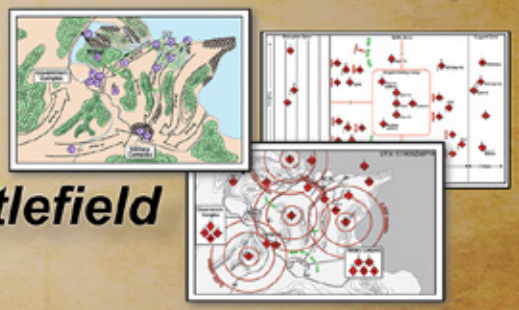
An Excerpt from ATP 2-01.3, *Intelligence Preparation of the Battlefield*



Editor's Note: The following text is from ATP 2-01.3,* Intelligence Preparation of the Battlefield, *1 March 2019 (paragraphs 1-54 through 1-60).

Multi-Domain Understanding of the Operational Environment

The interrelationship of the air, land, maritime, space, and cyberspace domains, the information environment (which includes cyberspace), and the [electromagnetic spectrum] EMS requires a multi-domain situational understanding of the [operational environment] OE. (See FM 3-0.) Seeing, understanding, and responding to windows of vulnerability or opportunity within each domain and the information environment can reduce risk to the force and enhance success in chaotic and high-tempo operations, such as large-scale combat operations. This makes situational understanding essential to managing risk.

When commanders and staffs seek to understand friendly and threat capabilities, they consider how, when, and why those capabilities are employed in each domain, the information environment, and the EMS. From this understanding, commanders can better identify windows of opportunity during operations. This allows a portion of the joint force to establish a decisive point for the multi-domain convergence of capabilities, which must be supported by continuous intelligence operations across the domains for the best effect. Since many friendly capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations.

Note. *Decisive point* is a geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an enemy or contribute materially to achieving success (JP 5-0).

During large-scale combat operations against a peer threat, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to shape the OE and gain a position of relative advantage for activities, such as joint fires, within the other domains. Once that position is achieved, operations would continue to increase the position of relative advantage in order to create a longer window of superiority to facilitate follow-on missions and operations across the domains.

Note. *Position of relative advantage* is a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage (ADRP 3-0).

Intelligence supports the commander by visualizing the threat and detecting possible threat [courses of action] COAs. Army forces must integrate and synchronize these actions across multiple domains to create opportunities to dislocate, isolate, disintegrate, and destroy enemy forces. (See FM 3-0 for more information on these defeat mechanisms.) Army forces strive to use intelligence, mobility, protection, and firepower to strike the enemy unexpectedly in multiple domains and from multiple directions, denying the enemy freedom to maneuver by creating multiple dilemmas that the enemy commander cannot effectively address. Intelligence supports these operations by facilitating situational understanding and supporting decision making. Intelligence assists commanders in seeing through the fog and friction of war.

Importance of Domain Interdependence

Domain interdependence refers to the reliance on one or multiple domains to leverage effects or information. Domains provide a means of viewing the OE based on how capabilities are arrayed and employed. An OE does not comprise a single domain; a capability's effects are not

limited to a single domain; and a capability is not employed in a single domain. For example, a satellite is launched from the ground and uses space as a medium for flight. The satellite may collect information from multiple domains and transmit that information using cyberspace as a medium to reach the ground, where the information can be processed, exploited, and disseminated. It is important for commanders and staffs to understand interdependence in order to visualize when and where capabilities can be leveraged by friendly, neutral, and threat forces.

Because a multitude of effects (including threat, terrain, and weather) can cross multiple domains, the interdependence of the domains, the information environment, and the EMS must be considered when performing [intelligence preparation of the battlefield] IPB. To do this, the S-2, with assistance from other staff members and possibly outside organizations, must address the operational framework considerations and view the OE holistically.

Operational Framework Considerations

A thorough IPB effort and intelligence analysis assist each echelon in focusing operations on all significant aspects of the OE in time and space across multiple domains. This prevents each echelon from focusing only on the close fight and current operations. A broad focus across the operational framework considerations assists commanders and staffs in better identifying friendly windows of opportunity and threat windows of vulnerability within and across each domain and the information environment. An *operational framework* is a cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations (ADP 1-01).

Table 1-1 lists the operational framework considerations and how IPB and subsequent intelligence analysis support each consideration. (See FM 3-0 for details on operational framework considerations.)

Operational framework considerations	*Intelligence preparation of the battlefield (IPB) and intelligence analysis support*
Physical considerations include geography, terrain, infrastructure, populations, distance, weapons ranges and effects, and known threat locations.	• Intelligence support begins well before the deployment of forces, through generate intelligence knowledge, which addresses the operational variables. Information gained during generate intelligence knowledge is used by commanders and staffs to assist in framing the operational environment during the Army design methodology. • IPB provides detailed analysis of the mission variables of threat, terrain and weather, and civil considerations to determine effects on operations. • IPB and intelligence analysis assist in determining relevant aspects within an area of operations (such as civil considerations characteristics) that are critical in determining how friendly operations may be impacted during the consolidation of gains. • Intelligence analysis is critical to the designation of a deep area, the fire support coordination line, and the area of interdiction.
Temporal considerations are related to time, including when capabilities can be used, how long they take to generate and employ, and how long they must be used to achieve desired effects.	• IPB is a process that is both geographically and temporally specific. • Developing threat courses of action during IPB is based on identifying threat objectives, goals, timelines, and end states. • IPB provides a temporal context using rates of movement, time phase lines, phases of threat fires, and other templates to capture threat timing.
Cognitive considerations relate to people and how they behave. They include information pertaining to threat decision making, threat will, the nation's will, and the population's behavior.	• IPB accounts for aspects associated with the center of gravity and the threat's morale and willingness to continue operations. • Intelligence support to continuous operational assessments considers many relevant aspects of the operational environment, including sociocultural factors. • IPB also considers all significant aspects of the operational environment associated with the various civil considerations.
Virtual considerations pertain to activities and entities, both friendly and threat, residing in cyberspace.	• IPB and intelligence analysis, in coordination with the cyberspace electromagnetic activities section, provide intelligence on the threat's likely activities within the information environment, which includes cyberspace.

Table 1-1. IPB and intelligence analysis support to operational framework considerations