FORWARD OBSERVER MANUAL SUMMARY

COMBAT COMMANDERS HANDBOOK ON INTELLIGENCE

ST 2-50.4 (FM 34-8)
U.S. ARMY INTELLIGENCE CENTER
SEPTEMBER 2001

FORWARD OBSERVER

Combat Commanders Handbook on Intelligence
ST 2-50.4 (FM 34-8)
U.S. Army Intelligence Center
September 2001
75 pages

Description: This manual is written primarily for combat commanders and their staffs involved in planning and executing operations in combat zones. Its purpose is to inform combat commanders of the options available to them regarding intelligence assets.

Much of the information contained in this manual is of no use or interest for community security planning, therefore information pertinent to low intensity conflict and community security will be outlined and summarized for your understanding.

For additional information, please visit https://forwardobserver.com or contact fostaff@forwardobserver.com.

Table of Contents

Notes for 'Chapter 1: The Intelligence Challenges for Commanders'

Intelligence is an invaluable tool available for commanders to help them plan operations and project force into an area or onto an enemy.

The purpose of an intelligence element is to provide timely, relevant, accurate, specific, and predictive or actionable intelligence to a commander. Armed with this intelligence, the commander is better able to make good decisions. (The intelligence element is the team or cell responsible for producing the intelligence.)

ISR refers to Intelligence, Surveillance, and Reconnaissance. Combat commanders must be able to understand ISR platforms -- things like sensors and drones -- and be able to plan and approve ISR operations so that these sensors can collect the information required to make a decision. (For instance, the commander who wants to move a platoon across a river might task ISR assets to find a bridge or suitable crossing point, if not already known.)

The commander who receives accurate intelligence and continuous information from ISR assets is more likely to understand the operating environment (weather and terrain, for instance) and the threat environment (the enemy situation). Commanders who don't have incoming intelligence will be blind to these changing conditions.

To facilitate this, the commander should plan and expect the intelligence element to do the following tasks:

Inform the commander of both the operating and threat environment:

- Perform Intelligence Preparation of the Battlefield (IPB), which helps the commander understand battlefield conditions.

- Perform Indications & Warnings (I&W), which provides the commander with early warning intelligence and helps prevent enemy surprises.

- Perform Situation Development, which allows the commander to understand the latest available information on the threat and their potential courses of action (COA).

Inform the commander with intelligence to effect targeting of the threat:

- Perform Targeting, which refers to either kinetic or non-kinetic (violent or nonviolent, respectively) actions in order to effect change on a threat. For instance, kinetic targeting could result in a kill or capture of an enemy, while non-kinetic targeting might influence a threat or potential threat to stop threatening activities.

- Perform Counterintelligence, which seeks to identify and disrupt enemy intelligence gathering capabilities. Identifying and countering enemy ISR assets -- whether human or mechanical -- will reduce the enemy's understanding of friendly operations, resulting in a higher likelihood of mission success.

Integrate ISR plans to increase the commander's situational understanding:

- Develop Priority Intelligence Requirements, which outline intelligence gaps (required information we don't already have), and prioritize them so that the information can be collected.

- Analyze Requirements and Resources Available, which refers to the management of intelligence collection. For instance, a commander who wants to confirm or deny that a bridge has been destroyed might approve of an ISR plan that sends overhead assets (like a drone) out to put 'eyes on' the area where the bridge is. But if the commander doesn't have an available drone, then he must analyze his available assets and choose a suitable alternative (such as a reconnaissance/scout element). As is often the case, there are too many intelligence requirements for available ISR assets to satisfy. In that case, our requirements have to be prioritized so that we are satisfying the most critical intelligence requirements first, and then secondary or less important intelligence requirements later.

- Develop ISR Plans, which refers to identifying suitable flight paths or other operational requirements, as in the case of sending out a reconnaissance or scout element. Availability, suitability, and survivability are among several considerations required prior to approving an ISR plan.

Notes for 'Chapter 2: Intelligence Preparation of the Battlefield'

Longstreet looked up the long rise. He could begin to see it. When the troops came out of the woods the artillery would open up. Long-range artillery, percussion and solid shot, every gun on the hill. The guns to the right, on the Rocky Hill, would enfilade the line. The troops would be under fire with more than a mile to walk. And so they would go. A few hundred yards out, still in the open field, they would come within range of skirmish, aimed rifles. Losses would steadily increase. When they reached the road they would be slowed by the fence there, and the formation, if it still held would begin to come apart. Then they would be in range of the rifles on the crest. When they crossed the road, they would begin to take canister fire and thousands of balls of shrapnel wiping huge holes in the line. As they got close, there would be double canister. If they reached the wall without breaking, there would not be many left. It was a mathematical equation. - Shaara, Michael. Killer Angels. New York, NY: Ballantine Books, 1974, p. 303.

Just like General Longstreet took the time to survey the battlefield and form conclusions about how the terrain would affect his assault, so should combat commanders. This process, formally, is called Intelligence Preparation of the Battlefield, or IPB.

As was covered in the last chapter, the intelligence element is responsible for completing IPB products. While IPB is a much larger topic than we have time and space for here (and because we cover it in the Area Intelligence Course), we won't go into IPB in great detail. Suffice it to say, however, that IPB for community security should cover six 'layers' of the operating environment: physical terrain, human terrain, critical infrastructure, politics/governance, military/security/law enforcement, and economic/financial characteristics of the Area of Operations.

The four steps of the IPB Process is a task of the intelligence element, and the commander will use IPB products to make operational decisions. Through IPB and other products, the intelligence element helps the commander visualize the operating environment. IPB products "paint the picture" for the commander. The four steps of the IPB Process are:

- **Define the Battlefield Environment**, which refers to identifying boundaries like the Area of Operations (AO) and Area of Interest (AI, or AOI). Designating this geographic focus is an important step to direct intelligence efforts. In this step, significant characteristics of the AO are also identified.

- **Describe the Battlefield Effects**, which refers to identifying how the AO's significant characteristics will affect both friendly and enemy operations. It's in this step that the intelligence element identifies strengths and vulnerabilities of the AO.

- **Evaluate the Threat**, which refers to conducting threat analysis. Understanding the threat will allow the intelligence element to identify how the threat might operate in the AO, and how enemies might use the operating environment in their own activities and operations.

- **Determine Threat Courses of Actions** (COA), which refers to project into the future what the enemy might do. Following from the last step, once we understand enemy strength and capabilities, we can identify how the characteristics of the operating environment will affect his operations, and then we can determine what the enemy is likely to do. The better the intelligence element understands the enemy and the operating environment, the more accurate they can be when alerting the commander as to potential Courses of Action the enemy might pursue.

Remember that the goal of the intelligence element is to inform the commander on the enemy situation, and not on the friendly situation. Information that the intelligence element shouldn't answer includes how many friendly troops are in an area, what kind of weapons the friendly units have, what upcoming operations are being planned for friendly units, and the objectives of those friendly units. All of these questions posed for the enemy unit is

where the intelligence element is focused.

In addition to using IPB to produce intelligence on the terrain, there are other required products which focus on the enemy. An Order of Battle, usually referred to as OB or ORBAT, is a breakdown of the enemy command structure and subordinate units. Through this product, the commander can better understand the enemy's force projection capabilities. Additionally, threat COA snapshots can be a valuable product. These snapshots illustrate potential courses of action the enemy might pursue.

Notes for 'Chapter 3: S2/G2 Organizations and Functions'

At both the Battalion and Brigade levels, the intelligence staff is referred to as the S2. The S2 -- the senior military intelligence officer -- is responsible for coordinating intelligence activities that support the mission and fulfill the commander's intent. It's here that the S2 works with the S3 -- or Operations staff -- to support future planning. The Battalion level is usually sparse in terms of manning and ISR platforms, while the Brigade level usually enjoys a greater number of personnel and assets.

For instance, when the commander wants to use a scout platoon, the S2 is responsible for informing the S3 about the operating environment. With input from the S2, the Operations staff plans the mission, to include identifying considerations for how the scout platoon will infiltrate into the area, what information of intelligence value the platoon will collect while in the area, and how the scout platoon will exfiltrate the area, along with other information. The S2's input in invaluable for planners who decide the 'how' while the S2 provides the 'what' (e.g., conditions in the operating environment). Once the scout platoon returns, it's up to the S2 to review and analyze their information for its intelligence value, and then update any intelligence products with the latest information.

Above Battalion and Brigade levels is the Division, which has a G2. With similar tasks and functions, the 'G' in G2 just denotes the Division level. Above the Division is the Corps, which has a C2 element.

The G2, at the division level, has a more robust set of ISR assets. In addition to these extra platforms, the G2 also has more specialized intelligence roles. Those include a Staff Weather Officer, a Terrain team, and an Electronic Warfare officer.

No matter the echelon of the intelligence element, the officers and analysts that comprise the S2, G2, and C2 all feed intelligence to their echelon's Operations staff, which we refer to as the S3, G3, and C3, respectively. ("3" denotes the Operations staff, just like "2" denotes the Intelligence staff.) The maxim "Intelligence drives the fight" is very real. The objective of the intelligence element at any echelon is to help drive operations.

Notes for 'Chapter 4: Military Intelligence Capabilities'

The Intelligence functions at each echelon are generally responsible for collecting as much of their own intelligence as is possible. When a battalion S2 has a requirement that it cannot satisfy (for instance, when the desired information can only be collected through a platform that the battalion doesn't have), it can request support from higher echelons.

Intelligence at every level is divided into (broadly) five disciplines:

Human Intelligence (HUMINT)
Imagery Intelligence (IMINT)
Measurement and Signature Intelligence (MASINT)
Signals Intelligence (SIGINT)
All-Source Intelligence

While technically a discipline, all-source intelligence is developed through a combination of other disciplines. For instance, HUMINT information that confirms or adds to SIGINT information, or MASINT information that confirms or adds to IMINT information, is considered an "all-source" approach to intelligence.

This all-source approach to intelligence is almost always more beneficial to both the intelligence element, the commander, and the command staff. This fusion of different types of intelligence information from different methods of collection is more likely to give analysts a full-spectrum understanding.

Additionally, there are two multi-discipline functions: Counterintelligence (CI) and Technical Intelligence (TECHINT). Counterintelligence is directed towards the threat's intelligence capabilities so that countermeasures can be identified and implemented. TECHINT seeks to understand and exploit how threat weapons, equipment, and technology work.

Human Intelligence involves collectors and sources. The HUMINT collector is involved in identifying potential sources, and then recruiting and developing them so that they can provide increasingly useful information. A HUMINT source is a person who either has access to information, or who can gain access to information, and is providing this information to a HUMINT collector. HUMINT operations represent a broad range of tasks including (on the least intrusive end of the spectrum) document exploitation and interviewing, to tactical questioning, interrogation, and source operations (on the most intrusive end of the spectrum).

Imagery Intelligence is derived from images and video. Closed circuit and security video cameras, photo cameras of all kinds, and drones equipped with electro-optical sensors are the most common IMINT platforms.

Measurements and Signature Intelligence is derived from sensors that measure vibration, ambient temperatures, and other technical indicators. Radars, lasers, and seismic and radiation detectors are all examples of MASINT platforms.

Signals Intelligence is derived from intercepted radio signals and internet traffic. SIGINT has three categories:

Communications Intelligence (COMINT)
Electronic Intelligence (ELINT)
Foreign Instrument Signals Intelligence (FISINT)

It's important to delineate between information and intelligence. Information (or "combat information") is raw, unverified, and usually highly perishable. A soldier engaged in a firefight to reports that the enemy broke contact and is fleeing into a nearby orchard is an example of combat information. The scout platoon who can confirm that a targeted bridge has been destroyed is reporting back combat information. The long-range surveillance (LRS) platoon who's spent the last week behind enemy lines to observe military traffic on a desolate highway is going to report combat information. By the time an intelligence report is written up for these events, this actionable information may be worthless; so it makes sense to report this information directly to the commander, usually over the radio. But it's important to note that all three examples are not actually intelligence; just information.

Intelligence, on the other hand, is information that's been triaged and assessed for intelligence value, analyzed for completeness and veracity, and then often synthesized with other information in order to produce a more complete picture of single pieces of information. The information from the scout platoon in the previous paragraph is added to the incoming information from the LRS platoon, and then an analyst is able to produce intelligence. Given that the targeted bridge has been destroyed (scout platoon confirmation) and the LRS platoon is still observing enemy military traffic, the enemy must have found another way to cross the river. This is intelligence. Once analysts can find the potential new route the enemy is using, then 'actionable' intelligence can be created and the commander can plan an operation to either destroy that crossing point or interdict the enemy movement in that area. SIGINT information from enemy radio traffic could allow analysts to identify the precise location of an enemy convoy, giving the commander additional information and options. This is the supreme value of tactical intelligence collection and analysis.

Although commanders should make the best use of available ISR assets, intelligence is not without its limitations. Here are some of them:

- Intelligence reduces uncertainty on the battlefield, but there will always be a "fog of war".
- Sometimes ISR assets take longer to collect required information than a commander has time to make a decision.
- There will always be a risk that these collection assets are unable to collect the desired information.
- A commander may be so overwhelmed with intelligence requirements that there aren't enough assets available to satisfy them.
- Some of these platforms may not be able to report back immediately the information gathered. That's a constraint affecting some platforms.
- Sensors are always susceptible to deception. Whether it's disinformation told to or via a human source, disinformation said during an intercepted radio transmission, or other form of disinformation, single-source sensors are sometimes easily fooled.
- Adverse weather conditions could affect some ISR platforms, especially drones.

Notes for the Appendices

The Appendices of ST 2-50.4 (FM 34-8) contain some good advice. They also contain numerous matrices and diagrams that aren't included in this summary. If you'd like additional information on any of these Appendices, then we recommend you refer to them.

Notes for 'Appendix A: Intelligence and the Military Decision-Making Process'

Appendix A covers the Military Decision-Making Process (MDMP), which is a list of steps that can better enable commanders to 'wargame' out their courses of action. The MDMP includes:

Step 1: Receipt of Mission
Step 2: Mission Analysis
Step 3: COA Development
Step 4: COA Analysis
Step 5: COA Comparison
Step 6: COA Approval
Step 7: Orders Production

Notes for 'Appendix B: Commander's Critical Information Requirements'

A Commander's Critical Information Requirement (CCIR) is information critical for the commander to make a decision or to achieve mission success. A commander develops his CCIRs so that the intelligence element knows that information to gather.

The Intelligence element refers to these as Priority Intelligence Requirements (PIR). These PIRs are considered mission critical and should be satisfied as soon as possible.

Along with PIRs, there are also information requirements (IR). These IRs should not be prioritized above PIRs, but should still be satisfied when and where possible.

Indicators are also important for the intelligence element. As is often the case, a PIR or IR won't be satisfied directly, however, there may be indicators -- observable or potentially observable clues -- which, if identified, could point in a positive or negative direction. While we may not be able to satisfy the PIR directly, the presence of indicators could provide evidence that could partially satisfy a PIR or IR. For instance, if one PIR asks, "Will the enemy launch an assault on Objective Sierra by 121630Z JUL 18?," then an analyst may begin looking for indicators. Via an ISR mission, the analyst observes that the enemy force is massing force in a nearby staging area, which could indicate that they're readying for an assault on Objective Sierra. Since this is a PIR, then the commander should be informed immediately of this indicator so that he can reach a decision.

Notes for 'Appendix C: ISR Integration Within the Synchronization Matrix'

Synchronizing ISR collection in support of upcoming or ongoing missions can result in timely intelligence. Staging times should be taken into consideration for ISR missions so that these ISR platforms are able to report back information while it still has intelligence value.

Similarly, if continuous ISR is required -- drone coverage over an area, for instance -- then flight speeds, loiter times, and other factors should be considered to ensure the continuous coverage.

Notes for 'Appendix D: Intelligence, Surveillance, and Reconnaissance Planning'

ISR is often a mission critical component for commanders, therefore, ISR assets should be tasked to find and report:

Gaps or vulnerabilities in the threat's operations
Defensive preparations, to include primary and second positions and pre-positioned supplies
Location of threat reserves and supporting forces
Obstacles, engagement areas, and potential ambush areas
Information that answers threat intentions and capabilities

Appendix D also contains numerous questions a commander should ask for each phase of ISR operations.

Notes for 'Appendix E: Foreign Language Support'

Appendix E includes information on linguistic support and staff functions available to commanders, and generally does not provide value to the mission of community security.

Notes for 'Appendix F: Stability Operations, Support Operations, and Intelligence Preparation of the Battlefield'

Stability and Support Operations are generally classified as being outside of traditional warfare, meaning mainly peacekeeping and nation-building missions. IPB is still critical in supporting these operations.

One of the major changes from war to operations other than war is how we refer to adversaries. In war, adversaries are referred to as the 'enemy'. In operations other than war, potential adversaries are referred to as 'threats'. The phases of IPB planning stay the same, however, we do substitute "threat" in place of "enemy".

Urban environments pose particular challenges in operations other than war. Terrain and weather in the urban environment, especially flooding, could cause major problems in peacekeeping missions. Political dynamics and the demands of a higher volume of people will also weigh heavily on IPB planning and decision-making.

// Only a Glossary follows.