Mitigating Electronic Magnetic Interference Vulnerabilities in MLRS/HIMARS

by SSG Kevin G. Rutherford
13M Instructor / Writer

Foreword

(U) Our adversaries train tirelessly to defeat United States tactics and aim to degrade our effectiveness. Some of the most lethal tools in the Commanders' pockets is the Multiple Launch Rocket Systems (MLRS) and High Mobility Artillery Rocket Systems (HIMARS). The family of munitions these systems deliver possess the ability to strike static targets from 300km and consistently hit within meters of the intended targets. The MLRS/HIMARS and its munitions receive guidance data from GPS-aided sources. Mission Command Systems rely on GPS data and digital reporting to provide timely information and commanders' situational awareness. Without these systems, our effectiveness will be degraded.

(U) Our adversaries might exploit these systems, detect our actions and destroy our capabilities in order to degrade our effectiveness. We must understand what methods and equipment our enemy may employ to diminish our success. Once we understand these tactics we can employ counter-measures and train against our adversaries' actions, in order to degrade their success.

Direction Finding

(U//FOUO) Russian Electronic Warfare (EW) troops possess the ability to use electronic directional finding tools to determine the location and type of equipment in use by US and allied forces. Russian EW units in conjunction with their artillery operations centers successfully target and strike their intended targets.

(U) "…example from Eastern Ukraine, a Ukrainian army unit was broadcasting a radio message when it received accurate artillery fire, sustaining multiple casualties." (Asymmetric Warfare Group, 2017).

(U//FOUO) Potential adversaries are able to detect and monitor communications equipment and may be able to determine the location of US Forces. This possibility poses an increasingly danger because Russian forces have demonstrated the ability to produce accurate indirect fire from radio signals.

(U) "As with the degraded communication environment, Cyber Meaconing Intrusion, Jamming and Intercept (MIJI) is a very real threat to U.S. formations." (Asymmetric Warfare Group, 2017). MIJI, now known as Joint Spectrum Interference Report (JSIR), has the capability to affect both tactical and strategic units. Commanders and all leaders must understand the potential significance of adversaries successfully coordinating EW with indirect fires.

Radio Jamming

(U) Radio Jamming is a method of creating "noise" to prevent radio receivers from "hearing" transmissions. Encryption alone will not prevent radio jamming. Encryption is used to hide voice or digital communication among signals.

(U//FOUO) "Brevity codes, burst transmissions, relay stations, and communications windows are all TTPs that will limit the exposure of a headquarters to enemy electronic detection." (Asymmetric Warfare Group, 2017). Understand the longer each radio transmission is, the easier the enemy will be able to locate friendly antennas. Commanders can direct the use of "Dummy Stations" to increase survivability and determine enemy capabilities. Leaders must understand that jamming of Frequency Modulation (FM/SINCGARS) or High Frequency (HF/Harris) frequencies may be possible even with encryption. However, HF signals can be more difficult to detect and can decrease the units digital signature. Understand that while using encryption Frequency Hop (FH) on SINCGARS, radio operators may change from FH to Single Channel (SC) on a predesignated frequency to attempt to "push through" the radio jamming. However, Soldiers must recognize that in doing so, the enemy can pin point their location nearly immediately. This should only be used in emergency situations, and immediate movement may be required.

(U) Units should also practice hand and arm signals while mounted during movement to commu-

Continued on Page 10, See Magnetic

Magnetic ... Continued from Page 9

nicate. These practices will decrease the unit's digital signal, thus decreasing the chance of detection. This will place more emphasis on squad/team leaders to make decisions independently from headquarters units on immediate actions without breaking radio silence criteria.

GPS Electronic Magnetic Interference Threats

(U//FOUO) "Jamming communications adds to battlefield confusion and degrades command and control required to prepare for enemy offensive operations." (Asymmetric Warfare Group, 2017).

(U//FOUO) GPS Jamming, similar to Radio Jamming, creates signal noise to the GPS receiver. This action prevents the GPS receiver from deciphering the GPS signals from space, and therefore may result in GPS signal loss. While encryption will assist in preventing GPS data signal loss, encryption alone may not protect US assets.

(U) GPS Spoofing is an Electronic Warfare (EW) tool that deceptively provides false GPS data to receivers. This forces the GPS device to provide the user with a false reading of location. If not detected, Spoofing attacks could degrade the accuracy of indirect fires. GPS Spoofing can vary from a few meters, to hundreds of kilometers off of the true GPS location.

(U//FOUO) It is also imperative to understand that not only radio transitions are vulnerable to intrusion, jamming and interception. Digital signals, to include GPS signals, are exploitable. E.g. the Chinese based Comet-1 GPS Jammer has been rebranded from North Korea, and has a GPS jamming range of approximately 200km.

(U//FOUO) "Certain platforms are used for protection, emitting an EW signal designed to overload electronic fuses on incoming fires. Guided munitions, both direct and indirect, will either detonate early or change course once they come in contact with one of these EW bubbles." (Asymmetric Warfare Group, 2017).

Mitigating GPS Electronic Magnetic Interference

(U) DAGRs with updated encryption keys have the ability to detect GPS jamming and spoofing. Units should use DAGRs simultaneously with other systems of navigation to ensure that the detection of EW is occurs quickly. Utilizing updated encryption keys on all crypto devices must be standard practice.

(U) Using a Terrain-Masking technique, units can mitigate the effects of jamming from a ground based jammer. Units can determine the location of the jammer by using a DAGR and the body shielding technique. Use intersection and resection of lines from two points to detect a general location of the ground based jammer. (See Figure 1.)

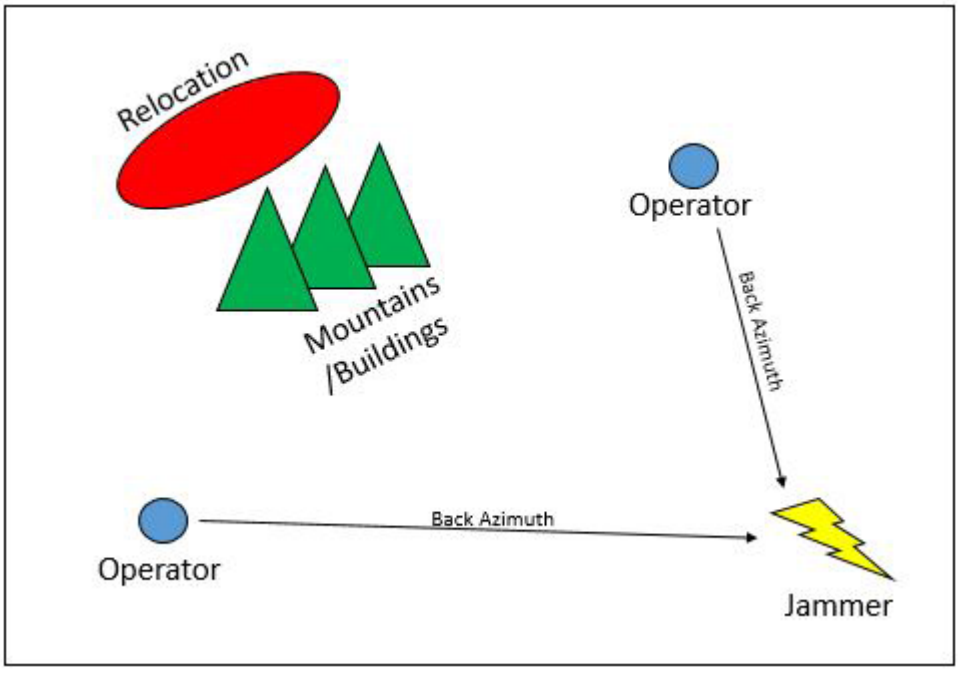

Figure 1. Example of two operators, using the body shielding technique and the back azimuth to determine jammer location. Then, selecting a relocation point.

Continued on Page 11, See Magnetic

Magnetic... Continued from Page 10

(U) Soldiers can then place objects such as buildings, terrain features or other vehicles between the GPS receiver and the jammer location. These objects can block the jamming signals from reaching the GPS receiver. If the location is "moving" this can indicate an airborne or mobile jammer. This type of activity must be reported to higher headquarters via GTA Card 40-01-002 and provides the information required. Units must establish TTPs to communicate these events to Commanders.

(U//FOUO) Soldiers must be proficient in GPS systems such as the DAGR, Blue Force Tracker and determining their own location with a map and compass. GPS Jamming on MLRS/HIMARS effects can be minimized if soldiers are trained to detect them. GPS Spoofing can adversely affect the known self-location if units are not using the proper encryption keys. If EMI is suspected, periodically check self-location using a map and compass. This can also be accomplished by using Survey Control Points (SCP) that were identified before EMI was suspected.

(U//FOUO) Utilize different means of survey if establishing SCPs prior to entering the EMI environment is not possible. Digital Imagery Exploitation Engine Version 2 (DIEE) can be a vital solution if proper planning and coordination are applied. DIEE can allow MLRS/HIMARS units maintain accurate self-known location by using predesignated locations, brevity codes, and marked locations.

(U//FOUO) MLRS/HIMARS family of GPS Aided munitions can achieve higher apogees above the EMI bubble. This will allow the munition to gain GPS data from satellites and increase the accuracy of the munition. However, if GPS data is not being received by the launcher, unaided mode must be used. While operating in unaided mode the GMLRS single or multiple rounds in open or closed-sheaf configurations may still be used.

Training Recommendations

(U) Units should adopt TTPs that would address EMI contested environments. Primary, Alternate, Contingency and Emergency (PACE) communication plans should be briefed, rehearsed and included in unit SOPs. Incorporate Single Channel (SC) frequency as an emergency only option. The SOP should identify hand and arm signals both mounted and unmounted in order to communicate. TTPs should also include battle drills that allows for Soldiers to communicate to Commanders the effects of EMI on each system. Breaking radio silence criteria should be strictly identified and enforced throughout training. Commanders should also institute periods of complete radio silence while coordinating with Signal Intelligence (SIGINT).

(U) Leaders at all levels should identify the power level required for FM and HF radios, and adjust as needed. The use of directional antennas should be used if practical and available. Practice radio etiquette with breaks in transmitting no longer than 3-5 seconds to avoid detection. Use digital sources (BFT or GDU) for sending routine reports rather than using lengthy voice reports. Brevity Codes should be utilized whenever possible to keep shorter transmission times. Leaders at all levels should practice operating in a communications "black out" zone. This would include, GPS, FM and HF to simulate active jamming. Unit TTPs must include for continuous operations without GPS, FM or HF. Alternatively, special tools can be utilized to conduct simulated jamming during home station training. This training must be coordinated through the electronic spectrum manager.

(U//FOUO) MLRS/HIMARS can shoot in a GPS denied environment by using Guided Multiple Launch Rocket System (GMLRS) Rockets. GMLRS can be shot accurately by firing single or multiple rounds in an open or closed sheaf configuration. However, accurate known self-location is required.

(U//FOUO) Consider, Russian artillery in Ukraine has demonstrated saturated indirect fire in over a 1000 square meters area after electronic detection of rebel forces. Increasing the distances between firing point, hide points and between launchers may increase survivability of launcher platoons. MLRS/HIMARS Commanders should evaluate local threats and consider expanding the Operational Area to allow over 1000 meters between Fire Points. This must be weighed against enemies entering the Operational Area, among other considerations. Mission Command and logistical support of units spread further apart will require additional planning.

Continued on Page 12, See Magnetic

Magnetic... Continued from Page 11

(U) Traditional land navigation skills should be utilized, when possible, in combination with automated equipment such as BFT or DAGR. Consider adopting alternative means of survey that does not rely on GPS, such as the DIEE system.

(U//FOUO) "Land Navigation is a perishable skill. Failure to use and practice it will result in a deterioration of Soldiers' abilities." All levels of leadership and soldiers need to train to use assets to navigate that the enemy is unable to disrupt or control. (Asymmetric Warfare Group, 2007)

(U) Consistent training, and knowledge of how to overcome EMI events, will allow units persevere. Establishing unit SOPs/TTPs and conducting frequent battle drills during home station training will allow for units to excel during EMI conditions.

References

ACE–Threats Integration. (2016). *Worldwide Equipment Guide Volume 1: Ground Systems.* Fort Leavenworth: TRADOC G-2.

Asymmetric Warfare Group. (2017, April). Russian New Generation Warfare. Fort Meade, Maryland.

Asymmetric Warfare Group. (2007, June). Korea Handbook: The Complex Operating Environment and Asymmetric Threats. Fort Meade, Maryland: U.S. Army Asymmetric Warfare Group.

Center for Army Lessons Learned. (2017, April 28). News from the CTC. *Replicating a Contested Electromagnetic Environment for Home Station Training.* Center for Army Lessons Learned.

Chairman Joint Chief of Staff. (2013, June 3). CJCSM 3320.02D *Joint Spectrum Interference Resolution* (JSIR) Procedures.

U.S. Army Field Artillery. (2016, October). Degraded Operation White Paper.

U.S. Army Field Artillery School. (2013, January 22). Guided Multiple Launch Rocket System (GMLRS) Unitary Rocket (M31/M31A1) Tactics , Techniques and Procedures (TTP). ST 3-09.63. Fort Sill, Oklahoma.

Find the CSM of the Field Artillery on FaceBook

https://www.facebook.com/CSM-of-the-Field-Artillery-School-418766494912364/