AUSA
ASSOCIATION OF THE UNITED STATES ARMY

LANDPOWER ESSAY NO. 23-8
DECEMBER 2023

Training Outside "The Box"

by CPT Daniel Eerhart, USA

Introduction

In October of 2023, paratroopers from the 82nd Airborne Division arrived at Fort Johnson, Louisiana, in preparation for a rotation at the Joint Readiness Training Center. Their rotation served as the culmination of an intense training cycle where the Soldiers spent countless hours in the field preparing themselves for the possibility of combat operations against one of the militaries engaged in a great power competition.[1] In the weeks prior to entering the training area, known as "the box," deployment operations mimicked those in preparation for combat. The Soldiers packed their equipment into Tricon containers that went on to receive civilian inspections for hazardous materials and to get proper blocking and bracing. The unit's vehicles underwent meticulous inspection and slotting on manifests. Civilian workers loaded the equipment onto rail cars for movement to the installation rail yard at Fort Johnson. Foreign actors did not interfere with manifests or rail switches during movement; however, in the modern age of information advantage, they likely would have.

Combat training centers (CTCs) should adopt infrastructure wargaming as part of their rotations in order to train units to better understand risks during pre-deployment operations.

The realities of modern warfare are that America's principal adversaries can disrupt any step in the deployment process, resulting in cascading gridlock.[2] The first time these Soldiers will contact the enemy will be at home station, through adversary information warfare.[3] While they are transporting their equipment, the enemy will take deliberate action to delay and disrupt Soldiers' ability to enter the combat theater. The enemy will be maneuvering in the cyber domain and exploiting publicly available information to disrupt and influence Soldiers before they even step on the battlefield.[4]

This paper contends that the addition of an information warfare company to the opposing force (OPFOR) battalions can better prepare rotational training units at combat training centers (CTCs) for the difficulties of modern warfare. Additionally, expanding the training scope to integrate pre-deployment infrastructure wargame exercises and adding a micro-targeting risk assessment team to the operations group would ensure that deploying Soldiers are prepared to confront the asymmetric challenges of the current multidomain battlefield.

Conduct Infrastructure Wargame Exercises

Most CTC rotations allow the rotational training unit to pack their equipment and to deploy their Soldiers to the training area unimpeded and as smoothly as possible. The reality of the era of great power competition is that domestic travel, in preparation for a deployment, is no longer uncontested. In 2020, the 3rd Infantry Division and Fort Stewart conducted an exercise, known as Jack Voltaic, with the Army Cyber Institute.[5] During the exercise, the 3rd Infantry Division was called upon to deploy into Europe to support contingency operations.[6] Simulating deployment operations helped to achieve one of the goals of

1. Department of the Army, Army Regulation 350-2, *Opposing Force (OPFOR) Program* (Washington, DC: U.S. Government Printing Office, 9 April 2004).
2. David Sanger and Julian Barnes, "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations," *New York Times*, 29 July 2023.
3. Roger Molander, Andrew Riddile and Peter Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, RAND Corporation: 1996).
4. Joe Littell, Maggie Smith and Nick Starck, "The Devil is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness," *Modern War Institute*, 20 September 2022.
5. Department of the Army, "Jack Voltaic 3.0 Cyber Research Report," *U.S. Army Cyber Institute*, September 2020.
6. "Jack Voltaic 3.0 Cyber Research Report."

the exercise, namely, to examine the impact of a cyber event on the Army's force projection abilities.[7]

Throughout the exercise, cyber threat actors severely degraded the 3rd Infantry Division's ability to get their equipment from Fort Stewart to the port: ship manifests developed inaccuracies, railroad operations were entirely compromised, and day-to-day operations in preparation for their deployment came to a standstill.[8] The U.S. military's reliance upon civilian infrastructure to deploy creates an inherent vulnerability that threat actors will seek to exploit. As interconnectedness increases dramatically throughout the world, civilian infrastructure is becoming more contested. As civilian infrastructure becomes a primary provider of military logistics, the term "military target" will continuously expand, resulting in civilian infrastructure and its operators becoming legitimate military targets.

The 3rd Infantry Division should not be alone in wargaming through friction points in its deployment plan. After all, wargaming, as part of the course of action analysis, is essential to any military decisionmaking process, and it should encompass more than just the tactical phases of the operation. However, the Army Cyber Institute does not have the resources to conduct Jack Voltaic exercises with every rotational training unit across the Army. To ensure that every tactical unit has such an opportunity, CTCs should work with the Army Cyber Institute and adapt a wargaming exercise involving all pre-deployment activities, enabling good actors to identify where an adversary might disrupt operations prior to entering "the box." Conducting real-life red team operations while an organization prepares for a CTC rotation would be dangerous and expensive; however, by implementing deployment wargaming as part of the CTC rotation, units can better understand their vulnerabilities and prepare for deployments that support major contingency operations. To avoid the additional costs associated with keeping Soldiers away from the home station and to enable garrison command teams to participate, the wargaming division at the CTCs could conduct the exercises remotely, providing flexibility for unit leaders while enhancing organizational training.

Infrastructure wargaming exercises would mimic the 3rd Infantry Division's wargaming with the Army Cyber Institute.

Expand Opposing Force to Include Information Warfare

Since the Russian invasion of Ukraine in February of 2022, the world has witnessed how a nation in great power competition can wage a direct-action war. The lessons of this conflict must be integrated into Army CTCs so that American Soldiers receive world-class training to confront the difficulties of modern combat. Tactical deceptions, small unit cyber operations and open-source investigations are all critical pieces of the war in Ukraine that CTC rotations can better integrate into the training environment.

CTC opposing forces are currently structured into an Infantry Battalion, meaning that the institutional knowledge in an operational psychological operations task force or tactical cyber and electromagnetic activities (CEMA) unit is absent.[9] However, expanding this battalion with one additional company that would provide an information warfare function seems prudent. This additional company would serve several functions.

First, the unit would have resources to implement tactical deception, mimicking those used in real-world combat operations. The war in Ukraine has demonstrated that physical objects and auditory deceptions are implemented on the modern battlefield to deceive adversaries.[10] While the rotational training unit would have enough resources to implement tactical deceptions independently, the infantry battalion OPFOR element must prioritize efforts—and knowledge regarding tactical deceptions may be absent from their organization. This OPFOR element would have inflatable vehicles and loudspeakers to match Russian and Chinese capabilities and have the task of deceiving rotational units regarding the location of OPFOR vehicles.[11] Auditory deceptions enable units to better train on the seven

7. "Jack Voltaic 3.0 Cyber Research Report."
8. "Jack Voltaic 3.0 Cyber Research Report."
9. Department of the Army, Army Regulation 350-50, *Combat Training Center Program* (Washington, DC: U.S. Government Printing Office, 2 May 2018).
10. Huw Dylan, David Gioe and Joe Littell, "The Kherson Ruse: Ukraine and the Art of Military Deception," *Modern War Institute*, 12 October 2022.

forms of contact and to rehearse reporting procedures for when Soldiers "hear something."[12] Employing tactical deceptions allows rotational training units to identify the tactics used by adversary forces, meaning that if they were to encounter these deceptions in an actual conflict, they would be better prepared to identify decoys.

Second, the information warfare company would serve the critical role of the information operations (IO) red team. The opposing force red team would ensure that the rotational training team understands the importance of the information environment. This IO red team would integrate with existing CTC assets, such as a simulated internet environment, media teams and civilians on the battlefield. The IO red team would be responsible for disseminating misinformation and disinformation consumed by the civilian population role players. If the rotational training unit chooses not to engage with the information, the result would be adversarial civilians leading up to protests and civil unrest. Through a tactical integration of the information environment, the rotational training unit can better understand how to engage in the information environment without allowing it to become the adversary's strength. During the Global War on Terror, tactical commanders learned the hard way how essential it is to engage in the information environment; CTCs have the opportunity to reinforce this lesson.[13]

CTC opposing force battalions should integrate an information warfare company to better reflect the challenges of a modern battlefield.

Third, the Information Warfare Company would integrate a tactical CEMA team. During the Army's pilot program to integrate cyber effects into tactical units, 1st Information Operations Command sent tactical CEMA teams to serve as OPFOR during CTC rotations.[14] Rather than pay TDY from Fort Belvoir to integrate on occasional rotations, the CTC OPFOR should have a permanent unit that handles the OPFOR cyber effects for rotational units. The Army's pilot program to increase cyber effects in tactical units has been under development since 2015, and the public anecdotes from the program have been that the teams added training value for the rotational training units.[15] The impetus for cyber integration increases as known cyber threat actors are in American infrastructure networks—and as Russian cyber-soldiers employ their abilities on the battlefield.[16]

Addressing the Problem of Microtargeting

While the CTCs provide world-class training venues that replicate the complexities of a combat environment, their training concentrates on unit-level operations. It does not address individual Soldier targeting that adversaries are known to conduct. Microtargeting is data-informed, individualized, targeted advertising, and it plays a significant role in how people receive information.[17] Microtargeting during IO can influence individual decisionmaking, as demonstrated by the Russian Internet Research Agency and Cambridge Analytica.[18] Soldiers have personal social media accounts, shopper discount cards and smart devices throughout their homes that collect data from them and influence their behavior in turn. The threat profiles for average citizens tend to be less significant than those for servicemembers, who are likely to be targeted by adversarial microtargeted influence warfare. Microtargeting is what lets YouTube and Amazon know what content will receive the highest engagement rate.

What does microtargeting have to do with preparing for conflict? The modern military understands that the best-performing Soldiers are the ones who are not experiencing distress in their personal matters.[19] Knowing this, if an adversary were to individually and personally distress Soldiers deliberately, how long would it be, i.e., how many Soldiers would they have to get to, before the overall unit was ineffective in combat operations? With public social media profiles and information on data aggregate websites, the opportunities to disrupt Soldiers have never been more significant; to amplify the problem, there is no organization with the designated responsibility of mitigating this risk. Researchers at Duke University were easily able to obtain personal data on thousands of U.S. Soldiers for as low as

11. Erin Snodgrass, "Ukraine says Russia's putting inflatable tanks on the battlefield - but the decoys deflated," *Business Insider*, 27 January 2023.
12. Ben Macintyre, "Decoys and Dummies can help to win wars," *The Times*, 15 April 2022.
13. Joseph Cox, "Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?," *School of Advanced Military Studies United States Army Command and General Staff College*, March 2006.
14. Mark Pomerleau, "US Army conducts first-of-its-kind exercise for tactical information warfare unit," *C4ISRNET*, 12 October 2020.
15. William Roche, "Combat Training Center rotations continue to drive evolution of Army Cyber-Electromagnetic Activities," *DVIDS News Hub*, 29 June 2017.
16. Grace Mueller et al., "Cyber Operations During the Russo-Ukrainian War," *Center for Strategic and International Studies*, 13 July 2023.
17. Jessica Dawson, "Microtargeting as Information Warfare," *Cyber Defense Review*, December 2021.
18. U.S. Senate Intelligence Committee, *Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections*, U.S. Senate, report to the 1st Session, 116th Congress, 18 August 2020.
19. Department of the Army, *The Army People Strategy* (Washington, DC: U.S. Government Printing Office, October 2019).

$0.12 per record; imagine what a threat actor with the motivations and resources of a nation state could do.[20] One approach that might be taken is integrating open-source risk mitigation into CTC rotations.

The CTC operations group should have a few trusted individuals responsible for conducting open-source risk assessments. Within 90 days before a rotational training unit arrives at a CTC, the risk assessment unit would conduct open-source investigations of the unit. Examples of points of emphasis might be: Is data publicly available for personal addresses? Are social media profiles active and public? Are individuals active on blogs or open forums? It may be tempting to claim that this risk assessment violates Soldiers' privacy. However, as this article is being read, actors in China, Russia, North Korea and Iran are developing individualized dossiers on American Soldiers, and there is no mitigation plan.[21] Additionally, open-source risk assessments would give the rotational unit an assessment of how impactful open-source information is to the mission and where its vulnerabilities lie. The trusted investigators would also weigh the information based on risk profiles; for example, a brigade commander with significant public information presents a greater risk to unit success than a vehicle driver fresh out of basic training.

CTCs should have publicly available information risk assessors that are able to assess units and to provide individualized training to reduce Soldier risk.

Following the CTC rotation, the risk assessors would provide personalized training to individuals in high-risk categories. Every organization member would receive general training to reduce the overall risk profile. The Army has programs to provide more highly individualized training for high-risk individuals, such as SERE training (SERE-C versus SERE 100). The microtargeting exercise would end 90 days after the CTC rotation, at which point the risk assessors would do a second investigation to determine residual risk and to identify if servicemembers have taken the necessary steps to secure themselves in the digital environment.

Conclusion

CTCs are the Army's premier training venues for its maneuver organizations; as such, they must inherently evolve and modernize to match the realities of modern warfare. By expanding the training scope of CTCs, the Army can ensure that units stand ready to face future adversaries while protecting its Soldiers from the asymmetric risks they face. Wargaming pre-deployment activities with an emphasis on critical infrastructure enhances the Army's ability to project force while simultaneously supporting the *National Cybersecurity Strategy's* emphasis on defending critical infrastructure.[22] Additionally, adding an opposing force information warfare company and assessing open-source risk would undoubtedly increase the difficulties for CTCs in providing their services to the Army. However, the increase in difficulties would pay substantial dividends whenever those units would be called upon to answer our nation's call.

★ ★ ★

Captain Daniel Eerhart is an Army Psychological Operations Officer currently serving as a Cyber Policy, Law and Strategy Research Scientist at the Army Cyber Institute. He previously served as a graduate student at the University of California, Los Angeles (UCLA), where he earned a Master of Public Policy degree specializing in Technology and Cyber Policy. He holds professional and graduate level certifications in Cybersecurity and Data Analytics.

20. Justin Sherman et al., "Data Brokers and the Sale of Data on U.S. Military Personnel," *Duke University Sanford School of Public Policy*, November 2023.
21. Insikt Group, "Private Eyes: China's Embrace of Open-Source Military Intelligence," *Recorded Future Threat Analysis*, 1 June 2023.
22. United States National Security Counsel, *National Cybersecurity Strategy 2023*, White House, March 2023.