‘Break, Break, Break, Clear the Net’

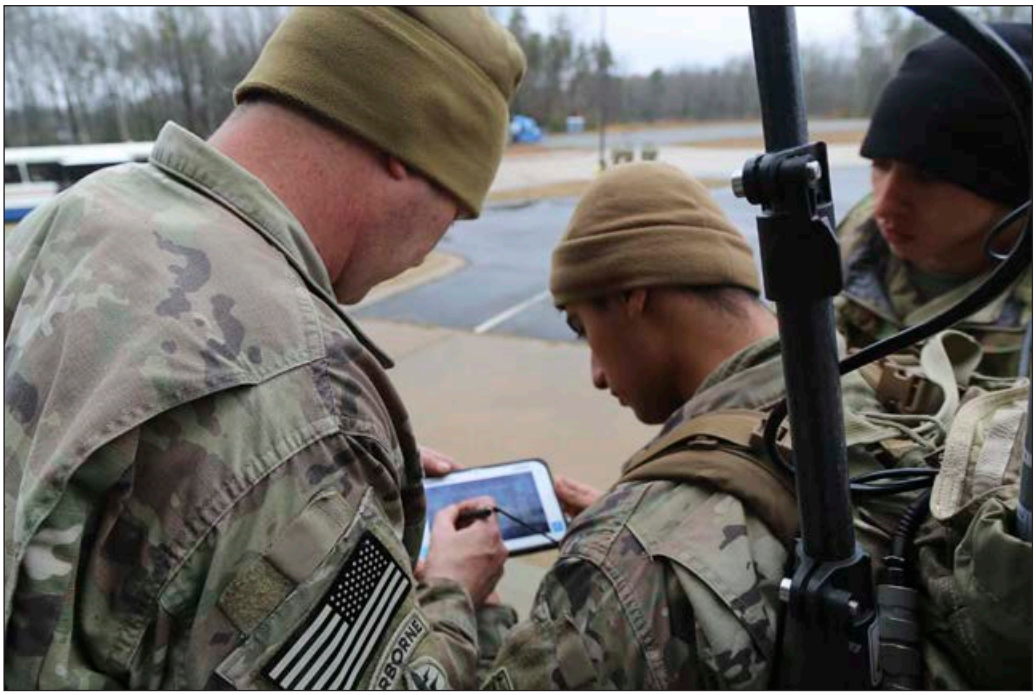
Understanding How Communications Enable Cross-Domain Maneuver While Conducting Multi-Domain Operations

CPT RUSSELL THORN

Shoot, move, and communicate” is a maxim that’s been a staple within military vernacular for decades. While these three words all continue to undergo their own respective evolutions within today’s multi-domain operations construct, the most complex and multifaceted transformation of the three is “communicate.” GEN Stephen J. Townsend’s July-September 2018 article on the recent doctrinal update of AirLand Battle to multi-domain operations highlights the complex transformation of communications in the digital age.[1] In addition to emphasizing the importance of communications on the modern battlefield, his article promulgates the need for cultural changes in how military leaders must now view the contemporary operational environment. GEN Townsend further emphasizes how communications — specifically our language — shapes a leader’s intent and the overall approach that the U.S. military takes toward maintaining overmatch against our adversities. This call for leadership to both examine and evaluate dictates that the traditional lens with which we view the very idea of “battle” must shift.[2] As part of this shift, the role that communications plays in tactical operations contributes even more to mission success or failure, and in some instances can even play a decisive role. While GEN Townsend’s article communicates with intent to influence our own formations, leaders must also remember that potential adversaries are also attempting to use communications to shape the viewpoints and plans of others.

Communicating in the Contemporary Operating Environment (OE)

The digital age provides the modern-day Soldier with a multitude of digital options enabling instantaneous real-time communications. Additionally, digital communications can provide a single user with the dynamic capability to rapidly and widely influence. Today’s standard smart phone enables service members to send and receive standardized report formats, operational graphics, and free text messages; participate in group messages better known as “group chats;” and display photos or video feeds to a countless number of people and social groups.



Members of Charlie Troop and Military Intelligence Company, 1st Squadron, 73rd Cavalry Regiment, conduct MOS cross-training during the Asymmetric Warfare Group Contested Micro Experiment. (Photos courtesy of author)

Adding to the complexity is the seemingly infinite number of messaging services and social media mediums.

Soldiers often disseminate information using messaging media or social media platforms without an understanding of the "maximum effective range" of the medium or platform. This is compounded by the fact that these digital communications occur without an awareness of the potential information fratricide that can occur from digital messaging or data transmission. Most Soldiers lack a comprehensive understanding of how these messaging and social media platforms transmit and receive voice and data. This lack of awareness of the "how" voice and data are transmitted is further exacerbated by a lack of awareness of "who" potentially monitors these mediums and platforms. These factors lend to a scenario which can allow for rapid exploitation by an adversary, resulting in catastrophic effects on friendly formations.

Just as with the considerations for employment of weapon systems, communication platforms emit a signature on the electromagnetic spectrum (EMS) which must be accounted for. All Soldiers, rank and position being immaterial, must be aware of these signatures and have an ingrained understanding that peer/near-peer adversaries may possess abilities to detect, target, and potentially exploit several types of communication platforms and arrays.

Take a moment to consider how much your formation utilizes computers, radios, tablets, and smart phones for conducting daily operations, both in the garrison environment and during tactical operations. Next, consider how much your formation utilizes chats, video, and other social media platforms for the routine tasks which encompass these daily operations. Finally, consider how much your formation uses mediums and platforms as a means of seeking out information and gaining knowledge, as well as utilizing them for simple entertainment or recreation. Like land, sea, or air, cyberspace has numerous hazards, obstacles, and scenarios which can unfold to result in significant negative consequences for your formation.

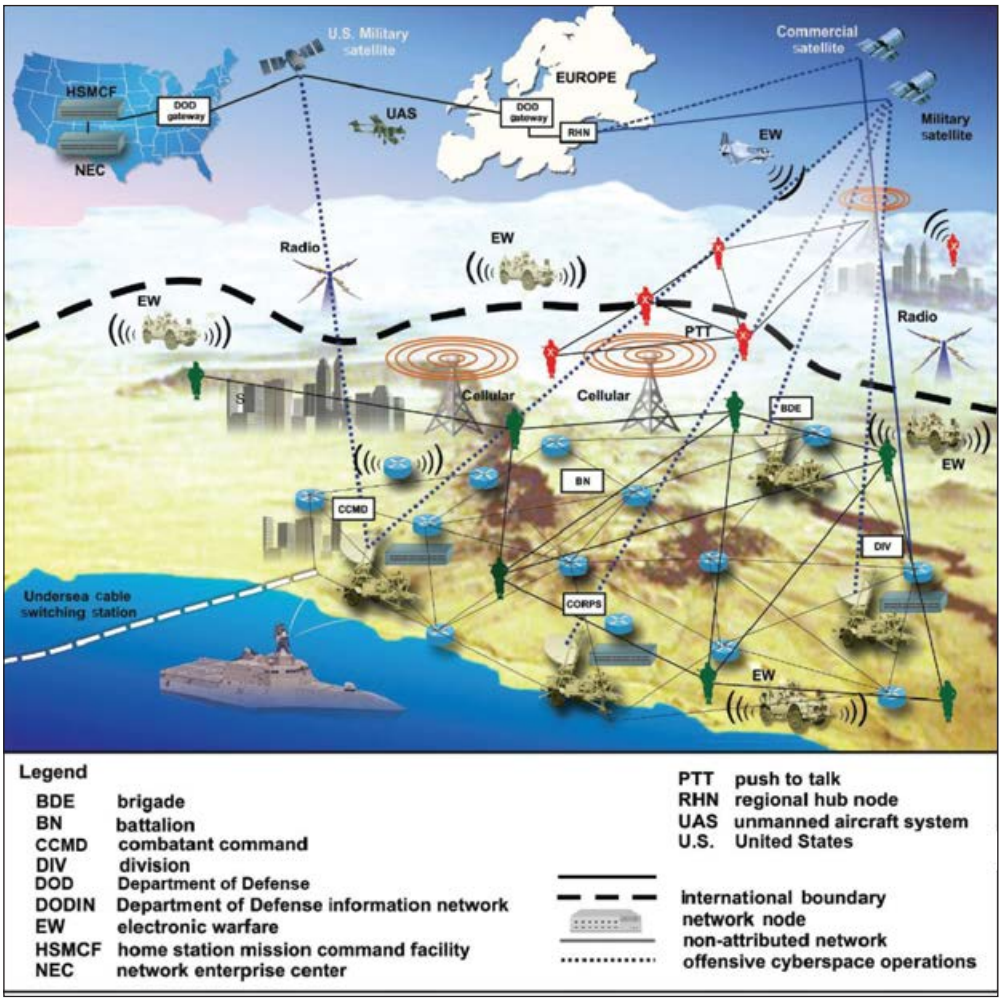
In the digital age, "communicate" is something the Army continues to evaluate and examine. High-tech communications and navigation equipment are tremendous tools that offer pinpoint precision and clarity, provide real-time situational awareness, assist with command and control, and facilitate movement and maneuver. There is little doubt that the Department of Defense will continue to seek out and develop state-of-the-art high-tech digital means of communicating. Along with the search for material advancements for communications and navigational hardware, the Army has also addressed the non-material aspect of digital age communications which we must also address.

Recognizing that digital advancements are one of the critical catalysts which have triggered a metamorphosis on the modern battlefield, Field Manual (FM) 3-0, *Operations*, was updated in October 2017. FM 3-0 now describes the sometimes contentious and complex relationship the U.S. Army has within the space cyberspace domains. Paragraph 1-35 states: "Rapid development in cyberspace and the EMS presents continuous challenges. While Army forces cannot defend against every kind of intrusion, commanders and staff must take steps to identify, prioritize, and defend the most important networks and data. They must also adapt quickly and effectively to an enemy and adversary presence in these networks."[3]

Paragraph 2-164 further states: "Army forces must retain the ability to shoot, move, and communicate during large-scale combat operations when space-based capabilities are denied, degraded, or disrupted. Training and rehearsing combat skills and ensuring the availability of analog alternatives to space (or cyberspace) enabled systems is critical to successfully persisting in the chaos and friction of modern, large-scale combat operations. Units must train to operate with widespread denial, degradation, or disruption of friendly space capabilities."[4]

When the implications of what FM 3-0 states are examined, an interesting dichotomy appears. Recognizing that space/cyberspace is an expanding domain which can result in impacts with equal and perhaps even greater implications than land, sea, and air, doctrine explicitly dictates that U.S. Army formations should be well versed in operating using analog alternatives.

Further examination of the complexity of the space/cyberspace domains has also resulted in the necessity for formations which can conduct cross-domain maneuver. FM 3-0 alludes to this necessity in paragraph 1-35 stating: "Cyberspace and the EMS will grow increasingly congested, contested, and are critical to successful operations. Army forces must be able to operate in cyberspace and the EMS, while controlling the ability of others to operate there."[5]



Cyberspace in the Multi-Domain Extended Battlefield (FM 3-0, *Operations*)

Assessing Communications Culture and conducting Cross-Domain Maneuver

The International Centre for Defense and Security publication *Russian Electronic Warfare Capabilities 2025* and the article "Victory without Casualties: Russian Information Operations" outline several areas and examples of Russian Federation strategy to influence and affect activities through the integration of electronic warfare and information operations as "force multipliers."[6] Further reinforcing GEN Townsend's comments regarding communication, both pieces hint that these force multipliers are part of a larger Russian Federation approach to both large-scale combat operations, as well as achieving objectives in operations just below the threshold of armed conflict. These "force multipliers" have been enabled on a wide range of platforms. These platforms can range from traditional military hardware such as fixed wing fighter jets all the way to common everyday communications and messaging mediums, social media platforms, and other spheres of influence which communicate a variety of messages, all driving towards a common endstate. This diverse approach presents a complex dilemma that can be presented by potential adversaries and suggests an implied requirement that U.S. formations' operating procedures and overall unit culture must be assessed and addressed.

With awareness for this implied requirement, the Asymmetric Warfare Group (AWG) set out to conduct just such an assessment. In March 2019, Paratroopers from C Troop and the Military Intelligence Company (MICO) of the 1st Squadron, 73rd Cavalry Regiment, 82nd Airborne Division, participated in the AWG Contested Micro Experiment (ACME). The ACME was a unique experience which placed the Paratroopers of 1-73 CAV in an OE replicating the hybrid warfare threat experienced by forces in the U.S. European Command (EUCOM) area of responsibility.

Among the many areas highlighted by the ACME was the incredible potential for cross-domain maneuver. The Paratroopers of C Troop and MICO developed a unique task organization consisting of Infantry, Signal, Electronic Warfare, and Intelligence Military Occupational Specialties (MOSs). This unique formation went beyond the idea

A scout observer from the 1st Squadron, 73rd Cavalry Regiment prepares to emplace a high frequency radio antenna during the ACME.

of elements of a dismounted reconnaissance troop simply integrated with "enablers" under the command and control of an Infantry command team. Moreover, Paratroopers within the task organization possessed both a basic understanding of the duties and capabilities of every MOS within their task organization and a rudimentary ability to execute these duties and provide these capabilities. By the end of the ACME, the C Troop and MICO formation demonstrated the ability to conduct cross-domain maneuver while conducting multi-domain operations.

The unique hybrid OE of the ACME provided the Paratroopers of C Troop and the MICO with firsthand exposure to the overall importance and vast complexity of communicating in an OE featuring a hybrid threat. These Paratroopers learned that communications can influence and shape the battlefield prior to any kinetic action even being taken. During the ACME, communication systems and standard operating procedures became decisive to the overall success or failure of Paratroopers' ability to conduct reconnaissance and surveillance, as well as execute cross-domain maneuver. Conversely, the ACME demonstrated that when critical facets of communications platforms are ignored or employed recklessly, hybrid adversaries can use communication systems and standard operating procedures against U.S. forces.

ACME highlighted the importance of disciplined, intentional communications plans. Early in the exercise, hybrid adversaries were able to exploit emissions by the C Troop and the MICO cross-domain formations for intelligence purposes.

As the ACME progressed, the dismounted reconnaissance teams, MOS-specific radio-telephone operators (RTOs), and troop sniper sections refined the overall unit communications architecture. By implementing a new communications plan by the later portions of ACME, the Paratroopers were able to remain virtually undetected during execution of reconnaissance and surveillance as well as the initial phases of their ground maneuver plan. This in turn resulted in a rapid tempo that kept the hybrid adversary off balance and allowed freedom of movement and maneuver throughout later stages of the ACME.

As the Paratroopers of C Troop and the MICO further progressed through the ACME, the success of the Paratrooper cross-domain formation was predicated by a strict adherence to two specific communications procedures. The first was a return to traditional tactics, techniques, and procedures (TTPs) generally associated with analog systems, basic soldiering skills, and utilization of field craft taught in courses such as the U.S. Army Ranger School, the U.S. Army Sniper School, and the Reconnaissance and Surveillance Leader Course (RSLC). The second procedure was a strict adherence to the use of reporting windows along with adherence to principals of mission command at all leadership echelons from the troop commander and first sergeant all the way to the most junior dismounted scout and intelligence analyst.

Application of ACME Lessons Learned

The ACME took place at the Asymmetric Warfare Training Center (AWTC), a facility offering a dynamic and unique OE through the use of enhanced realistic training. While the cross-domain maneuver conducted at AWTC provided the Paratroopers of C Troop and the MICO with tangible and measurable results — the communications lessons they learned along with the TTPs they developed and further refined — are transferable to any unit and training environment.

A great deal of success against a hybrid adversary occurs during intelligence preparation of the battlefield (IPB). It is critical that those conducting IPB develop a thorough understanding of all communications arrays, detection measures, and trends. While conducting terrain analysis, leaders must also examine the EMS. Does the OE have dense urban terrain, which features a vast array of layered communications networks and multiple systems, or in contrast does the OE feature rudimentary technology in austere locations with little to no preexisting communications networks and arrays? Next, a complete and holistic examination of the enemy's capability to detect, conduct reconnaissance and surveillance, and target your communication and mission command platforms must be performed. Finally, an examination of the effects that natural terrain and man-made structures have on communications, both digital and analog, must occur. This will enable leaders to build a robust communications architecture with several options to choose from as the ground situation changes or evolves.

A thorough understanding of your unit's own communications systems is both a beneficial and necessary requirement during multi-domain operations. Possessing a basic understanding of the associated signature(s)

Electronic warfare specialists partnered with a sniper team from the 1st Squadron, 73rd Cavalry Regiment to enable cross-domain maneuver during the ACME.

emitted by frequency modulation, high frequency, tactical satellite, and digital communications platforms should be a requirement for anyone who employs these various platforms. Noise level on the EMS, transmission duration, transmission signature, encryption level(s), and potential for the enemy to render effects against friendly units are factors which must be considered when communicating.

A layered approach to a unit's communications plan must extend beyond a generic overarching approach to the communications primary-alternate-contingency-emergency (PACE) plan at each respective echelon. Instead, a PACE plan for each echelon should be considered when overlapping with the enemy situational template (SITTEMP), linear and vertical distances between friendly units, and the frequency with which an echelon needs to communicate with its superior, adjacent, and subordinate elements. Finally, consideration for communications at each stage of the tactical operation should be weighed. Both the risk to the mission and the risk to the force may greatly change throughout the various phases of the operation. Movement, reconnaissance, and posturing for future kinetic actions may be the primary focus during the initial phases of an operation. The success of these initial events can hinge on the ability to remain undetected by a potential adversary. Conversely, the later stages of an operation may feature dynamic kinetic action through combined arms maneuver. Communications during combined arms maneuver may have far less risk of exploitation by a hybrid adversary due to the focus of the actual maneuver by both friendly and enemy forces.

Consideration for analog techniques which emit a limited or nonexistent digital signature must be the pillar of a unit's communications plan within an OE featuring a hybrid threat. In order to mitigate the potential for a peer/near-peer adversary to detect, target, and exploit communications, digital platforms and radio transmissions should be employed in a mindful manner with a respect for the signature(s) they emit. The Paratroopers of C Troop and MICO experienced great success with TTPs which centered on hand and arm signals, VS-17 panels, communication windows, whistles, and face-to-face meetings. While several of these TTPs already existed within the C Troop tactical standard operating procedure (TACSOP), they became the staple of the Paratroopers' force protection and command and control plans during the ACME. Moreover, these techniques are a matter of necessity for survival in an OE with a hybrid threat. When digital or radio transmissions were employed, they were done with a holistic view and assessment, thus enabling a shared common understanding for the second and third effects of using such mediums.

Finally, complete integration of all warfighting functions throughout all phases of the tactical operation is a necessity to unit success. Delegation of certain tasks and authorities to capable subordinates and other trusted agents can free leaders up to focus on relationship building and ensuring that their units are integrating service members not organic to the formation. Leadership from C Troop at all echelons greatly benefited from the diverse skill set the human intelligence collectors, electronic warfare specialists, MOS-specific RTOs, and intelligence analysts provided throughout the ACME. Complete integration of them into the reconnaissance and sniper teams to establish a formation capable of cross-domain maneuver helped establish a lexicon shared by all and shape a common operating picture for every Paratrooper immaterial of rank, branch, and MOS.

Conclusion

The above listed considerations were captured in a unique training environment that is unfamiliar to most units outside of Combat Training Center rotations. While an environment like this may be unique, Army leaders must consider the very real threat and capabilities that peer/near-peer adversaries currently possess. A concerted effort must be made to replicate this dynamic environment while training at any respective duty station.

Simple techniques can be employed to teach our junior leaders and squad-size formations the importance and value of adhering to the principals outlined in FM 3-0, as well as the lessons mentioned above. Leaders can ingrain a sense of realism in the formation by conducting tough and punishing mass casualty events. Those who are caught bringing their cell phones to a tactical training event, conduct an excessive amount of transmissions, conduct excessively long transmissions, and chose not to use encryption should experience hard and painful lessons now, so that our formations can avoid learning lethal lessons in the future.

Finally, leadership must capture these simple TTPs in the unit TACSOP. Unit leadership must ensure that the TACSOP is a frequently read, accessible, and rehearsed document. Units must place the TACSOP's contents into frequent practice in order to ingrain the principal of adherence into Soldier schema. While the communication

TTPs in use may require change which coincides with the latest hardware advancement or digital trend, the strict communications reminiscent of with tactical SOPs form the foundation of unit success and skill. Practicing communication discipline which emulates the tactical discipline found at Ranger School, Sniper School, and RSLC is what will ultimately ensure mission success and will save lives while conducting multi-domain operations on a future battlefield against a hybrid adversary.

Notes

[1] GEN Stephen J. Townsend, "Accelerating Multi-Domain Operations: Evolution of an Idea" *INFANTRY* Magazine, July-September 2018, https://www.benning.army.mil/infantry/magazine/issues/2018/JUL-SEP/PDF/7)Townsend-Evolution.pdf.
[2] Ibid.
[3] Field Manual (FM) 3-0, *Operations*, October 2017.
[4] Ibid.
[5] Ibid.
[6] Roger N. McDermott, "Russia's Electronic Warfare Capabilities" International Centre for Defense and Security, September 2017; T.S. Allen and A.J. Moore, "21st Century Political Warfare: Victory without Casualties: Russian Information Operations," U.S. Army War College Quarterly *Parameters*, Spring 2018.

CPT Russell Thorn is currently assigned as the executive officer for the 2nd Battalion, 58th Infantry Regiment (One Station Unit Training), Fort Benning, GA. He previously served in the 10th Mountain Division and 82nd Airborne Division. He has deployed in support of Operation Enduring Freedom and Operation Inherent Resolve. He was commissioned as an Infantry officer from U.S. Army Officer Candidate School and is a graduate of the University of North Carolina at Chapel Hill and Saint Joseph's University.