



Spc. William Ritter, a military policeman with 287th Military Police Company, 97th Military Police Battalion, 89th Military Police Brigade, Fort Riley, Kansas, prepares to launch a RQ-11B Raven, a Small Unmanned Aircraft System (sUAS), during the Allied Spirit VIII training exercise at Hohenfels Training Area, Germany, Jan. 26, 2018. (U.S. Army photo by Spc. Dustin D. Biven 22nd Mobile Public Affairs Detachment)

The Electromagnetic Spectrum

The Future of Warfare

By Sgt. 1st Class Michael Waxler

Asymmetric Warfare Group

The Army is modernizing the ability to plan and execute operations resulting from electronic warfare threats. Although this modernization is happening quickly, it may not be fast enough to mitigate the impact that electronic warfare will have on maneuver units. In fact, there are multiple types of weapons that are already changing the way that maneuver units operate in combat zones — especially with the current proximity to Syria and Yemen. The Army’s Asymmetric Warfare Group (AWG) has observed the effects of jamming in a congested and contested electromagnetic spectrum (EMS) on units in combat. According to *Joint Publication 6-01*, EMS is a “physical medium through which

joint forces conduct operations,” (Joint Chiefs of Staff, 2012, p. I-1) and is crucial to mastery of the physical battlefield.

The issue surrounding electromagnetic interference, as observed by AWG Operational Advisors (OAs), is that it is an intangible process with tangible effects. This can make it very difficult to understand for many of today’s combat leaders. Right now there are units losing Global Positioning System (GPS) signal on the battlefield, resulting in small Unmanned Aerial Systems (sUAS) that cannot reliably fly. In addition, the same interference affecting our sUAS are degrading Blue Force Trackers, hindering the common operational picture. Furthermore, the threat is evolving enough to potentially challenge



U.S. Army Sgt. Jacob Butcher, a squad leader for Company A, 1st Battalion, 18th Infantry Regiment, 2nd Armored Brigade Combat Team, 1st Infantry Division, troubleshoots the DUKE version 3 system, Sept. 11, 2015, during the testing portion of the Counter Radio-Controlled IED Electronic Warfare Specialist Certification, or CREW, training course at the Tactical Support Center on Fort Riley, Kansas. Butcher was one of more than 50 “Dagger” brigade Soldiers to successfully pass the 40-hour, two-week course. (U.S. Army photo by Staff Sgt. Tamika Dillard, 1st Infantry Division Public Affairs)

aircraft positioning or precision-guided munition systems.

Effects like these discourage commanders from patrolling contested areas, prevent proper target preparation, and increase the risk of civilian non-combatant casualties. For these reasons, units must deploy fully prepared to operate in today’s EMS, which means training in preparation to defend against adversaries and their potential to wreak havoc on our technologically-dependent systems.

There is evidence that supports the argument that, after 16 years of combat in multiple areas, the U.S. and coalition forces have become over-reliant on the use of technology (Black, 2018). On today’s battlefield, everyone from an infantry fire team to the combatant command staff must understand how electromagnetic interference (EMI), or jamming, degrades their Table of Organization and Equipment (TO&E) end items, and must be aware of the vulnerabilities of civilian-purchased items that Soldiers might use or rely upon. Soldiers and leaders can no longer unconditionally rely on second offset technologies like position, navigation, and timing, intelligence, surveillance, and reconnaissance, and precision-guided munitions.

The Army articulates this concern clearly in the Army Warfighting Challenges (AWFCs), a tool used by the Army Capabilities Integration Center to define current and mid-term military problems and gaps. AWFC 7, “Conduct Space and Cyber Electromagnetic Operations and Maintain Communications,” defines the underlying problems (in part) in the form of the following questions:

How can the Army better prepare its leaders and Soldiers to operate in denied, degraded, and disrupted space operational environments?

How does the Army develop and maintain situational understanding within the space and cyberspace domains to help create and exploit temporary windows of superiority?

How does the Army execute Navigation Warfare, ensuring that Army forces have assured and reliable access to position, navigation, and timing (PNT) information while denying the same to our adversaries? (ARCIC-F/TRADOC, 2010)

OAs from AWG, working in conjunction with technical experts from around the Department of Defense, have created steps that units can take to prepare themselves for a contested EMS.

First, ground combat units, combat service and support units, and aviation units need to go back to mastering basic skills. Beyond just map reading skills, leaders must also be proficient in route planning and execution using paper topographical maps. They should also be efficient in using a lensatic compass for navigation, and understanding which communication platforms will continue to work in a degraded environment. Understanding and overcoming these challenges begins at home station training and continues during combat training center (CTC) rotations in order to make units more effective when operating in an EMS disabled environment.

In addition, tactical operations centers (TOC) that are in the affected environment must understand how to use “analog style” battle tracking, using maps and overlays when necessary, and periodically check the accuracy of their electronic systems—at all echelons. TOCs must develop standard operating procedures (SOP) to pass on mission essential information such as operations orders and fragmentary orders, while maintaining analog redundancy at all times, etc. Home station training and CTCs should encourage units to operate without using organic electronic battle tracking assets.

One solution to mastering the EMS problem quickly is having an experienced spectrum manager at the brigade level. A manager who understands how the spectrum can affect equipment, and whether that equipment is from conventional, special operations forces, or partner forces, can make a huge difference in the tactical communications for the brigade and subordinate units.

Advisors in Iraq estimate that supported units deal with interference from both friendly forces and proxy forces (Ackerman, 2007). Electromagnetic interference is unbiased, and it can be just as catastrophic from friendly

forces as it is from threat groups. The fact that EMI is now unavoidable on the battlefield and can be received, either intentionally or unintentionally, from either side should be a driving force behind modern military units being proactive in spectrum management training and mastering basic skills.

Lastly, units should develop SOPs and tactics, techniques and procedures (TTPs) before deploying, so that EMI is not a phenomenon first experienced on the battlefield. Some tactical questions commanders and leaders should consider are as follows:

What is the procedure when the GPS link with UAS systems is lost?

What is the procedure to regain control of the UAS?

Are there enough “dumb bombs” loaded onto Close Air Support (CAS) assets in the event the aircraft cannot release precision guided munitions with confidence?

Are rotary wing system and UAS altitude sensors at risk of degradation?

How do recovery assets conduct personnel recovery and downed aircrew recovery in a degraded environment?

This is just a cursory list, however, as we continue to learn and understand this problem the list will surely continue to expand. Leaders should understand the importance of developing TTPs now, rather than



U.S. Army Spc. Anna Tran, a human resources specialist with the 461st Human Resources Company, checks her compass during the 642nd Regional Support Group Best Warrior competition at Fort McClellan, Alabama, Jan. 18, 2019. The competition, which Tran won, tested the candidates through events such as rifle marksmanship, an obstacle course race, day and night land navigation and a ruck march. (U.S. Army photo by Sgt. 1st Class Gary A. Witte, 642nd Regional Support Group)

during first contact with the enemy.

Global powers are empowering their proxies to carry out these types of disruption and jamming, but increasingly violent extremist organizations (VEOs) are not reliant upon trained technical advisors from Iran, Russia, China, or Korea. Many don't need a government sponsorship, as some hackers have demonstrated in public displays (Porup, 2015). Narrow band, single channel, and space-based downlines are particularly susceptible to EMI. This EMI can come from man-made sources, including homemade jammers, but also from natural or man-made sources that are only unintentionally interfering. A review of literature on commercially available signals intelligence and high-profile jamming events reveals a disturbing trend of hobbyists, self-trained experts, and freely available technology that can interrupt, intercept, and jam a wide variety of signals (Griffith, 2015; Weinbaum, Berner, and McClintock, 2017).

Modern hardware and software have lowered the barrier to entry for building homemade transceivers. These devices are ready now using low cost software-defined radios with open source and software to build very capable systems. The hacker / maker community has demonstrated the ability to intercept, decrypt, exploit and even disrupt a range of commercial communication technology groups (Franceschi-Bicchierai, 2015). It is imperative that U.S. forces both train in and plan for an operational environment that reflects emerging EMS and cyber threats.

Every technological advance has its own weaknesses embedded into it. For example, small arms weapons that are powerful enough to reach across the valleys and wide expanses of Afghanistan may turn out to be overpowered and unwieldy on a future urban battlefield. In this same way, the prevalence and reliability of unprotected, satellite-connected devices have made U.S. military units reliant upon orbiting space assets. Fortunately, this reliance is often temporary and psychological, and something U.S. forces can overcome with basic and realistic training. Electromagnetic and counter-space weapons represent an asymmetric threat. One that the U.S. is more susceptible to than less technologically-dependent militaries.

Currently, the technological arms race has evolved into a new age space race. The Center for Strategic and International Studies has recently stated "as the United States has developed more advanced national security space systems...potential adversaries have taken notice" ("Space Threat Assessment," 2018, para. 1). With the ease of conducting EMI, countries with fewer resources than the U.S. or China, such as Iran, or anti-U.S. violent extremist



U.S. Army Pvt. Thrush Beazer, a cavalry scout with the 2nd Brigade Combat Team, 1st Cavalry Division, launches a RQ-11 Raven unmanned aerial system during the basic operator's training course at Fort Hood, Texas, Dec. 12, 2018. (U.S. Army photo by Maj. Carson Petry, 1st Cavalry Division Public Affairs)

organizations, space weapons provide a way to punch above their weight and give Western powers a black eye, diminishing the U.S. advantage of second offset technologies.

Currently, most military units treat the electromagnetic spectrum like a utility and are reliant on permissive environments for assured access. A more durable approach is to treat the spectrum like a warfighting domain. Retired Gen. Robert Kehler stated "Urgent action is needed. Countering this new reality requires a clear understanding of the threats and an approach highlighted by renewed national commitment and increased investment" (Kehler, 2018, para. 4). Organizations must plan for operations in the spectrum, and execute as any other battlefield condition. It is useful to think of the EMS as weather. Units

must monitor, forecast, and consider the EMS as an operational condition to execute the mission.

Leaders should challenge their subordinate formations to start training in a degraded environment, just as they train to fight in poor weather conditions. Maneuver units can conduct exercises (or portions of exercises) without radios, without organic sUAS, and without GPS systems for navigation. It is not a perfect representation of the modern EMS threat, but leaders owe it to their units to challenge them and teach them how to think through these emerging possible conditions. Innovative training fosters adaptive leaders and makes units more combat effective and ready to face whatever challenges may arise. ■

References

- Ackerman, R. (2007, June). Iraq hones Army electronic warfare. *Signal*. Retrieved from <https://www.afcea.org/content/iraq-hones-army-electronic-warfare>
- ARCIC-F/TRADOC. (2010, May 12). Army Warfighting Challenges. *Army.mil*. Retrieved from https://www.army.mil/article/38972/army_warfighting_challenges
- Black, J. (2018, March 12). Our reliance on space tech means we should prepare for the worst. *Defense News*. Retrieved from <https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/>
- Franceschi-Bicchierai, L. (2015, July 31). This \$1,000 device lets hackers hijack satellite communications. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/xywjpa/this-1000-device-lets-hackers-hijack-satellite-communications
- Griffith, E. (2015, June 8). 4 places that need cell phone jammers. *PC Mag*. Retrieved from <https://www.pcmag.com/commentary/335086/4-places-that-need-cell-phone-jammers>
- Joint Chiefs of Staff. (2012, March 20). *JP 5-01: Joint Electromagnetic Spectrum Management Operations*. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_01.pdf


Kehler, R. (2018, April 12). Power and prestige in the space domain. *Center for Strategic and International Studies*. Retrieved from <https://aerospace.csis.org/power-and-prestige-in-the-space-domain/>

Porup, J.M. (2015, August 21). It's surprisingly simple to hack a satellite. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/bmqj5a/its-surprisingly-simple-to-hack-a-satellite

Space threat assessment. (2018, April 11). *Center for Strategic and International Studies*. Retrieved from <https://aerospace.csis.org/spacethreat2018/>

Weinbaum C., Berner S., & McClintock, B. (2017). SIGINT for anyone. *Rand Corporation*. Retrieved from https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE273/RAND_PE273.pdf

Sgt. 1st Class Michael Waxler is a fire support NCO in the United States Army. Waxler is currently serving as an operational advisor for the Asymmetric Warfare Group. He previously served as a platoon forward observer through battalion fire support NCO in 2nd Battalion, 87th Infantry Regiment, 10th Mountain Division (LI), and brigade fire support NCO in 2nd Brigade, 101st Airborne Division (Air Assault), deploying eight times in support of the Global War on Terrorism.



<https://www.armyupress.army.mil/Journals/NCO-Journal/>
<https://www.facebook.com/NCOJournal>
<https://twitter.com/NCOJournal>

Disclaimer: The views expressed in this article are those of the authors and do not necessarily reflect the opinions of the NCO Journal, the U.S. Army, or the Department of Defense.

