

Summary Report for Individual Task
150-IPO-0005
Analyze the Information Environment
Status: Approved

Distribution Restriction: Approved for public release; distribution is unlimited.

Destruction Notice: None

Foreign Disclosure: FD5 - This product/publication has been reviewed by the product developers in coordination with the Fort Leavenworth, KS foreign disclosure authority. This product is releasable to students from all requesting foreign countries without restrictions.

Condition: The unit has received an operations plan, or warning, operations or fragmentary order from higher headquarters and is conducting the military decision making process, or the commander initiates the military decision making process in anticipation of a mission. The unit has established communications with subordinate and adjacent units, and higher headquarters. The mission command system is operational and processing information in accordance with standard operating procedures. Some iterations of this task should be performed in MOPP 4.

Standard: Analyze the information environment and determine positive and adverse impacts of information (physical, informational, and cognitive dimensions) to the unit Area of Operations.

Special Condition: Not all units have an information operations officer (Functional Area (FA) 30) assigned. Any member assigned the duties of information operations officer may use this task to conduct an analysis of the information environment.

Safety Risk: Low

MOPP 4: Sometimes

Task Statements

Cue: Unit receives a warning order or operations order to conduct a mission.

DANGER
None

WARNING
None

CAUTION
None

Remarks: None

Notes: None

Performance Steps

1. Receive a warning order or planning guidance to undertake preparation for the conduct of operations within a unit's area or operations (AO).

a. Understand the unit mission and the commander's intent, two levels up.

b. Understand the mission, intent, and scheme of operations, two level up, for maneuver and information operations considerations.

c. Understand the higher echelon essential tasks for information-related capabilities.

d. Request geospatial information on the unit AO.

e. Review existing geospatial data on potential information environment physical or informational facilities or support infrastructures.

f. Determine the information warfare threat.

2. Obtain necessary information environment data pertinent to the designated unit AO.

Note: The operational variables of PMESII-PT is a way to frame and organize the information environment data.

a. Political: Identify political figures, parties, information, and information systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

b. Military: Identify friendly, neutral, adversary and threat, to include criminal, militia, paramilitary, and uniformed military, information and information systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

(1) Identify size and location of threat information warfare forces and assets.

(2) Identify Threat communication infrastructures and connectivity with civilian communications infrastructures.

(3) Identify locations and types of radars, jammers, and other non-communication network systems.

(4) Identify Threat communication related towers, nodes, switches, and facilities which can be used to support the flow of information within the AO.

c. Economic: Identify economic and business information and information systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

d. Social: Identify societal information and information systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

(1) Key individuals and organizations within the Area of Operations and their relationships both inside and outside the AO as well as known or suspected agendas.

(2) Societal demographics, population distributions, ethnicity, groupings, alliances and rivalries, and boundaries to include tribal groups, gangs, criminal groups, etc.

(3) Religion to include religious leaders, houses of worship, shrines or places of pilgrimage, religious boundaries, importance of religion on daily lives of people in the Unit AO, influence of religious leaders on daily lives of people in the Unit AO.

(4) Languages, to include dialects, spoken within the Unit's AO.

(5) Key dates, events, holidays, taboos.

(6) Information pathways employed by societal groups; perceptions, ideologies, and beliefs.

e. Information: Identify Information and Information systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

(1) Identify what types of information are considered important by friendly, neutral, adversary, and threat role players within the Unit's AO.

(2) Identify latest time information is of value (LTIOV) of Friendly, Neutral, Adversary, and Threat information within the Unit's AO.

(3) Identify radio stations, to include coverage area, in the AO.

(4) Identify television stations, to include coverage area, in the AO.

(5) Identify audio visual and print media sources, to include coverage areas, in the AO.

(6) Identify Telegraph, Telephone, Retransmission (Retrans), Satellite Communications (SATCOM) facilities and services, to include coverage areas, in the AO.

(7) Identify Cellular networks, towers, and service providers, to include coverage areas, in the AO.

(8) Identify Cyber Cafes and Internet Service Providers, to include service coverage areas, in the AO.

(9) Identify social media services and individuals linked to social media in the AO.

(10) Identify Friendly, Neutral, Adversary and Threat information systems and key nodes within the AO.

f. Infrastructure: Identify Infrastructure systems within the AO which may affect, either adversely or positively, the conduct of the Unit's operations.

(1) Identify electrical nodes and control facilities which can be used to support the flow of information within the AO.

(2) Identify road, rail, underground, and trail networks which can be used to support the flow of information within the AO.

(3) Identify air and waterway networks which can be used to support the flow of information within the AO.

(4) Identify extent of supervisory control and data acquisition (SCADA) systems in place which can be used to support the flow of information within the AO.

(5) Identify civilian communication related towers, nodes, switches, and facilities which can be used to support the flow of information within the AO.

(6) Identify effects of terrain and weather on the content and flow of information within the AO; consideration should be given to the canalization and compartmentalization of information as a result of terrain and weather.

3. Assess importance and impact of information environment data pertinent to the designated unit AO.

a. Political: Analyze effect, both adverse and positive, of political figures, parties, information, and information systems within the AO on the conduct of Unit operations.

b. Military: Analyze effect, both adverse and positive, of friendly, neutral, adversary and threat, to include criminal, militia, paramilitary, and uniformed military, information and information systems within the AOR and AO on the conduct of Unit operations.

c. Economic: Analyze effect, both adverse and positive, of economic and business information and information systems within the AO on the conduct of Unit operations.

d. Social: Analyze effect, both adverse and positive, of societal information and information systems within the AO on the conduct of Unit operations.

e. Information: Analyze effect, both adverse and positive, of Information and Information systems specific to the AO on the conduct of Unit operations.

f. Infrastructure: Analyze effect, both adverse and positive, of Infrastructure systems within the AO on the conduct of Unit operations.

g. Terrain and Weather: Analyze effect, both adverse and positive, of terrain and weather on information systems and flow of information within the AO; determine impact on conduct of Unit operations.

h. Center of Gravity Analysis: Identify critical threat information and information warfare capabilities, threat information requirements, and threat information and information system vulnerabilities in the Information Environment.

(1) Center of Gravity (CG): A threat component, either tangible or intangible, which the overarching threat system cannot function without; example a critical communications node which enables decisionmaking.

(2) Critical Capability (CC): Analyze the COG to determine which threat critical capabilities (functions) are needed by the COG to operate effectively.

(3) Critical Requirements (CR): Analyze each CC to determine which threat conditions, means, and resources that enable the CC to perform its role; will the absence or loss of the CR disable the CC.

(4) Critical Vulnerability (CV): Determine which CRs, or components thereof, are vulnerable to attack, interdiction, or neutralization.

(5)) Prioritize CVs: Prioritize CVs as targets based on; criticality to the threat, accessibility to friendly force attack assets; threat ability to recoup loss, threat vulnerability or exposure to friendly forces, ability to achieve desired effect, and is the threat critical vulnerability recognizable when observed.

4. Convey critical information about the information environment to key leaders and staff members

a. Support Intelligence Preparation of the Battlefield; Center of Gravity Analysis.

b. Support MDMP by relating critical factors of the information environment which could impact, either adversely or positively, Unit Operations.

c. Display analysis of the information environment.

(1) Develop a Combined Information Overlay; a graphic depiction of where and how the information environment will impact Unit operations.

(2) The CIO must depict sub-Information Environments and Key Terrain. Sub-information environments are areas in which the Information Environments characteristics are different from adjacent areas. Key Terrain is defined as critical information nodes.

(3) The CIO must tell the Commander and staff what is important about the information environment and how it will either adversely or positively affect the Unit's operations.

(4) Post combined information overlay on Mission Command systems for easy access and use by commanders and Staffs.

(Asterisks indicates a leader performance step.)

Evaluation Guidance: Analyze the information Environment from several perspectives: What are the command and control systems for the threat, friendly, foreign friendly, and neutrals within the AO? What are the other means of command and control? What is the best way to collect information from these systems or other command and control means? What are the threat short- and long-range goals? Can friendly forces affect them? Who are the decisionmakers? Where are they located? What information warfare capability does the threat have? Where are these capabilities located? What information-related capabilities are available to friendly forces in the AO. Where and how is the threat vulnerable? How can friendly forces exploit these vulnerabilities? How is the friendly force vulnerable? How do we keep the threat from exploiting friendly forces vulnerabilities?

Evaluation Preparation: The information operations officer collaborates with the G-2 (S-2) section in the analysis of the information environment. An initial IPB product should be provided to the Information operations planner. Reach-back capabilities information containing technical and military information warfare, information outlets, means and flow, and PMESII analysis should be provided.

Provide information on threat capabilities to use information against the operation.

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. Received a warning order or planning guidance to undertake preparation for the conduct of operations within a unit's area or operations (AO).			
a. Performed initial assessment and understood the unit mission and commander's intent and scheme of operations (two levels up) for maneuver and information operations considerations.			
b. Requested geospatial information on the Area of Operation (AO)			
c. Determined Information Warfare threat.			
2. Obtained necessary information environment data pertinent to the designated unit AO.			
3. Assessed importance and impact of information environment data pertinent to the designated unit AO.			
a. Identified sub-information environments.			
b. Identified key lines of information flow.			
c. Analyzed effect of terrain and weather on information flow and content, and on information systems within the AO.			
d. Conducted Center of Gravity Analysis.			
4. Conveyed critical information about the information environment to key leaders and staff members.			
a. Supported intelligence preparation of the battlefield (IPB); provided information that includes;			
(1) Religion, language, and culture of key groups and decisionmakers.			
(2) Agendas of nongovernmental organizations.			
(3) Size and location of threat information warfare forces and assets.			
(4) Military and civilian communication infrastructures and connectivity.			
(5) Population demographics, linkages, and related information.			
(6) Locations and types of radars, jammers, and other non-communication network systems.			
(7) Audio video and print media outlets and centers, and the populations they service.			
(8) Command and control vulnerabilities of friendly, threat and other groups.			
b. Ensured critical factors in the information environment were considered during MDMP, Targeting, and conduct of the Operations Process.			
c. Developed a CIO			
(1) Depicted effects of terrain and weather on information and information systems.			
(2) Depicted threat information warfare capability.			
(3) Depicted results of COG analysis.			
(4) Depicted sub-information environments.			
(5) Depicted key terrain.			
(6) Depicted what is important about the information environment and how it will either adversely or positively affect the Unit's operations.			
d. Posted and maintained CIO on Mission Command systems for Commanders and staffs use.			
5. Reviewed existing geospatial data on potential information environment physical or informational facilities or support infrastructures.			

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	FM 6-0	COMMANDER AND STAFF ORGANIZATION AND OPERATIONS	No	No
	JP 3-0	Joint Operations	No	No
	JP 3-13	Information Operations	No	No

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT.

Safety: In a training environment, leaders must perform a risk assessment in accordance with ATP 5-19, Risk Management. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection, FM 3-11.5, Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination.

Prerequisite Individual Tasks : None

Supporting Individual Tasks :

Task Number	Title	Proponent	Status
150-IPO-0009	Produce a Combined Information Overlay	150 - Combined Arms (Individual)	Approved
150-IPO-0003	Integrate Information Operations (synchronized IRC) into the Military Decision Making Process.	150 - Combined Arms (Individual)	Approved
150-IPO-0006	Develop Information Requirements for Information Operations	150 - Combined Arms (Individual)	Approved
150-IPO-0001	Employ Synchronized Information-Related Capabilities to Affect the Information Environment	150 - Combined Arms (Individual)	Approved

Supported Individual Tasks : None

Supported Collective Tasks : None

ICTL Data :

ICTL Title	Personnel Type	MOS Data
Information Operations Individual Critical Task List	Officer	AOC: 30A