds to ensure that at least one forward intelligence element is always operational.

Operation Spartan Chain

During Operation Spartan Chain, the 34th Infantry Division's mission command deployment within the larger Operation Spartan Shield contingency operation, the G-2 established a T-SCIF with connectivity to secret and top secret enclaves



Interior space of 34th Infantry Division's expandable van temporary sensitive compartmented information facility, displaying an Intelligence Fusion Server, Geospatial Intelligence plotter, and workstations. (U.S. Army Photo by SPC Tyler Becker)

within two hours. The G-2 can minimize set-up time further with the refinement of standard operating procedures and processes. The available space inside the expandable van allowed for one Geospatial Intelligence (GEOINT) Workstation, one GEOINT plotter, one Intelligence Fusion Server, and 10 classified network workstations with access to multiple web applications (e.g., AIDP, MAVEN, Chatsurfer). This allowed 10 intelligence Soldiers to operate inside the expandable van's T-SCIF at one time, representing all intelligence functions.

Recommendations Going Forward

To ensure robust intelligence support across a distributed command structure, a deliberate approach to node organization and communication is essential. These recommendations outline critical steps for division G-2s to optimize intelligence functions at each node, enhance cross-functional collaboration, and mitigate vulnerabilities inherent in dispersed operations.

Intelligence liaison officers at each node. Division G-2s should have a liaison officer with the command group and other distributed nodes. Working in a distributed environment isolates division staff sections from each other; however, staff collaboration within nodes is vital. For example, the field artillery intelligence officer needs to have a presence in the intelligence node to ensure an effective targeting process. Placing intelligence liaisons across nodes would ensure that updates to the common intelligence picture occur across all distributed CPs.

Cross-functional collaboration. When considering distributed nodes, division G-2s must consider how they allocate personnel by intelligence function to create the best situational understanding at each G-2 pod. Additionally, to synchronize with division efforts and facilitate cross-functional collaboration with the wider division staff, the placement of G-2 pods and systems within the division "starfish" must be a consideration in relation to the large-scale combat operational environment.

Approved collaboration peripherals. Collaboration peripherals are the tools that enable communication in distributed environments. SCIF collaboration peripherals must meet Department of Defense and Defense Intelligence Agency requirements as well as Intelligence Community Directive 705 specifications. The Accrediting Official must then approve their use. Division intelligence elements must ensure that adequate organic, approved collaboration peripherals are available at all distributed nodes.

Minimized electromagnetic footprint. MI systems, such as the TROJAN intelligence network system, have pronounced, identifiable signatures that make them easier to target. The intelligence warfighting function must allocate resources to determine how its systems can swim undetected within the electromagnetic spectrum. Until this is possible, division G-2s should consider holding distributed T-SCIFs in the rear for survivability.

Conclusion

Lessons and best practices from the 34th Infantry Division G-2's experience with distributed SCIF operations and ITN equipment highlight the importance of several key factors for ensuring CP survivability during large-scale combat operations. Involvement of the SSO and SSRs is crucial when planning, emplacing, and managing distributed SCIFs. Utilizing mobile T-SCIFs, particularly in vehicles such as expandable vans, offer a more flexible and adaptable solution than fixed or hardened SCIFs, while also conforming better to security regulations. Establishing a T-SCIF requires extensive planning and preparation, including site selection, design and construction, equipment and manning, personnel security, and training.

Additionally, T-SCIF operations require significant accreditation documentation. Staff should include military intelligence systems maintainers, who play a vital role in facilitating network access requests, communications security requests, and network testing of MI systems. In addition to these MI functions, dispersed operations compel the development of competencies in convoy operations and consideration of the wear and tear on intelligence equipment. Currently, there is not clear classification guidance for the ITN; this must be remedied to ensure effective communication and security.

The integration of near-term survivability principles, such as rearward functional echelonment, dispersion, signal management, and nodal movement, is crucial to ensuring CP survivability. The 34th Infantry Division G-2's experience with Operation Spartan Chain demonstrated the feasibility of establishing a T-SCIF and connectivity within a short timeframe. By applying these lessons and best practices, the intelligence warfighting function can operate more effectively and securely in a distributed environment during large-scale combat operations.

Endnotes

1. Milford Beagle, Jason Slider, and Matthew Arrol, "The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations," *Military Review* 103, no. 3 (2023): 10-24, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/.

2. Office of the Director of National Intelligence (DNI), Intelligence Community Directive (ICD) No. 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information* (2013), 2, https://www.odni.gov/files/documents/ICD/ICD-703.pdf.

3. Training and Doctrine Command (TRADOC) Proponent Office–Echelons Above Brigade (EAB), *White Paper: Near-Term Command Post Survivability*, Version 13 (Combined Arms Center, TRADOC, 2023).

4. Department of the Army, Army Regulation (AR) 380-28, *Army Sensitive Compartmented Information Security Program* (Government Publishing Office, 2018), 4.

5. Ibid., 5, 18.

6. Department of the Army, AR 380-28 *Army Sensitive Compartmented Information Security Program*; and Office of the DNI, ICD No. 705, *Sensitive Compartmented Information Facilities* (2010), https://www.dni.gov/files/documents/ICD/ICD-705-SCIFs.pdf.

7. Department of the Army, AR 380-28, *Sensitive Compartmented Information Security*, 18.

8. National Counterintelligence and Security Center, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, Version 1.5 (DNI, 2020), 47. https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.

9. Department of the Army, AR 380-28, *Sensitive Compartmented Information Security*, 18.

10. TRADOC Proponent Office–EAB, *Near-Term Command Post*.

CPT Austin Lind is the 34th Infantry Division Special Security Officer. He recently deployed to the U.S. Central Command area of responsibility in support of Operation Spartan Shield. He holds a degree in architecture and is currently studying for a master's of business administration at the University of Minnesota's Carson School of Management.