THE GLOBAL POSITIONING SYSTEM'S WEAKNESSES

The Global Positioning System's Weaknesses During Use in Combat

SGM Robert Scott

United States Army Sergeants Major Academy

Class #58

SGM Glenn Caspari

November 13, 2007

Abstract

This essay discusses the weaknesses of Global Positioning System (GPS) use in combat, and in particular its susceptibility to Electronic Warfare (EW). Jamming a radio signal has been a successful component of EW for decades, dating back to the pre-Vietnam war era. The success of the GPS depends solely on the accuracy of signals output by a satellite, and then received by a radio receiver (the GPS receiver). The ability to jam any type of radio signal impedes its accuracy, and therefore causes the signal to relay potentially false information. In the GPS world, the reliability and accuracy of the signal is the key to saving or costing lives because of the military's reliance on GPS for bombs, radio equipment and hand held receivers. Jamming, in particular, is a successful means of destroying the GPS signal and causing it to be useless in combat, or in peacetime.

Outline

Thesis Statement: The exploitation of Global Positioning System's (GPS) signals allows the adversary to gain a battlefield edge, and ultimately outweighs the effectiveness of its use during war.

I. Introduction

II. Exploitation of the GPS Signal

- A. Jamming Defined
- B. Types of Jamming Devices
- C. Jamming Effects

III. Conclusion

The Global Positioning System's Weaknesses During Use in Combat

The exploitation of Global Positioning System's (GPS) signals allows the adversary to gain a battlefield edge, and ultimately outweighs the effectiveness of its use during war. This essay explains the effectiveness in using a jamming signal to render GPS ineffective. It also explains the impact on the United States Army when GPS is not available, or is hindered. It impacts complex equipment like GPS guided munitions, while also impacting simple radio equipment used on a daily basis by Soldiers.

Jamming Defined

When GPS was developed decades ago, it was designed to operate in an electronic environment free from attack. The threat of exploiting the signal simply didn't exist. However, times changed during technological advances and Electronic Warfare (EW) became a significant part of the battlefield from the late 1980s and forward. Jamming is a component of EW. GPS receivers rely on an accurately transmitted radio frequency signal from a satellite. The signal literally travels thousands of miles through space before it reaches a GPS receiver. This satellite radio signal can be distorted either intentionally or unintentionally before it reaches the intended receiver. When the signal is made ineffective by another transmitted radio frequency signal it is said to be jammed (Mish, 2003). It is significant to note that the armed forces of the United States became more reliant on GPS technology and began to use GPS in a variety of ways. GPS guided munitions, radios with GPS capabilities, blue forces trackers, and hand held GPS receivers all have become commonly used on today's battlefield. These pieces of equipment all require that the GPS signal received from orbiting satellites is accurate and timely. If the signal is distorted in anyway, the grid coordinate calculated by the GPS receiver will not be as accurate as

it could be, and depending on the strength of the distortion, the grid coordinate could be adversely affected by hundreds of meters to a few kilometers. Simply put, when any type of distortion is caused to a GPS receiver, the receiver is confused and the resulting error can be very dramatic (Erwin, 2000). All EW experts agree that jamming a GPS satellite signal is a simple task, and only requires a bit of modest equipment to build a successful jamming device (Battle Against Terrorists, 2001). This is particularly important in Operation Iraqi Freedom (OIF). The adversary has proven its worth by using low cost resources that yield big results in disrupting coalition efforts. Building an inexpensive jamming device capable of jamming signals across a radius of several kilometers can cost less than 500 dollars, and can be built by following web based instructions (Battle Against Terrorists, 2001).

Types of Jamming Devices

Any transmitter that emits a signal can be used as a jamming device. Two radios that are keyed at the same time are not able to broadcast with clarity because they are actually jamming one another's radios. This is a simple example of jamming. Many types of radio frequency jamming devices exist in both the commercial and military worlds. These devices are made to be portable and relatively lightweight, and can be left to jam remotely without having the need for the presence of an individual to operate the system. Overseas manufacturers are designing jamming devices to specifically counter United States assets. One example is the Moscow produced jammer specifically advertised in a Paris, France air show to combat the effectiveness of the Tomahawk cruise missiles. The jammer weighs less than seven pounds, and emits a very low signal which makes it extremely difficult to detect and locate. The manufacturers claim that it's effective in jamming signals over a radius of hundreds of kilometers (Herskovitz, 2000). A less costly alternative can be made with easily obtained components for less than 500 dollars.

This jammer is a ridiculous three inches in diameter and is referred to as a hockey puck jammer. It transmits using only one watt of power, making it nearly impossible to detect. It was both tested and effective in jamming GPS signals (Herskovitz, 2000). Jammers can be classified into two categories: continuous wave and broadband. Continuous wave jammers operate by sending a constant signal on a specific frequency. These jammers are relatively easy to detect and counter. The broadband jammers are more effective, however. This jammer transmits a signal that bounces around randomly and is difficult to predict. Defending against the broadband jammer is a very difficult task (Erwin, 2000). The availability of information on how to build a jammer, combined with the already manufactured versions, make the GPS signal exploitable by the adversary.

Jamming Effects

The effects of jamming the GPS signals greatly degrade the armed forces of the United States. Soldiers rely on not only military issued GPS systems such as the Precision Lightweight GPS Receiver (PLGR), but also commercially purchased systems produced by such companies as Garmin. It is proven in tests in and around Baghdad, Iraq that the PLGR and commercial systems are very prone to jamming (Grantham, 2005). The negative impact of this jamming can be tremendous. Soldiers constantly use GPS receivers to determine exact grid coordinates to conduct raids on suspected terrorist locations in OIF operations. The consequences of conducting a raid on the wrong house in a particular village can be devastating to the overall goal of coalition forces. Innocent lives can be lost simply because of a grid coordinate error as small as 20 meters given by a jammed GPS receiver. Entire villages suddenly turn from supporting coalition forces, to condemning their actions. Extreme circumstances lead the villagers to stop cooperation with U.S. forces and side on the cause of the insurgents.

United States Air Force GPS guided missiles have both lived and died by their successes and failures in OIF. When these missiles are accurate, they provide an incredible advantage to the user; however, when they're inaccurate they most often times result in innocent lives again being lost. The ability to jam this GPS signal negatively impacts effective strategic targeting by U.S. forces, and creates a disadvantage when trying to win over the local Iraqi population. When homes are destroyed and innocent lives are lost, the world's media is quick to spread the story and share in the burden of the suffering. Naturally, public opinion is swayed and weapons technologies are ultimately questioned, at a minimum.

Blue forces tracker is another system employed by the U.S. forces that can be degraded by a jammer. Conducting simple operations such as vehicle linkups can easily turn into a fratricide incident because of jammed devices and faulty grid coordinates.

Conclusion

The adversary can gain a clear advantage by mastering the use of jammers on today's battlefield. Much of the equipment used by U.S. forces depends on the accuracy of the GPS signal, and this over reliance on GPS systems by U.S. forces is proving to be a weakness. If the adversary gains this advantage in the EW realm, the impact might be devastating for our forces. The separation of the fight provided by GPS guided missiles will be taken away. The ability to track friendly forces locations and activities through blue forces tracker will be gone. The individual Soldier having the quick ability to gain an individual position will be no more. One small signal emitting one watt of power might have a detrimental impact on today's battlefield, and future operations.

References

Battle Against Terrorists Heightens GPS Jamming Worries. (2001, October). *Satellite News, 24*(39), 1. Retrieved November 12, 2007, from Business Module database. (Document ID: 84471312).

Erwin, Sandra I. (2000, June). Threat to satellite signals fuels demand for anti-jam products. *National Defense, 84*(559), 23-27. Retrieved November 12, 2007, from Military Module database. (Document ID: 55064913).

Grantham, Scott D. (2005, October). Mixed Signals: Using Civil GPS Receivers in Combat. *United States Naval Institute. Proceedings, 132*(10), 72-73. Retrieved November 12, 2007, from Military Module database. (Document ID: 909635741).

Herskovitz, Don (2000, December). GPS insurance: Antijamming the system. *Journal of Electronic Defense, 23*(12), 41-45. Retrieved November 12, 2007, from Military Module database. (Document ID: 65226282).

Mish, Frederick C. (Ed.). (1980). *Merrian-Webster's Collegiate Dictionary Eleventh Edition.* Springfield, MA: Merriam-Webster