

WINNING IN A GPS- DEGRADED ENVIRONMENT

MAJ LARRY KAY

In March 2015, Headquarters and Headquarters Company, 4th Battalion, 9th Infantry Regiment, 1st Stryker Brigade Combat Team, 4th Infantry Division, deployed to White Sands Missile Range (WSMR), NM, in support of the Joint Navigation Warfare Center's Positioning, Navigation and Timing (PNT) Operational Field Assessment, which was a part of Exercise Global Lightning 2015. The purpose of this operation was to evaluate the effects of some anti-access/area denial (A2/AD) methods on a Stryker brigade combat team's organic vehicles. The company was given a simple tactical order, and for five days it attempted to complete its mission despite operating in a Global Positioning System (GPS)-degraded environment and being exposed to multiple electronic warfare systems.

What is A2/AD?

In 2003, the Center for Strategic and Budgetary Assessments defined anti-access as enemy action which inhibits military movement into a theater of operations and area-denial operations as activities that seek to deny freedom of action within areas under that enemy's control.¹ The National Security Strategy (NSS) concludes the nation must prepare for "...increasingly sophisticated adversaries, [and] deterring and defeating aggression in anti-access environments." Additionally, the *Quadrennial Defense Review* (QDR) acknowledges a challenging operational landscape that includes:

- Increasingly multidimensional conflicts (hybrid threats);
- Threats to the global commons and expansion into space and cyberspace; and
- Growing A2/AD capabilities, including ballistic missile threats.²

A2/AD pits strategic assets and dimensions of warfare (space and cyberspace) against the conventional tactical military superiority that the U.S. has enjoyed in recent history. Moreover, while the military has addressed the unconventional challenges posed by incessant counterinsurgencies, near-peer and peer competitors have significantly improved if not exceeded our offensive and defensive A2/AD capabilities. Consequently, as expeditionary warfighters, we have come to expect safe and routine deployments into a theater of conflict and the ability to gain and maintain air, space, and maritime superiority. Put in this context, the company learned quickly that this relatively small exercise was conducted to address a significantly large strategic problem.

The Scenario

During the exercise, the Stryker company was tasked to perform basic tasks that a unit would likely conduct in Afghanistan: routine patrolling and reconnaissance that was punctuated with reacts to contact. Since the company conducted this mission at WSMR, it was restricted mainly to roads due to unexploded ordnance (UXO) all over the area. Based on the coordination and limitations with the Federal Aviation Administration and the National Transportation Safety Board, all of the missions were conducted during the hours of limited visibility, which provided additional challenges for the Soldiers.

Prior to the start of the mission, experts from the Space and Missile Defense Command reviewed the use of the AN/PSN-13 Defense Advanced GPS Receiver (DAGR) and demonstrated the signs of degraded GPS. The experts focused on the importance of loading communications security (COMSEC) in the DAGR and an introduction to using the DAGR's "jammer detector." Undeniably, nearly every Soldier in the company was unaware that the DAGR is equipped with such a detector while a few also realized that the DAGR could be encrypted.

The company approached the first mission as it approaches missions in general — by using the "one-third, two-thirds rule" and focusing on rehearsals. Prior to mission execution, we conducted a communications exercise (COMEX), which included short-range and long-range communications checks, free text messaging, and operational graphics verifications on the Force XXI Battle Command Brigade and Below (FBCB2)/Blue Force Tracker (BFT) – Joint Capabilities Release (JCR).



Defense Advanced GPS Receiver (Image courtesy of the Direct Reporting Program Manager, Positioning, Navigation and Timing)

The company started movement at 2100. After the company reached all of its checkpoints, the scout platoon occupied its first observation post (OP) while the mortar platoon established its mortar firing point (MFP). About 30 minutes after reaching the OP, the FBCB2s indicated movements from subordinate units which were not expected in this operation. From a command and control perspective, the command was aware that what was observed digitally was not what was supposed to happen, yet the purported accuracy and reliance on FBCB2 compelled the command to verify locations of all friendly units. Once the command confirmed the frontline traces or locations of all of its units, the company continued the mission as planned and then returned to base. The damage was clearly done: leaders had lost confidence in their digital mission command systems. During the after action review, key leaders discussed what they had seen from their point of view and also what specific tactics, techniques, and procedures (TTPs) they had employed in response to the electronic warfare (EW) contact. The company would be sure to share and employ these TTPs for the remainder of the exercise.

The company approached the second mission differently. Now aware that the adversary had the ability to affect its digital systems, leaders could no longer trust them — or at least could not rely on them with the same confidence that they had in the past. Leadership had to rely on all of the other methods of command and control which existed prior to the advent of FBCB2. Leaders modified operational graphics, reduced the intervals between vehicles and elements, adjusted the rate of movement, modified the reporting requirements, and made the combined arms rehearsal (CAR) more in-depth with extensive radio rehearsals. During the CAR, the commander emphasized the importance of analog maps and graphics for all of the units, specifying that if the unit made EW contact with the enemy that it would completely ignore all of its digital systems and transition to analog. Of all of the additional planning considerations, the consensus was that the frequency modulation (FM) rehearsal was the most helpful.

The company began the next mission and almost immediately made EW contact. However, the additional planning and rehearsals mitigated the confusion that the FBCB2 displayed. During this mission, the mortar platoon executed a fire mission without the digital assistance verification to which all indirect assets and personal are now accustomed. The first round was slightly inaccurate, but fortunately the mortar platoon sergeant revolved his training plan around the basics, teaching his mortarmen the proper and effective use of plotting boards. The reward of his basic training

plan was that his Soldiers did not need digital systems to be lethal. As always, mastering the fundamentals is at the heart of being a lethal unit.

Prior to the third mission, leaders encouraged Soldiers to be adaptive and creative in fabricating “devices” which they thought would prevent the enemy from affecting their systems (v-shaped hulls initially began as metal plates welded onto the bottoms of vehicles by Soldiers). The results were both productive and amusing, ranging from electromagnets to taping water bottles and helmets around antennas. While the crews attempted to develop innovative solutions, the leadership met again to review the effectiveness of the TTPs that they had thus far developed. The company had now become accustomed to executing the mission without its digital PNT systems. The FCB2 served as nothing more than an instant messenger and lamp for an actual map and protractor. The company added one more tactic based on the graphics that had been provided: the first element to reach a checkpoint would drop an infrared chem light to mark it for following units. This turned out to be helpful to some of the crews and sections that were not as well trained at mounted navigation. While not a new technique, it was simple and effective. Finally, everyone recognized that simple wristwatches were unperturbed by enemy interference, so leaders manually added the date-time group to the free text messages over FCB2.

For the remainder of missions, the company was able to accomplish its mission objectives in a GPS-degraded environment. When you think about training your units, think about the following:

1. Every Soldier should have a map, compass, and protractor. We learned that this is not the case because it was either not on the packing list or there were not enough of them in the unit for issue. On an interesting note, DAGRs outnumber compasses three to one in most companies.

2. Rehearsals improve success in every environment, especially in a GPS-degraded environment. While not a new maxim, the importance is greater in a GPS-degraded environment. When leaders cannot just ask questions and receive immediate responses, it is critical that everyone knows what is going on. FM rehearsals with an operation schedule (OPSKED) or execution checklist (EXCHECK) are invaluable; they enable everyone to visualize the plan in time, space, and purpose. Keeping radio transmissions brief and poignant is absolutely essential.

3. Encrypt everything. While it does not completely defeat the EW threat, it does mitigate its effects. Many Soldiers (especially non-maneuver, fires, and effects types) do not know what equipment can be encrypted (DAGRs, LRAS3, etc...) and what cannot be encrypted. This should become part of the unit standard operating procedure (SOP), and the S6 should ensure the unit has the right COMSEC for every encryptable item. Commercially available GPS devices, which have become standard for small unit leaders, can easily be manipulated by civilian market GPS deception devices, and it doesn’t require a near-peer enemy to purchase these. Any small terrorist organization or non-state actor can purchase these on the Internet. It took leaders 10 minutes on Google to figure this out. In fact, many commands currently prohibit the use of store-bought GPS devices in a field environment. Despite the chagrin of many Soldiers, this restriction ultimately protects the force from adversarial threats in a complex environment.

4. DAGRs have a jammer finder. Educate and train Soldiers how to use this device and train them on what a “jammed” DAGR screen looks like. Leaders can use the jammer finder to learn what the baseline signal level (natural amount of frequency noise) is in their area of operation (AO) prior to starting the mission. Once jammed, they will be able to see what the difference from their initial reading is and then be able to tentatively determine an azimuth to the jammer. Multiple geographically dispersed DAGR jammer finders could potentially conduct an intersection to geo-locate the adversarial jammer. When moving, airborne or multiple jammers could hinder this process. Units can shield some of the effects of EW with both the hull of the vehicle and a Soldier’s body. Depending on mission variables, units can position their vehicles to assist in locating the jammers. Keep it within the commander’s intent, however, because some units were briefly distracted from mission accomplishment once they took EW contact. Units must immediately report EW interference by sending a meaoning, interference, jamming, and intrusion (MIJI) report and move on to the objective.

5. Master the basics. Many Soldiers were uncomfortable with terrain association, map reading, and mounted navigation. Intersection, resection, and modified resection were critical for the mortar and scout platoons when confirming their locations and enemy locations. The mortar platoon quickly adapted to the environment but was somewhat sluggish and uncomfortable with its transition to analog fire missions. All training should begin with the basics or fundamentals, and that requires pencil, map, protractor, plotting board, compass, and binoculars. These



All training should begin with the basics or fundamentals, and that requires a pencil, map, protractor, plotting board, compass, and binoculars. These items have always been impervious to electronic warfare, yet they are still susceptible to natural human error if proficiency is not sustained. (U.S. Army photo)

items have always been impervious to EW, yet they are still susceptible to natural human error if proficiency is not sustained. A July 2016 *Army Times* article mentioned that units are returning to the basics of soldiering. If trained properly and continuously, this will enable units to thrive in a GPS-degraded environment.³ Training plans should distinguish individual skills with and without technical devices, affording an equal amount of time to both.

6. Did the unit plan for it? The purpose of jamming is not to destroy but to disrupt. During the operations and military decision-making processes, did the unit account for this in its timeline? Did the battalion intelligence officer account for EW in the enemy action analysis? It is fair to assume that if an enemy has an A2/AD capability that they will also have night-vision capabilities, so ensure that your TTPs are mission-variable relevant. Combine a GPS-denied environment with an FM-interfered environment and try to visualize how chaotic a combined arms breach would be. A costly reality is that planning for the EW threat will reflect how units plan for chemical, biological, radiological and nuclear (CBRN) events, which is not much at all.

7. Practice mission command over and over. To build cohesive teams through mutual trust, a previous command relationship must exist in order for the art of mission command to complement the science of it. This may not be the case in other units that rely solely on the FBCB2 for their map, messaging, and mission command. Unless you train, it will not be natural. Unfortunately for many, command and control is as foreign as the enemy who is jamming them. Finally, commanders at all levels must temper their demands for immediate information when making requests of subordinates in a GPS-denied environment.

8. Balanced risk management. Does the assessed risk remain the same in an EW environment as it does in a normal environment? How well trained are the company mortars, fire direction center (FDC), battalion mortars, and battalion FDC? More importantly, how well trained are the forward units at providing their frontline trace without the aid of a DAGR? How does the unit manage airspace in a GPS-denied environment? We prefer simplicity, but simplicity is not always an option. We may just have to accept more risk, but training with the absence of technology will mitigate the risk significantly.

9. Develop an SOP that can survive in an EW environment. Engineers and experts frequently asked leaders, “What TTPs would you add to your SOP?” There is really no unique TTP designed specifically to counteract the effects of jamming, but a unit can absolutely mitigate it. How much emphasis do we place in the communications plan? Does the unit have signal operating instructions or just a primary, alternate, contingency, emergency (PACE) plan which consists only of P and A? Does the unit have a PACE plan for navigation? Does the unit have methods of marking and does it have enough in supply? Does everyone in the formation, to include staff sections and operational support elements, know hand and arm signals and have they trained to use them?

These TTPs will not completely counter the threat posed by our enemies. However, the challenges for small units posed in a GPS-degraded environment can be overcome if units focus on the fundamentals and basic soldier skills. If you take anything away from our experience, it’s that rehearsals are the most important part of surviving in a GPS-degraded environment. For this company, the focus and reliance on analog systems and conducting extensive and various rehearsals prevailed as the best TTP to combat the adversarial effects on all of the digital systems. It turned out that the best defense against 21st century modern warfare was to rely upon the fundamentals from the 20th century: maps with graphics, compass, and protractor.

Notes

¹ Andrew Krepinevich, Barry Watts, and Robert Work, “Meeting the Anti-Access and Area-Denial Challenge,” Center for Strategic and Budgetary Assessments (Washington, D.C., 2003).

² The Joint Operational Access Concept, Version 1.0. 17 January 2012.

³ Michelle Tan, “Back to the Basics: Army Dials up Traditional Soldiering Once Again,” *Army Times*, 5 July 2016.

MAJ Larry Kay is currently a student at the School of Advanced Military Studies. His last assignment was as the deputy chief of staff of the 4th Infantry Division’s Mission Command Element forward in Germany in support of Atlantic Resolve. His previous assignments include serving as commander of A Company, 1st Battalion, 22nd Infantry Regiment, 1st Brigade Combat Team, 4th Infantry Division; commander of A Company, 4th Battalion, 9th Infantry, 1st Stryker Brigade Combat Team, 4th ID; and commander of Headquarters and Headquarters Company, 4-9 IN. MAJ Kay is also a Strategic Studies Fellow with the University of North Carolina Chapel Hill’s Institute of Defense and Business. He is the author of “Innovation of Military Thought in the Postmodern Warfare Era” and “Managing the Gray Zone is a Gray Matter Challenge,” both published in the *Small Wars Journal*.