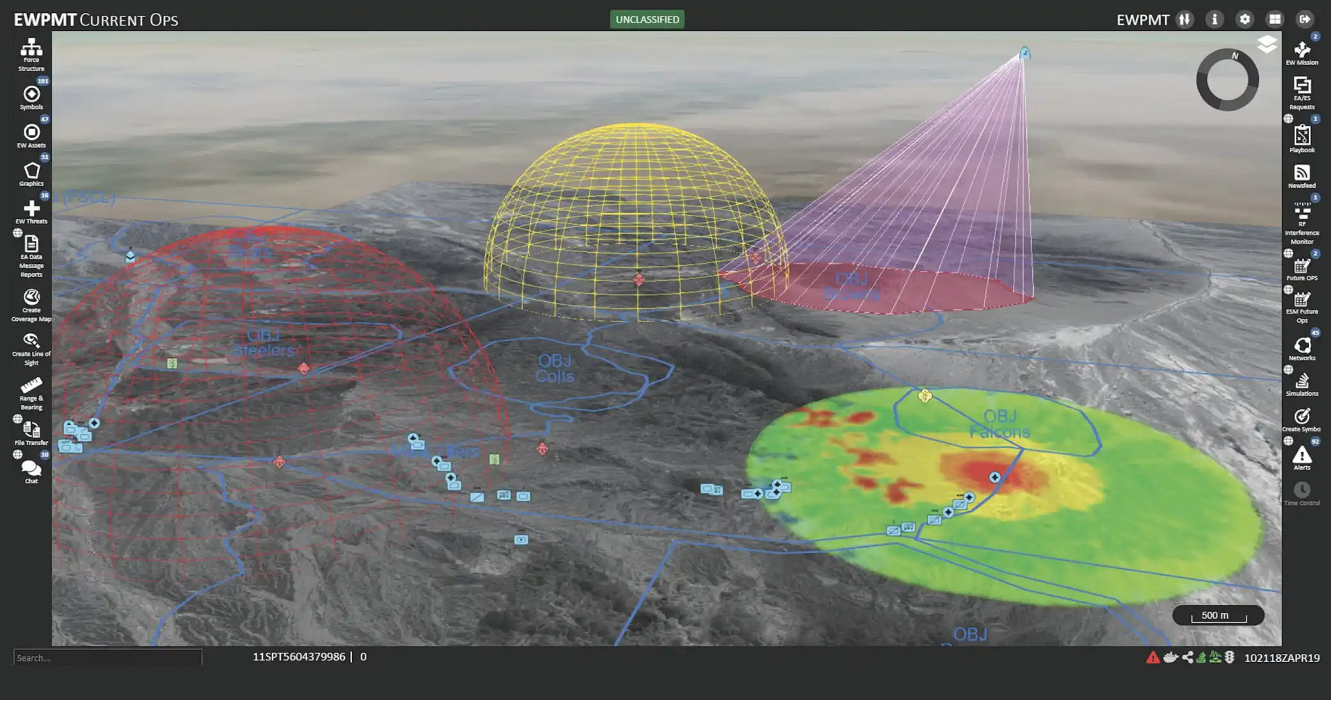


A screenshot taken from the Army's Electronic Warfare Planning Management Tool shows both threat and friendly electromagnetic spectrum data. During Combat Support Training Exercise 86-24-02, the 86th Training Division exercised its ability to conduct large-scale combat operations in a multidomain environment when its cyber or electromagnetic capabilities were denied or degraded. (Image courtesy of the U.S. Army)

# Operating in a Multidomain Environment

## Combat Support Training Exercise 86-24-02

Col. Jon V. Erickson, U.S. Army Reserve

To counter Army superiority in the land, sea, air, and space domains, America's adversaries have invested in cyber and electromagnetic activities (CEMA) capabilities to create multiple, simultaneous, and continuous threats in cyberspace and the electromagnetic spectrum (EMS). Adversarial capabilities have also created an operating environment, as described in Field Manual (FM) 3-0, *Operations*, in

which friendly forces are under constant observation and operating against a threat that is able to gain and maintain contact in multiple domains across the three dimensions of physical, information, and human.[1] This extended battlefield creates risks to Army forces, especially during the opening phases of an operation, where "Army units may find themselves facing superior threats in terms of both numbers and capabilities ... [and] must be prepared to fight while relatively isolated."[2] Faced with near-peer threats capable of challenging Army forces in multiple domains, the Army developed its newest warfighting doctrine to address this operating environment, culminating in FM 3-0.

To support FM 3-0's multidomain operations (MDO) concept, the 86th Training Division (TD) has been modernizing its training environment to allow Army units to practice operating in a dynamic and complex multidomain training environment against a peer adversary. In this first MDO iteration, the 86th TD focused on creating and executing CEMA effects because they are a critical element of MDO but also due to their proliferation, requiring leaders who can operate in a contested and congested cyber and EM environment. As the 86th opposing forces demonstrated, in the cyber domain there is no longer any fully secure area. Just as importantly though, units who participate in a combat support training exercise (CSTX) come away from the exercise with the ability to use their home-station training to continue to refine how they conduct operations when the use of cyber or electromagnetic capabilities have been denied or degraded.

## Setting Up a Multidomain Training Environment

The 86th TD created a multidomain training environment during CSTX 86-24-02 to prepare soldiers to operate in an environment in which they are constantly observed and challenged in the physical, human, and information dimensions of multiple domains. Training units received multiple opportunities to execute their warfighting functions in an immersive training environment that simulated the rigors of executing large-scale combat operations (LSCO) against a peer threat. As much as possible, the 86th TD executed live effects to assist leaders in understanding how to identify, protect, and defend friendly forces against an adversary operating in multiple domains and to mitigate the adversary's impact on the Army's ability to execute its warfighting functions.

In the CSTX training scenario, rear operations played a key role during the Army's transition from defensive to offensive operations, as forward operating units consumed more fuel and ammunition, required more maintenance and logistics support, and experienced more casualties. The adversary sought to attack the Army's sustainment-and-force-generation capacity in the rear, as they understood that the Army's sustainment capabilities determine the limits of depth and endurance of an Army operation. To maximize the effectiveness of its own combat capabilities, the adversary employed MDO to create windows of opportunity.

One of the key tenets of MDO is convergence—where actions are synchronized against combinations of objectives to achieve the desired overall effect.[3] Before conducting a large-scale kinetic attack, the adversary employed irregular warfare tactics to harass, probe, and gather intelligence. The adversary employed numerous forms of contact across multiple domains to maintain constant observation of friendly forces to understand U.S. capabilities, readiness status, and intentions. As an example of the forms of contact deployed against Army units (see figure), the adversary (1) employed proxy groups to conduct phishing email campaigns, electronic access, and signals intelligence gathering; (2) supported businesses and insider threats who could provide human intelligence gathering and electronic access methods; (3) executed aerial signals collection and intelligence, surveillance,

**Col. Jon V. Erickson, U.S. Army Reserve**, is a cyber and signal officer serving as the G-3/9 cyber director for the 335th Signal Command (Theater) but previously served as the cyber and electromagnetic activities effects chief for the 86th Training Division. He holds a bachelor's degree from the United States Military Academy and other degrees, which includes a master's from the Army War College. Recent assignments include G-6 for the 200th Military Police Command, S-3 for the 505th Signal Brigade, and Battalion Commander in the Army Reserve Cyber Protection Brigade. Erickson has three combat deployments—Iraq, Afghanistan, and Kuwait—and one overseas tour in Germany.

| Reconnaissance and intelligence gathering | | | | Setting conditions | | "Window of opportunity" | | | Disinformation |
|---|---|---|---|---|---|---|---|---|---|
| Day 0 | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 | Day 8 | Day 9 |
| S-2 Report: Phishing campaign | S-2 Report: SMS/text message attacks | Internet: Cyber attacks | Internet: Power outages | Action: Email phishing attacks | Action: Email phishing attacks | Action: UAS attack on logistics unit | S-2 Report: TAA identification via cell phone intercept | **Objective 1:** Neutralize Army C2 capabilities | **Objective 3:** Continue disinformation |
| S-2 Report: Electronics shop ties to adversary | S-2 Report: Adversary DDoS TTP | Internet: Dissemination of enemy flyer | Internet: Social media sightings of UAS | Internet: More social media sightings of UAS | S-2 Report: Local gov't impacted by phishing attacks | S-2 Report: Army share intel on phishing attacks | S-2 Report: Local gov't block IP address belonging to power plant | Action 1: DDoS attack on TAA<br><br>Action 2: FM radio jam | Internet: Blame US for hospital attack |
| Internet: Electronics shop offering discounted electronics | Internet: Increased UAS activity | Internet: UAS protection advisory | | | Internet: Social media sightings of UAS operator | S-2 Report: Civil unrest due to power issues<br><br>Internet: More DDoS attacks | Internet: Blame US for DDoS<br><br>Internet: UAS attack on logistics unit | **Objective 2:** Launch kinetic attacks<br><br>Action 3: Kinetic attack on TAAs | |

**C2**—command and control
**DDoS**—distributed denial-of-service
**TAA**—tactical assembly area
**TTP**—tactic, technique, and procedure
**UAS**—unmanned aircraft system

(Figure by author)

**Figure. Adversary Forms of Contact**

and reconnaissance; and (4) dropped off packages containing an electronic collection device.

Once the adversary had collected enough intelligence, it launched a conventional attack toward the end of the exercise. To create a relative advantage, the adversary focused on multiple supporting objectives against the Army—neutralize its command-and-control capabilities, launch kinetic strikes, and continue executing its disinformation campaign—to achieve its campaign objectives. First, the adversary employed multiple means of cyberattacks, such as an email phishing campaign to gain access to key IT systems. The adversary then combined the denial of those key IT systems with radio jamming to achieve the first objective of neutralizing the Army's command-and-control capabilities. Once achieved, the adversary then executed its second objective of conducting lethal kinetic attacks against the Army's rear operations to force the Army to reach its culminating point sooner. The third objective was for the adversary to continue its disinformation campaign against the Army to erode the positive views of the United States by the host-nation citizens. The intended overall effect of the adversary's actions was to erode the Army's combat power while delegitimizing the Army's presence among the local nationals and host-nation government.

While the theme of cyber pervades throughout the adversary's activities , intelligence operations drove their decision-making processes on how and where to best apply its limited combat power against the Army's weaknesses. The adversary largely relied upon easy to execute CEMA attacks and information warfare to set the conditions for its conventional attack.

For many adversaries, the use of inexpensive unmanned aircraft systems (UAS) able to support a diverse array of capabilities—such as intelligence, surveillance, and reconnaissance; signals/EMS collection; and fire control—will require Army leaders to develop a counter-UAS (C-UAS) plan. Minimizing the impact of a UAS on Army operations requires providing signal officers with the training and capabilities to account for EMS emissions. EMS emissions are the radiation and wireless electronic signals that emanate from devices that are simply turned on or wirelessly communicating. Army leaders must account for EMS emissions that all electronic devices emit by developing EMS emission control measures, which can include the following:

- minimizing length, frequency, and power of radio transmissions;
- establishing and enforcing the primary, alternate, contingency, and emergency communication (PACE) plan;
- using remote antennas; and
- dispersing formations and command posts.[4]

The 86th TD partnered with the Air Force's Spectrum Awareness and Resolution Team to map units' EM footprints, bringing capabilities that—in conjunction with wireless device detection provided by the 86th TD—would allow a commander to visualize their electromagnetic battlespace. Training units at CSTX understood how developing C-UAS and EMS emission control measures were important success factors in the new operating environment. For C-UAS, cover and concealment were additional measures some units took to protect their command posts. To limit EMS emissions, the 86th TD put out guidance to limit cell phone use during the day, but this was far from successful, as the cyber opposing force was able to successfully collect metadata from a large number of wireless devices and deceive users into connecting to malicious hot spots.

## Home-Station Training to Prepare for the New Operational Environment

As the Army prepares to conduct LSCO, it is even more critical for Army Reserve units to participate in combat support training exercises in Fort Hunter-Liggett, California, or Fort McCoy, Wisconsin. The speed and pace of LSCO demands combat support and combat sustainment support units that can operate with speed, tempo, and flexibility to extend operational reach and prolong endurance. It is only at CSTX and combat training centers that units can practice operating at echelon, stress their own capabilities, and appropriately stimulate their mission command information systems to coordinate and execute their warfighting functions.

The inability to stress capabilities was most noticeable when units were forced to exercise their PACE communications plans—as many were unable or limited in their ability to communicate when the adversary conducted denial of service attacks that took down fiber connectivity to the network. Participation in these exercises had the second-order effect of allowing unit commanders to review and update their home-station training to support the warfighter in a contested environment where their activities will be constantly observed in cyber, electromagnetic, air, and space. At the same time, the 86th TD's master scenario event list is tailored to support the unit commander's specific training objectives in a realistic and tough training environment.

The 86th TD conducted training workshops and visits throughout the year to ensure all training units understood that they would be operating in a multi-domain training environment in which they would be continually challenged to execute their warfighting functions against a peer adversary. One unit that particularly stood out was the 439th Multi-Functional Medical Battalion (MMB), and one reason was their signal officer's (SIGO) use of home-station training to set the conditions for success during their CSTX rotation.

Attending all the 86th TD's planning workshops as both the SIGO and trusted agent for the 439th MMB, 1st Lt. Bagdwal understood that he would be operating in a contested cyber and EM training environment. Bagdwal was in a prime position to ensure his commander would be able to maintain communications under multiple attack scenarios. At the planning workshops, 1st Lt. Bagdwal read the signal annexes for the 25th Infantry Division and the Combined Forces Land Component Command, which guided his training efforts from building his team's individual competencies to collective signal tasks such as setting up a battalion tactical operations center. Not receiving support from the few tactical communications nodes at the exercise made the 439th's communications plans tougher to maintain. Additionally, their unit was not fielded with solutions, such as the Joint Battle Command Platform, to provide contingent communications. Given the limited communication capabilities, the lieutenant's actions during CSTX made it even more remarkable that he was quickly able to overcome these challenges to ensure his commander could still communicate.

Once the 439th MMB arrived in theater and set up its field hospital on tactical assembly area (TAA) Justice, the unit operated under constant observation in multiple domains through aerial reconnaissance from adversary drones, reconnaissance activities through the EM spectrum such as EM emissions from

tactical radios and mobile devices, active device collection by rogue hotspots masquerading as free Wi-Fi hotspots, packages delivered to the TAA containing a wireless data collection device, and adversaries selling compromised cell phone sim cards at a local electronics shop to eavesdrop on conversations or text messages.

After actively and passively surveilling TAA Justice, the adversary attempted to black out communications for the 439th, hitting them with a denial-of-service attack that took down network access for their mission command information systems followed by jamming the frequency of the 439th's command net for their tactical radios. These simultaneous attacks took out the 439th's primary and alternate communications. Bagdwal recognized both attacks and began to execute his PACE plan. Bagdwal prioritized his efforts on reestablishing tactical radio communications with higher command. First, the lieutenant validated with the on-site observer-coach/trainer (OC/T) that their radio encryption keys were not compromised. Once the OC/Ts validated encryption keys were not compromised, the lieutenant coordinated with his S-3 to migrate the tactical operations center to the preplanned alternate radio frequency and, once radio communications were reestablished, relayed to their higher the new frequencies for the 439th. Next, the lieutenant determined that the denial-of-service attack only took down his classified communications and that the 439th could still communicate on their unclassified systems. In a span of fifteen minutes, the SIGO was able to preserve the commander's communication capabilities and coordinate with higher. A general observation out of CSTX-86-24-02 was that training units that did not write an annex H, read their signal operating instructions, or conduct home-station training to prepare for CSTX were greatly challenged with executing their warfighting functions in a multidomain environment without direct support from the 86th TD G-6 staff.

## Lessons Learned for Rotational Training Units

The challenges faced by the 439th MMB across multiple domains are but some of many hurdles that future commanders must confront and can overcome. The battlefield now extends into the virtual cyberspace and information environment. Modern militaries are employing information warfare, space, and CEMA capabilities to degrade their adversary's ability to achieve their own objectives or influence the adversary's actions. Soldiers and leaders must be prepared to operate in an unreliable and contested electromagnetic spectrum in which radio communications might not work; GPS might either jammed or providing inaccurate position, navigation, and timing; and use of a cell phone could result in deaths. Additionally, adversaries are exploiting the information dimension to influence the perceptions, decision-making, and behavior of individuals and groups to shape the operational environment to the adversary's favor with minimal expenditure of resources.

The following highlights the challenges that some units coming to CSTX must prepare for using home-station training time.

**Communications security (COMSEC) challenges and Level 1 Warrior Skills.** Many of the training units were challenged with finding a key management infrastructure operation account manager, previously known as a COMSEC account manager, to provide COMSEC. Additionally, most training units are not practiced in handling COMSEC or filling devices with the keys. Many of these are level 1 tasks that all soldiers should know and not just the signal personnel.

The lack of training was apparent to the 86th TD when training units made mistakes on their combat-net radios. Mistakes included setting the frequency-hopping radios to the wrong time, resulting in disconnected radio networks; setting radios to frequency hop master status, creating additional radio networks; emplacing antennas in locations that were ineffective; pushing too much or too little power to the radio systems; and more.

**Create, implement, and test PACE plan.** It was obvious that many training units arrived without working modified tables of organization and equipment needed to communicate during CSTX. Common issues included not bringing radios or antennas, not bringing batteries, broken equipment, not bringing the crimper tools needed to make network cable ends, etc.

Additionally, several training units did not arrive with an adequate number of trained signal personnel. Of the signal personnel available, many were not practiced in performing their tasks and battle drills. Training units are strongly recommended to provide attention and focus on precombat checks, precombat inspections, preventative maintenance checks and services, and training on their communications equipment

A small quadcopter drone lifts off to conduct a simulated convoy attack during Warrior Exercise 86-21-03, at Fort McCoy, Wisconsin. The 86th Training Division's counter-unmanned aircraft system capabilities were repeatedly tested during the division's Combat Support Training Exercise 86-22-02 in August 2022. (Photo by Sgt. William A. Parsons, 214th Mobile Public Affairs Detachment)

throughout the training year before arrival to CSTX. Doing so would ensure units have a viable primary, alternate, contingent, and emergency communications plan during their home-station training versus one that has only been exercised in PowerPoint briefs.

**Practice responding to jamming.** Units can easily replicate jamming by "hot mic'ing" their own radios. Units are supposed to drive their vehicles every month and can use this time to emplace and practice their battle drills for when their convoy is experiencing a jamming event. Additionally, events such as this would test the viability of the unit's signal operating instructions in addition to their PACE plan.

**Planning and executing home-station training events.** Commanders and their G-3/S-3 staff can set the tone for training by requiring soldiers to exercise their signal equipment such as their combat-net radios on convoys or simply during battle assembly weekends in the parking lots. Additionally, the commander can support their S-6 by carving out time in the training calendar for their signal personnel to conduct signal-specific training.

A biannual "signal rodeo" event in which all communications equipment is used can quickly validate a unit's mission status and proficiency at installing and operating the equipment. Additionally, during the signal rodeo, the S-3 and S-6 can coordinate to practice their procedure for receiving COMSEC, and soldiers can practice loading COMSEC in their own radios. Moreover, the S-4 can support the S-6 with facilitating the repair of signal equipment that is not fully mission capable.

## Takeaways and Resource Needs for Future Training Exercises

The 86th TD was able to deliver a realistic and relevant training environment in its first iteration, preparing soldiers and their leaders to execute their warfighting functions in a multidomain environment. Units like

the 439th MMB experienced what it was like to operate in an environment where capabilities were degraded, disrupted, or denied in both the cyber and EM domains. Units with a functional and redundant communication plan, such as the 439th, experienced the most realistic MDO training environment but were able to stay in constant contact across multiple domains. Operating in a contested CEMA training environment conferred the basic skills to allow commanders to maintain command and control by recognizing, reporting, and responding to cyber and EM anomalies such as a lack of internet access and electromagnetic interference.

The 86th TD establishing a challenging MDO training environment for CSTX 86-24-02, but there are many areas for improvement that other training units and centers can implement. Some areas will require further enhancement, and other areas will require tangible resources.

**Transforming the TD's cyber assessment and OC/T team to a CEMA effects team.** The main driver for this change is that the CEMA team knew the realistic cyber and electromagnetic effects that a unit could experience and the appropriate actions to take. The 86th TD CEMA effects team functioned as an extension of the effects and enablers team, creating effects in the master scenario event list (MSEL) and implementing them in the training environment. Doing so allowed training units to experience operating in a contested environment across multiple domains. Effectively creating electromagnetic effects will require, at a minimum, one soldier who is familiar with, if not trained, in EMS management. The 86th CEMA team was able to focus on executing live effects only because the 84th training command provided cyber assessment and OC/T individuals who assessed the training unit's ability to perform their warfighting functions while experiencing cyber and EM effects.

**PACE plan.** The 86th TD CEMA effects team executed live cyber and EM effects to force units to exercise their PACE plans. The CEMA team's attacks were concentrated into three distinct categories of reconnaissance, intrusion, and denial. This simulated an adversary's steps to deny, degrade, or disrupt the Army's ability to command and control through cyberspace or the electromagnetic spectrum.

For reconnaissance, all training divisions, specifically the opposing force, should be fielded with a capability to detect wireless devices. The 86th TD employed an open-source wireless geographic logging engine application to provide data points to the OC/Ts and the division G-2. This would later be shared with commanders and senior leaders of the rotational training units for their awareness of how many wireless devices were beaconing the unit's location in the EM spectrum. Additionally, the Air Force' Spectrum Awareness and Resolution Team mapped the electromagnetic footprint, bringing capabilities that, in conjunction with wireless device detection, would allow a commander to visualize their electromagnetic battlespace.

In terms of intrusion, a mission training complex or simulation office should have a capability for CEMA teams to send phishing emails as part of a phishing campaign and provide metrics on user engagement. All training divisions should have a wireless auditing solution that mimics wireless networks but functions as a rogue access point, training end users to not connect to unsecured public wireless networks. The CEMA team employed the rogue access point in a couple ways. In one scenario, it functioned as a rogue access point and was hidden in a delivery box for drop-off at various units to test that unit's physical security vulnerabilities and collect device information. In other scenarios, the rogue access point would be set up right after a denial of service or radio interference to entice users to connect.

The last attack method was denial. Methods include FM radio interference and network denial through a simulated denial of service attack. The type and mix of attacks were dependent upon the training unit's communications posture and the OC/T's confidence in the signal team. To conduct radio interference but also minimize the training unit's ability to identify the source of the jamming, the 86th TD employed a portable FM radio manpack operating on the same frequency as the target. The 86th TD CEMA team would then hold the hand mic and play an adversary's national anthem to ensure the training unit understood they were experiencing a radio jamming attack scenario. In the future, the opposing force should be outfitted with a manpack radio and the training unit's signal operating instructions so they can simulate radio jamming.

**Challenging versus frustrating a unit.** The goal for the CEMA team was to create a stressing effect that would challenge a unit's ability to execute its warfighting functions versus a frustrating effect that a unit

could not do anything against. To achieve this goal, all three CEMA attack methods were synchronized, coordinated, and nested in the master scenario event list to ensure training platform partners—effects and enablers, OC/Ts, exercise control, G-6, and others—all knew whether communications issues were the result of an attack by the CEMA effects team or due to the equipment itself. One important reason for coordinating throughout the exercise is to, for example, ensure there is an OC/T in the area to assess and be aware of when an effect is executed. Another reason is that executing a radio jamming effect when the unit is still trying to establish radio communications has no effect. Worse, when a unit finally establishes network connectivity only to experience a network denial effect shortly thereafter creates confusion as to the reason and wastes valuable training time. Learning from CSTX-86-23-02, the CEMA team ensured every effect that could impact the unit was entered into the MSEL. For added precaution, effects that did not impact the unit, such as passively gathering electronic devices near a TAA or mapping the EM footprint, were also entered on the MSEL to ensure training platform partners had awareness of the CEMA team's presence and reason. An example of the benefit of this coordination is that when a network denial effect was executed, the G-6 help desk was aware and could role-play their part in the event.

**Next-generation constructive environment.** To continue pushing forward on the development of the Army's next-generation constructive environment, where a simulation engine is driving the Warfighter exercise, the 86th TD partnered with the Army Reserve Cyber Protection Brigade; the U.S. Army Combat Capabilities Development Command; and the Program Executive Office Simulation, Training and Instrumentation. The combined team successfully executed a proof of concept to capture and record the activities of a cyber protection team (CPT) to then emulate in a cyber simulation platform. The goal is to capture the activities of an on-mission CPT to then be "replayed" in the simulation platform for future training exercises as a virtual CPT. And if the simulation platform is connected to the exercise network, then the virtual CPT can create live cyber effects on the training audience. This solution provides training audiences the opportunity to experience an on-mission CPT and minimizes the need to physically send a CPT to an exercise, thereby providing the CPT more training time.

The 86th TD recognizes that the key to countering near-peer threats requires mastering MDO. The 86th TD created and executed a world-class exercise in which training units were exposed to a multidomain environment in support of LSCO. Additionally, the 86th views CSTX as an opportunity for capability providers to field test new capabilities, such as with U.S. Army Combat Capabilities Development Command testing its cyber simulation platform. The innovation and new capabilities that the 86th TD invested into its training platform for CSTX-86-24-02 resulted in soldiers and their leaders understanding how to execute their warfighting functions in a contested and congested multidomain training environment. ■

## Notes

1. Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 2022), 1-4, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.
2. Ibid.
3. Ibid., 3-3.
4. Ibid., 3-12.