NEWS FROM THE FRONT

28 October 2018

Theater Intelligence Primer

Theater Strategy and Campaigning

COL Mark Haseman
Department Of Military Strategy,
Planning and Operations
U.S. Army War College

Theater Intelligence Primer
22 October 2018

The intent of this primer is to educate commanders and senior staff to be involved, supportive consumers of intelligence. The goal is not to repeat doctrine—although doctrine references are noted. To quote from the introduction of the classic book *Intelligence is for Commanders*, this is

> "written primarily for commanders, because intelligence is for commanders. Intelligence is not an academic exercise nor is it an end in itself. The prime purpose of intelligence is to help the commander make a decision, and thereby to proceed more accurately and more confidently with the accomplishment of his mission."

COL Mark Haseman
DMSPO, Editor

> As a commander, know the value of accurate intelligence, the methods by which it is produced, the manner in which it is used—and then insist on getting adequate service.
>
> LTG Manton Eddy
> *Intelligence is for Commanders*

Provide Focus to the Intelligence Enterprise.

A Combatant Command Commander (CCDR) should develop relationships with the defense intelligence enterprise and drive the intelligence effort. CCDRs need to specify intelligence priorities—both formally via Priority Intelligence Requirements (PIR), and informally in planning discussions. Each PIRs should include the decisions needed and the types of information that would facilitate such decisions. Commanders should identify PIRs as early as possible to focus limited intelligence resources, and the Commander and staff should frequently review PIRs and update them to match changing situations. Commanders should also integrate intelligence planners early in the planning process, and with the final plan, continue to engage them as they execute. Proactive intelligence professionals should work to understand what the J5/J3/CCDR needs, and share the tools they have available. Part of operations assessment involves answering the question, "How do I know if my plan is working?" The intelligence enterprise can contribute to this answer.

Example: The J2 worked with the CCDR and senior staff to develop formal PIRs that directly supported CCDR engagements and decisions. In addition, the CCDR huddled quarterly with his intelligence leaders informally to ensure that they understood topics of interest that he wanted covered in his intelligence feeds. (JP 2-0 I-7 to I-10)

The Intelligence Enterprise

The intelligence enterprise is a network of capabilities that helps develop understanding using data, information, and intelligence. From the CCDR's perspective, the intelligence enterprise comprises organic and external intelligence collecting and producing organizations and measures that complement or satisfy policies, processes, procedures, and products of the intelligence elements of the Joint Staff, CCMDs, Services, and other DoD elements that perform National Intelligence, Defense Intelligence, CI, security, and intelligence-related functions.

Optimizing the Intelligence Enterprise within the Combatant Commands

Within each Combatant Command (CCMD), a network of intelligence entities exists to support all intelligence operations. The CCDR can leverage these organizations to answer specified PIRs. Planning processes and feedback to analysts contribute towards a quality product and result.

Joint Intelligence Operations Center (JIOC). The JIOC is the CCMD's focal point for planning, synchronizing, and integrating all intelligence operations. Composition of JIOCs varies among CCMDs, but all have representatives from defense/national intelligence agencies. JIOC assets and functions include systems representing every intelligence discipline, indications and warning, current intelligence watch, analysis/production, collection management, processing, exploitation, dissemination (PED), targeting, foreign disclosure, Special Security Officer (SSO), intelligence mission management, and plans. (JP 2-0 III-6 to III-8; JP 2-01 II-3 to II-7)

Military Intelligence Brigades (Theater) MIB (T). The U.S. Army Intelligence and Security Command (INSCOM) provide intelligence support through seven theater MI Brigades OPCON to the Army Service Component Commands (ASCCs) that provide Intelligence support to units operating in the region.

- 66th MI Brigade: US Army Europe
- 513th MI Brigade: US Army Central
- 470th MI Brigade: US Army South
- 500th MI Brigade: US Army Pacific
- 207th MI Brigade: US Army Africa
- 505th MI Brigade: US Army North
- 501st MI Brigade: US Eighth Army

These brigades offer theater-level, multidiscipline intelligence collection, intelligence architecture, and data analysis to support unified land operations, security cooperation activities, and force protection missions.

Additionally, INSCOM provides support to the Army, Joint, and Interagency through the following MI Brigades:

- 902nd Military Intelligence Group (counter intelligence)
- 116th Aerial Intelligence Brigade (fixed wing ISR)
- 780th MI Brigade (Cyber)
- 704th MI Brigade (SIGINT)
- 706th MI Brigade (SIGINT)
- National Ground Intelligence Center (NGIC)

Joint Intelligence Preparation of the Operational Environment (JIPOE). JIPOE is the continuous process through which J2 manages the analysis and development of products that help the commander and staffs understand the complex and interconnected operational environment (OE)—the composite of the conditions, circumstances, and influences that affect the employment of capabilities that bear on the commander's decisions. JIPOE must be "front loaded" in the sense that the majority of analysis is completed early and factored into the commander's decision-making effort. JIPOE supports mission analysis by enabling the commander and staff to

visualize the full extent of the OE, to distinguish the known from the unknown, and to establish working assumptions regarding how adversary and friendly forces will interact within the OE. JIPOE also assists commanders in formulating their planning guidance by identifying critical OE factors, such as weather and terrain; the locations of key geography; environmental and health hazards; attitudes of indigenous populations; potential land, air, and sea avenues of approach; and considerations in the information environment. Analysts refine their assessments of adversaries' centers of gravity (COGs), potential enemy courses of action (ECOAs), and other factors. (JP 2-0 I-12 to I-18; JP 2-01.3 JIPOE)

The Intelligence Planning Process. The Intelligence Planning (IP) Process is integrated with the overall CCMD planning effort. The IP Process has a dual focus:

1: Providing Intelligence Support to Joint Operation Planning. This includes the production of intelligence assessments and estimates of adversary intentions, capabilities, and COAs. This requires integration of external DoD and intelligence community support into CCMD planning. Specific outputs include tailored products from the JIPOE process, which culminate in the production and maintenance of the intelligence estimate.

2: Planning Intelligence Operations. This includes identifying information gaps, prioritizing intelligence requirements, developing federated production and integrated collection plans, and assessing intelligence capabilities to identify shortfalls and mitigation strategies. Specific outputs are the CCMD J2 staff estimate (which identifies available CCMD intelligence capabilities and anticipated shortfalls), Combat Support Agency and Service intelligence center estimates, and the Annex B (Intelligence) to a campaign or a contingency plan. Additional outputs may include intelligence resource demand signals articulated through the CCDR's Integrated Priorities List or Request for Forces. (JP2-0 I-5 to I-18)

Feedback to Analysts. When an intelligence product is particularly useful (in other words it impacts planning COAs), its consumers should ideally provide positive feedback to the analysts. This helps the J2 analysts focus their efforts in key areas, and can lead to further Intelligence Community production in these areas. Conversely, intelligence consumers should also provide feedback when intelligence products are insufficient. Analysts disseminate Intelligence products to large audiences, so fixing errors or processes helps the team.

Example: Positive feedback on a line of reporting led to collection assets being refocused on a CCDR focus area. A flawed SIGINT report received an additional footnote that highlighted why the conversation contained incorrect information.
(JP 2-0 I-21 to I-22)

"Why" do you need this intelligence product? CCDRs sometimes ask follow-up questions about the intelligence they receive. It is useful to the J2 to have the context of why the CCDR made the request—what specifically the CCDR is looking for and to what end does the CCDR intend to use the intelligence? The same goes for requests to make intelligence products releasable—with whom does the CCDR intend to share it? The context provides those who are producing the follow-up products the parameters to work through those intelligence products. The Intelligence Community can tailor products to suit a commander's needs.

Example: Threat picture in Afghanistan for the British Deputy SACEUR was tailored at a high classification level. Iranian missile capabilities were produced at an unclassified level from open source documents, which enabled the commander to share threat ring graphics to a wide audience.

Considerations for Interacting with the Wider Defense Intelligence Enterprise

The intelligence community is eager to support theater commands. When a CCDR or senior staff requests a product, it gets high priority attention. CCDRs and staffs can enhance this responsiveness by building relationships with the IC during visits to Washington, DC and by inviting senior intelligence leaders to the theater. While the J2 staff might have analytic relationships within the IC, having command level attention cannot be beat.

Example: During a visit to DC, the CCDR met with the National Intel Officer for Europe and senior CIA European directors, which resulted in a series of products the CCDR desired. (JP 2-0 III-3 to III-4; JP 2-01 II-11 to II-27)

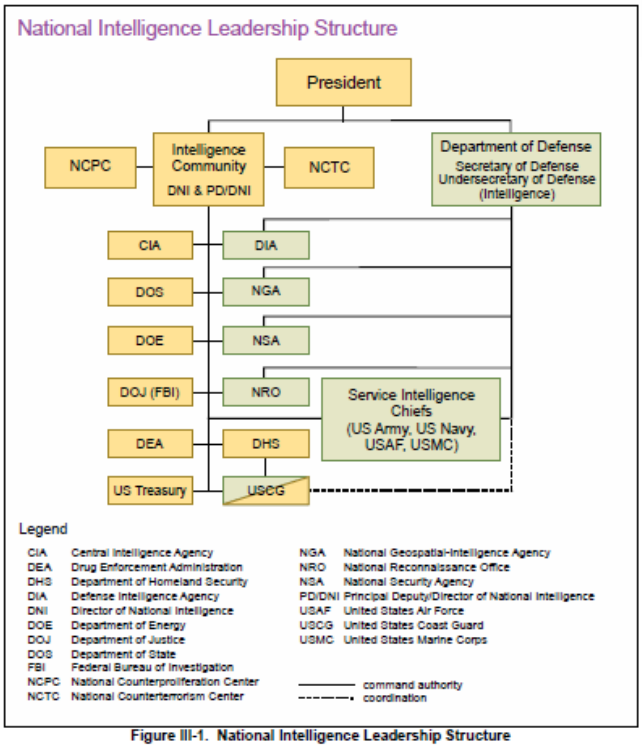

Figure III-1. National Intelligence Leadership Structure

Collaborative and Federated Production. A collaborative environment enables CCMDs to develop, coordinate, and integrate intelligence. A single CCMD JIOC often does not have enough personnel, resources, or analytic capacity for the effective production of comprehensive joint intelligence alone. Sometimes senior leadership will need to be involved to motivate federated production across CCMD organizations, multinational partners, and the Intelligence Community. This frequently requires permanent stationing of liaison personnel.

Example: When Russia moved into Syria, EUCOM had to work very closely with CENTCOM to determine who was responsible for what analysis. Intelligence analysts stationed in the continental US support the intelligence operations of a CCMD abroad. They may work the same duty hours as their counterparts in another country to stay on the same battle rhythm. (JP 2-01 II-7 to II-9)

Defense and Service Intelligence Centers. Defense and Service Intelligence Centers have the time, levels of expertise, and unmatched target knowledge to provide highly specialized intelligence on issues that the CCMD JIOC cannot supply. These organizations routinely work with other intelligence community members. These centers include:

- The National Ground Intelligence Center (NGIC)
- Marine Corps Intelligence Activity
- National Air and Space Intelligence Center
- National Maritime Intelligence Center

- Missile and Space Intelligence Center
- The National Center for Medical Intelligence

Example: NGIC produces scientific and technical intelligence and military capabilities analysis on foreign ground forces required by warfighting commanders, the force modernization and research and development communities, DoD and national policymakers. NGIC's general military intelligence mission focuses on foreign ground forces from the operational through small-unit level, maintaining detailed knowledge of current foreign ground force capabilities as well as a focus of 5, 10 and 20 years into the future. It includes irregular and conventional warfare analyses examining foreign ground forces from a perspective that includes battlefield operating systems, doctrine, tactics, techniques and procedures, training, maintenance, logistics and order of battle. NGIC's Foreign Materiel Program generates intelligence from foreign materiel which we acquire.

Demand High Quality, Predictive Analysis. Intelligence organizations can easily compile a vast quantity of data/information. CCDRs should demand the high quality analysis that goes further than assessing the environment and reporting on past events—they should get predictive analysis on problems the intelligence enterprise assesses are coming (percentage of confidence will vary with the intelligence available). The fusion of several different sources of intelligence results in higher quality products. Organizations must examine individual current intelligence reports in the context of trends/long-term analyses. The J2 can also provide alternative analyses and red team perspectives, which can illuminate dissenting opinions as well as theater and Intelligence Community positions. Intelligence professionals provide candid analyses and are able to speak truth to power—even if it is not what the command wants to hear.

Example: A CCDR expressed frustration with what he considered "Jane's Defense" type reporting and demanded all-source trends for future weapons development. Additional example: A single source report provided a slightly skewed perspective that was clarified by putting data into a comprehensive context, which included fused all-source and historical analysis. Regarding confidence levels examples: North Korea will not conduct another nuclear test in the next 6 months—assessed at low confidence (not supported by many trusted intelligence sources); whereas Russia will try a cyber attack against a NATO Ally in the next 6 months—assessed at high confidence (backed by several pieces of fused intelligence). (JP 2-0 II-12)

Intelligence Sharing. Try to base the decision on the extent to which you share intelligence on risk versus gain, on the sources, methods of collection, and the operational environment. Analysts must write United States intelligence information for release at the most appropriate classification level and given the fewest possible dissemination restrictions within foreign disclosure guidelines. The J2 must establish networks and procedures for efficiently separating shared intelligence from sources and methods. Intelligence agencies often use a "tear line" in classified reports to separate

compartmented information from intelligence that can be widely disseminated. Partner nations' intelligence systems can add unique and valuable capabilities, and can assist in establishing a multinational collection management element, which is crucial for coordination. Commanders have a role to play in evaluating trust and risk factors, forecasting sharing needs, emphasizing writing for release, fielding sufficient foreign disclosure officers (FDOs), and supporting acquisition of linguists. The Information Technology (IT) infrastructure, policies, and procedures must support the intelligence sharing effort in the organization's home location as well as in the deployed environment.

Example: ISAF J2 revamped bureaucratic procedures to expedite the sharing of threat information to coalition and Afghan partners. CENTRIX and BICES are examples of networks established for multinational sharing. A proposed initiative to extend CENTRIXS-K services from the Eighth Army command post to the ROK tactical forces would provide an immediate capability to the ROK forces to see the Combined Operational Picture. An example of poor intelligence sharing prior to 9/11 allowed information stovepipes denying the opportunity for a total threat picture to be developed. (JP 2-01 II-34 thru II-39)

Understand Intelligence Challenges and Limitations. Intelligence consumers often have misplaced expectations that intelligence should always provide warning of all threats and should accurately predict the future. However, intelligence has limited collection and analysis resources (ISR platforms, analysts, linguists, expeditionary bandwidth, etc), competing priorities, and differing consumer needs (national, theater, and tactical). Since the competition for limited intelligence resources can be intense, CCMDs must state clear, prioritized requirements. Within a CCMD, a collaborative relationship between the J2 and J3 on management of ISR collection assets is crucial; while the J3 side is in control of the assets, the J2 should get a vote before employment so valid intelligence or CCIR requirements are driving ISR operations.

Example: Commanders often weigh heavily on a favored collection asset which may not be the best, nor most accurate to provide the facts on the ground. ISR involves all modalities of intelligence collection—not just Full Motion Video (FMV). With the tyranny of distance in larger AORs, you may have the asset but you don't have the endurance/dwell time to cover the requirement. While many intelligence organizations remain threat focused, some have focused more on cultural and environmental factors—intelligence organizations in Iraq and Afghanistan formed elements to examine tribal, cultural, and environmental factors in the AO. (JP2-0 I-13 to I-15)

Intelligence Engagement. Intelligence is a powerful engagement tool, vital for key leader engagements and security cooperation. It often does not require large budgets or footprints. Many partners desire increased intelligence engagement with CCMDs, and these interactions can open doors to other engagements, especially when U.S. policy might restrict our interaction. Intelligence officers are often experienced with working through U.S. embassy cohorts—such as Defense Attaché Officers, Regional

Security Officers, and interagency representatives—and can assist with outreach efforts.

Example: Initiating a new intelligence engagement platform in Japan opened the door for the Japanese to engage with AUS, NZ, KOR, and the PHIL. It also served as the only mini-exercise which put the Japanese off island, in an expeditionary scenario. (JP 2-0 I-25 to I-26)

Intelligence Operations. Intelligence operations are "operations" (though often underappreciated). Comprehensive planners see the value of intelligence operations, which may lead to other activities (kinetic, influencing, or deception). Aggressive commanders use intelligence operations in day-to-day campaigning to shape further plans and generate opportunities for Cyber, IO, PSYOP, PAO, and engagement. (JP 2-0 II-4 to II-5)

Capturing Historical Information. Commanders and their staffs should recognize how vital their efforts are to the intelligence picture. Every interaction / key leader engagement is another inject into the complete picture of a situation. They should access the intelligence enterprise's resources to capture, store and analyze these activities. Intelligence personnel are adept at gathering, analyzing, and storing information that maneuver units collect in their day-to-day operations; thus, a commander's focus, determination, and advocacy for intelligence products is a critical variable in their effectiveness.

Example: Lessons from Bosnia, Kosovo, Afghanistan, and Iraq point to U.S. ground forces having excellent knowledge of critical infrastructure, key players, rivals, personalities, and trends...only to have that knowledge disappear when the unit rotated out of theater.

Crisis Intelligence. Often in crisis situations, the O3/O4 senior intelligence watch officer provides the immediate assessment of events in theater; therefore, there should be a good lash up between intelligence and operations counterparts, as well as a clear crisis response action SOP. *Overnight Ops-Intel briefs have proven to be good forcing functions to ensure information flow and avoid any waste of time or assets.* In the midst of a crisis, intelligence assessments may follow a simple outline such as: "here's what we know, here's what we don't know, and here's what we think." Collection assets could be required to shed light on what we don't know, or to improve confidence in what we think.

Example: We know which runways have been cratered, and what the adversary surface-to-air missile threat rings are; however we don't know what the adversary reaction would be to coalition flying in reinforcements—we think that the adversary will not shoot down coalition aircraft (75% confidence). (JP 2-01 Appendix A)

Conclusion

The Intelligence Enterprise consists of those intelligence collection, analysis, and production elements that are both internal and external to the CCMD. Those entities within the command are easier for the CCDR to access. However, the quality and accuracy of intelligence is bolstered by looking to the wider intelligence enterprise where in depth analysis and expertise resides. Finally, articulating the commander's requirements with clarity will yield the best result. Demonstrating the operational need, priority, and potential risks incurred gives analysts important context which contributes to higher quality intelligence products.

References:

(1) U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-0 (Washington, DC: U.S. Joint Chiefs of Staff, (October 22, 2013).

(2) U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01 (Washington, DC: U.S. Joint Chiefs of Staff, (July 5, 2017).

(3) Headquarters, Department of the Army, *Intelligence,* Army Doctrine Publication 2-0 (Washington, DC: Headquarters, Department of the Army, September 2018).

(4) Glass, Robert and Davidson, Phillip, *Intelligence is for Commanders* (Harrisburg, PA, Military Service Publishing, 1948).

(5) Decades of experience from Strategic Intelligence officers posted in theaters around the world.