Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum

Major General Patricia Frost
Captain Clifton McClung
Lieutenant Colonel Christopher Walls
Edited by: Lieutenant Colonel Daniel Huynh

ABSTRACT

While the United States (US) fought two wars over the past decade, its adversaries were evolving their technology for fighting in the electromagnetic spectrum (EMS). In his 2014 monograph, Dr. Larry M. Wortzel writes "the PLA [Chinese People's Liberation Army] is updating 21st century mechanized and joint operations, combining them with electronic warfare—what the PLA calls "fire power warfare"–and precision strike." [1] New doctrinal concepts ranging from the tactical to operational levels of employing traditional signals intelligence and electronic warfare lead this change movement in China. [2] Included in the transition is cyber warfare, which details both kinetic and non-kinetic effects across the EMS. [3] We have seen similar advances in capability from Russia in the ongoing conflict in Ukraine. The Ukrainian military has witnessed first-hand the actual effectiveness of Russian electronic warfare (EW) technology and tactics. [4] Russian artillery has demonstrated the synergistic effects of EW and commercial off-the-shelf (COTS) small-UAS platforms when paired with jamming, indirect fire, and direct fire assets [in Ukraine]. [5] The Russians have utilized EW capabilities to geolocate Ukrainian signals and their associated forces, then fixed the formation with UAS, and finished these forces with jamming of mission command frequencies while delivering devastating barrages.

While the U.S. Army modernized its network and networked systems, it also encountered a paradigm shift as the network transitioned from a service to a warfighting platform that is now critical to all Army operations. These advantages through the EMS have significantly increased each formation's lethality from the infantry fire team to the brigade combat team. As a result, the Army significantly increased its reliance on devices and systems that communicate within the complex EMS to maintain this

Major General Patricia A. Frost assumed the role as Director of Cyber, Office of the Deputy Chief of Staff, G-3/5/7, Headquarters, Department of the Army in July 2016. A career intelligence officer, MG Frost has been working in the Cyber domain for the last 4 years.

MG Frost has held command and staff positions across all levels of the Army with assignments in the United States, Iraq, Afghanistan, Philippines, and Germany. Prior to her appointment as Director of Cyber, MG Frost served as the Deputy Commanding General for Operations for U.S. Army Cyber Command.

advantage. In Iraq and Afghanistan, the Army enjoyed overmatch in the spectrum without heavy investment in the modernization of EW capabilities due to the threat's inability to contest US capabilities in the EMS. Our adversaries in Iraq and Afghanistan relied mainly on commercial communications technologies. Meanwhile, other near-peer countries such as Russia and China made significant investments in modernizing and honing their EW skills and capabilities, which puts the US military at a significant disadvantage.

Army leaders have realized after shifting from the War on Terror to Multi-Domain Battle that there is a significant EW capability gap. With this realization that the US no longer enjoys an advantage in the EMS, the Army as a whole must adapt to the implications of operations in a complex EMS environment. The development of secure communication and other EMS capabilities must continue to be a priority for Army R&D and science and technology communities. The Army must also speed the process to bridge gaps through rapid capability development and agile acquisition processes. US adversaries already possess EW capabilities that provide overmatch, and the threat will continue to evolve. The Army must invest to transform as well to address this threat.

Historically our Soldiers were taught radio discipline; tactics such as only talking on a radio for three to five seconds, and the use of pro-words or brevity terms.[6] The rationale behind such brevity was that an enemy could triangulate using ES direction-finding (DF) capabilities to locate and target our position. Once located, the adversary could then engage with either jamming, direct, or indirect fire. Fast forward to the present day, and it is easy to see the impact of how technology has shaped the battlefield. SIGINT, EW, and DF technology has grown

Captain Clifton McClung is the Electronic Warfare Officer (EWO) for the Army Cyber Institute's (ACI) CEMA Integration Group (CIG). He commissioned as an Infantry Officer in 2008 and served as a Mechanized Infantry Platoon Leader and Battalion Signal Officer in the 3rd Infantry Division in support of Operation Iraqi Freedom and Operation New Dawn. From 2013-2016 he served as a Brigade EWO, Deception Planner, and S3 Plans Chief for three years in 1-2 Stryker Brigade Combat Team, Joint Base Lewis-McChord. As a member of ACI's CIG, he contributes to shaping the Army's Electronic Warfare strategy and the integration of emerging threat scenarios into combat training centers at the tactical level. CPT McClung is currently preparing to transition to graduate school to pursue a Master's Degree in Information Security and Technology.

exponentially faster and is more accurate and effective. Current COTS direction finding systems and EW equipment can rapidly triangulate the location of a transmitter. This provides a greater reason why the Army must leverage its experience and re-institute our 'historical' training to reduce our signature when facing an adversary with advanced EW capabilities. We must make greater strides in integrating EW into combined arms maneuver, and more importantly, the Army must philosophically change the way it employs and exercises mission command throughout the Multi-Domain Battle Re-focusing on EW and long-range precision fires capabilities will significantly enhance Army readiness for future conflicts.

Through a series of critical questions, this paper hopes to inspire the thought leadership required to operate in a complex EMS environment. It will further detail and discuss how and why mission command is so critical to the evolution of EW, and how we must change to fight and win in the EMS by increasing lethality. The current mode of Army EW operations will not achieve even a limited window of tactical advantage. Our Army's continued heavy reliance on devices and digital systems operating within the EMS will be our downfall if we do not recognize and work to mitigate our vulnerabilities, and our techniques for operating in a contested environment.

Commanders and their respective staffs face significant issues in the spectrum and should address certain questions to understand how to fight and win within the EMS.

1. **How should I think differently about the operations process when it comes to an EMS environment that is highly congested, contested, and degraded?** Commanders must integrate integrate

Lieutenant Colonel Christopher Walls is a Cyber Warfare Officer, currently serving as the Deputy Division Chief for Strategy and Policy in the Cyber Directorate of the Department of the Army G3/5/7. He was commissioned as an Infantry Officer and served in both mechanized and airborne units with numerous combat deployments. In 2010, LTC Walls began his cyber career at U.S. Cyber Command and has since served operational and institutional assignments at Army Cyber Command and the Army Cyber Center of Excellence. Among LTC Walls many distinguished accomplishments, he most recently led the development of *Army Field Manual 3-12 Cyberspace and Electronic Warfare Operations* and is an acknowledged expert on full spectrum cyberspace operations within the Department of Defense.

SIGINT and EW operations into all phases of operations. As described in the recently published Army FM 3-12, the Cyber Electromagnetic Activities (CEMA) staff section is responsible to plan, integrate, and synchronize both offensive and defensive cyberspace and electronic warfare operations. The CEMA section utilizes existing processes, intelligence, collection management, military decision-making process (MDMP), targeting, and others to plan, integrate, and synchronize electronic warfare operations into a unit's operations. Commanders and staffs must integrate EW considerations into the planning and execution of operations to increase lethality and effectiveness. Specific examples include ensuring that commander's intent includes a vision for EW, requiring an electronic order of battle to understand threat EW capabilities, ensuring that intelligence requirements (IRs) are established, developing targeting guidance that addresses adversary EW capabilities, requiring and enforcing electronic protection measures, and integrating EW considerations into home-station training.

2. **How do I maintain situational awareness of my EMS signature?** Commanders and staffs must understand that the EMS signature is the electromagnetic radiation emitted by their unit's emitters, such as communication systems, and networked capabilities. These systems, based on the amount of power they are using, can produce a signature that adversary receivers can detect, locate, collect, and target with lethal and non-lethal effects. We need to evaluate the

Lieutenant Colonel Daniel P. Huynh serves as a senior cyber research scientist at the Army Cyber Institute. He is currently a Cyber Warfare officer, and a former Field Artillery officer and FA53, Information Systems Engineer. He is a 1999 graduate of the United States Military Academy with a Bachelor's Degree in Computer Science. Additionally, he has a Master's Degree in Computer Science from the Naval Post Graduate School. LTC Huynh's most recent assignment was with the Cyber National Mission Force, as a National Cyber Protection Team Operations Officer and Cyber Network Defense Manager. LTC Huynh holds numerous professional security certifications which include: CISSP, GXPN, GPEN, GCFA, GMOB, MCITP, CASP, CEH, CSA, and SEC+.

use of these systems from a force protection and survivability perspective. We cannot afford to have continuous transmissions of hour-long Battlefield Update Briefs (BUBs) that occur throughout the day. Electronic protection measures provided by the CEMA section should include guidance on active and passive measures that unit and subordinate commanders can take to reduce their signature and increase survivability. All devices that transmit and provide a targetable signature must be carefully used to minimize risk. Commanders must assume risk only when operationally necessary. The risk of physical travel to meet to exchange information may be high, but still lower than creating a targetable signature for the adversary. Because of this threat, commanders should increase the use of mission-based orders enabling staff to understand and execute their intent and lower the requirement to continually transmit orders. Dissemination of products via the spectrum should also factor in the threat of enemy detection. Commanders should continue to stress and train disciplined initiative into their subordinates for them to execute operations based upon intent and reduced feedback loops.

3. **What types of EW assets are available to me? Which are organic and which must I request?** Capabilities available to commanders will vary by echelon and unit. Electronic warfare support (ES), actions taken to search identify and locate signals (and associated units) to support operations, can be conducted by organic EW or signals intelligence (SIGINT) systems. Actions taken

to conduct SIGINT and ES may be very similar and should be mutually supporting. Both capabilities can be used to answer intelligence requirements or support future operations. Ground, airborne, and terrestrial SIGINT platforms can confirm commander's critical information requirements (CCIR) to support the intelligence section and CEMA Cells' information requirements. CEMA and intelligence support can request joint platforms from the Navy, Marines, and Air Force.

There are a limited number of EW systems currently fielded, but additional capability is entering the force through Army rapid capability development and expedited acquisition efforts. While current systems are limited to short range dismounted and repurposed remote counter IED systems, future EW capabilities will include integrated dismounted, mounted, and aerial systems. Today's most relied upon system–the Prophet–can sense and identify emitters. When this system is integrated with other platforms, it can locate enemy emitters and multiple UAS systems. These systems are an improvement in capability for US forces, but are not suited for fighting a near-peer adversary with similar EW capabilities.

4. **How can both ground and aerial EW assets enhance my Information Collection Plan?** The EMS environment may either be a target rich space or sparse landscape based upon adversarial tactics, techniques, and procedures. It is the staff's responsibility to help develop intelligence requirements and prioritize collection assets. The number of assets used against an adversary will always be a constraint, so it is critical to understand how both SIGINT and EW passive and active measures can affect each other. The Electronic Attack effect of communications denial (an example of an active measure) requires a detailed understanding of the adversary's communications architecture and allocation of additional EA resources to achieve a 'denial' effect. However, selective disruption, which may include periods of denial of specific systems, can be used to 'herd' the enemy from one system to another. The enemy is forced to exercise his PACE (Primary, Alternate, Contingency, and Emergency) plan, which can enhance SIGINT collection. As part of the greater collection and targeting plan, SIGINT collection and EW activities should be synchronized and de-conflicted to increase effectiveness and reduce unintended consequences.

5. **What is the emission control (EMCON) posture by phase, and what are our triggers to shift in the PACE communications plan?** The S6, S2, and CEMA Cell must collaborate to identify where the enemy will locate collection and EW assets throughout the battlespace, and how they will likely be employed. Based on these assumptions, the S6 should develop a dynamic signal concept of utilizing friendly-based, enemy-based, terrain-based, and time-based triggers to shift the communications plan as required. This includes identifying windows ranging

from the limited use of continuous transmission of satellite communications to not deploying these systems at all. When the mission requires a higher discipline of EMCON to achieve surprise or survivability, the staff must also develop alternate communications to synchronize and maintain Mission Command at a minimum one-level up and one-level down. Examples include, but not limited to tactical radios using short data burst communications, convoy flag or hand and arm signals, and pyrotechnical signals.

6. **How can I detect if my unit is experiencing an electronic attack?** Units should have battle drills in place to determine cause or sources of electromagnetic interference (EMI) to include troubleshooting of systems and determining breadth (frequency bandwidth and physical distance) of interference. One of the keys to successfully identifying the source of electromagnetic interference is accurate reporting in conjunction with analysis, while other collection capabilities can assist in determining the source of the EMI. Units must establish and implement EMI resolution procedures as described in Enclosure D "EMI Characterization and Resolution at the Local Level"; CJCSM 3320.02A, "Joint Spectrum Interference Resolution (JSIR) Procedures", for every mission command system.[7] These procedures are a Soldier skill, and just as important as learning how to load, clear, and reduce stoppage on an assigned weapon system. Since it is entirely possible that the Soldier will come in contact with EW effects prior to direct fire contact with similar or greater consequences it is imperative to train our forces to recognize and respond to indicators of an electronic attack. The CEMA Section at echelon may tailor the joint doctrinal procedures, and create their own battle drills and standard operating procedures for their specific echelon and mission.

Some basic questions, tied to CCIR, to ask during interference would be:

- What specific radios or systems affected?
- Are alternate frequencies affected?
- Who and where are the affected units?
- Is disruption occurring laterally and vertically across the unit?
- Can friendly systems' frequency, Julian date, time, or hopset be changed?
- Can friendly forces use a system in another band or frequency?
- Have you submitted SIGINT requests for collection for your frequencies, in front of the forward line of troops (FLOT), at a higher power level than yours to identify possible enemy EA effects; and if so, are you now cross-cuing with imagery intelligence (IMINT) to confirm enemy systems in that area?

- While the S6 may focus on the standard troubleshooting of internal and external communication, they should also share information with the S2 and CEMA cell to process proper reporting to higher headquarters. This request could be made through a Joint Spectrum Interference Report (JSIR) by the unit(s) experiencing EMI and submitted vertically to the respective CEMA Section/S6/G6 (ref. Enclosure E "Joint Spectrum Interference Report format"; CJCSM 3320.02A, "Joint Spectrum Interference Resolution (JSIR) Procedures).[8] It is highly recommended that unit S6/G6s build and disseminate a JSIR format for radio and digital systems for increased efficiency and accuracy of reporting; e.g., making and publishing a fill-in-the-blank JSIR for JCR similar to a call for fire request. Typically only SIGINT platforms at brigade and above can confirm or deny if interference is the result of adversary EW effects. It is immaterial to the type of interference (technical communications issue or enemy overt/covert EA effects) at company or battalion levels; units should shift in their PACE plan and continue the mission.

7. **How can we minimize and mask our EM signature from the enemy?** The use of terrain to mask transmissions from combat network radio (CNR) propagating toward enemy collection platforms should be implemented whenever possible as a tradeoff to extending CNR range. For example, the masking of electronic signatures by establishing radio transmission sites on the military crest of hilltop versus the physical crest to mitigate radio wave propagation into enemy EW or SIGINT systems. The same terrain that will impede your ability to communicate from surface to surface communications, such as large stands of trees or dense vegetation, hills obstructing line of sight, and potentially large bodies of standing water, will affect the enemy's ability to use their organic ground-based ES assets to collect signals of interest. If the enemy is using an airborne EW or SIGINT platform, even high frequency (HF) radio communications have an increased risk of direction finding or jamming. The use of masking communications emissions with terrain can decrease the probability of detection and jamming. Radio frequency line of sight is often much greater than physical line of sight. Some radio signals and energy can "bend", reflect, or refract off or around terrain, thus both extending your ability to communicate and the enemy's ability to direction find or jam. If the enemy attempts to jam a CNR network that you are retransmitting around your area of operations, you could potentially retransmit the enemy's jamming signal as well, thus another reason to mask your CNR retransmission sites. This will reduce your CNR footprint, but increase survivability and preserve mission command.

Minimizing EM signatures ties into and reinforces the previous point about the use of out of band methods to communicate. The enemy cannot detect and locate a unit that does not transit nor identify a unit that is continuously obfuscating themselves and implementing an effective electronic protection plan by shifting in their communications frequency bands.

8. **How can I assess my unit's digital and electromagnetic spectrum footprint during training and while deployed?** As described in the new FM 3-12, the Spectrum Manager, who works for the cyber planner in the CEMA Cell, is responsible for maintaining the situational understanding of the EM environment. This is accomplished through the deployment of organic directional and omnidirectional spectrum analysis equipment. This same equipment could be used to locate sources of interference but requires a deliberate sustainment training plan to maintain a highly technical and perishable skillset. A spectrum manager will have a significantly harder time identifying the source of interference if they do not have theequipment or training to establish an EMS baseline in their operating area to compare before and after experiencing interference. These requirements are new to spectrum managers and will require commander support to enable these individuals to grow into this new mission.

9. **How do we train to fight and win in a degraded or contested EMS during Home Station Training (HST)?** We emphasize CEMA at HST because you should not rely on your next Combat Training Center rotation to train in a contested or degraded EMS environment. Integrating EW individual, collective, or staff battle drill tasks into all major training exercises is a key component to maintaining Mission Command and physical survivability. HST should be done at all levels and include a mix of live play use of available systems, constructive effects, and/or conceptual TOC or communication exercises. Generic adversary EW capabilities is a good starting point for how CEMA effects should be integrated into HST. Whether the replicated threat is notional or simulated, units still need to have the necessary confidence and basic proficiency in their digital and communication systems. Their ability to recognize and respond to adversary EW activities should be achieved through routine digital gunnery. Only through repeated practice and rehearsals of decentralized mission command, execution of communication PACE plans, and deliberate out of band communication will units improve their readiness levels. Units must also integrate CEMA into planning and operational processes. Whether your unit is utilizing internal assets or requesting external assets (live or constructive), creativity and experimentation can go far in ensuring training is realistic and challenging. The repurposing of a Combat Network Retransmission (CNR) team to attack a portion of an operational radio network is an example of how a unit might replicate enemy EW effects. Localized GPS jammers might also be

used to reinforce analog battle tracking, navigation, and fire mission processing. While conducting training, it is essential to recognize the need for advanced coordination with your Range Control and Local Spectrum Management office. Lead times for approval for use due to the required coordination may take weeks to months for initial requests, so allow extra time to ensure proper coordination.

10. **How can my staff and I further increase our knowledge and understanding of CEMA planning considerations?** A great starting point for references is FM 3-12 Cyberspace and Electronic Warfare Operations dated April 2017. Additional recommended professional reading is from the valuable repository of Lessons Learned from CTC "CEMA Support to Corps and Below" rotations supported by U.S. Army Cyber Command (ARCYBER). The RAND Corporation recently published two worthy studies on Tactical Cyber employment for Corps and Below.[9] Regarding training, a relevant course for staff would be Army Leader Cyber Operations Course (ALCOC), which gives the fundamentals of Cyber and EW employment considerations. A course that non-EW personnel may take for familiarization with Army and Joint EW concepts, fundamentals, doctrine, and capabilities is the Electronic Warfare Integration Course (EWIC). This course is 40-hours and is taught by 1st Information Operations (IO) Command to provide IO Officers familiarization for incorporating EW support to Information Operations. The 1st IO Command offers two other courses that EW personnel at brigade and above could attend: Military Deception Planners' Course and Cyberspace Operations Integration Course.[10] For additional reference material for EW Officers and Warrant Officers, see DA PAM 600-3.[11] Lastly, it would be wise to lean heavily on your BCT's EWO and EWO Technicians to be the subject matter experts in this area, and to provide Leader Professional Development (LPD) training for you and the staff.

CONCLUSION

As a commander, fighting and winning within the EMS does not require a degree in Electronic Warfare. However, being a commander who embraces the need for an evolution in thought about mission command will undoubtedly improve unit readiness and set the right conditions to win on the battlefield of today and tomorrow. The importance of fostering an environment that emphasizes disciplined initiative is not a new idea, but when put into context against a realistic threat who can directly affect mission command through EW means, only further drives home this topic of relevance. As with many other competing priorities that a commander and staff must deal with, CEMA is not something that can be dealt with as an after-thought. The integration of CEMA into all warfighting functions will increase our Joint warfighting capability. Only by placing emphasis and resources towards training CEMA, will staffs and subordinate units improve their understanding and proficiency. Even though the Army still has many roads ahead to conquer with the integration of both friendly and enemy EW capabilities into live, virtual, and constructive training—this should not preclude tactical units from experimenting with and getting creative in training CEMA now. Understanding where we are in today's military environment, and where we are going with technology, one might think about a continuum of how we should train. Whether we are fully automated and digital, or fully analog and manual, we must not lose sight of how important and influential a commander's personal emphasis, training guidance, and philosophy can be in shaping the EMS fight.

NOTES

1. China have spent their military budgets on modernization of EW doctrine, http://www.dtic.mil/dtic/tr/fulltext/u2/a596797.pdf.

2. "Russia have spent their military budgets on modernization of EW", http://thediplomat.com/2016/04/russias-surging-electronic-warfare-capabilities/.

3. Russia destroys 85% of two Ukrainian Army Battalion, http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/.

4. https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

5. http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/.

6. STP 21-2 (Warrior Skill Level 1); CH 3, Task: 113-COM-1022, "perform voice communications".

7. *Enclosure D "EMI Characterization and Resolution at the Local Level";* CJCSM 3320.02A, *"Joint Spectrum Interference Resolution (JSIR) Procedures,* January 20, 2006.

8. *Enclosure E "Joint Spectrum Interference Report format";* CJCSM 3320.02A, *"Joint Spectrum Interference Resolution (JSIR) Procedures,* January 20, 2006.

9. RAND Corporation, *"Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below",* https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf; RAND Corporation, *"Reimagining the Character of Urban Operations for the U.S. Army: How the Past Can Inform the Present and Future",* https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1602/RAND_RR1602.pdf.

10. 1st Information Operations Command sponsored courses, http://www.1stiocmd.army.mil/Home/iotraining.

11. U.S. Army, DA PAM 600-3 "Commissioned Officer Professional Development and Career Management", 26 June, 2017.