The Centreville Fort in Virginia using "Quaker guns" in March 1862. Military deception is probably as old as war itself, but the earliest photos of dummy weapons date from the 1861–65 American Civil War, when Quaker guns were used by both sides. The "guns" were in fact logs, mounted to give distant, telescope-squinting generals a false impression of firepower. (Photo by George N. Barnard and James F. Gibson via the Library of Congress)

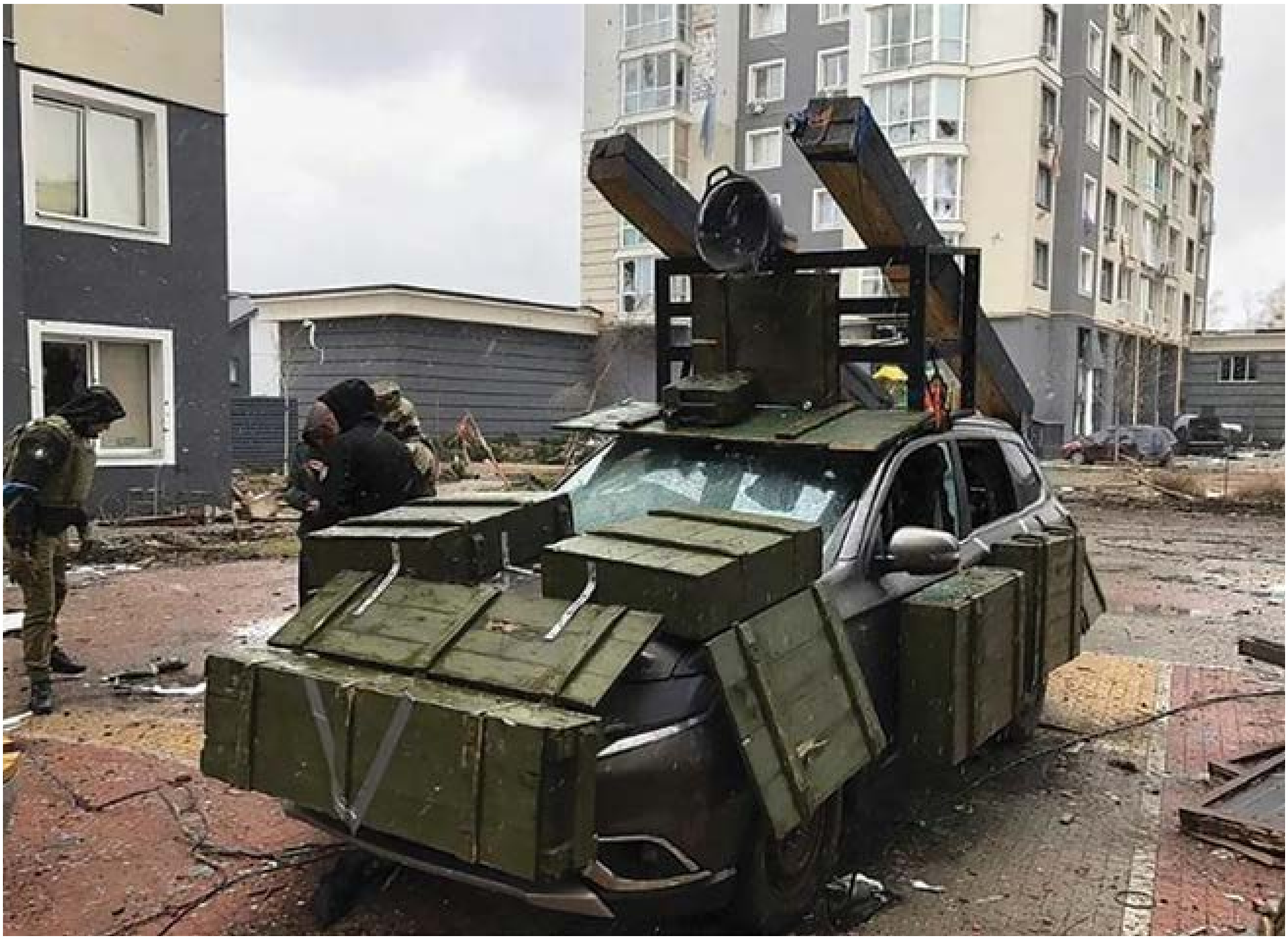
Hiding in Plain Sight

Maj. Tony Formica, U.S. Army

Capt. Chris Pabon, U.S. Army*

An airborne division's staff conducts its final rehearsal before launching a joint forcible entry mission into Donovian-controlled territory. During this process, two crucial staff groups present their plans. The maneuver team showcases the principles of mass and audacity in their plan to rapidly seize an airfield and build up combat power, while the joint fires community presents a simple, coordinated symphony of destruction that will overwhelm enemy antiaccess and area denial capabilities, enabling paratroopers to seize the airfield.

Once the commanding general (CG) has considered the presented information, he turns to a collection of staffers seated alongside the fires team and asks, "How are we going to control what the enemy thinks before and during execution? What will we conceal from the enemy, and what will we reveal to him?"

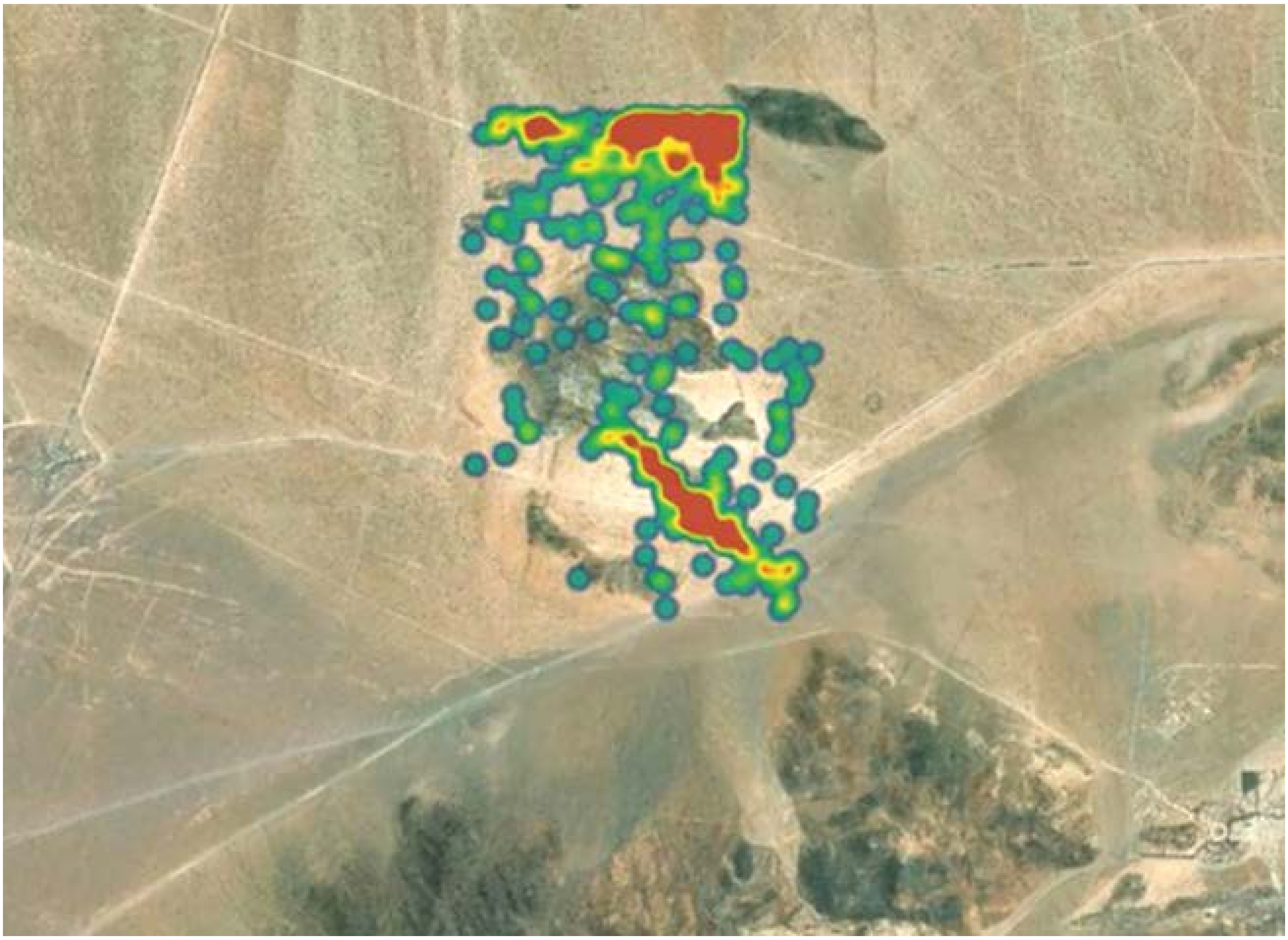


A passenger car is disguised as a Strela-10 antiaircraft missile launcher May 2022 in Ukraine. Ukraine uses wooden decoys like this that resemble advanced rocket systems to trick Russian forces into attacking them using long-range cruise missiles. Reportedly, Russian drone sensors have had great difficulty in distinguishing Ukrainian decoys from actual rocket systems. (Photo courtesy of Novynarnia)

One officer in the group, a young information operations (IO) captain, stands and begins answering the CG's questions and is soon followed by an electronic warfare (EW) technician. Convinced his division will prevail in seizing the airfield, the CG concludes the rehearsal.

The actual joint forcible entry, which occurs a few days later, confirms the CG's beliefs. Civilian tail watchers have difficulty determining the destination of the C-17s carrying the division's paratroopers, thanks to the division staff's advanced coordination and planning with joint partners and implementation of operational security (OPSEC) measures appropriate for the digital age. The enemy's intelligence, surveillance, and reconnaissance (ISR) assets observe dozens of apparent position areas for artillery and battalion command posts flowing off the seized airfield. The electromagnetic spectrum (EMS) does not help them separate a decoy from what is real as U.S. forces emit dozens of believable electronic signatures, confounding the enemy's best-trained EW technicians and therefore deceiving the opponent into firing on what they believe are real units. Subsequently, in response to their misguided actions, their long-range artillery is targeted and destroyed by the division's higher headquarters.

In this fictitious airfield seizure, the airborne division's information warfare played out almost entirely in the physical dimension and resulted in the opponent commander's disorientation and inability to make timely decisions. The U.S. division seized the initiative in this scenario because it controlled what the enemy commander saw in the air, on the ground, and in the EMS. This, in turn, influenced the commander's behavior in a way that was advantageous for the U.S. paratroopers and their survival in the critical early



A satellite image shows the electronic emissions signature of a battalion-size element training in May 2020 at the National Training Center (NTC), Fort Irwin, California. The highly conspicuous electromagnetic signature illustrates the challenge of concealing modern-day command posts from detection and attack. The opposing force at the NTC uses its electronic warfare systems to generate images like this as training tools to show visiting units what their digital signatures look like in the electromagnetic spectrum. The opposition force also uses them to target those units to be as realistic a threat as possible. (Photo by Col. Scott Woodward, U.S. Army, via Twitter)

hours of the operation. Despite the enemy's plethora of advanced sensors and linked, long-range precision fires, U.S. forces were able to hide in plain sight and force the enemy commander into the unenviable position of either surrendering the initiative or risking his own forces by striking at units that they could not verify as real or fake.

The core concepts of multidomain operations (MDO) and convergence demand that all Army echelons, including tactical formations, be proficient in continually merging effects in both the physical and digital world.[1] However, despite the necessity, the Army's tactical formations—divisions and brigade combat teams (BCTs)—are not prepared to meet this demand in the distinct case of information warfare, nor are they equipped to address information advantage (IA) activities more broadly. These formations must change the way they organize their staffs, equip their formations, and train in their use of information to both survive on and dominate the modern battlefield. Failing to do so will be fatal, whether in Kabul, Kharkiv, or in the large-scale combat operations (LSCO) of tomorrow. Success requires Army divisions to develop the ability to overwhelm an adversary's capacity to perceive reality and make timely decisions, which necessitates the integration of a host of disparate capabilities within both divisions and BCTs.

Clarification of Terms

The effects described in this article are in pursuit of *information advantage*. IA is defined in the draft form of Army Doctrine Publication (ADP) 3-13, *Information Advantage Activities*, and is intended to replace the Army's current concept of IO. Its proposed definition is "a condition when a force holds the initiative in terms of the use, protection, denial, or manipulation of information to achieve situational understanding, improve decision making, and affect relevant actor behavior through the coordinated employment of relevant military capabilities."[2] IA supports a unit's ability to achieve *decision dominance*, another draft term that describes the ability to sense, understand, decide, act, and assess faster and more effectively than one's adversaries.[3] We are choosing to use these terms because, in line with the Army's MDO concept, they combine the extant capabilities of Army formations into a cohesive doctrinal construct aimed at gaining a position of relative advantage over our adversaries.[4]

> The cold truth of multidomain operations, particularly in large-scale combat operations, is that a division cannot prevail in information warfare by selectively applying one or another of its core information capabilities. These must all work together continuously throughout operations to succeed.

Similarly, we employ the draft term *core information capabilities* (CICs) in lieu of the more commonly understood term *information-related capabilities* to describe "forces specifically trained and equipped in the use, protection, denial, or manipulation of information for the purpose of gaining and maintaining an information advantage."[5] It is important to highlight that CICs, especially under the IA construct, include not only military information support and public affairs operations but also prominently feature cyberspace operations and electronic warfare.[6] Division IO planners, brigade cyberspace electromagnetic activities (CEMA) noncommissioned officers, and public affairs officers across echelons are all examples of a division's CICs.

The draft concept of IA paints a vision in which Army commanders, including those at the tactical level, leverage their CICs in conjunction with their organic capabilities along five distinct, logically differentiated lines of effort. The conduct of information warfare and its associated focus on affecting threat decision-making cycles, command and control, and information warfare capabilities is one of these lines of effort.[7]

Information warfare is where we see the greatest risks and opportunities for today's tactical formations and their ability to achieve decision dominance. We believe units that are organized, equipped, and trained to leverage their full suite of CICs in information warfare will thrive in future conflicts. In contrast, units that are not prepared in this fashion will not survive a conflict's opening engagements.

Why This Is Necessary: Learning to Hide from a Million Eyes

Today's battlefields are characterized by persistent ISR; widespread electromagnetic sensors; long-range precision fires; and ubiquitous civilian-driven, open-source intelligence reporting fed by commercial satellites, cell phones, and social media.[8] Concealment, surprise, and information protection have never been more difficult for tactical units to achieve. U.S. units will struggle to hide on the modern battlefield because their enemies will be adept at converging advanced sensing capabilities on the ground, in the air, and in the EMS with lethal and accurate long-range fires.

Furthermore, reliable electronic sensor equipment at the brigade level and above in most top-tier militaries means that our adversaries will increasingly and actively look to the EMS to determine where U.S. tactical units' command-and-control (C2) nodes are located.[9] Adversary EW specialists, and the future algorithms that will replace them, will quickly assess whether a suspected U.S. C2 node is real or a decoy on the basis of its electronic emissions alone. Tactical units' ability to conduct information warfare

Soldiers assigned to 1st Squadron, 7th Cavalry Regiment, and 1st Battalion, 4th Infantry Regiment, conduct electronic warfare training during Combined Resolve XV, 23 February 2021 at the Hohenfels Training Area, Germany. Combined Resolve XV is a multinational exercise designed to build readiness and enhance interoperability with allied forces and partner nations. (Photo by Sgt. Julian Padua, U.S. Army)

and affect adversary decisions and C2 systems is at a premium.

All of this suggests that Army divisions must become masters at employing their core information capabilities to dominate their adversaries' decision-making cycles. The primary target audience for division and below CICs is enemy commanders and their understanding of the physical reality—the arrayal, composition, disposition, and strength—of the friendly forces opposing them. Tactical CICs allow commanders to establish that physical reality by controlling what the enemy commander sees through OPSEC measures, planned deception operations, or the employment of CEMA assets to manipulate the EMS.

The cold truth of MDO, particularly in LSCO, is that a division cannot prevail in information warfare by selectively applying one or another of its CICs. These must all work together continuously throughout operations to succeed. For perspective, consider a simple extension of the vignette used to open this essay involving deception operations, which fell within the draft information warfare's IA activity of affecting enemy decision-making.[10]

Part of the U.S. division's success in confounding the enemy commander during the airfield seizure stemmed from its ability to construct decoy command posts that not only looked realistic but also emulated a battalion command post's electromagnetic emissions, which includes everything from radio traffic to satellite uplinks. The fictitious division did this not because it *could* but because it *had to*. Distracting the enemy's attention and causing them to waste time and resources to sift through reality was the only way to survive and ultimately defeat their integrated fires complex.

When applied to real Army operations, deceptive measures like the decoy command post may not fool an

Army Reserve soldiers from the U.S. Army Civil Affairs and Psychological Operations Command (Airborne) participate in Command Post Exercise–Functional 22-02 at the Military Training Center on Fort Leavenworth, Kansas, 28 June 2022 to develop functional expertise in providing civil affairs, psychological operations, and information operations support to a division- or corps-level staff. (Photo by Maj. Xeriqua Garfinkel, U.S. Army)

enemy's national-level capabilities, but it will more than likely fool an enemy battalion or brigade staff who are sleep deprived and under strict time constraints. They may believe that the fake U.S. command post in their ISR feed is real, especially if it looks, moves, and emits frequencies on the EMS in ways indistinguishable from a genuine command post.

Getting to this point requires a significant amount of planning and coordination on the part of a U.S. division. Not only would a division operations officer need to order a subordinate unit to load decoy construction materials onto a plane, but that unit would also need to be proficient in the construction of decoys. Additionally, a whole-of-staff effort would be required to synchronize the establishment of the false command post with the rest of the division's operations. The IO officer would need to prepare and submit a tactical deception packet for approval to higher echelons, while the CEMA chief would have to coordinate with the BCTs' CEMA platoons to integrate emitters capable of replicating a battalion command post's emissions. The division's fires, protection, and maneuver planners would be required to synchronize with both individuals to create a construction and occupation plan convincing enough for the enemy commander to believe. Most importantly, this deception would have to support the division's overall mission of seizing the airfield to allow the buildup of combat power for subsequent offensive operations.

In the vignette, the deception supported the mission because the decoy positions lured the enemy commander into exposing his artillery assets to counterfire when he decided to engage them. Thus, the loss of their long-range fires capability removed the enemy commander's most potent tool for preventing the projection of U.S. combat forces from the airfield over the next several days.

Such a degree of planning and synchronization is imposed on U.S. divisions by the realities of modern, multidomain conflict, especially where information and physical dimensions meet in the form of the EMS. A decoy command post can be visibly indistinguishable from an authentic one, and a battalion can make a convincing show of emplacing the command post with security, but if the decoy does not emit frequencies like a C2 node, with the same variety of systems that ebbs and flows in communications traffic like a real C2 node, then the deception will fail.

Deceiving enemy commanders is just one of a host of tactical applications of information warfare that divisions will have to leverage going forward. Electronic attack, precision messaging, delivering technical effects, and implementing OPSEC measures are all tasks that will be indispensable to a division's ability to survive on the multidomain LSCO battlefield. Each of these is an extraordinarily complex affair, both from an organizational and technical perspective.

However, it is also important that U.S. tactical formations do not over-appreciate the problem. The difficulties divisions will face in achieving decision dominance are formidable but manageable. More importantly, these same difficulties work both ways and afford U.S. tactical commanders several opportunities to overwhelm their adversaries.

Situations arising when information overload disorients individual decision-making will soon cease to be an academic abstraction and will become a lived experience for company and battalion commanders in not only U.S. but also adversary formations.[11] The sheer volume of data modern staffs are capable of ingesting means that separating truth from fiction can cause significant delays in an organization's ability to make timely decisions based on information. Simple exercises in epistemology can, potentially, bring operations to a standstill. U.S. forces should anticipate this trend and prepare to exploit it to the fullest potential.

Changing the way tactical staffs and maneuver elements currently do business is the only way to effectively implement such a strategy. Staffs must merge their separate CICs, such as CEMA and IO, to gain efficiencies and drive innovation. Fighting formations must acquire cutting-edge technology like our example decoy emitters. Finally, both staffs and fighting formations must go through enough tough, gritty, and realistic training scenarios where the fight for decision dominance becomes instinctive.

> “The sheer volume of data modern staffs are capable of ingesting means that separating truth from fiction can cause significant delays in an organization's ability to make timely decisions based on information.”

How to Do This: Engineering a Decision Dominance Machine

Senior Army leaders have already recognized a need for division staffs to establish IA-focused entities and have explicitly tied CEMA to that construct.[12] We recommend that division staffs physically combine their IO, CEMA, and space operations core information capabilities under one roof into an information warfare task force (IWTF). Having these technical specialists working together is both valuable and necessary.

The value in placing these CICs into a single staff section is that they gain efficiencies and synergy by working together that they would not achieve if left to their own devices. It has been our experience that when IO personnel are not tied to other core information capabilities, they tend to direct their energies to understanding online sentiment as reflected in social media, typically by aggregating reports and analyses prepared by higher echelons. CEMA personnel focus on fielding new equipment to brigade EW platoons with little leftover bandwidth for thinking through how to meaningfully integrate those capabilities into a battalion or brigade's combat operations. Space/technical operations personnel, meanwhile, are frequently preoccupied with managing their exquisite capabilities and keeping their facilities accredited. This is the staff equivalent of a deadweight loss. While all the above parochial activities are good and essential to the division's operations, they do not optimize each CIC's ability to inform and support the division's aggregated IA activities.

The U.S. Army Communications-Electronics Research, Development, and Engineering Center has identified fifteen soldier-vetted technologies intended to lighten and make more mobile command post infrastructure while also increasing capabilities and lowering the electronic signature. (Image courtesy of the U.S. Army)

As we described earlier, the division's deception professionals—the IO officers—need to have a seamless working relationship with their CEMA counterparts for their deceptions to have any real validity. Likewise, modern-day electronic support activities such as electronic sensing are significantly enhanced by the integration of space-based collection capabilities. The possibilities for cross-domain synergy among division CICs are limitless, but they will not occur through serendipity. Division commanders must make a conscious decision to place them into a single, coherent organization.

This implies a requirement for leadership. An IWTF must be headed by an officer who has both peer access to staff primaries and who can demystify the highly technical nature of the core information capabilities for the rest of the staff. It is easy to be intimidated by the technical jargon that typically accompanies most CICs' work. Discussions of waveforms, frequencies and amplitudes, orbital mechanics, and multiacronym program names are inseparable from CIC tradecraft. However, IA is commanders' business, and that means that commanders' staffs must be able to quickly understand the capabilities CICs bring to bear on the fight.[13] Having a clearly identified individual who can interact with staff primaries as an equal and who can rapidly translate CICs into operational timelines and graphics will enable staffs to relentlessly pursue decision dominance.

All the staff brilliance in the world, however, will not materially increase divisions' capabilities to achieve IA at the tactical level. This is why combining the CICs into an IWTF-like structure is vital. Tomorrow's U.S. tactical formations will employ a host of technical capabilities that operate on the principle of concealing through revealing that are actively under development through the federated Department of Defense research and development enterprise. Whether flooding the EMS with multiple plausible U.S. signatures, spoofing adversary radars with the appearance of seemingly dozens of aircraft, or employing unmanned robotics to jam enemy communications, tomorrow's brigades and battalions will compete for decision dominance using technologies fundamentally designed for information warfare.[14] Somebody will need to think critically about not only evaluating these emerging technologies, but integrating them into the organization, doctrine, and training of division formations. We recommend that the IWTF fill this role. Nobody else in the division staff is better postured, by virtue of both formal training and inherent roles and responsibilities, to test, evaluate, and integrate technologies such as decoy emitters into tactical formations with an eye for decision dominance than the division's IO, CEMA, and Space CICs.

Russia's frustrated information warfare campaign in Ukraine, particularly regarding its underwhelming efforts to control the EMS, further suggests that staffing and equipping are necessary but insufficient.[15] Robust training environments are indispensable for making staffs seamless in their processes and fighting formations proficient in the complex collective tasks they will be required to perform in combat.

Division staffs must learn to not only set up their command posts and displace but also figure out who is responsible for setting up decoy command posts to prevent the enemy from drawing a target on their location. Brigades and battalions must utilize their CEMA platoons as opposition forces (OPFOR) to deliberately jam their own units during squad and field training exercises. Units should only be able to fly their unmanned aircraft system platforms beyond line of sight if they successfully locate and destroy the jammers that would deny them this capability in LSCO environments. Denied, degraded, and disrupted communications and geolocation technologies must become a fact of life in home-station training: our staffs and the soldiers they support need to learn to fight through the foggy information environment that is characteristic of MDO. BCTs will require multiple experiences against a thinking, adaptive enemy to become experts in leveraging their core information capabilities to both survive and prevail in a contested information environment.

The combat training centers (CTC) have their own work to do in preparing and validating tactical formations as ready for future conflict.[16] Their OPFOR must be equipped to impose a contested EMS on U.S. formations, and they must similarly become adept at obscuring their composition, disposition, and strength through the combined use of OPSEC, deception planning, and decoy electronic emitters. Brigade and battalion commanders can no longer get a pass on competing in the information environment by merely having their IO officers present them with the top social media trends in the simulated information dimension of the CTC. An IO officer who has read *LikeWar* and who spends a CTC rotation trying to tweet at the enemy is likely doing very little to affect the enemy commander's decision-making process.[17] CTCs need to help staffs break out of this habit by making it possible and necessary for them to directly attack OPFOR command and control systems, kill chain timelines, and perceptions of reality using the CICs organic to their own formations.[18]

Conclusion: A Culture Committed to Information Advantage

We have focused our arguments and recommendations chiefly on the implications that modern and future battlefields portend for U.S. formations and their ability to wage information warfare. This does not obviate the requirement for a comprehensive assessment of how to staff, equip, and train our tactical units for all the activities that are required to truly gain and maintain IA. How, truly, do U.S. divisions protect friendly information in an age of ubiquitous cell phones and commercially available satellite imagery? Is the payoff worth the effort for a U.S. brigade to try to meaningfully influence foreign audiences? How do U.S. formations remain relevant and timely when informing the American public in an age of media echo chambers?

Each of these are important questions with profound implications for the ways U.S. tactical formations prepare themselves to deploy, fight, win, and survive in future conflicts. We do not propose to have the answers, but we believe that the best universal action the Army can take is to change its culture. IA activities, and all the highly technical core information capabilities that support them, need to become part of the basic operating objectives of platoons and companies as much as they need to become a muscle memory for division and brigade staffs. Whatever changes to their organization and equipment divisions make, continuous validation in tough, gritty, and realistic training will drive the habits of heart necessary to compete for and gain decision dominance.

The surest sign that tactical formations have fully internalized the importance of IA activities will not be found in a staff replete with brilliant technicians, or in a BCT replete with and proficiently trained on the latest EW equipment. It will be found on the flight line of the fictitious U.S. airborne division we saw at the beginning of the article, when a young squad leader deliberately prioritizes the loading of his platoon's decoy emitters on an aircraft because he knows he will need these to stay alive and win on the airfield he is about to seize. ■

The authors would like to thank Lt. Col. David Rousseau, the 82nd Airborne Division aviation chief, for his mentorship and guidance during the writing process for this article.

Maj. Tony Formica, U.S. Army, serves as the operations officer for 2nd Battalion, 501st Parachute Infantry Regiment, in the 82nd Airborne Division's 1st Brigade Combat Team. He served previously as the chief of the 82nd Airborne Division's Information Warfare Task Force and deployed twice with the division headquarters in that capacity, most recently to Poland in response to Russia's aggression in Ukraine. He holds a BS from the U.S. Military Academy and an MA from Yale University's Jackson School of Global Affairs, which he obtained through the Downing Scholars Program. Formica deployed in support of Operation Enduring Freedom with 1st Stryker Brigade Combat Team, 25th Infantry Division, and in support Operation Atlantic Resolve-North as a company commander with the 173rd Infantry Brigade Combat Team (Airborne). He has also served as an observer-controller at the Joint Readiness Training Center.

Capt. Chris Pabon, U.S. Army, serves as the 82nd Airborne Division's Information Warfare Task Force deputy and deployed with the division headquarters once in this capacity to Poland in response to Russia's aggression in Ukraine. Pabon also deployed in support of Operation Enduring Freedom with the 1st Battalion, 502nd Infantry Regiment, 101st Airborne Division. He has served multiple tours of duty in the 3rd U.S. Infantry Regiment (The Old Guard). Pabon holds a BA in criminal justice from American Military University and an MS in global studies and international relations from Northeastern University. **He is the main writer for this article.*

Notes

1. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 20.

2. Army Doctrine Publication (ADP) 3-13, *Information Advantage Activities* (Draft) (Washington, DC: U.S. Government Publishing Office [GPO], forthcoming), Glossary-4; Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. GPO, 27 November 2012, Incorporating Change 1, 20 November 2014), GL-3.

3. ADP 3-13, *Information Advantage Activities*, 6-1.

4. Ibid.,1-9–1-10.

5. Ibid., 1-18.

6. Ibid.

7. Ibid., 6-1.

8. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 8.

9. Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, EE: International Centre for Defence and Security, 18 September 2017), 5–6, accessed 13 March 2022, http://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf; Jonas Kjellén, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces* (Stockholm: Swedish Ministry of Defence, 1 March 2018), accessed 13 March 2022, https://www.foi.se/rest-api/report/FOI-R--4625--SE.

10. George I. Seffers, "Combat Commanders Must Grapple with Info Ops," *SIGNAL Magazine* (website), 17 August 2021, accessed 5 May 2022, https://www.afcea.org/signal-media/technology/combat-commanders-must-grapple-info-ops.

11. JP 3-13.4, *Military Deception* (Washington, DC: U.S. GPO, 14 February 2017), A-1. Jones' Dilemma: "MILDEC generally becomes more difficult as the number of sources available to the deception target to confirm the 'real situation' increases. However, the greater the number of sources that are deceptively manipulated, the greater the chance the deception will be believed."

12. James McConville, *Army Multi-Domain Transformation Ready to Win in Competition and Conflict*, Chief of Staff Paper #1 (Washington, DC: Department of the Army, 2021), 8, accessed 2 August 2022, https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf.

13. ADP 3-13, *Information Advantage Activities*, 6-9.

14. Seffers, "Combat Commanders Must Grapple with Info Ops"; Walker Mills, "A Tool for Deception: The Urgent Need for EM Decoys," War Room–U.S. Army War College, 27 February 2020, accessed 6 May 2022, https://warroom.armywarcollege.edu/articles/tactical-decoys/; Sydney J. Freedberg Jr., "Army Explores Robot Decoys and Cannon Fired Jamming Pods," Breaking Defense, 23 August 2019, accessed 6 May 2022, https://breakingdefense.com/2019/08/army-explores-robot-decoys-cannon-fired-jamming-pods/.

15. JP 3-85, *Joint Electromagnetic Spectrum Operations* (Washington, DC: U.S. GPO, 22 May 2020), I-7; David Ignatius, "Russia Is Losing on the Electronic Battlefield," *Washington Post* (website), 3 May 2022, accessed 6 May 2022, https://www.washingtonpost.com/opinions/2022/05/03/russia-ukraine-electronic-warfare/.

16. Katherine K. Elgin, "How the Army Is Not Preparing for the Next War," War Room–U.S. Army War College, 25 September 2019, accessed 6 May 2022, https://warroom.armywarcollege.edu/articles/the-next-war/.

17. Peter W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Houghton Mifflin

Harcourt, 2018). This book explores modern-day interconnectedness and describes how vulnerable humanity is to the onslaught of state and nonstate information actions, especially perception-based social media influence. It is featured on multiple senior leaders' reading lists, including the chief of staff of the Army's, because of its examination of the way technology and social media inform modern information warfare. Our own experiences, however, caution against leaders placing too much emphasis on the effects described in this book, because they are fundamentally concerned with strategic-level information operations and have little bearing on the tactical fight for decision dominance.

18. Jeffrey H. Fischer, "A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine," Defense Post, 13 April 2022, accessed 6 May 2022, https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/.