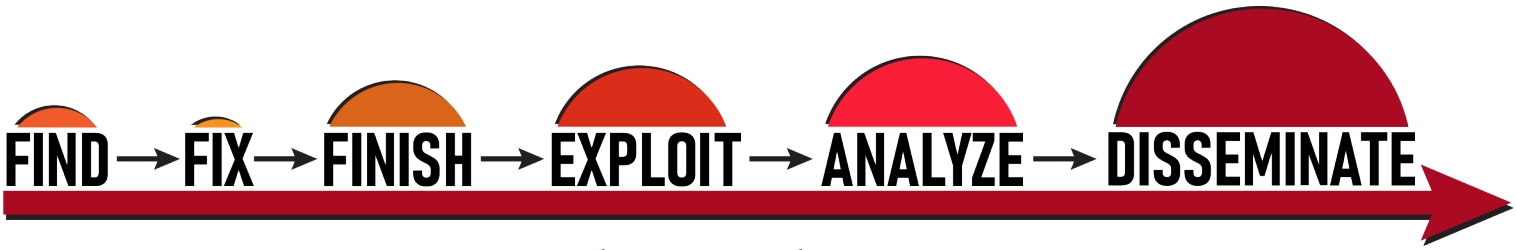

Optimizing the Alternate Targeting Methodology F3EAD

by Major Michael J. Fox, Major Matthew Otterstedt, Major Bernard Wheeler, and Major Kevin H. Caliva

Editor's Note: This article was written prior to the publication of ADP 3-13,* Information*, which provides the fundamental principles for considering how Army forces use, protect, and attack data and information to achieve objectives while affecting the threat's ability to do the same. This doctrine is based in the premise that all activities have inherent information aspects that generate effects which contribute to or hinder the threat from achieving objectives during competition, crisis, and armed conflict. It establishes the fundamental principles and guidance to plan, prepare, execute, and assess the use of information during operations.

Introduction

The U.S. Special Operations Forces (SOF) must optimize the organizational force structure to adequately leverage emerging technologies. These technologies must focus on increasing the effectiveness associated with SOF's diverse and challenging missions against increasingly sophisticated adversaries. The purpose of SOF is to create strategic, asymmetric advantages for the Nation in competition, crisis, and conflict. To maintain these asymmetric advantages in the modern operational environment, SOF must lead the integration of cyberspace operations into targeting through their application of the alternate methodology—Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD).[1] SOF can also increase efficiency and effectiveness in future military engagements by employing cyberspace capabilities, such as artificial intelligence and quantum technology, to enhance the intelligence architecture during future operations. Optimizing the F3EAD targeting methodology by applying an enhanced intelligence architecture and cyberspace effects will increase the lethality and efficiency of SOF operations.

SOF missions frequently support high-visibility overseas contingency operations and rely on a targeting approach "predominantly used for counterinsurgency and high-value individual targeting known as F3EAD."[2] With the F3EAD targeting methodology, SOF may recognize, locate, and target enemy units and conduct intelligence exploitation and analysis on captured enemy high-value targets and equipment.[3] The process often emphasizes speed to not only remove high-value targets from the battlefield but to gain and maintain additional intelligence on the enemy within the area of operations. Creating a symbiotic interaction between the operations and intelligence warfighting activities is the most crucial feature of F3EAD. Operations continuously guides the overall intelligence effort, and intelligence, in turn, provides operations with the data they need to complete the mission.[4]

SOF's threats are multifaceted—near-peer adversaries in Eastern Europe and China; transnational terrorist organizations in the Middle East and North Africa; and failed or failing states with a regional terrorist presence. The *National Security Strategy* states that our "strategy is rooted in our national interests: to protect the security of the American people; to expand economic prosperity and opportunity; and to realize and defend the democratic values at the heart of the American way of life."[5] The complexity of the threats facing SOF in current operational environments has led to a shift in requirements for the intelligence architecture and tactics, techniques, and procedures (TTP) of the intelligence warfighting function. The problem sets, the complexity of operations, and the rapid-response nature of the SOF missions across geographically diverse theaters requires a reshaping of the intelligence architecture and TTPs within the framework of the mission set. It also requires an assessment of SOF's organic capabilities to collect, analyze, and exploit intelligence information in a coalition or joint framework.

Digital Anchor Point

During SOF operations in austere areas where no significant collection platform is available, the intelligence warfighting function is responsible for coordination at higher echelons to acquire up-to-date and accurate intelligence reports.[6] Intelligence personnel must be prepared to deploy and operate within a low-bandwidth communications architecture and with limited cross-domain solutions. This must include

minimizing enemy targeting opportunities by reducing electronic signatures and keeping pace with maneuver force dispersion and survivability efforts. The development and advancement of the Department of Defense Information Network's (DoDIN) cyberspace operations could facilitate a geographically separated digital anchor point capable of reach-back support using the Distributed Common Ground System-Army backbone. Through this digital anchor point, SOF would be able to provide agile, adaptive responses to complex problem set. The digital anchor point should be designed as a digital, continuous analytical bridging solution that provides elements on the forward edge with the intelligence architecture capable of real-time, reach-back support in tailorable force packages to meet specific threats.

The digital anchor point would improve SOF communications and architecture shortfalls by rapidly establishing an information flow and promoting situational awareness, decreasing the risk to forces and the mission. For example, currently, fully establishing the forward-deployed intelligence architecture during an airborne operation occurs once conditions are set. The digital anchor point would provide a common operating picture and intelligence update to the assault command post upon establishment of communications. This would enable the intelligence warfighting function to visualize the threats and relevant aspects of the operational environment, helping the commander decide when and where to concentrate combat power to defeat the enemy. The SOF intelligence warfighting function should develop and incorporate the digital anchor point as a geographically offset and tailorable package that can support continuity through information collected by national and theater assets, databasing and situation development for the operation in near real time, and continuous analytic support with the human dimension isolated from threat factors and environmental conditions.

The task organization of SOF, the requirements of joint forcible entry operations, the variety of potential mission sets tied to contingency plans, the interoperability with multinational partners, and the threats present in the operational environment underline the need to reshape the architecture with modified TTPs. In large-scale combat operations with a peer or near-peer, the intelligence warfighting function must operate with a reduced electromagnetic signature to degrade enemy targeting opportunities and keep pace with maneuver force dispersion and survivability efforts.[7] The digital anchor point would provide the intelligence architecture and support mechanisms to maintain the commander's perspective of the battlefield while also supporting survivability aspects of the operational environment. The digital anchor point could perform this function in both time and space, away from the threat or environmental factors that degrade mission command and adversely affect elements of the human dimension. Integrated systems and expanded bandwidth capabilities within the intelligence architecture, down to the lowest command level of SOF, would allow the historical clients of intelligence reports to be both receivers and producers of intelligence. Battalion-level production and information sharing through the digital anchor point would increase the intelligence warfighting function's ability to receive, process, analyze, and disseminate information and further enhance the commander's ability to gain and maintain perspective on the battlefield. An increased number of intelligence production nodes on the battlefield would also increase F3EAD lethality and survivability of SOF within multidomain operations. The success of the digital anchor point is contingent on a robust DoDIN communications package and strong digital bridging (i.e., data sharing) solution with various multinational partners.

The F3EAD Process

While F3EAD is very well suited for lethal targeting operations against high-value targets, it is equally effective in identifying and prioritizing targets for nonlethal targeting to achieve cross domain effects. SOF can bolster targeting by employing offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and electronic warfare (EW) capabilities. "Finally, while doctrine views F3EAD as a hasty decision process, many units also utilize F3EAD in deliberate planning."[8] Incorporating cyberspace operations and EW capabilities into the targeting process will yield increased effectiveness and efficiency.

Find. Simply put, the find step of F3EAD establishes "a starting point for intelligence collection."[9] These start points frequently take the form of the bed down locations, last known locations, or other last known multisource reports. F3EAD practitioners use the full range of intelligence assets to acquire a starting point.[10] However, substantial amounts of data make it difficult to conduct efficient analysis, producing a latency issue for any timely combat information that leads to actionable intelligence. Within the joint force, processing, exploitation, and dissemination (or PED) cells are crucial links between the collection assets and the ground force commanders making targeting decisions. The abundance of publicly available information offers additional means that were not available in past years. This offers options for OCO, DCO, and EW operations to engage in the find step and bear fruit through the speed of their actions. Artificial intelligence also has the potential to bolster F3EAD by improving positive identification, specifically with facial recognition technology, to increase the speed the United States can find and fix a targeted individual.

Fix. The fix step of F3EAD occurs when intelligence collection on a given target has developed enough to execute a mission.[11] Once a target is positively identified, a wide range of collection capabilities are leveraged on a target to develop

patterns of life. A well-developed pattern of life focuses on where and when a target will maneuver on the battlefield. The predictive nature of the pattern of life enables operations for nonlethal or lethal effects at the time and place of choice. The joint force depends on targeting teams to triage the data and provide predictive pattern of life analysis. This model, centered around human capacity and capability, becomes difficult to manage throughout daily activities and schedules. Much of the resident knowledge on a given target's pattern of life leaves when a targeteer tracking the target leaves the organization. Adopting OCO, DCO, and EW operations into the fix step can facilitate a more rapid corroboration of a targets pattern of life. Artificial intelligence, specifically, has the potential to aid F3EAD by enabling faster analysis to expedite decision making. This advancement to pattern of life development and analysis can hasten triggers to act, reduce overall resource requirements, and increase targeting efficiency throughout a designated area of operation.

Finish. F3EAD's first two steps (find and fix) provide the triggers for decision makers to approve risk tolerant operations against an adversarial target. "The window of opportunity to engage the target requires a well-trained and rehearsed finish force and a well-developed SOP [standard operating procedure]."[12] Forms of operations related to the finish phase include lethal strikes via terminal guidance, launching a raid force, or the use of surrogates to close with and destroy an adversary's personnel, weapons, or equipment. However, the finish phase can just as quickly be nonlethal.[13] Integration of OCO, DCO, and EW operations into the finish portion will provide additional advantages for SOF operations to achieve objectives through the employment of lethal and nonlethal effects. Artificial intelligence will further enable OCO, DCO, and EW by leveraging autonomous bots for ubiquitous employment, terminating with a nonlethal finish. In addition, artificial intelligence has the potential to enable unmanned aerial vehicle swarming capabilities, increasing the range of military targeting options for a lethal finish.

Exploit. "The 'exploit' phase, as the main effort of F3EAD, is the most critical single step in the process as it leads to finding, fixing, and finishing of the next target and the perpetuation of the cycle."[14] The emphasis on exploitation is what makes F3EAD different from other targeting models.[15] The exploitation effort aims to yield sufficient actionable intelligence to continue the F3EAD methodology as quickly as possible. In most cases, collected exploitable material (CEM) is manually sorted and tagged for time-sensitive information, which includes any intelligence leading to a fleeting start point or "find." This manual work is both costly and time intensive, resulting in missed targeting opportunities. In modern and emerging operational environments, artificial intelligence can provide a decisive military advantage to any country able to wield, employ, and integrate it into the multidomain battlefield. Artificial intelligence can reduce the cost and manpower required to sift through, process, and exploit CEM.

In other cases, data and enemy "reflections" can be sorted and analyzed by all-source analysts. However, by leveraging artificial intelligence this data and analysis could become a much more efficient and effective process, providing a quicker feedback mechanism to the ground force commander.

Analyze. The analyze phase is where the CEM gathered transforms into intelligence that can drive future operations.[16] "Analysis can be performed by SOF in theater, or information and material can be sent to CONUS [continental United States] for further in-depth analysis."[17] Unlike the exploit phase, intelligence professionals take a deep dive into the CEM, or reflections from an action taken against an enemy, to tip and cue additional targets to find. This not only speeds up the analysis process but also reduces the risk of error or inconsistencies. However, similarly to the exploit phase, artificial intelligence will reduce the cost and manpower required to sift through, process, and analyze CEM.

Disseminate. "The last step in the F3EAD process is the "disseminate" phase. One of the keys to success of F3EAD is creation of a wider dissemination network than what has traditionally been practiced inside the U.S. intelligence community."[18] To further the scale and security of information sharing during the dissemination phase, SOF should invest in quantum technology to translate the principles of quantum physics into technical applications. Moreover, artificial intelligence and quantum technology can help make disseminated data more accessible by converting it into different formats and languages.[19] This can help overcome language barriers and ensure that data is accessible to a wider audience. This dissemination would increase interoperability, interdependence, and integration of the joint force during any fight or targeting operation. In general, quantum technology has not yet reached maturity; however, it could hold significant implications for the future of military encryption and communications.

Optimizing for the Future

Optimizing the SOF F3EAD targeting methodology by applying an altered intelligence architecture and cyberspace effects will increase the lethality and efficiency of SOF operations. SOF should continue to modernize its cyberspace capability to improve the intelligence architecture during an operation. SOF efforts to employ artificial intelligence and quantum computing into the F3EAD process will increase speed and efficiency for decision makers. An altered intelligence architecture, artificial intelligence, and quantum computing seek to address and define the complex, multitiered threats that will continue to face SOF in current and future operational environments. The problem sets, the complexity of airborne

operations, and the rapid-response nature of the mission—across geographically diverse theaters, against adversarial forces who constantly evolve and adapt—will continue to drive the way SOF thinks about intelligence support to the commander. It will reshape the framework of the intelligence warfighting function.

Endnotes

1. Department of the Army, Field Manual (FM) 3-60, *Army Targeting* (Washington DC: U.S. Government Publishing Office, 11 August 2023), I-1.

2. Ibid.

3. Charles Faint and Michael Harris, "F3EAD: OPS/Intel Fusion 'Feeds' The SOF Targeting Process," Small Wars Journal, January 31, 2012, https://smallwarsjournal.com/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process.

4. Department of the Army, FM 3-60, *Army Targeting*, I-2.

5. Joe Biden, *National Security Strategy* (Washington, DC: White House, 2022), 7, https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.

6. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-0, *Joint Intelligence* (Washington, DC: Joint Staff, 26 May 2022), I-4–1-5.

7. Johan Jersbald and Niklas Alund, "Why signature analysis is crucial for combat survival," SAAB, 18 November 2021, https://www.saab.com/newsroom/stories/2021/october/why-signature-analysis-is-crucial-for-combat-survival.

8. Faint and Harris, "F3EAD: OPS/Intel Fusion."

9. Ibid.

10. Ibid.

11. Ibid.

12. Department of the Army, FM 3-60, *Army Targeting*, I-6.

13. Faint and Harris, "F3EAD: OPS/Intel Fusion."

14. Ibid.

15. Department of the Army, FM 3-60, *Army Targeting*, I-6.

16. Faint and Harris, "F3EAD: OPS/Intel Fusion."

17. Ibid.

18. Ibid.

19. "How to Overcome Language Barriers with AI," Mosaicx, February 16, 2023, https://www.mosaicx.com/blog/how-to-overcome-language-barriers-with-ai.

MAJ Michael Fox is a graduate student assigned to the Air Command and Staff College with concentrations in national security; intelligence, surveillance, and reconnaissance and cyberspace; and electronic warfare and cyberspace. His previous special operations assignments were as the 75th Regimental Special Troops Battalion S-2, the 75th Ranger Regiment assistant S-2, and the 75th Ranger Regiment military intelligence company commander. MAJ Fox's military education includes the Signals Intelligence Course, Air Assault School, Airborne School, and Jumpmaster School. He is a 2012 graduate of The Citadel, The Military College of South Carolina.

MAJ Matthew Otterstedt is a graduate student assigned to the Joint All Domain Strategist program at the Air Command and Staff College. His previous special operations assignments were as a company commander and air officer for 3rd Battalion, 75th Ranger Regiment and command group operations officer for the 75th Ranger Regiment. MAJ Otterstedt's military education includes the Reconnaissance and Surveillance Leaders Course, Airborne School, and Jumpmaster School. He is a 2012 graduate of the U.S. Military Academy at West Point, NY.

MAJ Bernard "BJ" Wheeler is a graduate student assigned to Air Command and Staff College. His previous special operations assignments were as the commander and the regimental air for Headquarters and Headquarters Company, 75th Ranger Regiment. MAJ Wheeler's military education includes the Ranger School, Airborne School, Air Assault School, Pathfinder Course, and Advance Airborne School Jumpmaster Course. He is a 2012 graduate of Southern University A&M in Baton Rouge, LA.

MAJ Kevin Caliva is a graduate student assigned to Air Command and Staff College. His previously special operations assignments were as the commander for Headquarters and Headquarters Company 7th Special Forces Group and the detachment commander for SFOD-A 7232. MAJ Caliva's military education includes the Ranger School; Airborne School; U.S. Army High-Risk Personnel Security Course; Special Forces Qualification Course; Special Forces Detachment Leader's Course; U.S. Army Military Freefall School; Special Operations Static Line Jumpmaster Course; and Survival, Evasion, Resistance, and Escape-C (High Risk). He is a graduate of Louisiana State University.