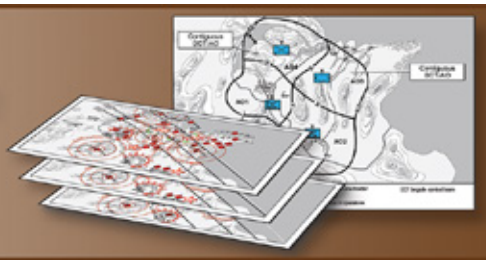
ATP 2-01.3, *Intelligence Preparation of the Battlefield:* Why the Update?

by Major James H. McMillian, Jr.



Introduction

Commanders and staffs need timely, accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and courses of action to successfully execute offensive and defensive tasks in large-scale combat operations.[1]

***FM 2-0,* Intelligence**

Many intelligence professionals recall using FM 34-130, *Intelligence Preparation of the Battlefield*, first published in 1989. This Cold War era publication contained unique products and narratives for the analysis of peer threats conducting conventional warfare. When operations in Iraq and Afghanistan began, counterinsurgency became the priority. Since that time, the proliferation of advanced technologies, such as unmanned aircraft systems, cyberspace warfare, and antiaccess and area denial capabilities, has leveled the playing field in some instances for conducting operations against our adversaries in contested operational environments. The shift from counterinsurgency to large-scale ground combat operations called for a review of the intelligence preparation of the battlefield (IPB) process to ensure we addressed characteristics of the operational environment and complex operations across all steps of the process.

The publishing of FM 3-0, *Operations*, in 2018 marked the return to an emphasis on large-scale ground combat operations. LTG Michael Lundy, Commanding General of the Army Combined Arms Center and Fort Leavenworth and Commandant of the Army Command and General Staff College, states in the foreword to FM 3-0 that the manual "provides the tactical and operational doctrine to drive our preparation, and when necessary, execution."[2] IPB is key to preparing for large-scale ground combat operations described in FM 3-0, and it is the cornerstone of what intelligence analysts do—use the IPB process to develop an accurate picture of threat courses of actions and determine how threat capabilities may be used over time and space.

Updating ATP 2-01.3

The update to ATP 2-01.3, *Intelligence Preparation of the Battlefield*, began in February 2017 with a 3-day workshop at the U.S. Army Intelligence Center of Excellence (USAICoE). Intelligence professionals from across the Army attended the workshop, including representatives from the National Training Center, U.S. Army Cyber Command, 173rd Airborne Brigade, U.S. Army Training and Doctrine Command G-2 Intelligence Support Activity, and Capabilities Development and Integration Directorate at USAICoE. Participants provided insight into how we needed to revise the existing ATP 2-01.3, issued in 2014. Their objectives were to—

- Understand the Army's major trends and intelligence challenges and their applicability with regard to updating ATP 2-01.3.
- Learn about complex operational environments and the effect they have on IPB.
- Acquire an understanding of how intelligence analysts can address a complex operational environment considering all relevant aspects and domains.
- Obtain consensus for the way ahead.

The workshop's primary task was to facilitate a discussion to increase understanding of how IPB addresses the complexities of today's operational environments across all relevant environmental aspects within and across each domain. The purpose of the event was to ensure ATP 2-01.3 would provide guidance for analyzing those complexities and describe the hybrid threats that are likely to exploit areas of technological overmatch. The end state was an open and honest discussion, anchored in doctrine, which was capable of achieving specific solutions to update ATP 2-01.3 so that it would support analysts' needs.

The accumulated experience of the workshop's participants included a former chief warrant officer of the Military Intelligence Corps and a senior intelligence officer at the National Training Center. All participants assisted in the review of ATP 2-01.3 and the subsequent identification of areas that needed to be addressed to shift the focus to large-scale ground combat operations. All parties agreed the current steps and sub-steps of IPB remain sound and allow analysts to determine a multitude of possible threat courses of actions based on threat characteristics and capabilities. For example, the four steps of IPB facilitate an analyst's ability to account for advanced technologies, such as the use of cyberspace, antiaccess and area denial capabilities, and precision long-range fires, as well as capabilities typically seen in counterinsurgency environments such as improvised

explosive devices and small arms ambushes. The thoroughness of the four steps speaks to IPB's continued relevancy. Its framework can be used successfully against any threat, environment, and capability.

IPB Process

The IPB process consists of the following four steps:

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat courses of action.

It is important to note that IPB is a continuous process. Continuous analysis and assessment are necessary to maintain situational understanding of an operational environment in constant flux.[3]

The workshop's assessment concluded that the use of advanced technologies also forces analysts to determine how these technologies may affect the operational environment in ways they may not have previously considered. An example of this is how cyberspace may extend the area of influence and the area of interest during a given operation. This occurred during the Arab Spring of 2011 when the use of social media played a part in the Arab uprisings, spreading from Tunisia to other countries in the region. Another example is Hamas's use of the subterranean environment in Gaza to infiltrate Israel, which effectively extended the battlefield and increased course of action possibilities for the threat commander. These examples demonstrate the multitude of possibilities that staffs must account for over time and space when considering how and when threat forces may attempt to affect friendly operations.

The workgroup determined the current IPB framework of steps and sub-steps is optimized to account for any new threat and range of complex environments. The group also determined the need to—

- Discuss the peer threats, operational framework, multi-domain operations, and identification of windows of opportunity.
- Provide adequate details covering all domains, significant aspects of each domain, and potential capabilities of a hybrid threat across the entire publication.
- Emphasize staff inputs and outputs and the importance of leveraging national to tactical intelligence.
- Improve PMESII, ASCOPE,[4] and civil considerations (with an emphasis on the information environment).
- Emphasize the use of the information environment in threat courses of actions.
- Highlight unique environments such as littoral, urban, and subterranean.

Staffing ATP 2-01.3

Using recommendations from the workshop, doctrine writers and subject matter experts created the new document and disseminated it for worldwide staffing, from 25 June to 31 August 2018. The USAICoE Doctrine Division received 580 comments (4 critical, 55 major, 439 substantive, and 82 administrative) from 18 organizations. During the 3-month adjudication process, Doctrine Division personnel determined how best to address each comment, which sometimes required contacting organizations for clarification. They edited and formatted the draft, and then submitted it for review by the USAICoE Commanding General, who approved the document on 18 December 2018.

Photo courtesy of Israel Defense Forces Spokesperson's Unit

An Israel Defense Forces soldier overlooking a Hamas-built tunnel in Gaza during Operation Protective Edge, 20 July 2014.

Additional Considerations

Precise intelligence is critical to targeting threat capabilities at the right time and place to open windows of opportunity across domains. Commanders and staffs receive effective intelligence when they direct and participate in intelligence warfighting function activities…Close interaction between the commander, G-2/S-2, G-3/S-3, and the rest of the staff is essential, as the entire staff supports unit planning and preparation through the integrating processes and continuing activities.[5]

***FM 2-0,* Intelligence**

The intelligence staff cannot conduct IPB in a vacuum. So one of the main areas of emphasis in the updated ATP 2-01.3 is the importance of staff collaboration. Each staff section plays an integral part in determining relevant aspects of the operational environment. Without staff collaboration, it is difficult if not impossible to give the commander a holistic and accurate picture of the operational environment. Chapter 1 of the updated ATP 2-01.3 describes staff collaboration by individual staff sections. Given the complex operational environments and the capabilities that reside within them, it is important to leverage the resident experts in their fields. It is also important to understand the roles and responsibilities of each staff section as well as the commander, executive officer, and G-3/S-3. This ensures synchronization of the staff and facilitates a shared understanding of the threat.

The update of ATP 2-01.3 also involved detailing the same emphasis that ADP 3-0 and FM 3-0, *Operations*, had put on multi-domain operations and large-scale ground combat operations. This included considerations for all domains. For example, in ATP 2-01.3—

- Appendix D, IPB Cyberspace Considerations, discusses cyberspace considerations for each IPB step;
- Chapter 7, Section II, Unique Environments, highlights littoral, urban, and subterranean environments; and
- Chapter 8, Additional Considerations for Operational Environments, discusses additional considerations for each domain (air, land, maritime, space, and cyberspace), the electromagnetic spectrum, and the information environment.

Conclusion

During large-scale ground combat operations, our peer threats will use conventional and unconventional tactics, and our area of operations will likely include unique environments (littoral, urban, and subterranean). We will also rely increasingly on the information environment. Therefore, we must gain a deeper understanding of how the threat will employ capabilities across the domains (air, land, maritime, space, and cyberspace), the electromagnetic spectrum, and the information environment to achieve an end state at a time and place of its choosing.

The updated ATP 2-01.3 will help intelligence analysts to adopt a holistic approach when analyzing operational environments. Providing an analysis of the time and place of this end state will allow friendly commanders to develop multiple courses of action and decision points to identify windows of opportunity outside the threat's decision cycle. Operating outside the threat's decision cycle and providing the friendly commander multiple options across multiple domains is key to conducting multi-domain operations and large-scale ground combat operations.

Endnotes

1. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 6 July 2018), vii (common access card login required).

2. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), foreword. Change 1 was issued on 6 December 2017.

3. Department of the Army, Army Techniques Publication 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. GPO, 1 March 2019), 1-3.

4. PMESII—political, military, economic, social, information, and infrastructure; ASCOPE—areas, structures, capabilities, organizations, people, and events.

5. Department of the Army, FM 2-0, 6-2.

MAJ James McMillian, Jr., is the executive officer for the Directorate of Doctrine and Intelligence Systems Training at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. He commissioned through Officer Candidate School in 2002. He has a bachelor's degree in philosophy from the University of North Carolina at Chapel Hill. His prior assignments include observer-coach-trainer and intelligence planner at the National Training Center, Fort Irwin, CA, and intelligence officer for Port of Entry Transition Team 4251 in Rabia, Iraq.