2019 LtGen Bernard E. "Mick" Trainor Military Writing Award: Honorable Mention

Closing the Gap

Electronic warfare training at TBS

by 2ndLt Wesley Eller

>2ndLt Eller was a student at The Basic School, graduating class 3-19. He has a BS in Aerospace Engineering from California Polytechnic University and an MS in Space Systems Engineering from Johns Hopkins.

The Marine Corps should begin providing more training on EW at TBS. *(Photo by LCpl Larisa Chavez.)*

Hail storm of bullets, Medal of Honor sprints, and charges into battle are three visions every officer candidate dreams of before leaving for Quantico, VA, and Officer Candidates School. However, for most of the successful candidates, the profile of their career is very unlikely to be shaped by any of these. Even those who find themselves an Infantry Officer will likely see at most a few hours of combat in their careers—at least kinetic combat. This is not the case for electronic warfare (EW). The pervasive influence of technology into every aspect of civilian and military life has made this domain dominant in shaping the battlefield of modern warfighting when compared to only one generation prior.

EW is something of an enigma to most people. The phrases "cyberspace" and "electronic warfare" conjure images of a man in black rapidly typing to a matrix of green figures on a cramped computer screen. Those initiated into the dubious brotherhood of hackers, both ethical and unethical, will chuckle at this image. It is much more boring than any movie cares to depict. I remember experimenting as a teenager with a close friend, attempting to break into the simple security system of his parent's wi-fi and discovering that it took an extraordinary amount of patience. (We also discovered it was often easier to fool a person than a computer, which explains my deep appreciation for good operational security as an adult.)

During his time as Commandant, Gen Robert B. Neller repeatedly emphasized and implemented his vision for a Marine Corps trained and equipped to win in the digital battlespace.[1] The Marine Corps founded the cyberspace operations MOS in 2016 and continues to move forward with acquiring the expertise and materiel to compete. The call to digital arms has echoed from Congress to the DOD and around popular culture. America is onboard; the time to act is now—which leads to the key question.

Why is EW so conspicuously absent from the combat modes taught at TBS? Hand-to-hand combat is covered immediately, rifle and pistol training follows shortly after, and the interdependence between the rifleman and the communications Marine is emphasized throughout the Basic Officer Course (BOC). Supply, logistics, finance, and aviation have their representatives. Deep concern for the effects of EW on our operations is repeated often—the reason for justifying training officers in the use of the ancient and reliable floating dial compasses and paper maps is a near-peer enemy who might spoof our GPS and listen to our conversations. However, despite the extent to which they create the environment the infantry officer must operate in, these concerns and darkly painted scenarios are the limit

of the advance into this warfighting region. I argue the fundamentals of EW should be taught at TBS based on the intent of the BOC and weight which this content bears on the mission of the Marine Corps.

First, what is EW? The *Joint Publication 3-51, Joint Doctrine for Electronic Warfare* defines it as:

> In military operations, the term electronic warfare (EW) refers to any military action involving the use of electromagnetic or directed energy to control the EM spectrum or to attack the enemy.[2]

The publication further breaks EW into three subsections: electronic attack, electronic protection, and EW support. It is the art and science of controlling the electromagnetic spectrum which allows us to move information as we want while preventing our enemies from doing so. The prime examples considered throughout this article are GPS jamming, GPS spoofing, and triangulation because they are immediately and obviously relevant to the infantry officer. This is of critical importance since it is the infantry officer's mission which primarily drives the intent of TBS.

The intent of TBS is given in the TBS campaign plan, which states:

> To train and educate newly commissioned or appointed officers in the high standards of professional knowledge, esprit-de-corps, and leadership to prepare them for duty as company grade officers in the operating forces, with particular emphasis on the duties, responsibilities, and warfighting skills required of a rifle platoon commander.[3]

This creates a new question: can the rifle platoon commander ignore the fundamentals of EW? Looking ahead, the answer is a resounding no! In a February 2019 article in *Military and Aerospace Electronics*, a more detailed look at the oncoming expectations for the individual soldier and Marine is examined:

> Throughout the history of warfare, 'boots on the ground' has been the catch phrase for the successful defeat and conquest of an enemy (the atomic bomb-forced surrender of World War II Japan notwithstanding). In the 21st Century, the value of [the] individual warfighter has increased as they have become nodes in the battlespace network—walking sensors and EW/cyber warfare platforms to combat close proximity enemy electronics like robots, radar installations, communications, and precision-guided munitions. Combined with advanced vehicle-mounted EW capabilities, they will be crucial to dominating the electromagnetic spectrum.[4]

The vulnerability of ground combat units to EW attacks has been closely considered by Marine Corps leadership, and one of the prime responses has been to modify training programs to more effectively meet the expected challenges. However, the changes made may not have gone far enough. Training new lieutenants in the use of a compass allows them to survive and lead in a GPS denied environment. The development of a unit dedicated to employing and defending against EW in both the electromagnetic and cyber environments demonstrates a commitment to meeting this danger head on. Therefore, it is critical these same young leaders are trained in methods to recognize when they are the victims of these complex attacks and are able to employ them at the tactical level.

From the same *Military and Aerospace Electronics* article,

> As the warfighter evolves from the concept of 'every shooter is a sensor' to every shooter is an EW/cyber warfare node, the need to bring all that new data back to the commander—from the smallest unit to higher headquarters—as useful information to make real-time tactical decisions also increases.[5]

Detection, response to, and the employment of EW is now a critical skill for the on-the-ground commander and will likely grow increasingly more so. Given this conviction, what skills should specifically be trained?

I argue that the detection, response to, and employment of three basic attacks and tactics should be well understood in at least the abstract by all tactical leaders: GPS jamming, GPS spoofing, and triangulation.

GPS jamming denies the use of GPS in a given area.[6] It is common knowledge that a GPS unit requires constant communication with multiple satellites in order to function. Not dissimilar from a radio, the GPS receiver unit listens on a particular frequency (different for civilian and military systems) for a rather quiet set of signals descending from the heavens. Each message it receives on this frequency lists who sent it, where that satellite was when it sent the message, and what time it was sent. The key word, in this case, is the signal is quiet. A large amount of signal noise in the vicinity can make the receiver simply unable to hear the necessary messages, and no navigation data will be produced. The tactical commander's ability to navigate is not destroyed—but it is markedly impaired. More valuable than the ten-digit grid produced is the time spent attempting to troubleshoot the system when a GPS denial likely signals imminent contact. The detection of this attack is as easy as opening our electromagnetic ears. Robust signal monitoring systems do not have to be heavy or complex, and they can rapidly answer the question, "Is my receiver not getting enough signal, or far too much?"

GPS spoofing is when an actor sends out a signal which mimics the authentic GPS signal in order to cause a GPS system to produce incorrect data. It is obvious how this can have disastrous effects on the ground if it remains undetected. A variety of techniques for spoofing detection can be found in technical literature, but the rifle platoon commander need not worry about them.[7] The key takeaway is spoofing a small unit's GPS can create a gap in that unit's plan, making it ripe for exploitation. The rifle platoon commander must weigh the voice of software, which acts as a Marine constantly poring over the stream of signals, searching for the patterns which indicate a problem. It is in the commander's hands to respond to detected attacks and understand what those attacks entail.

Triangulation: if you can see me, I can see you. Triangulation is the practice of determining a signal source's physical location by monitoring that signal using two or more receivers.[8] Perhaps

more so than the other forms of attack discussed, this is a key enabling capability which appears under-utilized from the perspective of the TBS lieutenant. Given a known enemy signal, we can find the enemy, and if they can identify one of our signals, they can find us. This capability appears crucial for a near-peer conflict in which the enemy does not need to crack our crypto to gather key intelligence on our units but only needs to find the frequency our units are operating on—the fundamental paradigm we use to determine when to communicate is forced to shift. Communications is key to command and control, but we must now treat electromagnetic communication as carefully as the overheard spoken word in a tactical scenario by finding the electronic version of hand and arm signals and taking care to listen for poor digital discipline in our enemy's maneuvers.

The rifle platoon commander lives in an increasingly complex tactical environment. The enemy no longer inhabits only the kinetic realm, they compete with us in the information domain as well. This dimension of the competition cannot be ignored, and training officers in good habits of thought and action in all domains is a critical step in meeting this challenge. The introduction of these key concepts into the training program for new officers is likely to have several important effects. First, the obvious familiarization with the particular tactics of EW discussed. Second, this familiarity is likely to reduce the trepidation felt by many nontechnical Marines when discussing EW. The underlying complexity of the topic can be intimidating, but it need not be more difficult to apply the tools than any other complex system. We do not need to understand carburetors to drive a car, but we will lose every race if we compete with cars on our feet.

The final effect of introducing these topics into the BOC is to spark innovation and integration of these tactical capabilities with other tactical core skills and systems. The more comfortable and familiar a Marine is with these concepts, the more likely they are to try them and then try something new. The process of mastering the fundamentals and then adding to them is key to pushing any organization into the future and remaining competitive; the Marine Corps must remain competitive.

The enemy competes with us across the information domain and lieutenants must begin to develop a familiarization with EW tactics, techniques, and procedures. ***(Photo by Cpl Bernadette Plouffe.)***

EW fundamentals should be taught at TBS. They must become part of the rifle platoon commander's repertoire. The mission of TBS is to train new officers in leadership and core Marine Corps skills using the infantry model as a base. Just as every Marine may be called upon to hold a weapon and use a radio, in the next conflict any Marine officer may be called upon to make decisions based on EW information. Introducing these concepts to future decision makers as early as possible is a powerful means of enabling the Marine Corps to keep winning, even in a shifting battle space.

Notes

1. Staff, "Top Marine Discusses Technology, Innovation Strategy," Department of Defense, (Online: June 2018), available at https://dod.defense.gov.

2. Todd Corillo, "As Marine Corps Looks to Future Cyber Warfare, Recruiting and Retaining Older Marines Could be Key," *WTKR*, (Online: June 2018), available at https://wtkr.com.

3. Joint Chiefs of Staff, *Joint Publication 3-51 (JP 3-51), Joint Doctrine for Electronic Warfare,* (Washington, DC: 2000).

4. Commanding Officer, The Basic School, *TBS Campaign Plan, 2019–2025*, (Quantico, VA: 2018).

5. J.R. Wilson, "Electronic Warfare on the Ground," *Military & Aerospace Electronics,* (Online: February 2019), available at https://www.militaryaerospace.com.

6. A.F. Van Niekerk and Ludwig Combrinck, "The Use of Civilian Type GPS Receivers by the Military and Their Vulnerability to Jamming," *South Africa Journal of Science*, (Pretoria, SA: Academy of Science of South Africa, January 2012).

7. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. Position Location and Navigation (PLAN) Group," Schulich School of Engineering, (Calgary, CDN: University of Calgary, May 2012).

8. David Adamy, "Location of Communications Emitters," *Journal of Electronic Defense*, (Alexandria, VA: Association of Old Crows, 2008).