Cross-Domain Obscuration: *'More Than a Smoke Grenade'*

ANDY YERKES

Vignette

D*uring a training exercise, LTC Clark, commander of the 4th Battalion, 56th Infantry Regiment (Mechanized), pulled his company commanders in for a detailed back brief after giving an operation order (OPORD). The company commanders began their initial visualization of the fight ahead, nested within their battalion commander's intent. CPT Key, the commander of Bravo Company, intended to fight the way he had trained. As the commanders and the S2 began to discuss the operation though, he realized his knowledge and training had not been thorough enough; his company was vulnerable in areas the enemy would exploit and he would need to use all available means to enable his company to win the coming engagement.*

The movement from the assembly area to the assault position was almost 60 kilometers and set to begin at 0300. The company and battalion would track the single-column movement along the route via Joint Battle Command-Platform (JBC-P) and other Army Battle Command System (ABCS) platforms to synchronize the sequencing and timing of the support-by-fire (SBF), breach, and assault forces in the battalion. To ensure that a company or platoon didn't get too far in front or behind, there would be multiple radio calls to speed up or slow down. The fires cell would continue to shift the targets and confirm the shift with both a radio and digital information burst. Unmanned aerial vehicles (UAVs) would also fly in front of the formation to identify any potential enemy threat.

Alpha Company, the SBF force in the lead, would have about 30 minutes in the assault position and complete final radio checks with the battalion. The battalion fire support officer would join them, but the link up would be easy due to the JBC-P signature between the two elements. Final battalion graphics would also be disseminated via JBC-P as the battalion slowed and then stopped its movement in the respective assault positions to confirm timing of maneuver. The battalion would begin its maneuver from those positions based on both radio and JBC-P confirmation, moving to gain direct fire contact with the enemy to accomplish assigned tasks.

CPT Romano, the S2 who would be playing the opposing force (OPFOR), then said: "Sir, as the enemy commander, you've given me everything I need to defeat you quickly. Let me explain how."

CPT Key listened intently as CPT Romano described the multi-domain sensor capabilities the enemy would use to detect, locate, and target the companies in the battalion. In the assault position for the breach force, he realized he would be looking at smoking hulks of Bradley Fighting Vehicles and Abrams tanks in the SBF position. The enemy would wait until the majority of combat vehicles had arrived, and as the friendly artillery smoke began to billow, pre-planned enemy artillery would be concentrated in that specific area. Once that occurred, CPT Key knew if he reached for the hand mike to raise battalion for guidance, he would be unable to talk to anyone on either the company or battalion net. The JBC-P screen will have gone hay wire. Continually reaching for the hand mike to try and raise his battalion commander or battalion headquarters would result in an enemy answer — artillery rounds falling on his position. He realized he would be reliant on analog navigation capabilities (also known as a map and a compass).

Following CPT Romano's brief, SGT Burns, an attached Cyber NCO from the division, began to list multiple offensive capabilities that he would bring to the fight to enable the battalion's systems to continue to function during the fight. He highlighted specific enemy capabilities that he would request be targeted during Phase II into Phase III in the cyber domain to confuse the enemy's massive sensor array on the battlefield. CPT Key realized that SGT Burns was making reference to the joint phases found in Army Doctrine Reference Publication (ADRP) 3-0, Unified Land Operations*. SGT Burns continued to brief, but the commanders struggled to understand how to integrate the capabilities he was talking about in the close fight.*

CPT Key was learning that in the current and future operational environment (OE), the enemy will use multiple domain (land, air, maritime, space, and cyberspace) sensors to detect any signature he provides across the electromagnetic spectrum (EMS) to target and destroy his company. Most of the senior NCOs and leadership in B Company still

operated with the belief that night-vision capabilities, thermal optics, and encrypted communications gave his company an insurmountable edge over the enemy. Now, he grasped that he needed a far better understanding of an adversary's sensor capabilities, not just in the "land domain" but in the aerial, space, cyberspace, and maritime domains as well. He also needed a more intensive level of training on his own equipment and how to implement tactical measures to reduce his signature. CPT Key began to understand the need for cross-domain obscuration.

Cross-Domain Obscuration

The employment of obscuration is not without significant training and leader knowledge considerations. To fight and win this and future fights, CPT Key must understand and then prepare his company to win by training in degraded modes and adjusting the conditions in training to replicate the threat's ability to acquire friendly units across the EMS. Some training techniques are:

- Conduct land navigation without Global Positioning System (GPS) or JBC-P, with only certain elements allowed to turn on their systems during a coordinated time.
- Develop brevity codes for routine radio traffic.
- Train to operate at night under night-vision devices (NVDs).
- Train platoons to utilize different movement techniques and formations over wide areas with link up at night.
- Train to employ company mortars for their obscuration effects.
- Train to engage targets that are obscured by friendly obscurants.
- Train at the company level to communicate in an allocated window of time for routine reports.
- Leave personal cell phones at home station and rely on a rear headquarters for important messages from the rear (operations security [OPSEC]).
- Request support from the military intelligence company (MICO) to replicate an electronic attack or cyber attack.
- During staff exercises, specifically address obscuration requirements from higher headquarters.

Company commanders need to understand the implications of Russia's demonstrated ability to detect, locate, and target both Ukrainian and Syrian rebel forces effectively from a variety of domains utilizing different platforms (UAV, satellites, ground sensors, special purpose forces, small boats, social media) in the EMS, which is public record. This will make them knowledgeable about the threat as they do their own intelligence preparation of the battlefield. To be successful in the current and future OE, maneuver leaders across echelons must plan to protect their formations from observation from advanced sensors employed from a variety of domains simultaneously. Russia and other adversaries will use advanced thermal and electro-optics on their tanks and fighting vehicles, unmanned aerial systems (UAS), and aircraft that detect radio traffic. Enemies will visually confirm friendly locations utilizing satellites in space that detect electronic signatures as well as social media to identify U.S. formations.

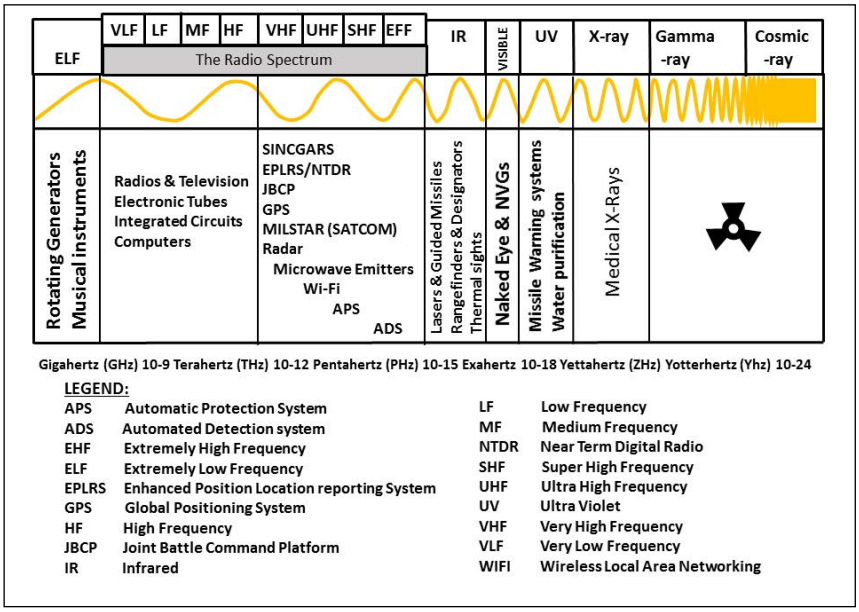

Figure 1 — The Electromagnetic Spectrum to Military Applications

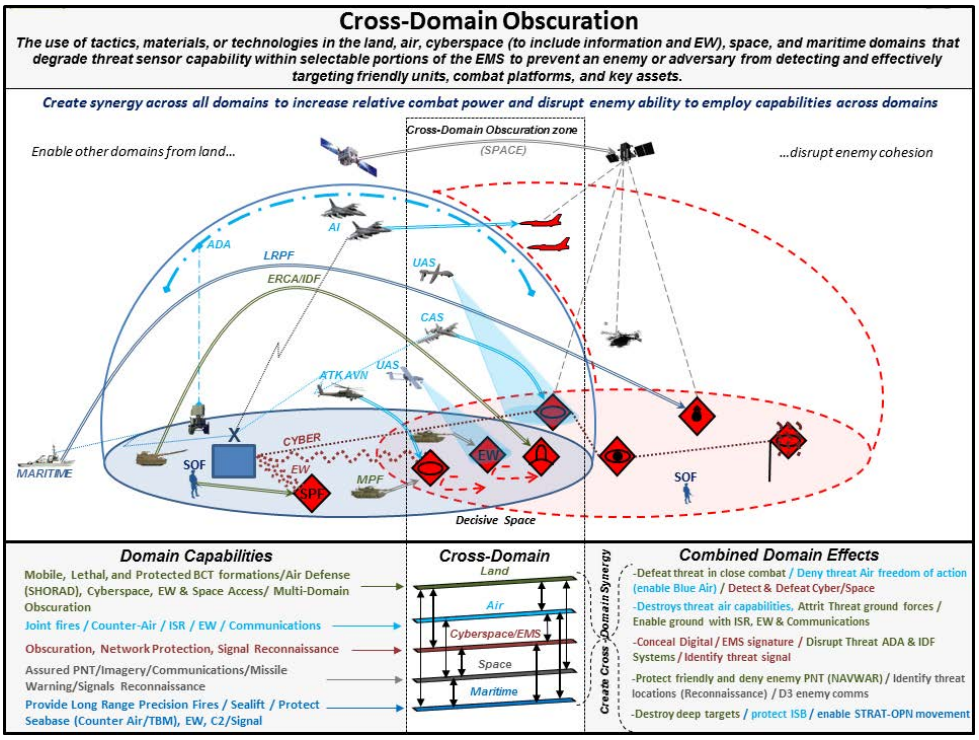

Figure 2 — Cross-Domain Obscuration

This highlights the critical requirement that companies, battalions, and brigades must obscure their signatures from targeting and attack in all domains. This required capability is cross-domain obscuration. The objective of cross-domain obscuration is to deny enemy forces the ability to acquire and target friendly forces across the EMS. Since infantry and armor companies possess limited resources to constantly obscure themselves throughout an operation, they will rely on their higher headquarters for most of their obscuration requirements.

In the vignette, CPT Key began to understand how his company could be seen in the EMS because his company would "emit" targetable signatures across various domains. He would need to use a variety of obscuration techniques and coordinate for resources in time and space across the EMS in multiple domains to prevent detection and engagement by the enemy.

The EMS is more than just radio frequencies. Enemy sensors — from satellites and UAVs to tank optics and social media — search across the EMS for movement, use of radios, computers, vehicles, and people. Units move and produce seismic signatures that are heard in the audible band. Units talk on the radio, utilize computers, and communicate via JBC-P with satellites, all producing a different signature in the radio frequency portion of the EMS. Soldiers and vehicles give off heat that can be seen in the infrared portion of the EMS. NVDs enhance the threat's ability to see in low ambient light, and units are seen in the visible light portion of the EMS during daylight hours (see Figure 1).

Commanders must understand what the enemy will use as sensors. A commander must "see himself," identifying the type, how, when and where emissions are being broadcast and then plan for how to obscure it based on the mission assigned. Companies, battalions, and brigades will be most vulnerable to detection in the radio spectrum as threat sensors become more technologically able to detect and collect across the EMS using UAVs, radars, ground sensors, and ground-based signal collection assets.

Consider the different types of threat sensors by domain and spectrum:

- On **land**, the threat will use special purpose forces, scouts, and other reconnaissance forces that rely on "the naked eye" and electro-optical thermal sights mounted on vehicles. Unattended ground sensors that detect vibration and sound will be placed across likely avenues of approach. The enemy will utilize passive ground-based EMS, utilizing systems like the battlefield surveillance radar SNAR 10 or Krasukha electronic warfare (EW) system to detect radio frequency traffic and its source.[1]

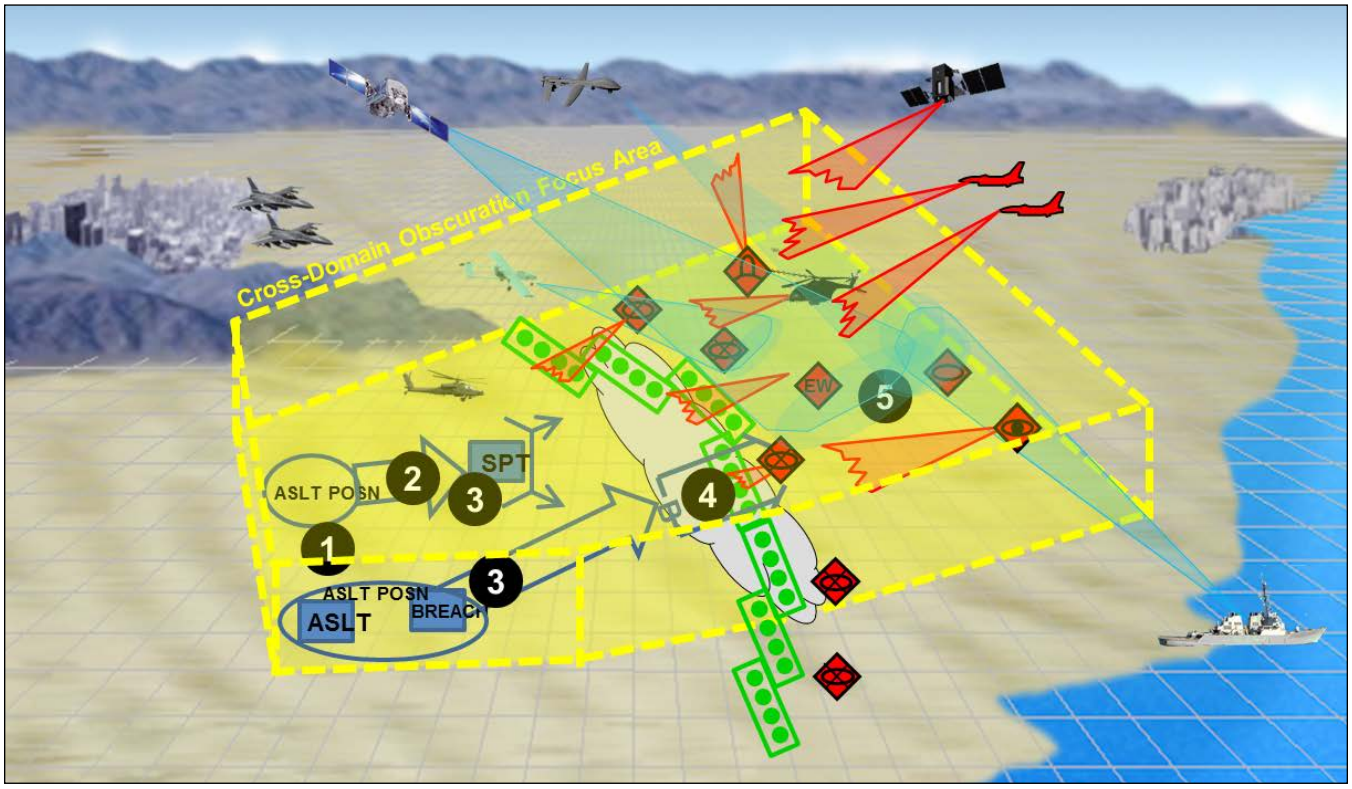

Figure 3 — Cross-Domain Obscuration Focus Area

- In the **air**, enemies will utilize a variety of manned and unmanned aerial systems (like the ZALA or PCHELA-1K) in various roles that sense with a variety of infrared and/or enhanced optical sights, or signal intelligence (SIGINT)/ electronic intelligence (ELINT) sensors.[2] They will be employed in a variety of sizes (small/medium/large) and tied to various echelons (maneuver battalion, a fires battalion/brigade, or theater army) of an enemy formation. These systems will be used to extend the depth of an enemy's battlespace.

- Enemies will utilize the **cyber** domain to generally detect and locate units. An open source Google search on www.Instagram.com for #OperationAtlanticResolve in December 2016 brought up 336 posts with personnel and locations tied to them. In the same vein, the unit's Facebook page or the Soldier whose Snapchat story details his unit's deployment is detectable in the cyber domain.

- In the **space** domain, enemies will utilize a variety of satellites capable of enhanced optical observation, electronic intelligence, high-resolution optical observation, as well as data-relay satellites and remote-sensing satellites.[3] Commercially available satellites will be used for their satellite imagery as well.

- Enemies will search from the **maritime** domain for any type of detectable EMS signature. They will utilize radars to detect anything in the air, to include UAVs, as well as passive EMS collection systems similar to the Krasukha EW that search for traffic in the radio frequency portion of the spectrum.

A company commander who does not "see himself" broadcasts a continuous identifiable signature and does not understand that enemy sensors are actively searching for organizations across the EMS from different domains, which significantly increases the risk of being targeted for rapid destruction by an enemy. In today's increasingly lethal environment, to be detected is to be targeted and destroyed. A company commander must coordinate and integrate obscuration assets throughout the tactical operation to effectively obscure movement and maneuver at critical times.

In the vignette, CPT Key cannot obscure his entire element from the time before it crosses the line of departure to when it consolidates and reorganizes after the attack, so the initial planning focus should be on how to execute obscuration in the close fight. This requires coordinating and employing a variety of obscuration resources and techniques in time and space across the EMS to prevent being detected and engaged by an enemy. The commander

selects those times in the tactical plan where obscuration is most required, what type of obscuration is needed, and how that obscuration will enable his/her organization. When a company is given the task of conducting a combined arms breach or is assigned a task to breach, assault, or conduct an SBF as part of a larger task force, the commander considers those tactical tasks relative to obscuration type, size, and duration required to accomplish those tasks:

(1) Obscuration actions required in the assault position.
(2) Obscuration actions required for movement to the SBF position.
(3) Obscuration actions required in the execution of the SBF.
(4) Obscuration actions required during execution of the breach.
(5) Obscuration actions required during penetration and exploitation of the breach.

These obscuration actions must consider several things, to include:[5]

- The threat's sensors capabilities (platform, unmanned, UAV, human intelligence [HUMINT]).
- The threat's direct and indirect fire weapons ranges.
- The templated size of the threat's battle position.
- The distance from the threat's battle positions and the conventional portions of an obstacle.
- The friendly force's tactical tempo and speed for the relevant platforms and weapons systems.
- The estimated amount of time to complete friendly tactical tasks in the degraded conditions caused by friendly obscurants and other battlefield effects.

After CPT Key builds his plan around his critical task, he then needs to consider other ways to obscure his movement. One way to obscure visual signature is to break into smaller maneuver elements that utilize different routes. This requires platoons that can navigate at night using darkness as another way to prevent detection by the naked eye; however, this is a coordinated movement that must be rehearsed. This may be just as effective as having a different asset obscure movement. Another technique is to operate in radio-listening silence using very short radio transmissions and brevity codes at precise times.

Once he completes the tactical plan and identifies the obscuration requirements, CPT Key then needs to coordinate in time and space for higher-level obscuration assets to:

- Deny/degrade detection in the cyber domain prior to moving into the assault position (computer systems) to prevent early targeting.
- Deny/degrade detection in long wave frequency spectrum (HF/VHF communications) when in the SBF position.
- Deny/degrade detection in the visual spectrum through the utilization of smoke and other physical obscurants when conducting the breach.
- Deny/degrade detection micro-wave spectrum (position/navigation and timing) after penetrating the main defensive belt and conducting follow on attacks.

Epilogue

The commanders of 4-56 IN (M) revamped their plan after CPT Romano pointed out how it would be defeated. LTC Clark prescribed communications "black out windows," and the signal officer broke out the brevity codes for reporting. LTC Clark also spoke at length with the brigade commander, who agreed to put a priority on detecting and targeting any threat electronic jammers during the close fight. The brigade commander also got the division headquarters to coordinate for obscuration of threat space and cyberspace sensors to cause further confusion during the movement to attack positions from the line of departure. All the companies were prescribed avenues of approach that were unique to them, and within those avenues of approach, there were recognizable checkpoints tied to the terrain. CPT Key directed the first sergeant to have the platoon sergeants collect all cell phones and turn them off. Then he talked with his platoon leaders and made sure they put their best land navigation leader in front in each platoon, and he further spaced the platoon movement over several kilometers. CPT Key changed the movement formations and techniques, waiting until the last possible moment to consolidate as a company. The JBC-Ps would be turned on at prescribed times during movement and only for a short duration. CPT Key knew that by considering obscuration when doing his pre-combat checks and developing the company plan (and nesting it within the battalion's plan and brigade's cross-domain obscuration plan), the enemy would not have any advantage.

Notes

[1] Worldwide Equipment Guide (WEG) 2015, Volume 1: Ground Systems.
[2] Ibid and WEG 2015, Volume 2: Air and Air Defense Systems.
[3] http://www.russianspaceweb.com/spacecraft_military.html, retrieved 13 January 2017.
[4] Field Manual (FM) 3-21.20, *The Infantry Battalion* (December 2006), section VI.

Andy Yerkes was commissioned in 1990 at Bowling Green State University as an Infantry officer. His assignments include serving as a rifle platoon leader and executive officer (XO) for a both a rifle company and HHC in the 25th Infantry Division; commander of a Bradley rifle company in the 1st Cavalry Division; battalion motor officer and assistant S3 in the 1st Squadron, 5th Cavalry; Cavalry squadron XO and S3 in 10th Mountain Division; and transition team chief in 1st Infantry Division in Iraq. He retired in 2010 as a lieutenant colonel. He currently works in the Maneuver Center of Excellence's Concept Development Division at Fort Benning, GA.