

Technical Perspective

by Chief Warrant Officer 5 Aaron Anderson
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence



Teammates,

As a nation, we once again find ourselves in the midst of a transitioning global security environment, often characterized as a *great power competition* or a *long-term strategic competition*. The most recent National Defense Strategy describes the strategic environment as “an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations.”¹

Within this security environment, the National Defense Strategy highlights China, Russia, North Korea, and Iran as actors of primary concern. These peer and near-peer challenges are the focus of this quarter’s *Military Intelligence Professional Bulletin*.

Regardless of the adversary, the battlefield of the future is sure to be more complex and more lethal, with a faster operational tempo than ever before. Without losing our collective ability to understand and execute counter-insurgency operations, military intelligence (MI) leaders must be increasingly agile, with a deep understanding of near-peer and conventional threats across all domains. We must be prepared to operate more and more in the competition phase, parsing disinformation campaigns and dealing with digital security concerns, such as “deep fakes” within a disconnected, intermittent, and low-bandwidth environment. As intelligence practitioners, we must fully understand our adversaries’ capabilities and weaknesses. This is paramount. It is also critical that we are able to provide relevant and precise intelligence to commanders in real time, affording them the opportunity to make informed decisions on the battlefield.


Our adversaries have spent several decades examining U.S. tactics, capabilities, and equipment to identify operational gaps and material weaknesses. We must now shift



our collective efforts to closing those gaps and building new capabilities to counter emergent threats. The enemies we faced in Iraq and Afghanistan generally “lacked capabilities in the form of sustained long-range precision fires, integrated air defense systems, robust conventional ground maneuver, and electronic warfare.”² Our near-peer competitors possess all these capabilities and have the ability to contest us in multiple domains while employing varying antiaccess and area denial strategies.

While neither combatant in the recent conflict between Armenia and Azerbaijan over the disputed Nagorno-Karabakh region is considered a near-peer threat, military planners would be wise to gain an increased understanding of the technology and tactics used during the fighting. According to open-source reporting, the effective use of Azerbaijani drones and drone swarm tactics played a major role in the destruction of nearly 175 main battle tanks and armor.³ According to the Director of the Security and Defense Research Program at the Istanbul-based Center for Economics and Foreign Policy Studies, Armenian forces lacked “adequate sensors, electronic warfare cover, or counterdrone weaponry” to defend against Azerbaijan’s Unmanned Aerial Vehicles (UAVs).⁴

As we anticipate this new operational environment, we must continue to increase both rigor and complexity in our training in order to gain or maintain overmatch with near-peer competitors. In order to better educate our warrant officers here at the U.S. Army Intelligence Center of Excellence, we continue to adapt our training within the Warrant Officer Training Branch, enabling all courses to deliver material relevant to large-scale ground combat operations and multi-domain operations, reinforcing both digital and analog methods in our training. These changes are critical as we work to meet the demands of tomorrow across the intelligence enterprise.

As I close out this column, I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in defense of our Nation. I would especially like to recognize those MI Soldiers who are currently serving in forward locations. Your contributions to the MI Corps and Army mission are greatly appreciated. 

Endnotes

1. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., 2.

2. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 6 October 2017), 1-2–1-3. Change 1 was issued on 6 December 2017.

3. Ron Synovitz, “Technology, Tactics, And Turkish Advice Lead Azerbaijan To Victory In Nagorno-Karabakh,” Radio Free Europe/Radio Liberty website, November 13, 2020, <https://www.rferl.org/a/technology-tactics-and-turkish-advice-lead-azerbaijan-to-victory-in-nagorno-karabakh/30949158.html>.

4. Ibid.

Always Out Front! and Army Strong!

ATP 2-19.4, *Brigade Combat Teams Intelligence Techniques: The Update*

by Mr. Richard Garza

Introduction

The update to ATP 2-19.4, *Brigade Combat Teams Intelligence Techniques*, describes doctrinal techniques for intelligence support to brigade combat team (BCT) operations. Last published in 2015, ATP 2-19.4 details capabilities, organizations, and structures for brigade and below intelligence elements. It also describes the latest configuration of the BCT’s military intelligence company designed to support the various requirements placed on the infantry, armored, and Stryker BCTs. The Army has since modified its foundational doctrine to reset the doctrine library to focus on large-scale ground combat operations against a peer threat. This shift in core Army doctrine and the changes to BCT intelligence capabilities, organizations, and structure were the driving forces behind the update. In order to maintain consistency with validated Army doctrine, ATP 2-19.4 covers—

- ◆ BCT intelligence support to the warfighter through the Army’s strategic roles.
- ◆ BCT intelligence support to the operations process.
- ◆ Revised verbiage to ensure consistency with operations and intelligence doctrine and terminology.
- ◆ BCT intelligence considerations such as training strategies; pre-deployment preparation; intelligence architecture; primary, alternate, contingency, and emergency (also known as PACE) communication planning; collection management; and targeting.

Development

The development team collaborated with personnel from multiple intelligence organizations within and outside the U.S. Army Intelligence Center of Excellence (USAICoE) to develop the Army techniques publication throughout 2020. Those organizations within USAICoE included the Requirements Determination Directorate (RDD), Force Design, Information Collection Planner’s Course (ICPC), and Lessons Learned. The primary personnel outside USAICoE included instructors from the Digital Intelligence Systems Masters Gunners Course (DISMGC). Personnel from DISMGC, ICPC, and RDD assisted by providing input to the publication’s intelligence architecture appendix. The exhibited collaboration was a beneficial side effect of the coronavirus disease 2019 work environment that turned into a doctrine best practice.

ATP 2-19.4 underwent two worldwide staffings, including senior leadership reviews, which produced approximately 600 comments requiring adjudication. The collaborative development of the publication is a testament to the commitment—from doctrine leadership, the development team, and the force at large—to create unique doctrine that is both relevant and timely with the goal of enhancing the readiness of the force. We anticipate final publication of ATP 2-19.4 in mid- to late-spring 2021. 