Electromagnetic Spectrum Survivability in Large-Scale Combat Operations

CPT JEREMY HOFSTETTER
CPT ADAM WOJCIECHOWSKI

The command post tent is buzzing with concurrent planning and operational tracking. With faces painted, vehicles camouflaged, camo nets carefully laid over all the equipment, and everything concealed in the wood line, everything is seemingly ready for the start of another rotation at the Joint Multinational Readiness Center (JMRC) in Germany. In many conventional aspects, units such as those training at JMRC might feel like they have done everything possible to obscure themselves from the opposing force (OPFOR), but they have done little to no deliberate masking of the tremendous electromagnetic signature given off by signals equipment and digital mission command systems. As the unit conducts mission planning, the OPFOR has already detected the electromagnetic emissions generated from the cluster of antennas attached to the tactical operations center (TOC) vehicles and cell phones in every Soldier's pocket. OPFOR is quickly homing in and targeting the training unit's command post.

The U.S. Army has a wealth of experience operating in an environment where it possesses overwhelming electronic warfare (EW) dominance. During the years of war in Afghanistan and Iraq, the U.S. did not have to worry about these methods of attack. But, the conflicts the Army now prepares for encompass threats with peer/near-peer capabilities. Some of the Army's greatest assets that facilitate constant communication and a never-ending stream of position location information now present pronounced liabilities.

This became a stark reality for Ukrainian forces fighting against Russia in eastern Ukraine's Donbass region. Russia was able to effectively detect, jam, and destroy Ukraine command posts using their EW platforms.[1] During 20-plus years of counterinsurgency warfare, the U.S. Army's focus on its EW practices and procedures waned. As the Army transitions to fight in large-scale combat operations against peer/near-peer threats, units must equip, train, and fight in an EW-contested environment.

Soldiers from the 173rd Airborne Brigade adjust a portable antenna during Exercise Allied Spirit VI at Hohenfels Training Area, Germany, on 20 March 2017. (Photo by SGT Matthew Hulett)

A prime contender in the EW realm is Russia as it uses its current operational environments to test and train this experience. In the article "The Russian Edge in Electronic Warfare," Madison Creery states that Russia is at the forefront of EW innovation and use according to many experts in the field.[2] Their experience in EW began during the 2008 Russo-Georgian War, where they suppressed Georgia's air defense systems through jamming.[3] After the loss of numerous aircraft, Russia prioritized EW modernization. This effort resulted in 80-90 percent of EW equipment modernization and in 2009 the creation of dedicated EW units.[4]

Russia, as part of its strategy to mitigate vulnerabilities in other areas, has and will continue to invest heavily in EW equipment. For instance, the Borisoglebsk-2 system is capable of jamming mobile satellite communications and radio navigation units. This system, used in Ukraine, impedes the usage of drones by blocking incoming GPS signals. At the center of Russia's electronic countermeasure arsenal is the Moska-1, which is able to monitor electronic emissions within a 400-kilometer range on all frequencies; this system is able to both gather intelligence and conduct jamming and electronic suppression whenever needed.[5]

Several Russian systems specifically inhibit enemy systems in order to gain tactical and strategic superiority. The Krasukha-2 not only has the ability to analyze signal types and jam radar, but it can also provide a false target to the jammed system.[6] The Krasukha-2 has the ability to spoof GPS signals, providing false locations to GPS receivers.[7] During the Ukrainian conflict, Russia used electronic warfare systems to both fix positions for artillery strikes and facilitate psychological operations by targeting Ukrainian soldiers' cell phones with negative text messages.[8]

Russia has built its military strategy around maximizing its EW assets, whereas the U.S. has seldom considered the effects of electronic warfare in its doctrine, equipping, or planning at tactical levels. In 2015, COL Jeffrey Church, then chief of the Army's Electronic Warfare Division at the Pentagon, explained the gap between the U.S. and Russia as such:

> "The Russians train to it. They have electronic warfare units, they have electronic warfare equipment that those trained soldiers use, and then they incorporate it into their training. We do not have electronic warfare units, we have very little equipment, and we do very little electronic warfare training. It's not that we could not be as good as or better than them, it's just that right now we choose not to."[9]

Although western powers still hold a broad-spectrum technological advantage over Russia, it is clear that Russia views electronic warfare as a force multiplier that will negate western and particularly U.S. superiority. Russia allows its EW assets to permeate all levels of command whereas in the United States nearly all EW assets reside at echelons above division.

Dealing with a contested EW environment is a challenge with the current training environments and recent conflicts. In Iraq and Afghanistan, EW was primarily used on a very limited scale to defeat the triggering mechanisms for roadside bombs and later in the conflict to disrupt insurgent communications when attempting to call for reinforcement during an attack. The first time U.S. forces contended with peer/near-peer EW capabilities was when members of a special-purpose Marine task force deployed to Syria in 2018.[10] The head of U.S. Special Operations Command, GEN Raymond Thomas, called Syria "the most aggressive electronic warfare environment on the planet from our adversaries. They are testing us every day, knocking our communications down, disabling our EC-130s, etcetera."[11]

At JMRC, large-scale combat operations scenarios are commonplace; however, the rotational training unit may rarely consider peer/near-peer electronic warfare. Units commonly home in on refining that which they are most comfortable with, namely traditional kinetic threats. The bulk of planning and preparation occurs within the comfort zone, and minimal, if any, emphasis for planning against or mitigating the EW threat transpires.

Brigade and battalion TOCs normally focus on visual camouflage but overlook concealment of their electromagnetic footprint. Compounding the problem, command and control (C2) for many brigade combat teams can be highly dependent on digital systems that emit electromagnetic signatures. Trends at JMRC show a heavy reliance on FM radios, satellite communications and navigation, and commercial off-the-shelf WiFi devices. This highlights the issue with the need to leave personal cell phones behind. Furthermore, cell phones can lead to unsecured means of communication when more conventional means of communication seemingly fail.

One way to mitigate the usage of our digital-aged "easy button" is to implement mandatory communications exercises prior to field immersion of the training environment. A unit's lack of comfort across the board with

A Soldier assigned to the 1st Battalion, 503rd Infantry Regiment, 173rd Airborne Brigade, conducts a radio check during Saber Junction 2019 on Germany on 22 September 2019. (Photo by CPT Joseph Legros)

seamless shifting between the primary, alternate, contingent, and emergency (PACE) communication methods seems to stem from the lack of planning and practice of its PACE plan. Often, the unit presents the scheme of mission command but rarely conducts communications exercises at home station or immediately prior to a JMRC rotation in an environment that physically presents challenges far superior to motor-pool terrain. Lacking preparation, trends tend to one of two general outcomes: cell phone usage or an almost complete shutdown of the current operations cells while the S6 shop "fixes the problem."

Another noticeable trend at JMRC is that electromagnetic masking rarely makes the list during the planning phase when selecting TOC locations. In fact, it is usually quite the opposite; TOCs end up at locations with the best line-of-sight for FM communications. Trends additionally show that the execution intent for retransmission (RETRANS) is to saturate as much terrain as possible. Moreover, many radios are set to the highest power setting possible, regardless of the distance of the receiving station. This simplifies the problem of mission command, as establishing communications with another station can be difficult even during the best of times. The unintentional consequences of these oversights are the opportunity for the OPFOR electronic warfare teams to exploit unmitigated targeting opportunities likely essential to their high-payoff target list.

It is recommended that units take steps to camouflage their electromagnetic footprint similar to the effort placed on their visual signature. Simple mitigation techniques such as placing antennas on the side of a hill to provide maximum exposure to friendly forces but limit line-of-sight to the enemy will cut down on electromagnetic signatures.

Similarly, it is a common trend for units to place large amounts of antennas near or even attached to their TOC. While this makes setup quicker and reduces the visible physical signature, it has the opposite effect on the electromagnetic footprint. It is a good practice to place antennas as far away from the TOC as possible. Consider using equipment such an antenna multiplexer to reduce the number of antennas needed, further reducing the electromagnetic footprint.

Just as units practice poor behaviors masking their electromagnetic signature with the use of FM, they also tend to practice poor procedures when operating the equipment. Broadcasts are often long in duration, allowing enemy EW teams ample time to target the transmission. Furthermore, the use frequency hopping is normally good at

the onset of a rotation, but as the exercise carries on and communications security becomes compromised, units have a tendency to abandon their standard operating procedures and begin transmitting in single-channel mode to overcome multiple challenges of synchronizing across the unit. Operating in the open submits communications to many enemy systems that can effectively listen, locate, and therefore, target the origin of the signal.

Satellite-based communications are also widely used during rotations at JMRC, most notably tactical satellite (TACSAT), Joint Battle Command Platform (JBCP), and Warfighter Information Network-Tactical (WIN-T), all of which are vulnerable to jamming. A common trend witnessed when there is an upper tactical internet denial is that the S6 section spends much of its time troubleshooting equipment and little to no time analyzing the possibility of a cyberattack or satellite blocking attack. In fact, at the battalion level there is little means of detecting this kind of attack, and lower echelons are dependent on higher levels to provide this information.

Units and, by assumption, many Soldiers rely heavily on GPS (commercial and standard issue) for positional information. Rarely do units train or set requirements to operate in a satellite-denied environment. In many cases, units lack the equipment readily available to operate in a digitally degraded environment. To compensate for digital degradation, trends show an increase in analog proficiency for systems. Often, units understand that analog tracking is the medium that is not as susceptible to enemy attack. Maintaining synchronization across digital and analog mediums will continue to be a linchpin for success in mitigating digital degradation.

A final trend relates to cell-phone usage, which is often deemed essential in the day-to-day lives of most Americans, and unfortunately, this carries over to the battlefield. It is common during rotations to regularly see or otherwise know that Soldiers utilize their personal electronic devices. This presents an EW problem as none of these devices offer military encryption. Most of these devices emit electromagnetic signatures, which expose the user to targeting much easier than military equipment. Cell phones are also a vulnerability that can be used by an enemy to send psychological operations messaging directly to soldiers, as witnessed in Ukraine. Clearly cell phones are a liability on the battlefield; this prompted the commander of the 82nd Airborne Division (among others that visit JMRC) to order paratroopers to leave personal phones, computers, and all electronic devices behind when the unit received an alert for a short-notice deployment to the Middle East amid escalating tensions with Iran.[12]

The United States has allowed its EW expertise to atrophy during the years of war in Afghanistan and Iraq, while potential threats seized upon the opportunity to use electronic warfare to their advantage. By observing the conflict in Ukraine and elsewhere, it is apparent that EW will play a significant factor in shaping the battlefield in any future near-peer or large-scale operation. The U.S. must be competitive in the EW arena; this will take an investment in training, equipment, and a fundamental change in the way the military conducts ground operations. Planning and consideration for EW must be taken into account at the tactical level. EW will be a decisive domain in future battles, and the U.S. must be ready.

Notes

[1] COL Liam Collins, "Russia Gives Lesson in Electronic Warfare," Association of the United States Army, 26 July 2018, Accessed from https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare on 22 March 2020.

[2] Madison Creery, "The Russian Edge in Electronic Warfare," *Georgetown Security Studies Review*, 26 June 2019. Accessed from https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/ on 22 March 2020.

[3] Collins, "Russia Gives Lesson in Electronic Warfare."

[4] Creery, "The Russian Edge in Electronic Warfare."

[5] Ibid.

[6] Ibid.

[7] C4ADS, "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," 2019. Accessed from https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf on 23 March 2020.

[8] Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," (Tallinn, Estonia: International Centre for Defence and Security, 2017), accessed from https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf on 22 March 2020.

[9] Ellen Mitchell, "Army's Electronic-Warfare Training Seen as Lagging Behind Russian Efforts," *Inside Defense*, 8 December 2015. Accessed from https://insidedefense.com/daily-news/armys-electronic-warfare-training-seen-lagging-behind-russian-efforts on 22 March 2020.
[10] Gina Harkins, "Marines Are Getting a Taste of What War with Russia Might Look Like," *Task & Purpose*, 9 February 2019. Accessed from https://taskandpurpose.com/news/marines-russia-war on 22 March 2020.
[11] Ben Brimelow, "Syria Is Now 'The Most Aggressive Electronic Warfare Environment On The Planet,' SOCOM Says," *Task & Purpose*, 26 April 2018. Accessed from https://taskandpurpose.com/military-tech/syria-aircraft-disabled-electronic-warfare on 22 March 2020.
[12] Kyle Rempfer, "No Cellphones, Laptops Were Allowed to Go with Army 82nd Paratroopers Deploying to Middle East," *Army Times*, 6 January 2020. Accessed from https://www.armytimes.com/news/your-army/2020/01/06/no-cell-phones-laptops-were-allowed-to-go-with-82nd-paratroopers-deploying-to-middle-east/ on 22 March 2020.

CPT Jeremy Hofstetter, a Signal officer, is currently the Fire Support Training Team (Vampires) signal observer-coach-trainer (OCT) at the Joint Multinational Readiness Center (JMRC) in Germany. He has served on the division G6 staff of both the 10th Mountain and 82nd Airborne Divisions and has deployed in support of OEF. He completed his branch-qualifying time with the 82nd Airborne's Combat Aviation Brigade as both a battalion S6 and company commander.

CPT Adam Wojciechowski, a Military Intelligence (MI) officer, is currently the Fire Support Training Team (Vampires) battalion intelligence OCT at JMRC. He has experience in both U.S. Army Training and Doctrine Command (TRADOC) and Forces Command (FORSCOM) organizations where he deployed during Operation Enduring Freedom (OEF) XII-XIII. CPT Wojciechowski completed his branch-qualifying time across the 173rd Infantry Brigade Combat Team (Airborne) Brigade Support Battalion, 304th MI Battalion, and most recently as the opposing force (OPFOR) S2 at JMRC.