
HALL

The Army's Gap in Operational-Level Intelligence for Space as Part of Multi-Domain Operations

Maj. Jerry V. Drew II, U.S. Army

As the Army moves toward its strategic vision of a multi-domain force by 2028, it faces no shortage of challenges. Equipment modernization, maintaining a global presence, and training for large-scale combat operations are just a few of the most pressing challenges. In the midst of these efforts, the Army continues to support the establishment of a new combatant command for space operations while reevaluating its own roles and responsibilities vis-à-vis the space domain.

In this effort, there are many ideas for making space operations more effective for the ground force, but the need to reframe operational-level intelligence through the lens of space operations is one area that demands immediate consideration. Specifically, the gap exists in applying space domain considerations to operational-level intelligence processes. To become an effective multi-domain force, the operational-level Army must begin linking both strategic- and tactical-level space intelligence to plan the operational-level fight, to convey the Army's intelligence needs to the joint force, and to provide meaningful analysis to tactical echelons—as is currently done for ground and air threats.

For the operational-level Army today, the mental model of space intelligence largely equates to the tasking, collecting, processing, exploiting, and disseminating (TCPED) process. Operational-level intelligence professionals use this process to leverage intelligence, surveillance, and reconnaissance assets to inform the commander's decision-making for a ground campaign.[1] This process is certainly an important one, but it addresses only one aspect of space capabilities—the collection aspect—and it does not mirror the way in which intelligence professionals consider other domain capabilities in the intelligence preparation of the battlefield (IPB) process. In simplest terms, "space intelligence" should not be a separate effort but an institutionalized part of the overall intelligence effort for operational-level formations.

A more holistic view of operational-level IPB—one that includes the space domain—provides the opportunity to consider what expertise is necessary within an operational-level command and how the Army as an institution might begin to think about a clearly defined space operational environment, potential gaps in the understanding of the space environment's effects, and the enemy's multi-domain capabilities. This discussion is necessary to scope the current gap in the Army's operational-level intelligence, especially if the Army (and the joint force) is to become an effective multi-domain force capable of defeating enemies with space and counterspace capabilities.

Soldiers with 2nd Platoon, Company A, 1st Battalion, 503rd Infantry Regiment, 173rd Airborne Brigade Combat Team, set up a tactical satellite communication system 9 August 2010 in Shekhabad Valley, Wardak Province, Afghanistan. (Photo by Sgt. Russell Gilchrest, U.S. Army)

IPB Process

All Army commanders employ the IPB process that consists of four doctrinal steps: (1) define the operational environment, (2) describe the environmental

Medium earth orbit (MEO)

–Satellites are transient

–Satellites traverse the area of responsibility (AOR) in hours

–Example: GPS, global navigation satellite system (GLONASS) constellations

Geosynchronous orbit (GEO)

–Satellites are nearly stationary relative to the Earth's surface

–Satellites remain generally over the equator but provide services to the entire hemisphere

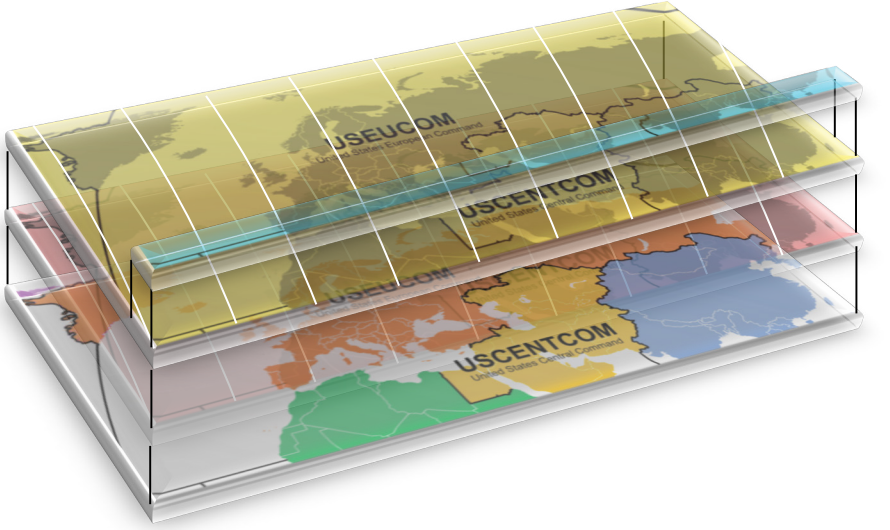
–Examples: wideband global satellite communication (WGS), ultra-high frequency follow-on (UFO) constellations

Low earth orbit (LEO)

–Satellites are highly transient

–Satellites traverse the AOR in minutes

–Examples: imagery satellites, the Iridium constellation



(Figure by author. This graphic depicts the three primary orbital regimes and provides the salient characteristics and typical mission types/constellations found in each.)

Figure 1. Initial Considerations for Defining the Orbital Aspects of the Operational Environment

effects on operations, (3) evaluate the threat, and (4) determine the threat courses of action.[2] For the extended, multi-domain battlefield, these steps take on new meanings uncodified in doctrine as yet.

Step 1: Define the operational environment. Since space operations encompass both on-orbit assets and globally positioned assets, the first problem that arises is attempting to define the operational environment in a meaningful way. In Army doctrine, the first step of defining the operational environment requires defining the commander's area of operations and area of interest (AOI). Importantly, the AOI is the area that is of concern to the commander and "from which information is required to facilitate planning and the successful conduct of the command's operation."[3] By this definition, the AOI of every operational-level commander includes portions of orbital space and possibly terrestrial locations of space assets in the AOR of a different combatant command. In addition, the orbital portion of the AOI has multiple layers that all interact differently with the ground force.

To begin understanding these layers, a deep/close/support operational framework may be a useful point of departure if adapted vertically. In the case of space operations, the framework translates into geosynchronous orbits (GEOs, ~23,000 miles from Earth) as the deep area and low-Earth orbits (LEOs, up to 1,000 miles from Earth) and medium-Earth orbits (MEOs, ~12,000 miles from Earth) as the close area.[4] This close area could be further subdivided into close-LEOs and close-MEOs.

Figure 1 depicts these orbital regimes and provides the salient characteristics and typical mission types/constellations found in each. Importantly, GEO satellites (e.g., many communications satellites) remain relatively stationary over their equatorial orbital slots, but satellites in the other two orbital regimes become more transient as their altitudes decrease. As a result, LEO satellites may traverse over an AOR within minutes and require

different considerations in the IPB process (e.g., shorter uplink or collection windows) than the GEO satellites. The ground stations that control these satellites or channel data from them constitute the "support area," but this support area will be noncontiguous; ground stations may be in the corps' consolidation area, the theater army's joint security area, or the strategic support area. Following this line of thinking, the operational-level commander now has a horizontal deep/close/support/consolidation construct and a vertical deep/close/support construct to frame the operating area.

Step 2: Describe the environmental effects on operations. Broadly, space operations require consideration of space environmental effects and terrestrial environmental effects. The space environment may affect the space and link segments of space systems, and the terrestrial environment may affect the link and ground segments of space systems. Intelligence professionals will likely be more familiar with terrestrial environmental effects, but as with the terrestrial environment, the space environment can and does affect military operations.

Gravity itself is the dominant physical force within the space environment. Because of gravity, the orbital patterns of satellites are repetitive and are therefore predictable for both friendly and enemy assets. Furthermore, it is because of their gravitational properties that GEO locations are highly valuable. Planners should consider the orbital slots themselves for designation as key terrain; the satellites in those slots may qualify as critical/defended assets.

If gravity was the only consideration, the space environment would be fairly benign, but three other factors contribute to the space environment's general harshness: extreme temperatures, solar and galactic radiation, and sixty years of orbital debris. Because of these factors, satellites may fail in orbit at any time, and it is thus important for intelligence and operational planners to address contingencies for the potential loss of space systems that bear directly on the mission. Thankfully, the temperatures a satellite will experience are fairly predictable, and engineers build satellites to withstand these anticipated temperatures.

Solar activity, however, is largely unpredictable. Such activity may disrupt normal function of the satellite by causing errant electrical discharges within the spacecraft. Solar activity may also affect the link segment either directly, by interfering with the signal as it travels through space, or indirectly, by causing charging of the ionosphere—which degrades space-to-ground communications. Since disruptions related to solar activity are as hard to predict in advance as solar activity itself, it is best to develop robust communications plans, especially for those systems whose signals may be affected.[5]

Orbital debris routinely puts satellites at risk. To protect on-orbit assets, maintaining situational awareness in space, largely through ground-based radars, is an essential support mission for successful space operations, and intelligence planners should keep in mind the Combined Force Space Component Command (CFSCC), the unit responsible for space situational awareness, as a source of intelligence.

Inside the atmosphere, the assessment of environmental effects must also include terrain and weather effects on both the link and the ground segments of space systems. For these segments, terrain may block GPS or satellite communications (SATCOM) signals—effects that organic, operational-level space staff can model throughout planning and execution. Terrestrial weather, of course, brings its own effects. For space systems, rainstorms may limit SATCOM connectivity on certain frequencies, employment options for mobile space or counterspace assets, and launch timetables. Furthermore, cloud cover or periods of limited visibility may hinder imagery collection and delay satellites' warnings of missile launches. As with a communications plan, the intelligence collection plan and the theater missile warning/defense plan

Maj. Jerry Drew, U.S. Army, is the battalion operations officer (S3) for 1st Space Battalion, 1st Space Brigade. He holds a BS in art, philosophy, and literature from the U.S. Military Academy and an MS in astronautical engineering from the Naval Postgraduate School. Additionally, he is a 2017 Art of War Scholar and a 2018 graduate of the School of Advanced Military Studies. In his previous assignment as a planner for the U.S. Army Space and Missile Defense Command G5, he led the planning team that transitioned Army Service Component Command support to U.S. Space Command (USSPACECOM) and served as an original member of the planning teams that established USSPACECOM and conducted initial planning for the U.S. Space Force.

must consider the limitations of available assets and the possibility of employing alternate means. Furthermore, friendly key terrain (on the ground) may demand measures designed to protect them from space-based surveillance (e.g., camouflage, radio silence procedures, military deception, or counterspace operations).

Finally, civil considerations come into play with space operations just as they do with traditional fire and maneuver. Does the civilian population get its information from government-controlled satellite broadcasts? Are there local television or radio stations that ground forces could commandeer? How vulnerable are ground stations to peering locals or projected refugee flow patterns? How will the local use of electromagnetic radiation affect the ability of friendly forces to operate in the way that it wants (green-on-blue interference)? For that matter, how will the use of friendly systems interfere with other friendly systems (blue-on-blue interference)? All of these questions require consideration to holistically assess the environmental effects. Figure 2 provides a synopsis of general battlefield effects of the space environment and of the terrestrial environment on space systems.

Step 3: Evaluate the threat. Doctrinally, space systems consist of three segments: the space segment (satellites), the ground segment (control and data processing stations), and the link segment (the electromagnetic radiation that connects the two and allows for the passage of data). Closely tied to—but not part of—the space system are the servers, networks, and software programs that allow for the transfer of data from ground site to ground site; these elements are within the cyber domain but bear consideration in both the conduct of space operations and in multi-domain IPB.

Just as with ground operations, a space-centric evaluation of the threat requires extensive knowledge of the enemy's order of battle (OOB) for all segments and the manner in which the enemy typically employs their forces. Thus, just as large-scale combat operations require OOBs, doctrinal templates, and situational templates for the enemy ground force, multi-domain operations require the same basic products for the enemy's space forces. At present, the most significant limitation to holistic analysis is the development of the four constituent OOBs for enemy space forces: satellite, link segment, ground segment, and cyber segment. As the cyber segment falls outside of the space domain, it is not herein addressed in detail. However, each of the other OOBs bears explanation.

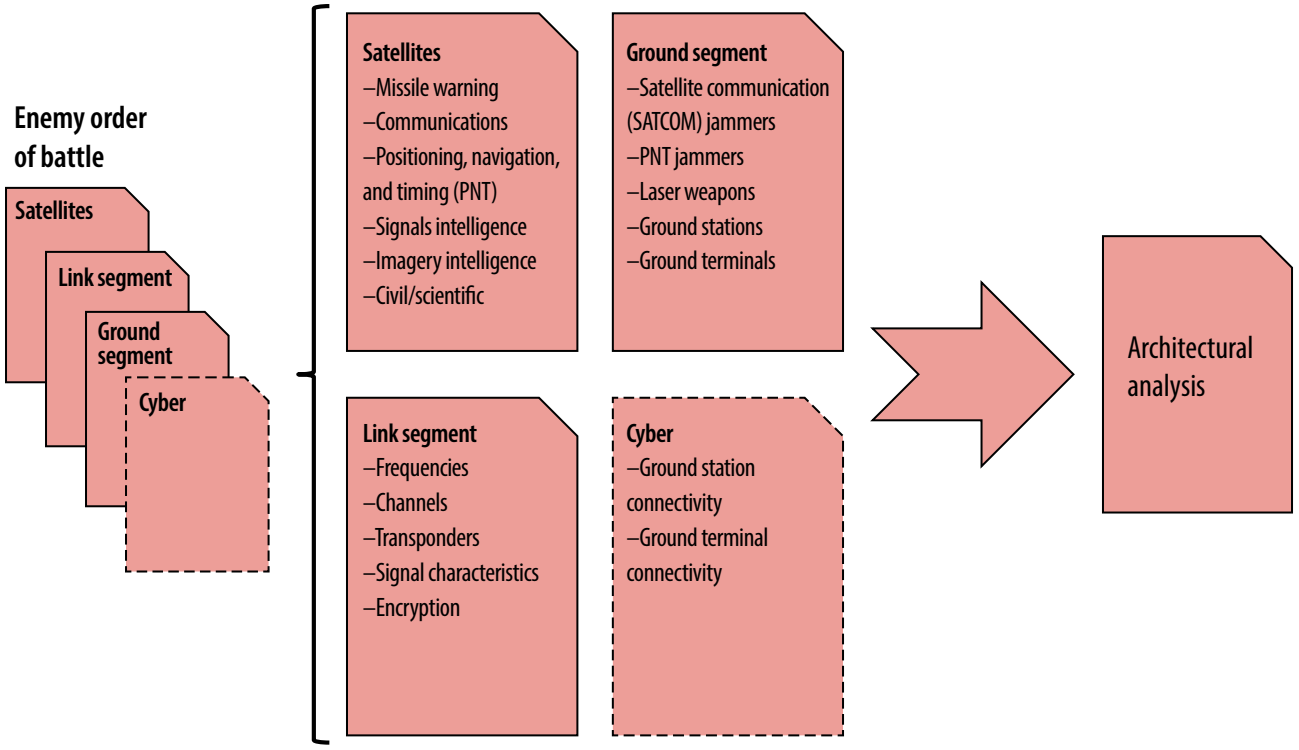
1. Due to gravitational effects, orbital patterns repeat and are therefore predictable. Geosynchronous orbits are highly valuable and should be considered for designation as key terrain; the systems in those slots are likely candidates for critical/defended asset designation.
2. The harshness of the environment may cause spacecraft failure at any time; robust alternate, contingency, and emergency plans are necessary for all systems.
3. Orbital debris may put satellites at risk; space situational awareness is essential for protection of on-orbit assets.
4. Solar activity may disrupt normal satellite operations/signal propagation, causing perception of intentional interference.
5. Terrestrial weather may interfere with certain transmission frequencies; employment of mobile space/counterspace assets; and conduct of reconnaissance, early warning, and launch missions.
6. A crowded electromagnetic spectrum may cause interference with space-based signals.
7. Civil populations may depend upon satellite systems for information/entertainment; ground stations may be vulnerable to negative public opinion, hostile observation, or refugee flow.

(Figure by author)

Figure 2. Initial Considerations for Defining Space Domain Environmental Effects on Operations

An enemy satellite OOB may take on many forms. A satellite OOB may group satellites by orbital regime, ownership, function, or some combination thereof. An orbital regime grouping would divide capabilities along the lines of orbits described above (GEO, MEO, LEO) with the addition of a fourth type of orbit, the highly elliptical orbit, which is particularly useful for polar surveillance or communications.

An ownership grouping would divide satellites by who operates them. Typically, satellites belong to



*A comprehensive order of battle will drive intelligence collection, the targeting process, force protection measures, development of options for the joint force commander, and an appreciation for the options available to the enemy.

(Figure by author. The graphic outlines a framework of the products and analysis that emerge from step 3 of the intelligence preparation of the battlefield process. Though not a constituent part of the space order of battle analysis, the cyber order of battle is necessary for a complete architectural analysis.)

Figure 3. Evaluate the Threat Products and Analysis Framework

four types of owners: militaries, intelligence communities, civil-government agencies (e.g., the National Aeronautics and Space Administration or the National Oceanic and Atmospheric Administration), or commercial entities (e.g., Intelsat, Iridium, and Eutelsat). In large-scale combat operations, all government satellites of the enemy may be legitimate targets, and it may be possible to target commercial assets, depending on circumstances. It may, however, not be wise to target all types. A Cold War norm, for example, holds that the targeting of an enemy's strategic missile warning satellites may be viewed as a prelude to a nuclear strike.

The third type of grouping is by function. Satellites that support joint operations include communications; missile warning; position, navigation, and timing; intelligence, surveillance, and reconnaissance; and environmental monitoring. Satellites with an attack function, so-called kamikaze or "kidnapper" satellites, form another category.[6] According to the Union of Concerned Scientists, approximately two thousand operational satellites currently orbit Earth.[7] Simply maintaining situational awareness of all these satellites (not to mention other orbital debris that require tracking) is a full-time endeavor; translating what this information means to an operational-level commander is an entirely different effort that requires a significant dedication of resources.

If the prospect of compiling and analyzing a comprehensive satellite OOB is daunting, doing the same for a comprehensive link segment OOB may be nearly impossible. Satellite links come in two broad types: command-and-control links to manage satellite operations (uplinks) and data links that provide the data that fulfills the satellite's purpose (downlinks). Communications satellites, for example, operate through a command-and-control uplink. To fulfill its downlink function, a satellite may use multiple beams, channels, frequencies, waveforms, and types of encryption. Furthermore, controllers switch users from channel

to channel or from frequency to frequency as the mission requires. Again, building the catalog is only part of the problem. Determining which part of the catalog is relevant to the operation at hand and how to make it operationally useful is a problem that requires a full-time commitment and expansive employment of signals intelligence assets and experts.

The results of step 3 will reveal options:

1. On-orbit options may include repositioning satellites to optimize the constellation or employing an on-orbit space situational awareness satellite to observe a particular satellite of an adversary.
2. Within the link segment, the enemy may reprioritize user traffic, reduce the size of their beams to focus support and reduce vulnerability to jammer attack, or update encryption protocols.
3. Ground-based options may involve the employment of jammers, the displacement of ground-station operators to more secure facilities, or preparations for the launch of a new satellite to provide additional capability.

Consideration of these options by phase/effort allows planners to develop holistic, multi-domain enemy courses of action, which will, in turn, drive comprehensive friendly courses of action.

(Figure by author; a synopsis of general threat options that may combine with other domain options to form a holistic threat course of action.)

Figure 4. Determine Threat Courses of Action

Finally, the ground segment bears consideration, and for this analysis, the operational-level Army is better postured. While numbers of enemy infantry divisions, armored brigades, and bridging assets are important, so too are the enemy's ground-based space assets. This OOB includes ground stations for satellite control and data processing, the headquarters that give the ground stations their orders, fixed and mobile SATCOM jammers, GPS jammers, and ground-based lasers or antisatellite missiles. Also included in the ground segment are radar and optical sensors that track satellites in order to maintain the orbital catalog. For the ground segment, the discipline of navigation warfare (NAVWAR) becomes particularly important. NAVWAR deals with understanding how friendly and enemy forces use position, navigation, and timing data to enhance operations. For example, the enemy may use GPS or a variety of GPS-like systems to employ precision-guided munitions, to achieve accurate timing for their encryption systems, or to command and control ground forces (as U.S. forces do through Blue Force Tracking systems). A detailed investigation of NAVWAR capabilities often involves the study of specific types of warheads, radios, receivers, or other hardware.

With comprehensive space, link, and ground-segment OOBs available, the next step is to piece together the enemy's space systems architectures. Each constellation—sometimes each individual satellite—will have its own architecture for command and control and for data dissemination. With a complementary cyber OOB, the architecture becomes more complete. These architectures become part of the threat models that are the output of step 3 of the IPB process.[8] A second type of threat model that emerges is the concept of how enemy operations might employ their ground-segment forces, particularly mobile counterspace systems. Figure 3 (on page 75) depicts a schematic of the products and analysis that emerge from this process, which feed into step 4 of the IPB process.

Step 4: Determine the threat courses of action. With an agreed-upon definition of the expanded battlefield, an understanding of its effects, and a comprehensive threat evaluation, the next step is to determine the threat courses of action. These courses of action, of course, are situationally dependent, so a general discussion of possible enemy options must suffice. On-orbit options may include repositioning satellites to optimize a constellation of satellites or employing an on-orbit space situational awareness satellite to observe an enemy satellite. Ground-based options may involve the employment of jammers, the displacement of ground-station operators to more secure facilities, or preparations for the launch of a new satellite to provide additional capability. Within the link segment, the enemy may reprioritize user traffic, reduce the size of their beams to focus support and reduce vulnerability to

jammer attacks, update encryption protocols, or offload military traffic onto commercial systems.

At the operational-level, integrating these space-domain options into a wider course of action that considers all domains is essential. Very often, the traditional maneuver and fires plan emerges with concepts for the other warfighting functions, and space and cyber aspects are "bolted on" near the end of the process. Without courses of action that include enemy space options, however, operational-level intelligence planners cannot develop holistic courses of action that force the ground formation to anticipate the enemy across all domains. Figure 4 (on page 76) provides a synopsis of the discussion on step 4.

"At the operational-level, integrating these space-domain options into a wider course of action that considers all domains is essential."

Who Is Responsible and for What?

By function, strategic-level organizations like combatant commands focus on joint processes, which are more holistic; as a consequence, they are less detailed. Tactical-level organizations, like Army divisions, focus primarily on their domain-specific segment with consideration of the most relevant capabilities of the other domains (e.g., air support capacity throughout the operation). As one might expect, Army divisions dedicate significant effort to detailed understanding of the battlefield and the enemy's potential within it. Linking the strategic level and the tactical level, however, are the operational-level commands, and this is where the connective tissue in the intelligence picture of the space domain is lacking across the Army.

Presumably, three types of Army formations bear the responsibility for conducting operational-level IPB: the field army, Army corps headquarters, and the Army service component command (ASCC). Among these, the United States currently only fields one field army, the Eighth Army in South Korea. Given the proximity and nature of the threat this field army faces, its IPB is singularly focused. On the other hand, while the Chinese and Russians field significant space-based capabilities that bear consideration in the regional analysis, the North Koreans have little to speak of, except counterspace systems.

According to Field Manual 3-94, *Theater Army, Corps, and Division Operations*, "a corps headquarters is the Army's predominant operational-level formation," but it can also serve as a tactical-level formation as part of a joint or combined force land component command.[9] In either role, it prepares for combat operations that control multiple divisions and support assets based on its theater planning priorities. I Corps, for example, aligns to U.S. Indo-Pacific Command planning priorities and is currently leading the Army in its multi-domain task force (MDTF) experimentation. Although a tactical element, the MDTF, with its organic intelligence, information, cyber, electronic warfare, and space (I2CEWS) battalions, seems a likely candidate to contribute to operational-level intelligence for space operations, but it will require significant support from its corps headquarters and possibly from ASCCs with which its corps headquarters will be in coordination.

It is important to note that ASCCs currently come in two types: ASCCs to functional combatant commands and ASCCs to geographic combatant commands (or theater armies). The functional ASCCs are presently U.S. Army Special Operations Command, Surface Deployment and Distribution Command, and U.S. Army Space and Missile Defense Command (USASMDC). The rest of the Army's ASCCs (including the U.S. Army Cyber Command) are designated theater armies, though the U.S. Army Cyber Command, in its organizational structure and mission sets, exhibits a functional flavor.[10]

Among these ASCCs, USASMDC retains the preponderance of the Army's space operations personnel and significant intelligence production capabilities and seems to have the greatest responsibility for linking strategic intelligence of the space domain to tactical

action. As a peer organization to the theater armies, USASMDC formally serves as a force provider of allocated forces and a supporting organization for things like satellite communication management. Informally, however, USASMDC often provides modeling and analysis, opines on tactics and techniques for the employment of low-density assets, and incorporates feedback from the field for capability development. Additionally, it enjoys a close working relationship with the CFSCC, which is currently an operational-level space organization under U.S. Space Command (USSPACECOM). While important resources in the quest for comprehensive operational-level space intelligence, neither USASMDC nor the CFSCC currently have the capacity or the mandate to answer the operational-level space intelligence needs of the Army; and despite the formal establishment of the U.S. Space Command, it will likely require multiple years to achieve full operational capability.

Conclusion

Given the current organization of the operational-level Army, the designated need for a holistic approach to multi-domain IPB, and a shortage of institutional expertise and capacity, the Army faces a gap that may prohibit it from achieving a multi-domain force by 2028. The roadblocks to operational-level space intelligence practices result from the institutionalization of a faulty model on what space intelligence is, namely the TCPED process. While strategic-level organizations (the Defense Intelligence Agency, the National Security Agency, and others) provide some of the pieces to the space intelligence puzzle (and tactical-level organizations provide others), the connective tissue between the strategic and tactical is missing. The establishment of USSPACECOM has created a military-strategic organization responsible for space, and it seems highly possible that USSPACECOM—at some future date—will be the keeper of the master order of battle and the majority of the Department of Defense's military space expertise. Furthermore, it will coordinate with other combatant commands through formal integrated planning elements, which will augment combatant command staffs throughout the operations process. At tactical echelons, the MDTF with its intelligence, information, cyber, and electronic warfare and space battalions will execute space activities and will likely aid in intelligence collection. But what is in the middle?

It is apparent that a part of the solution is institutional change. The military intelligence community should reevaluate its training programs for space- and cyber-specific skills, and the Defense Intelligence Agency should reevaluate its distribution of responsibilities through a revised Defense Intelligence Analysis Program—one that probably shifts significant space-related TCPED responsibilities to U.S. Space Command. But traditional notions of space operations and a revised Defense Intelligence Analysis Program will not be sufficient for the operational-level Army. Effective incorporation of space systems requires a reconception of the extended battlefield and how to divide responsibilities within it. It further requires a holistic approach to order-of-battle development—the space, link, and ground segments—and an understanding of the architectures that allow them to operate. Such an understanding is essential for friendly as well as enemy forces. With this work done—which is essentially the first three steps of the IPB process—planners can incorporate space operations options into multi-domain courses of action.

The operational level of the Army must be among the first to adopt these changes and must strive to incorporate them into its routine processes. While each of these formations contain both military intelligence and space operations personnel, the intelligence personnel are not typically space experienced, and the space personnel do not typically have an intelligence background. Thus, in cases where space support elements enjoy better-than-average integration with their intelligence partners, the results seem to be in spite of institutional norms not because of them. USASMDC and CFSCC provide valuable resources but neither their structure, capacity, nor designated missions allow them to fulfill the needs of the Eighth Army, the three Army corps, or the eight other ASCCs.

Moving forward, theater armies should insist upon conceptual clarity on the definition of the extended battlefield, including the space portion, within their combatant commands. These concepts are not yet doctrinally defined (a problem for USASMDC to address), and no battlefield frameworks seem quite adequate for the task, although the deep/close/support/consolidation framework may provide a useful starting point. Theater armies should continue to focus on the ground threat and demand support for more extensive space (and cyber) orders of battle. In this effort,

national agencies, USSPACECOM (potentially with a dedicated military intelligence formation organic to it), USASMDC, and CFSCC have parts to play. As global commands, however, these organizations will not have an appreciation for the theater-specific problem sets of the other operational-level commands. Albeit with support through integrated planning elements, allocated forces, and reach-back support, it remains the responsibility of the theater armies to map the intelligence to their particular problem sets and to determine what it means to their projected courses of action.

Regardless of any changes that may or may not occur within the intelligence and space enterprises, the Army will continue to move toward its vision of a 2028 multi-domain force. Space operations are essential to that vision, but gaps that exist in current models and processes may preclude their effective incorporation into the multi-domain fight. It is certainly true that intelligence gained from strategic space systems is essential to the manner in which the joint force wages military operations, but viewing space systems simply as process enablers causes them to be overlooked as critical pieces of the multi-domain operations puzzle. Thus, the Army, as an institution, must address this shortfall to prepare ground combat commands for an uncertain future. ■

Notes

1. The Defense Intelligence Agency manages this process through the Defense Intelligence Analysis Program, which allocates and prioritizes resources across the intelligence community. For example, if U.S. Transportation Command requires geospatial intelligence products, the Defense Intelligence Analysis Program provides for the command to have an external intelligence node that conducts tasking, collecting, processing, exploiting, and disseminating on behalf of the U.S. Transportation Command and provides the command with the desired finished product. This model assumes that space-based intelligence formations do not need to be organic to a particular formation, effectively allowing the Defense Intelligence Agency to outsource this capability on behalf of combatant commands.

2. Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. Government Publishing Office [GPO], 2019), 1-3. Within the context of multi-domain operations, the word "battlefield" itself may imply a false limitation. The Marine Corps' use of "battlespace" or the joint force's use of "operational environment" are more precise terms. The March 2019 version of ATP 2-01.3 retains "battlefield" in the process name but considers the entire operational environment; this is a significant change from the 2014 version of the same publication. The analytical planner or operator must be willing to consider an extended battlefield—one that potentially extends into outer space.

3. Ibid., 3-4. To add to the confusion, areas of operations and areas of interests (AOIs) are operating areas within the area of responsibility (AOR). The commander of the U.S. European Command, for example, is responsible for an AOR as defined in the Unified Command Plan. Prior to the most recent update to the Unified Command Plan, the commander of U.S. European Command was notionally responsible for everything within those defined boundaries—from the bottom of the ocean to the furthest reaches of space. In the most recent update to the Unified Command Plan, the U.S. Space Command AOR was defined as orbital space with altitudes greater than one hundred kilometers. In the future, it is possible that AORs may disappear as a construct altogether. In any event, as a practical matter, an operational-level commander has to consider an AOI for space that is physically and psychologically removed from traditional notions of AOIs. The March 2019 revision of ATP 2-01.3 aids greatly in fostering such a mindset.

4. For additional details on these orbital regimes, see figure I-1, "Orbit Type and Characteristics," in Joint Publication 3-14, *Space Operations* (Washington, DC: U.S. GPO, 10 April 2018), I-11.

5. Although difficult to predict in advance, the Air Force Weather Agency is able to monitor and assess solar activity after it happens. This function is important because it can rule out the possibility of intentional interference, an enemy activity that drives the decision cycle.

6. Jim Sciutto and Jennifer Rizzo, "War in Space: Kamikazes, Kidnapper Satellites and Lasers," CNN, updated 29 November 2016, accessed 1 June 2019, http://www.cnn.com/2016/11/29/politics/space-war-lasers-satellites-russia-china/.

7. "UCS Satellite Database," Union of Concerned Scientists, updated 31 March 2019, accessed 1 October 2019, https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.XES1xvZFxYc.

8. See ATP 2-03.1, *Intelligence Preparation of the Battlefield*, para. 5-20. It is worth noting that the previous version of ATP 2-03.1, *Intelligence Preparation of the Battlefield/Battlespace* (2014), the Marines adopted the term "adversary model" instead of "threat model," which lends itself toward a more expansive application of the intelligence preparation of the battlefield process across the continuum of conflict.

9. Field Manual (FM) 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. Government Printing Office, 2014), 1-2; FM 3-0, *Operations* (Washington, DC: U.S. GPO, 2017), 2-11.

10. For outlines of the specific roles and responsibilities of each of these Army service component commands, see Army Regulation 10-87, *Army Commands, Army Service Component Commands, and Direct Reporting Units* (Washington, DC: U.S. GPO, 2017).