Photo by Markus Rauchenberger

UNDERSTANDING GPS:

THE IMPORTANCE OF A MILITARY RECEIVER IN A GPS-CONTESTED ENVIRONMENT

MAJ RUSSELL NOWELS
MAJ MATTHEW FECHTER

The global positioning system (GPS) is a space-based satellite navigation system that is deeply integrated into the U.S. military. More precisely, the military is critically dependent on the GPS satellite system due to its ability to provide three-dimensional positioning, navigation, and timing (PNT) information for countless military systems. Comprised of 24 satellites (with on-orbit spares available), the GPS constellation provides a number of advantages to include accurate and efficient navigation information, positioning data for the precise deployment of guided munitions, and the timing signal that synchronizes both space and ground-based communications and computer systems. The heavy reliance on PNT services means that it is an increasingly critical consideration during mission planning and execution.

As a result, Army staffs, units, and individual users must understand the vulnerabilities associated with their GPS and its aided systems. Current combat operations in the Central Command area of responsibility (AOR), as well as potential combat operations in the European Command AOR and the Pacific Command AOR, have adversaries who possess GPS-denial equipment which could degrade or deny basic GPS services to our forces. Due to the proliferation of the GPS-denial equipment, Soldiers must appreciate the advantages of properly using their assigned military-grade GPS (such as the Defense Advanced GPS Receiver — DAGR) as opposed to commercial systems to guarantee they are receiving the most accurate data while simultaneously mitigating adversary attempts to degrade or deny this capability.

Increased Use and Reliance on Civilian GPS Systems

At the start of combat operations in 2001, the U.S. Air Force leveraged the GPS positioning capabilities to guide precision munition strikes from aircraft miles above the battlefield. Likewise, land forces used the GPS navigation capability to efficiently move through challenging environmental terrain, conditions, and congested urban areas. Additionally, all forces enjoyed the benefit of the precise timing signal that enabled synchronized battlefield communications as well as the ability to command and control forces through the friendly forces tracking (FFT) system across vast space and distances. These simple examples are just a few of the many capabilities enabled or assisted by GPS functions.

Standard military-grade GPS systems were used by the bulk of the forces during the initial combat operations in Afghanistan and Iraq. The success of these systems created a demand for more GPS navigation aids, especially as the number of dismounted operations inherent in counterinsurgency and stability operations grew. In fact, many units (especially mechanized organizations) did not possess adequate GPS receivers to enable simultaneous mounted and dismounted operations. As a result, Soldiers sought to address this capability gap by purchasing inexpensive civilian GPS receivers. These commercial GPS receivers, like those made by Garmin and Magellan, became even more appealing to Soldiers because they were smaller, lighter weight, relatively inexpensive, and far easier to use and understand than the equivalent military system. Gradually, the use of civilian GPS devices by ground forces increased to the point that many organizations were purchasing the devices for use in combat environments.

The increased use of commercial GPS systems exposed the shortcomings of the common Army GPS system, the DAGR. Specifically, the DAGR is comparatively challenging to operate because it is not functionally intuitive or easily accessible. Additionally, many DAGRs are tied to vehicle platforms, which results in Soldiers going through the hassle of disconnecting them for dismounted operations. Further, DAGRs are heavier and cannot be easily carried in a quickly accessible position like the Garmin wrist devices. These challenges drove Soldiers away from the issued military receiver in favor of the increasingly user friendly and more affordable commercial systems.

GPS Threat Basics

Two primary GPS threats exist that inhibit proper system function: jamming and spoofing — both are referred to as electronic attacks. Jamming is the emission of a signal powerful enough to bump the GPS signal from a user's receiver. Once the receiver loses its GPS signal, the jamming signal is strong enough to prevent the user from re-acquiring the proper signal. The degraded GPS environment caused by the jamming signal prevents the receiver from displaying any type of relevant data. Spoofing is the transmission of false signals that result in a GPS receiver tracking the incorrect signal and reporting a position controlled by the spoofing source. Since spoofing affects the accuracy of PNT, these signals negatively impact the maneuver forces and weapons targeting effectiveness. The potential outcome of a spoofing threat is significant since a user may not know that incorrect data is being generated and displayed. Ultimately, spoofing is responsible for erroneous navigation or inaccurate use of precision-guided munitions.

Electronic Attack Examples

Jamming scenario: 1st Platoon is navigating across the open desert at the National Training Center (NTC) at Fort Irwin, Calif., when all the GPS receivers within the platoon suddenly freeze, display a warning for a "Jamming Environment Detected," or go blank. This is likely the effect of GPS jamming. The GPS receiver is now ineffective due to the powerful jamming signal, which prevents the GPS receiver from acquiring the actual GPS signal. Time to pull out the map and compass!

Spoofing scenario: 2nd Platoon is responsible for establishing a support-by-fire (SBF) position during a night mission at NTC. The platoon follows their pre-determined GPS route directly to the assigned position and begins to establish its position at the exact grid coordinates. As dawn begins to break, the platoon leader uses his map and terrain association to determine that his platoon is established on the objective despite correct coordinates displayed on his GPS receiver. The platoon has been spoofed!

The Value of the DAGR in Future Environments

The DAGR offers protection in a GPS-contested environment that makes it far superior to its commercial equivalent. As such, Soldiers must get comfortable using a military receiver in future conflicts and contingencies. Our adversaries are aware that GPS-aided systems provided a marked advantage that contributed directly to tactical success in Afghanistan and Iraq. These adversaries intend to minimize this GPS advantage in the next conflict by contesting the military's assured access to the GPS signal. This intent is progressively realistic as the proliferation of GPS-denial equipment provides both nation states and non-state actors the means to execute this plan.

In future GPS-contested environments, commercial receivers will lose their lock on the GPS signal and not function properly; however, a DAGR combats the effects of electronic attacks through the Selective Availability Anti-Spoofing Module (SAASM), which accesses the P(Y) code and is only present in a properly keyed, military-grade GPS receiver. The anti-spoof P(Y) code was developed to encrypt the military signal, a separate signal from the GPS satellite that commercial receivers cannot use. This makes it more difficult to degrade or deny when used with a keyed DAGR because the military signal requires authentication from the receiver. This military signal is broadcast on two frequencies from the satellites while the commercial signal is only broadcast on one. This encrypted signal and the use of two frequencies offer greater resistance to adversary electronic attack.

Unfortunately, the civilian receivers carried by many Soldiers lack the encryption capability to authenticate the P(Y) GPS signals. This means that the civilian GPS receivers are more susceptible to electronic attack of the GPS signal. Simply put, a properly keyed DAGR has a greater resistance to an adversary's electronic attacks than the commercial GPS devices, which will more easily lose the ability to track satellites and thus give an accurate position to the user.

Conclusion

GPS services provide a combat-multiplying capability to the Army; however, assured access to the GPS signal is no longer automatic. Adversaries now possess the ability to degrade or deny the signal that enables our GPS advantages, especially when our troops use a commercial receiver. In the GPS-contested environments posed on future battlefields, Soldiers must transition their confidence from commercial receivers to the DAGR or other military-grade receivers.

Relying on civilian-purchased GPS receivers will make units vulnerable to the loss of GPS services by electronic attack. To ensure the use of these services, unit leadership must ensure that commercial GPS systems are used only for redundancy and never in place of a keyed military-grade GPS receiver. In addition, unit leadership must ensure that the military-grade GPS receivers they used are keyed in order to access the P(Y) code. A military receiver without a current key has no greater protection from enemy electronic attacks than a commercial receiver. Finally, Soldiers must continue to train in non-GPS-related land navigation techniques and use those skills to continuously monitor the DAGR position and cross reference with a map. This technique mitigates the potential effects of GPS electronic attack. In summary, a keyed military-grade GPS receiver and proficient land navigation skills are absolutely critical to the movement and maneuver of military forces on the battlefields of the future.

MAJ Russell Nowels is the chief of training and exercises at the Joint Navigation Warfare Center at Kirtland Air Force Base, N.M. His most recent assignments include serving as an instructor, Department of Physical Education, U.S. Military Academy (USMA), West Point, N.Y.; and commander, A Troop, 1st Squadron, 10th Cavalry Regiment, 2nd Brigade Combat Team, 4th Infantry Division, Fort Carson, Colo. MAJ Nowels holds a bachelor's of science degree from USMA in geography and a master's of science degree from Indiana University in kinesiology.

MAJ Matthew Fechter is a current operations support officer at the Joint Navigation Warfare Center at Kirtland AFB. His most recent assignments include serving as commander, B Company, 2nd Battalion, 34th Armor Regiment, 1st Brigade Combat Team,1st Infantry Division, Fort Riley, Kan; and regional instructor for the Counterinsurgency Training Academy, Kabul, Afghanistan. MAJ Fechter has a bachelor's of science degree in geology from the South Dakota School of Mines.