Operationalizing cyber, electronic warfare, space, special technical operations for decisive action

By Lt. Col. Clint Tracy

Army cyber and electronic warfare Soldiers are routinely conducting day-to-day operations that have little to do with their unique skillset. They are being used as school noncommissioned officers, Defense Travel System administrators, permanent gate guards, battle captains, battle non-commissioned officers, and the list goes on. This is an unfortunate circumstance that is the result of lack of understanding on what options these Soldiers can provide for a commander. In the aggregate, this results in poorly trained formations that have no ability to mitigate the enemy’s maneuver in the electromagnetic spectrum with cyber and electronic warfare equipment to disrupt, degrade and deny command, control, communications, computers and intelligence within their formations.

Since cyber and electromagnetic activities (CEMA) are relatively new to the Army, and there are no programs of record (minus the counter-improvised explosive device systems) there is a perception that CEMA Soldiers don’t bring much to the fight. There is a reluctance to ask what is in the realm of possibility because there is the assumption that without equipment there is little they can contribute. As a result, units maintain the status quo of “We’ll figure it out when it happens.” Unfortunately, in the cyber domain or the electromagnetic spectrum, your odds of “figuring something out” on the fly is practically zero. The prep work required for CEMA personnel to understand current threat capabilities, potential mitigation techniques, and the enemy’s vulnerabilities is extensive. The 1st Cavalry Division just completed a warfighter exercise and it took a full six months of homework to be prepared for execution of the Warfighter mission. That was six months of daily research on Joint Worldwide Intelligence Communications System and Secret Internet Protocol to understand enemy ca-
pabilities, frequencies and vulnerabilities. Six months of building and refining processes for targeting, CEMA working group, generating and synchronizing requests and building standard staff products. Six months of training personnel on Command Post of the Future, staff interaction, and information receipt, analysis and distribution, and we still left capabilities on the table because we were not as informed as we needed to be. Especially with regard to cyber capabilities during execution.

CEMA, much like the G2, requires daily engagement and research to maintain currency on threats and potential mitigation techniques. Cyber threats pose a great risk not only to our networks but the very lives of our Soldiers. Imagine a cyberattack that shuts down a brigade’s upper Tactical Internet while they are in the middle of a movement to contact, or worse, while they are in contact. While not directly affecting maneuvering platoons that are probably communicating on FM, it has the ability to sever their link to the Fires battalion that is supporting their maneuver, can break the link to their sustainment support and potentially sever the links between them and the supporting close air support or rotary wing. Combine that cyberattack with GPS and communications jamming and you have a unit that is unable to communicate ... soon to be followed by an inability to shoot or maneuver as they run out of ammo and fuel because they are unable to request resupply. While we may think this is a stretch, the Russians have already used similar techniques linked to lethal Fires in Ukraine with devastating effects on Ukrainian Army units. A cursory search of the Russian doctrine of “Information Confrontation” that combines cyber, electronic warfare, propaganda and information operations and how it has been used in Ukraine should be a wake-up call to everyone in the United States military.

As you read this article, the Russians, Chinese, Iranians, North Koreans and others have developed sophisticated cyber teams and tools, and have an arsenal of electronic warfare jammers and collectors that dwarf the current capabilities that exist in the U.S. Army. The first step in countering this growing capability is to start with employing electronic warfare Soldiers in their military occupational specialties and insisting they provide subject matter expertise when developing plans and orders in order to help mitigate the capabilities we know our enemies possess.

In the six months we spent training for Warfighter, the structural flaws of the division CEMA section became very clear. The 153 individual and collective tasks can’t be accomplished by a five-man team that is spread between a division tactical command post and the main command post both conducting 24/7 operations. The ability to not only attend the required working groups, but to maintain situational awareness and to generate all of the required requests to support targeting can’t all be simultaneously executed with five personnel, even if they are all in one place. Multiple times during the day there are more requirements than personnel and at some point people must sleep. The first step in solving a problem is to see yourself, and the five-man section looks anemic when compared to all of the requirements. In discussion with our G2, we discussed the CEMA section absorbing the space and special technical operations (STO) personnel into a combined CEMA, Space, and STO section. It provided three more personnel but more importantly it combined three sections that all possess complementary effects. After consideration and looking at the nine-man FDU proposal for a CEMA section I decided to use the additional personnel as a proof of principal, so we rolled the Space and STO sections into CEMA and we started training.

One of the initial objectives was to fully understand everything space and STO could offer and to train those officers on what CEMA could provide. This was a critical step in developing a cohesive team, as they understood what options I wanted to provide for the commander. In a very short amount of time, we all began to see where we could integrate the collective capabilities into an overarching plan, this layering of effects would later prove to be extremely effective.

Access and understanding
Access and understanding were initially two areas we struggled with. It would not be beneficial for the combined CEMA section to have all of the knowledge and simply interject ideas or “effects” during targeting if the staff around us did not have an understanding of what we could do or at least a concept of what was possible – the how we would do it was really irrelevant, it was the end effect they needed to understand. With that in mind, we began to develop a list of personnel that needed to be read-on to specific programs we could use during the exercise. The read-on was really less important than the baseline of information it provided to the commander and the selected group of senior leaders and primary staff members who would be involved in targeting. Once we had established a baseline of information on capabilities, we developed and named “CEMA Operations” that targeted specific enemy capabilities. In actuality, this prevented us from needing to have TS discussions and allowed discussion around the table at the targeting working group under this guise. This allowed us to focus on the effects at the working group and work the specifics for how to achieve the effect in an area with the appropriate classification in a small CEMA huddle. This smaller huddle was really where we leveraged the capabilities of the combined section and synchronized the effects in time and space with the maneuver and Fires plans. As we talked through the effects we wanted to achieve, we were able to discuss the options available from each functional area and then determine how best to employ those capabilities so that we did not establish patterns. As an example, we would use different capabilities on a daily basis to deny enemy command and control, this prevented the enemy from figuring out how we were denying their command and control and thus allowed us to maintain the ability to use capabilities throughout most of the exercise.

Structure, roles, responsibilities
As mentioned, we utilized our Space and STO team of three personnel to help round out the section, but there was still not enough manpower to accomplish all of the essential tasks. Doctrinally, there are 153 collective and individual tasks that must be conducted in the CEMA Section in order to meet the requirements of 71-DIV-5900 Conduct CEMA. With five personnel in a division CEMA section it’s not possible to meet the requirements, much less be able to conduct 24/7 CEMA in a high operational tempo environment. The CEMA section we built with Space and STO added was responsible for integrating and synchronizing cyber, electronic warfare, space, and STO operations within the division and as part of the corps. This required continual integration with the G2 as the CEMA section was a customer of electronic intelligence, signals intelligence, human intelligence, and imagery intelligence among others. This also required integration with the G6 in order to maintain situational awareness of the threats the G6 was seeing on the network and compare those threats to the reporting that the G2 was receiving with
regard to cyber threat actors. The CEMA section was also integrated with the Fires section joint air ground integration cell (JAGIC) and division current operations (CUOPS) in order to control EA aircraft on station, receive tactical elint (TACELINT reports and push requests to the Combined Air Operations Center for confirmation/location so identified threats could be targeted and engaged by the JAGIC. Finally, the CEMA section was integrated with targeting and plans in order to ensure the right assets were requested and synchronized in time and space to enable the division’s operations in the deep fight.

Luckily the section received another warrant officer just before the Warfighter and we pulled two 29Es from our subordinate brigades for a total now of 11 personnel. As those brigades were not training audiences for the exercise and had adequate manning for CEMA there was no impact on their brigade operations (see figure above).

The structure provided the manpower necessary to effectively integrate with the staff and to generate the required requests to support division operations. In order to adequately integrate and synchronize with the staff, a CEMA section needs a minimum of eight CEMA personnel, two FA40 space officers and one STO officer. This places two 17 series personnel in the T-SCIF to provide 24/7 capability to generate offensive cyber operations requests and to integrate with Space (two personnel), STO (one officer), G2 SIGINT, collection and the field artillery intelligence officer. This enables real-time receipt and analysis of intelligence reporting and provides the ability to pass the analyzed information for lethal targeting to the FAIO for potential immediate strike. The importance of this integration in the G2 shop can’t be overstated. The minute-to-minute receipt of intelligence followed immediately by the discussions and decisions on how to attack the threats in real-time was key to our success.

Three personnel were placed in the JAGIC, this provided 24 hours of coverage plus an NCO who was on-duty focused on EA requests working 16 to 18 hours a day. This cell in the JAGIC was the central point of EA requests (JTASRs (DD1972s) and EARFs), refinement of EA requests, management of subordinate EA requests, management of aircraft on station, central point for receipt of TACELINT reports from the CEMA personnel in the temporary sensitive compartmented information facilities or G2 SIGINT, and the principal integration point with the CAOC for confirmation of emitter locations. This proved to be an essential link in providing immediate input to the JAGIC for the targeting of fire support, air defense artillery, and electronic attack equipment on the immediate strike list. Once the process was ironed out we were able to routinely destroy enemy emit-
The establishment of these positions with the previously described responsibilities allowed the section to simultaneously receive, analyze and distribute information, request, synchronize and integrate capabilities and provide options to the commander throughout division operations. This presented the enemy with complicated problems as his reconnaissance, mission command, and Fires systems progressively moved from disrupted to degraded to denied.

Integration
The roles and responsibilities described above would have been only moderately effective without integration and buy-in from the other staff sections. We worked to build relationships, especially with the G2, G6 and Fires in order to establish cohesive teams through mutual trust, create shared understanding, enable the exercise of disciplined initiative and inform the commander where it was prudent to accept risk. The result was ironclad trust in the information we were providing and receiving from the staff. The ability to rely on the information provided to be correct every time accelerated the throughput during analysis and ultimately helped the section synchronize both lethal and non-lethal effects on enemy formations throughout the depth of the division area of operation.

Final thoughts
Our success was directly attributable to task organizing for combat and our division leadership trusting we could deliver on the effects we were describing. Being given the latitude to define what the combined CEMA section needed to do up front (visualizing, describing and directing) and then working through our shortfalls with regard to personnel and capability was an ongoing process. After action reviews and discussion within the shop following every command post exercise allowed us to arrive at the right mix of personnel which equated to capability for the division. Unlike the warfighting functions where capabilities change in increments of years, CEMA, Space and STO all change in increments of weeks. In order to be value added to a commander, these Soldiers must be focused daily on learning and understanding the capabilities our adversaries possess; understanding tactics, techniques and procedures we can use to mitigate enemy systems or effects; and most importantly understand how to operationalize the effects we can deliver while integrating with the division staff, thus providing options for the commander. This only happens with command emphasis and recognition that daily work must be done by these Soldiers that is focused on CEMA, Space and STO. Ninety percent of the capability we will be able to provide for a commander is the result of months of homework, requests and condition setting. Due to the lead time required for many capabilities in these fields, all of the homework and training must be completed in Phase 0.

If you expect that a small section within the division or a brigade will be able to truncate the homework, training, or request process in Phases 1, 2 or 3, be prepared to “Figure it out when it happens” and quickly be combat ineffective. As stated above, our adversaries are investing heavily in these areas, as an Army we must recognize these threats and train our force to utilize the capabilities we have to their full extent. We must have nothing at rest when it comes to CEMA, Space and STO capabilities in order to provide our commanders the best options for defeating our near peers in an increasingly complex and contested cyber, electromagnetic and space environment.

Lt. Col. Clint Tracy is the Cyber and Electromagnetic Activities chief for the 1st Cavalry Division and has been assigned to the division since October 2017.