U.S. Army photo by Staff Sgt. Felicia Jagdatt

A Data Storage Issue: The Clash Between Electromagnetic Warfare and Signals Intelligence

by Major David Schott

This article reflects the views of the author. However, the article does not reflect the official position of the U.S. Army Intelligence Center of Excellence or the U.S. Army Cyber Center of Excellence. What the author characterizes as a policy shortfall and cumbersome oversight is in fact critical to ensure compliant electromagnetic warfare and signals intelligence operations. Additionally, what the author characterizes as data loss, only occurs from an electromagnetic warfare perspective. Within signals intelligence operations, the data is properly databased and maintained through the proper procedures and technical authority.

Introduction

The Army recently added an electromagnetic warfare (EW) platoon to their tactical military intelligence companies. The addition of the EW Soldiers adds unique opportunities to detect and disrupt threats leveraging the electromagnetic spectrum; however, electromagnetic spectrum tradecraft is traditionally the responsibility of signals intelligence (SIGINT). As these two tribes begin to coalesce, a systemic collection issue will materialize: specifically, the issue of data loss and data storage. The data loss occurs when EW Soldiers purge the signals data either intentionally or unintentionally after operations. This article aims to illuminate the structure and policy shortcomings that contribute to these data loss and data storage issues. Additionally, it provides a set of practical recommendations to mitigate the effects while proposing an optimal solution for consideration.

Background

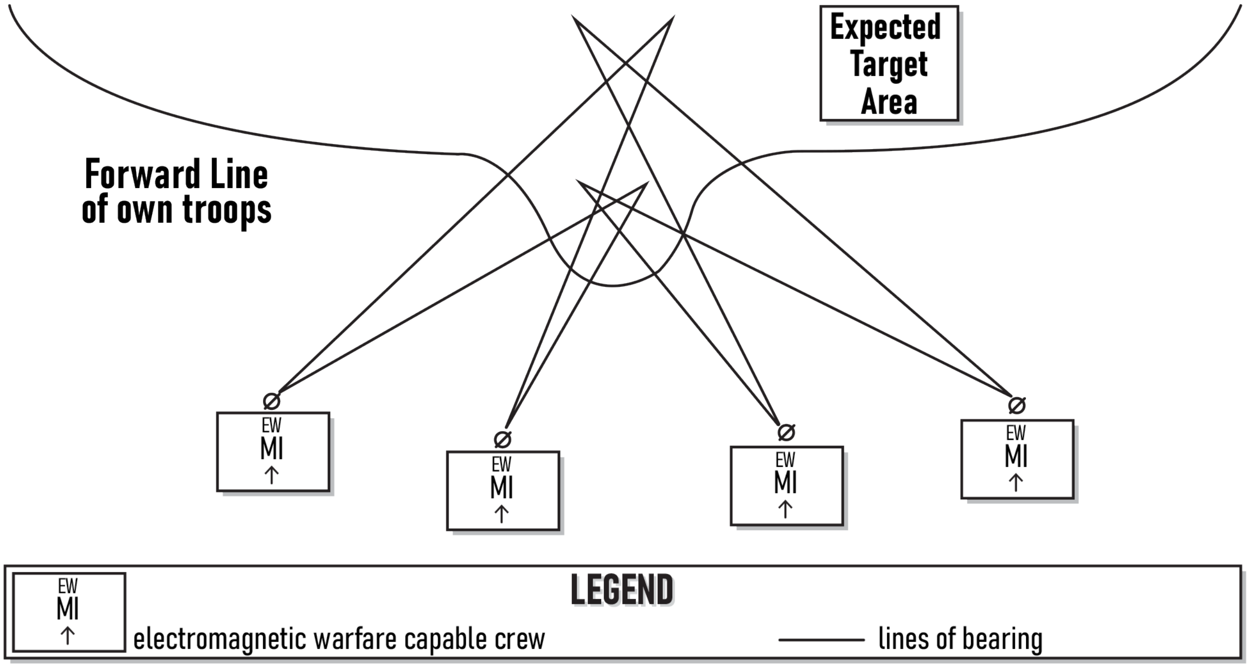
In 2018, the Army began modernizing its intelligence warfighting function by implementing a plan to add an EW platoon to tactical intelligence formations.[1] The modernization effort was necessary for tactical commanders to harness the organic forces to plan, coordinate, and respond to threats in the multidomain environment. Despite the much desired force structure overhaul, the anticipated advancements in understanding and visualizing the electromagnetic spectrum on the battlefield during operations have scarcely been achieved. A factor contributing to the delay is that EW is not an *intelligence activity.* Instead, it is a *warfighting activity,* and as such, the procedures for handling the collected information are governed by different authorities under U.S. law than the Title 50 intelligence authorities. The Title 10 general warfighting authorities are much less sensitive and do not require special handling.[2] To better understand the differences between EW and SIGINT a brief explanation is necessary.

EW and SIGINT differ based upon the information's intended use, timeliness of the analytical effort, detail of the information provided, and the type of equipment used. EW is vital on today's battlefield because it uniquely provides tactical units with a tool to deny, degrade, destroy, or locate threat emitters. The classic EW operation focuses on finding and jamming enemy communications to enable friendly force operations. As such, the military defines EW as "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[3] EW activities are separated into three divisions that support each other. They are: electromagnetic attack, electromagnetic protection, and electromagnetic support (ES).[4] For the scope of this article, we will focus on ES because this division most closely resembles SIGINT activities.

Joint doctrine states that ES involves actions "tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional or unintentional EM [electromagnetic] radiation for the purpose of immediate threat recognition, threat avoidance, homing, targeting, planning, and conduct of future operations."[5] The important factor is that ES actions support an operational commander for a varying time ranging from immediate to future operational planning. The issue with this description is the unclear language of the time of support. If ES actions may be used at the time of collection and for future operations, then how are these activities different from SIGINT?

SIGINT is a reliable intelligence source known for its formal relationships with intelligence partners and its contributions to the intelligence process. Throughout the years, SIGINT has modernized to meet the communications technical advancements. Joint doctrine describes SIGINT as "intelligence produced by exploiting foreign communications systems and noncommunications emitters."[6] Much like EW, SIGINT is divided into three subcategories: communications intelligence (COMINT), foreign instrumentation signals intelligence, and electronic intelligence.[7] COMINT is the subcategory relevant to the data loss issue, and, therefore, a brief explanation is necessary.

COMINT activities are "intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means."[8] In contrast to ES, the Director, National


Expected Target Area
Forward Line of own troops
EW MI
EW MI
EW MI
EW MI
LEGEND
EW MI electromagnetic warfare capable crew
lines of bearing

Electromagnetic Support Techniques: Concave Baseline[9]

The Terrestrial Layer System is the Army's next generation tactical vehicle based system integrating signals intelligence, electromagnetic warfare, and cyberspace operations. The system is currently in development. (U.S. Army photo)

Security Agency/Chief, Central Security Service, or an operational commander delegated SIGINT operational tasking authority, tasks SIGINT assets.[10] Processing of COMINT, as a single-source intelligence activity, occurs within its technical control channels and is then released to the intelligence community and tactical customer.[11] Latency becomes the chief challenge associated with this procedure because the technical control measures restrict the direct dissemination of SIGINT to the tactical customer. However, this cumbersome oversight process may contribute to the reliability, authenticity, and accuracy of the SIGINT reports. After release of a report, the data and intelligence are stored because SIGINT has the authority, equipment, and formal architecture to do so.

EW and SIGINT exist for separate purposes yet often support the same efforts. Their methods and procedures for collecting, processing, and reporting are different, but the signals data collected is similar. Data retention and storage is the issue because SIGINT systems are authorized to store COMINT data while EW platforms are limited and only encouraged to do so. According to Army doctrine, EW sensors monitor enemy communications to generate situational awareness and "some information gathered. . . may simultaneously feed into intelligence channels."[12] ES data that does not transfer into intelligence channels because of unit-level procedures for the transfer of ES data remains unprocessed by intelligence. This policy shortfall is the constraint on units to transferring "*select data* from electromagnetic support activities,"[13] which unintentionally contributes to data loss. In practice, EW Soldiers purge all data from their equipment following operations losing access to the transferred and non-transferred information. EW limitations continue considering they may only share combat-related information such as location, direction, frequency, and signal type. Although EW combat-related information has its purposes at the point of collection, that information may also have additional benefits to a SIGINT analyst. This leads to the question; how does the Army change to ensure the storage of all signal-related data for immediate and future processing?

Solutions

Three opportunities exist to regroup the Army's EW and SIGINT assets to efficiently store collected signals data. These solutions each come with different advantages and disadvantages and various lengths of time to integrate. They are:

- ✦ Create combined EW/SIGINT teams.
- ✦ Develop new authorities/procedures.
- ✦ Remove the ES function from EW.

Integrating the two tribes allows the teams to leverage both EW and SIGINT capabilities. Combining EW and SIGINT elements to create combined teams is the optimal solution because of the ability to rapidly implement the integration with limited restrictions. The benefit of this model is that there are no major organization or culture shifts while still maintaining the existing training and developmental pathways for each discipline. The detriments include a tactical limitation and a role identity problem. Tactically, the size of an EW/SIGINT team may be too bulky for its operational requirements, while joining the two elements may create a role primacy challenge.

The next recommendation is to develop new policy and procedures to grant EW Soldiers the same authorities as SIGINT Soldiers. This would allow the inclusion of EW signal data into the same data repositories as its SIGINT relative. The positives with this option are that it increases the amount of signals collection assets while enabling storage of the desired data. The negative of this option is the amount of time required to institute a policy change and train Soldiers to be compliant with the policies and procedures.

Removing ES from EW is a final option. It would solve the problem by giving exclusive authority to SIGINT for signal collection actions. This recommendation causes the most disruption but does solve the problem. This recommendation's strengths are that it gives one entity the sole responsibility for managing the signals environment while avoiding costly redundant equipment. Its weaknesses lie in the requirement for SIGINT to support the other divisions of EW. Consequently, the electromagnetic attack response times may suffer because of SIGINT mission prioritization and synchronization challenges.

Conclusion

The Army collects but does not retain and store all ES signals environment data because of organizational and policy issues. EW and SIGINT are complex; each has a unique yet similar role. Data retention and data storage has emerged as a dysfunctional problem connecting the two complementary capabilities. The proposed solutions provide options for addressing the issue. The optimal solution is to create combined EW/SIGINT teams because of the ability to promptly implement the teams and the limited intrusion on existing training standards. As intelligence and EW professionals continue to advance the tactical EW/SIGINT model, collaboration is necessary to reveal the best approach to integrate these capabilities and maximize electromagnetic signature and intelligence collection. If no action is taken, commanders must accept that pieces of the larger puzzle may be lost because of administrative constraints.

Endnotes

[1] Meritalk Staff, "Army's Electronic Warfare Teams Will Strengthen Cyber Force," MeriTalk, December 3, 2018, https://www.meritalk.com/articles/armys-electronic-warfare-teams-will-strengthen-cyber-force/.

[2] Mark Pomerleau, "Army working through intelligence and electronic warfare management on integrated platform," FEDScoop, August 25, 2022, https://www.fedscoop.com/army-working-through-intelligence-and-electronic-warfare-management-on-integrated-platform/.

[3] Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-85, *Joint Electromagnetic Spectrum Operations* (Washington, DC: The Joint Staff, 22 May 2020), I-5.

[4] Ibid.

[5] Ibid., I-6.

[6] Office of the Chairman of the Joint Chiefs of Staff, JP 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 26 May 2022), B-12.

[7] Ibid.

[8] Ibid.

[9] Figure adapted from original, Department of the Army, Army Techniques Publication (ATP) 3-12.3, *Electromagnetic Warfare Techniques* (Washington, DC: U.S. Government Publishing Office [GPO], 30 January 2023), 6-7.

[10] Office of the Chairman of the Joint Chiefs of Staff, JP 3-85, *Joint Electromagnetic Spectrum Operations*, I-6.

[11] Department of the Army, ATP 2-01, *Collection Management* (Washington, DC: GPO, 17 August 2021), 2-2.

[12] Department of the Army, ATP 3-12.3, *Electromagnetic Warfare Techniques*, 6-2.

[13] Ibid., 3-18, (emphasis added).

MAJ David Schott is the 3rd Multi-Domain Task Force Collection Manager at Fort Shafter, HI. His previous deployments to Afghanistan were as the Cyber Electromagnetic Activities company commander, 75th Ranger Regiment and as the Cryptologic Services Group officer in charge, 704th Military Intelligence Brigade. He is a distinguished graduate of the Command and General Staff College and a graduate of the Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance. He holds master's degrees in business and in intelligence from the University of Kansas and the American Military University.