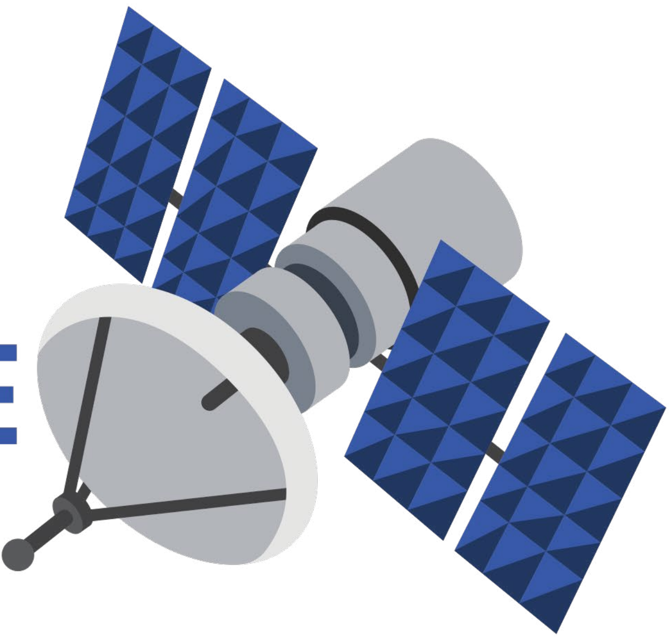
INTEGRATING SPACE DOMAIN CONSIDERATIONS INTO INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT



FIRST LIEUTENANT TAYLOR A. REIHELD
& CHIEF WARRANT OFFICER 3 ANDREW R. GARLAND

Introduction

The importance of the space domain to the 21st-century military has been well-documented and thoroughly described. Unfortunately, all too often it is considered a separate entity, distinct from the established warfighting functions. This is, however, a misguided perception. In fact, the space domain provides both complementary and reinforcing capabilities to the warfighting functions. This artificial distinction leads to many aspects of the space domain being overlooked or inconsistently applied, if not intentionally disregarded, especially among the warfighting elements whose connection to space may not be immediately apparent.

Maneuver commanders have a variety of factors to consider as they make decisions. They rely on their intelligence staff to supply fully developed intelligence preparation of the operational environment (IPOE) products to support that decision making. The intelligence staff can improve their standard IPOE products by integrating space domain considerations. They can then present these products to maneuver commanders in familiar ways without requiring any specific training.

Intelligence Preparation of the Operational Environment

Chapter 8 of ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, contains considerations for the space domain within operational environments. It focuses on the relevant physical aspects of the environment, space weather, and space weather phenomena.[1] This article, while not claiming to be all-inclusive, intends to expand the Army Techniques Publication's discussion.

Step 1: Define the Operational Environment. Analysts can incorporate space domain considerations meaningfully when describing the significant characteristics of the area of interest and the area of operations. Topography, terrestrial weather, and space environmental effects can all affect signal transmission between orbiting satellites and the users below. Will the sheer size of the area of operations require satellite-enabled communication? Does the area of operations include terrain features that could inhibit direct, point-to-point communications? Will the prevailing climate conditions influence those communications? Analysts should also consider space-related facilities when assessing critical infrastructure, as an unassuming neighborhood office building could be the access point to worldwide communication and influence.

Step 2: Describe the Environmental Effects on Operations. The five military aspects of terrain are observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment, commonly referred to by the acronym OAKOC.[2] Space domain considerations influence all five aspects, which can, in turn, influence some space systems.

Observation and Fields of Fire. Space-based and space-enabled assets can expand the conditions under which the battlefield can be observed. Radar can penetrate cloud cover, haze, smoke, darkness, and even foliage to provide persistent, near real time observation beyond line-of-sight. The commercialization of space has made these capabilities available to nonstate actors and states that may not have access to governmental reconnaissance satellites. At least one commercial imagery provider offers synthetic aperture radar imaging with frequent updates available.[3]

Avenues of Approach. Space-based and space-enabled assets can also shed new light on potential ground-based avenues of approach. Besides the obvious benefit from updated overhead photography, commercially available assets can provide polarized imagery. Polarization can help, for example, by differentiating between trafficable grassland and severely restricted forests, despite both appearing as similar "green spaces" on overhead visual imagery.

Key Terrain. Key terrain can include threat communications nodes that restrict information flow. At least seven countries have tried, or intend to try, to isolate their civilian population by restricting internet connectivity through a centralized, state-controlled infrastructure.[4]

Obstacles. Electromagnetic obstacles are an entirely new entry in this category. Intentional adversary action is a more usual concern, but terrain conditions can also impinge electromagnetic signals. Most notably, global positioning systems (GPS) are susceptible to multipath errors, which occur when a GPS signal reflects to a GPS receiver and provides information based on the reflected location instead of the actual location. This is a common phenomenon in cities, where the vertical metal and concrete in tall buildings and overpasses create "urban canyons" that can confuse and disorient GPS systems, but the issue can also arise over mountainous terrain, cliffs, and lakes. Inaccurate positioning can have disastrous consequences. As an example, the margin of error roughly doubles for GPS position fixes taken under coniferous trees versus open areas.[5] Careful terrain analysis should include areas where GPS signals may be disrupted or degraded, and these areas can be depicted on the modified combined obstacle overlay in the same way as restricted terrain.

Cover and Concealment. Traditional obscuration and camouflage can be effective from ground level but may present a different view to overhead assets. Space platforms surround the planet without regard for borders and boundaries, potentially providing adversaries with clear views of concealed positions. Additionally, space-based platforms may offer added sensor capabilities, unlike those expected to be available to the adversary. For example, as previously mentioned, commercial assets can provide polarized imagery that may discern differences between foliage and camouflage netting, with its value limited only by the turnaround time from imaging to exploitation.

Space Environmental Effects. Events in the space environment, sometimes known as "space weather," can impact maneuver operations. Radio and navigation signals can be disrupted, high-altitude aircraft in support roles may have to alter flight plans, and intelligence, surveillance, and reconnaissance (ISR) capabilities provided by satellites may be degraded by space weather. To varying degrees, analysts can incorporate these effects into the weather brief and weather effects matrix using information provided by the National Oceanic and Atmospheric Administration's Space Weather Prediction Center.[6]

Just as the space environment can affect terrestrial operations, the terrestrial environment can affect space operations. For example, some space assets are enabled by mobile transporter-erector-launcher vehicles, which are constrained by the well-known vulnerabilities inherent to ground vehicles. As another example, anyone who has used a modern satellite television service understands how severely Ku band frequencies can be affected by moderate to heavy rain. The high bandwidth of the Ku band makes it attractive for deployable satellite communication, but the wavelength is especially susceptible to interference from rain.[7]

Step 3: Evaluate the Threat. The purpose of this step is to identify capabilities available to the threat, and that must include space-enabled capabilities. Does the adversary have access to precise positioning, navigation, and timing? Can the adversary access national or commercial imagery sources to support their version of IPOE? Predicted overflights of adversary satellites are available using satellite reconnaissance advanced notice reports from the Army Space Support Team, typically found at echelons division and above.[8]

High-value and high-payoff targets are identified in this step and could include access points for space-based capabilities. For example, disrupting the electrical supply to a ground station could neutralize an otherwise unreachable multimillion-dollar orbital platform. The type, quantity, status, and location of any GPS and satellite communications signal jamming equipment should be identified to the greatest extent possible.

Step 4: Determine Threat Courses of Action. It is unlikely that space-enabled assets will significantly alter the adversary's objectives and desired end-state, but they could influence the selection of specific courses of action. Improved ISR may allow the adversary greater situational awareness, thereby increasing the feasibility of some courses of action. To properly consider the feasibility of potential threat courses of action, they should be fully developed so the impact of space-enabled assets is discernible. The likely courses of action should be compared to determine where events may occur that would differentiate between the potential courses of action. This will help support intelligence planning and collection.

Conclusion

The traditional steps of IPOE are complete, but the process is cyclical and iterative. As time and information allow, continue to refine and develop the product. Incorporating space domain considerations into this iterative process as early as possible can only improve the commander's decision making.

Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: Government Publishing Office, 1 March 2019), 8-4. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024.

2. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 3-6.

3. Umbra Lab, Inc., https://www.umbra.space/.

4. Liam Scott, "Repressive Regimes around the World Are Nationalizing the Internet and Isolating People," Authoritarian Tech, Newsletter, Coda, 18 October 2022, https://www.codastory.com/newsletters/breaking-up-global-internet/.

5. Christopher Deckert and Paul Bolstad, "Forest Canopy, Terrain, and Distance Effects on Global Positioning System Point Accuracy," *Photogrammetric Engineering & Remote Sensing* 62, no. 3 (March 1996): 317-321, https://www.asprs.org/wp-content/uploads/pers/1996journal/mar/1996_mar_317-321.pdf.

6. Space Weather Prediction Center, National Oceanic and Atmospheric Administration, https://www.swpc.noaa.gov/.

7. Patrick Gannon, "What Is Rain Fade?" *Satellite Industry Latest* (blog), *BusinessCom Networks*, 14 February 2018, https://www.bcsatellite.net/blog/what-is-rain-fade/.

8. "Army Space Forces–Enabling the Joint Warfighter," Association of the United States Army Background Brief No. 100, October 2004, https://www.ausa.org/sites/default/files/BB-100-Army-Space-Forces.pdf.

1LT Taylor A. Reiheld is an intelligence officer and assistant S-2 for the 1st Space Brigade at Fort Carson, CO. She holds a bachelor's degree in construction management.

CW3 Andrew R. Garland is an all-source intelligence technician assigned to the 1st Space Brigade S-2 at Fort Carson, CO. He previously provided intelligence support at the battalion, division, combatant command, and national agency levels, including three combat deployments. He holds a master's degree in U.S. history.