

Training and Evaluation Outline Report

Task Number: 71-8-2210

Task Title: Perform Intelligence Preparation of the Battlefield (Battalion - Corps)

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	ADRP 3-0	Unified Land Operations	Yes	No
	ADRP 5-0	The Operations Process	Yes	No
	ADRP 6-0	Mission Command	Yes	No
	FM 2-01.3	INTELLIGENCE PREPARATION OF THE BATTLEFIELD/BATTLESPACE	Yes	Yes

Condition: The command has received an operations plan, or warning, operations, or fragmentary order from higher headquarters and is exercising mission command. The commander has issued guidance on performing intelligence preparation of the battlefield. The command 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. The unit has received guidance on the rules of engagement. Some iterations of this task should be performed in MOPP.

Standard: The staff, led by the Intelligence section, performs Intelligence Preparation of the Battlefield (4 step process) by defining the operational environment; describing the environmental effects on operations; evaluating the threat; and determining threat courses of action. The staff refines higher headquarters intelligence products and/or develops their own intelligence products producing a modified combined obstacle overlay and threat courses of action that include doctrinal templates, situational templates, identification of high-value targets, an event template, initial priority intelligence requirements and intelligence requirements to support the unit decision-making process. The staff shares Intelligence Preparation of the Battlefield products with subordinate and adjacent units to facilitate parallel or collaborative planning.

Note: Task steps and performance measures may not apply to every staff, unit or echelon. Prior to evaluation, coordination should be made between evaluator and the evaluated staffs or units' higher headquarters to determine the performance measures that may not be evaluated.

Special Equipment: None

Safety Level: Low

Task Statements

Cue: None

DANGER

Leaders have an inherent responsibility to conduct Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

WARNING

Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All soldiers have the responsibility to learn and understand the risks associated with this task.

CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

Remarks: Task content last updated: 24 May 2012.

Notes: None

TASK STEPS

1. The staff, led by the Intelligence section, applies the four steps of the intelligence preparation of the battlefield (IPB) process to analyze and visualize the mission variables of: threat, terrain, weather, and civil considerations in the unit's area of operation (AO) for the current or future operation or mission.

2. The entire staff participates in the IPB process and provides input to support the running estimate and the military decision making process (MDMP) by performing the following steps:

a. Defining the Operational Environment (Step 1 of IPB) in order to conduct further analysis on specific features of the environment or activities within it and the physical space where they exist that may influence available courses of action (COA) or the commander's decision by:

(1) Analyzing the terrain characteristics to assess the existing situation and to develop the military aspects of the terrain to include: hydrological data, elevation data, soil composition and vegetation.

(2) Describe the weather (weather forecast) to support a planned future operation to include: visibility, wind, cloud cover/ceiling, temperature, humidity, atmosphere pressure (as required).

(3) Identifying the limits of the command's AO, to include: the extent of subordinate's area of influence when defining subordinate's AO, confirms the AO is encompassed by the area of influence, and confirms the area of interest as specified by the operation order or operation plans from higher headquarters that defines the commander's mission.

(4) Establish the limits of the area of influence and the area of interest.

(5) Evaluate existing databases and identifies intelligence gaps.

(a) Examine national, multinational partner(s), joint and higher echelon databases to determine if the information is already available.

(b) Identify and prioritize gaps in the current holdings, using the commander's intelligence requirements and intent to set priorities.

(c) Identify gaps that cannot be filled within the time allowed for IPB.

(d) Discuss with the commander and the staff gaps not expected to be filled and formulate assumptions to fill them.

(6) Initiate collection of information required to complete IPB by:

(a) Initiate collection or requests for information to fill intelligence gaps.

(b) Include collection against all identified significant characteristics of the operational environment, not just threat forces, in priority order and continuously update the IPB products as additional information is received.

(c) Inform the commander if assumptions made during the initial mission analysis and IPB process are confirmed.

(d) Inform the commander if any assumption made during the initial mission analysis must be reexamined.

(e) Develop an understanding of the operational environment to closely match the actual situation on the ground.

(f) Begin developing databases once intelligence gaps are filled on the threat, terrain, weather, and civil considerations.

b. Describe Environmental Effects on Operations (Step 2 of IPB) to determine how the environment affects both threat and friendly operations by analyzing the environment in accordance with mission variables (METT-TC) of terrain, weather and civil considerations.

(1) Identify aspects of the environment that favor one type of operation (offense, defense or stability operations).

(2) Collect, analyze, and interpret geographic information on natural and manmade features of the terrain, combined with other relevant factors to predict the effects of terrain on military operations.

(3) The geospatial engineer element conducts the major portion of the terrain analysis by combining extensive databases with the results of reconnaissance.

(4) The geospatial engineer element coordinates with the Air Force's Staff Weather Officer to incorporate the effects of current and projected weather conditions for: engagement areas directed against aerial and ground targets, battle positions, infiltration routes, exfiltration routes, avenues of approach (AA), specific system or asset locations, observation posts, ambush sites or positions, and weapon system employment.

(5) The geospatial engineer element coordinates with the G2/S2 to exploit imagery, reconnaissance information and reports, as well as other all-source data collected by the G2/S2 to supplement their standard terrain database and to provide direct support to the unit using following computer – generated applications to address: cross-country mobility, lines of communications (LOCs) (transportation, communications, and power), vegetation type and distribution, surface drainage and configuration, surface materials, subsurface (bedrock) materials, obstacles, infrastructures, flood zones, helicopter landing zones, and amphibious landing zones.

(6) The entire staff evaluates the military aspects of terrain using observations and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (OAKOC).

(a) Evaluate observation and fields of fire for potential engagement areas, defensible terrain and specific equipment or equipment positions, areas where friendly forces are most vulnerable to observation fires and areas of visual dead space.

(b) Identify and evaluate air and ground AA mobility corridors in order to identify the suitability of access to key terrain and adjacent avenues, the degree of canalization and ease of movement, use of military aspect for terrain, sustainability (LOC support) and access to the objective.

(c) Identify key terrain whose seizure, retention, or control affords a marked advantage to either combatant.

1 Identify key terrain in an urban environment.

2 Identify high ground in the AO.

3 Identify draws and/or wadi in open and arid environments.

4 Identify and recommend decisive terrain whose seizure and retention is mandatory to mission success.

(d) Identify obstacles that disrupt, fix, turn or block the movement of threat forces and imposes additional losses in personnel, time, and equipment.

1 Identify obstacles as natural, manmade or a combination of both.

2 Identify other affect of obstacles on mounted and dismounted forces such as improvised explosive devises, alarms, anti-intrusive devises and tripwires.

3 Determine the effects of each type of obstacles on the mobility of the friendly and threat forces.

4 Combine the effects of individual obstacles into integrated products, such as the modified combined obstacles overlay (MCOO).

5 Develop a MCOO that identifies: severely, restricted and unrestricted terrain.

(e) Identify cover and concealment:

1 Identify protective concealment from observation and surveillance that include manmade and natural sources.

2 Identify protective cover from the effects of fire, exploding rounds, flame, nuclear effects biological agents, and chemical agents.

(f) Evaluate the terrain's effects on the COAs available to threat and friendly force by using one of the following techniques:

1 Concentric rings.

2 Belt.

3 Avenue in depth.

4 Box.

(g) The air force weather team in coordination with the geospatial team and the intelligence section analyze the weather's direct effects on terrain and other aspects of the environment by:

1 Integrate climate, forecasts, and current weather data with terrain analysis and the overall analysis of the environment.

2 Provide detailed descriptions of weather effects on each equipment systems and subsystems.

3 Evaluate each aspect of the local climatology and then fine-tune the evaluation with the most current forecasts available.

4 Describe the effects on the range of friendly and enemy personnel, weapon sensors, logistics and tactics.

5 Analyze the military aspects of weather in accordance with METT-TC, to include:

a The effects of visibility such as: begin morning nautical twilight (BMNT), begin morning civil twilight (BMCT), sunrise, sunset end, evening civil twilight (EECT), ending evening nautical twilight (EECT), moon rise and moon set.

b The effects of the wind.

c The effects of precipitation.

d Cloud cover.

e The effects of temperature.

f The effects of relative and absolute humidity.

(h) Analyze civil consideration.

1 The staff determines the impact on operations to include the selection of objectives, location, movement and control of forces, use of weapons, and protection measures.

2 The staff uses areas, structures, capabilities, organizations, people and events (ASCOPE) when analyzing civil considerations:

a Determine the effects of key civilian areas within the AO that may not be of any military significant but how they may affect the following areas: Political boundaries, such as districts within a city or municipalities within a region; location of government centers; social, political, religious, or criminal enclaves; agricultural and mining regions; trade routes; possible sites for the temporary settlement of displaced civilians or other civil functions.

b Determine the effects of existing structures such as: high-payoff targets (such as bridges, communication towers, power plants, and dams), cultural sites that international or other agreements generally protect (such as: churches, mosques, temples, national libraries, hospitals, and clinics), and other facilities with practical applications (such as: jails, TV broadcast stations, radio stations and print plants).

c Analyze capabilities in terms of those required to save lives, sustain, or enhance life or the ability of local authorities (host nation) aggressor nations, that provide a populace with key functions such as: public administration, public safety, emergency services, food and technology.

d Analyze how organizations (nonmilitary groups or institutions inside and outside of the AO) in the AO influence and interact with the populace, the force, and each other that include: church groups, fraternal organizations, patriotic or service organizations, labor unions, criminal organizations, community watch groups, multinational corporations, intergovernmental organizations (IGOs) (such as United Nations agencies), and international organizations (such as the International Committee of the Red Cross), other government agencies (such as Central Intelligence Agency), and nongovernmental organizations (NGOs), which are private, self-governing, not-for-profit organizations.

3. Evaluating the Threat (step 3 of IPB). The staff, lead by the intelligence section evaluate the threat in order to portray the threat as accurately as possible in how they normally execute operations, how they've executed operations in the past, and what they are capable of doing giving the current situation.

a. The staff identify the threat, which may include military forces, paramilitary, or small-cell-oriented organizations.

b. Determine the maximum capabilities of the unit to acquire targets and physically dominate the threat.

c. The staff identify and evaluate the threat to determine all factors to include their capabilities, equipment, understanding their doctrine and tactics, techniques and procedures (TTP) and their history.

d. The staff, lead by the intelligence section focus on the two sub-steps of step 3, Evaluate the threat:

(1) Update or create threat models.

(2) Identify threat capabilities.

e. The intelligence section analyze the commander's intelligence holdings to determine how the threat normally operates under similar circumstances or against a new or less-defined threat.

f. The intelligence section develop or expand intelligence data bases and threat models.

g. The intelligence sections conduct threat characteristic (order of battle) for each group identified by identifying:

(1) Composition- identify threat cells or forces, their affiliated political, religious, or ethnic organizations; for conventional forces identify the units equipment and personnel make up.

(2) Disposition - identify the geographic location of threat elements and how they are deployed, employed, or located.

(3) Tactics - identify the threat's strategy, method of operation, and doctrine as well as political, military, psychological and economic considerations.

(4) Training-identify the type and level of individual and group training that threat forces have received.

(5) Operational Effectiveness – identify the ability of the threat to replace personnel losses and ability to conduct operations at various levels of expertise.

(6) Logistics - identify the effectiveness of threat's logistical capabilities.

(7) Communications – identify how and what methods the threat uses to communicate their plans, orders or other information...high-frequency short wave radios, cellular phones, internet, mail, couriers, face-to-face meetings, citizen band sets, ham radios, etc.

(8) Intelligence – identify how the threat conducts a variety of intelligence tasks in preparation for operations and understand the political and physical strengths/weaknesses of their intelligence capabilities.

(9) Recruitment – identify how the threat recruits people to become members of a cell and how they develop a network of supporters of the organization who may or may not claim membership.

(10) Support – identify the various forms of support they may receive to further their operations or goals, such as:

(a) Local support.

(b) Regional support.

(c) National support.

(d) International support.

(e) Popular support from the local, regional, national, and international levels that result in safe havens, freedom of movement, logistical support, financial support, intelligence support and new recruits.

h. Anticipate future and on order missions.

(1) Finance – identify how the threat pays for services, or items purchases and how the threat sustains and continues future support.

(2) Reach – identify how the threat obtains data on friendly forces.

(3) National agencies – identify the threat's ability to leverage national agencies to assist with their operations/goals.

(4) Law enforcement agencies - identify how a national, regional, or local enforcement agencies may impact the threat's military capabilities by providing information or other support.

(5) International, Intergovernmental, and Nongovernmental organizations – Identify the threats ability to influence international, intergovernmental, and nongovernmental organizations to their advantage.

(6) Personality – identify critical personalities, their interest and their group associations that are linked to know or unknown elements of threat organizations.

(7) Other Threats - identify nonmilitary threats such as chemical, radiology material, biological material, diseases, natural threats, and toxic industrial materials.

i. The intelligence sections updates or create threat models to piece together information, identify gaps, predict threat activities or COAs and plan information collection by: converting threat doctrine or patterns of operation to graphics, describing the threat's tactics and options, and identify high-value targets (HVTs) and high-pay off targets (HPTs).

j. The intelligence section convert threat doctrine or patterns of operation to graphics by:

(1) Graphically template how the threat might utilize its capabilities to perform the functions required to accomplish its objectives.

(2) Scaling threat templates to depict the threat's disposition and actions for a particular type of operation (defense, offense, insurgent ambush, or terrorist kidnapping operation).

(3) Depicting the template as an overlay, on a support system, or through some other means.

(4) Constructing threat templates that analyze intelligence databases and an evaluation of the threats past operations.

k. The intelligence section determines how the threat normally organizes for combat and how threats deploy and employ their forces and assets by:

(1) Continuously refining the threat patterns and practices.

(2) Tailor threat templates to the needs of the unit or staff creating them using the warfighting functions of intelligence, movement and maneuver, sustainment, mission command, fires, and protection.

(3) Monitor the flow of information from higher to lower echelons in order to fill gaps and lessen the degree of uncertainty.

l. The intelligence section describe the threat's tactics and options by:

(1) Describe the threat's preferred tactics.

(2) List the options available to the threat should the operation fail or succeed.

(3) Prevent the threat model from becoming more than a “snapshot in time” of the operation being depicted.

(4) Mentally wargaming the operation over the duration and during the development of threat COAs and situational templates.

(5) Address typical timelines and phases of operations, points where unit's transition from one form of maneuver to the next and how each warfighting function contributes to the success of the operation

(6) Describe and make a determination of what goal or goals the threat is trying to achieve.

(7) Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE (size, activity, location, unit, time, equipment) reports.

(8) Identify assets that are key to executing the primary operation or sequels.

(9) Determine how the threat/adversary might react to the loss of each identified HVT.

m. The intelligence section identify threat capabilities or COAs and supporting operations that influence accomplishing friendly missions by:

(1) Describe the threat's tactics and options.

(2) Identify HVTs and HPTs.

(3) Determine how the threat might react to the loss of each identified HVT. Consider the threat's ability to substitute other assets as well as adopt branches or sequels.

n. The staff, led by the intelligence section, determine if the amount of detail required is feasible within the time available by:

(1) Define the threat's capabilities using capability statements.

(2) Define other capabilities to include attack, defend, reinforce, retrograde or specific types of operations, as well as operations that would allow the threat to use a COA that would not normally be available or would severely be hindered if the supporting operation were not conducted.

(3) Review the full set of threat models and consider the threats ability to conduct operations based on the current situation and the threat's own METT-TC conditions.

(4) Consider cultural awareness that assist friendly forces in identifying groups or individual members of the population that may be friendly, somewhere in between, or both and what capabilities those personnel can bring into the existing or new COA.

4. Determine threat courses of action (step 4 of IPB). The staff lead by the intelligence section determine the threat's COAs by:

a. Identify the threat's likely objectives and desired end state.

(1) Depict the threat based on the commander's guidance.

(2) Determine likely objectives and the desired end state.

(3) Evaluate propaganda, graffiti, and gang symbols in order to determine likely propaganda objectives, propaganda campaigns, production sources, target audiences, themes, and desired end states.

(4) Determine how the threat has conducted past operations.

b. Identify the threat's likely objectives and desired end state.

(1) Consider the threat's COAs that the threat believes are appropriate to the current operation and the identification of the threats likely objectives.

(2) Understand the threats decisionmaking process as well as gaining an appreciation for how the threat perceives the current situation.

- (3) Identifying threat COAs that may go outside the boundaries of known threat's doctrine or TTPs.
- (4) Identify recent activities and events that may determine current threat COAs.
- (5) Identify threat COAs that are distinct and evaluate each based on its effects on the friendly mission and protection.
- (6) Compare the consolidated list of threat capabilities identified in step 3 of the IPB process and eliminate any COA that the threat is incapable of executing.
- (7) Select a threat model that has the potential to accomplish the threat's likely objectives.
- (8) Examine how the effects of the operational environment will influence applications of its COA.
- (9) Consider the effects of terrain, weather, and civil considerations on a set of threat COAs.
- (10) Define each general threat COA as a set of specific threat COAs by integrating the threat models from step 3 of IPB with the description of the operational environment effects identified in this step.
- (11) Consider the following factors when defining the general threat COAs into specific threat COAs:
 - (a) The threat's intent or desired end state.
 - (b) Likely attack or counterattack objectives.
 - (c) Effects of the operational environment on operations and COAs.
 - (d) Threat vulnerabilities or shortages in logistics or personnel.
 - (e) Location of main and supporting efforts.
 - (f) Current disposition of forces, groups, or cells.
 - (g) Threat perception of friendly forces.
 - (h) Threat efforts to present an ambiguous situation or achieve surprise.
 - (i) Threat perception of friendly forces.
 - (j) Threat efforts to present an ambiguous situation or achieve surprise.
- (12) Use the same criteria for evaluating threat COAs; suitability, feasibility, acceptability, distinguishable, and completeness.
- (13) Determine the doctrinal requirements for each type of operation it is considering, including doctrinal tasks to be assigned to subordinate units.
- (14) Examine each (changing, adding, or eliminating threat COA's as appropriate) to determine if it satisfies threat COA collective criteria.
- (15) Avoid the common pitfalls of presenting one good threat COA among several "throw away" threat COAs.

(16) Account for the effects of friendly dispositions or threat perception of friendly disposition when determining the COAs the threat believes are available.

c. Identify the amount of detail required on each area of the operation or each threat force to support planning.

d. The commander and staff evaluate and prioritize each COA after developing a plan that is optimized to one of the COAs, while allowing for contingency options should the threat choose another COA.

(1) The staff evaluate each threat COA and prioritizes it according to how likely the threat will adopt that option by establishing an initial priority list to allow the staff to plan friendly COAs.

(2) The staff may have to reorder the list of threat COAs following the commander's selection of a friendly COA.

(3) The staff prioritizes each COA by considering the following:

(a) Analyze each COA to identify threat strengths, weaknesses, decision points and potential center of gravity.

(b) Evaluate how each COA meets the criteria of suitability, feasibility, acceptability, distinguishable and completeness with threat doctrine, their previous operation, and TTPs.

(c) Evaluate how well each COA takes advantage of the operational environment.

(d) Evaluating how the operational environment encourages or discourages selection of each COA.

(e) Analyze the threat's recent activity to determine if there are indications that one COA has already been adapted.

(4) The staff considers the possibility that the threat may or may not choose the predicted COA over another COA.

(5) The staff compares each COA to the others and determines if the threat is more likely to prefer one over the other.

(6) The staff uses judgment to rank the threat COAs in their likely order of adaption, modify the list as needed to account for changes in the current situation.

(7) The staff develop each threat COA once the complete set of threat COAs are identified in as much detail as the situation requires given time available.

(8) To ensure completeness, each COA must answer six basic questions:

(a) Who the threat is and its makeup.

(b) What type of operation is the threat conducting.

(c) When the threat action occur, usually stated in terms of earliest time that the threat can adapt the COA under consideration.

(d) Where are the objectives in the AO.

(e) How or the method by which the threat will employ its assets such as disposition, location of the units main effort, scheme of maneuver, or time and place of an attack, and how it will be supported.

(f) Why the threat intends to accomplish its objective or end state.

(9) During a conventional fight, the staff consider forces to at least one level of command above and two below the friendly force when developing each COA.

(10) The staff's developed COAs has three parts.

(a) Situation templates that depict possible threat COAs that are part of a particular threat operation and consist of:

1 Identify the threat model (conventional or asymmetric) representing the operation under consideration.

2 Overlay the threat template on the products that depict the operational environment effects on the operation, normally represented by the modified combined obstacle overlay (MCOO).

3 Use analytical judgment and knowledge of threat TTP and doctrine, adjust the dispositions depicted on the threat template to account for the operational environment's effects.

4 Check the situational templates to account for all the threat major assets and functions, and that none of them have been inadvertently duplicated.

5 Ensure that the template reflects the main effort (conventional) or potential multiple targets (asymmetric) identified for the COA.

6 Compare depicted dispositions to the threats' know doctrine.

7 Consider the threat's desire to present an ambiguous situation and achieve surprise.

8 Include as much detail on the template as time and the situation warrants or allow.

9 Ensure the template depicts the location and activities of the HVTs listed in the threat models.

10 . Using the description of preferred tactics that accomplish the threat template as a guide.

11 Mentally war-gaming the scheme of maneuver or scheme of activities from positions or locations depicted on the template through to the COA's success or failure.

(b) Threat COA and options that consist of:

1 Write a narrative description to a detailed synchronization matrix depicting activities of each unit, warfighting function, or asymmetric activity in detail.

2 Address the earliest time the COA can be executed, timelines and phases associated with the COA, and decisions the threat commander will make during execution of the CAO and afterwards.

3 Use the COA description to support staff wargaming and to develop the event template and supporting indicators.

4 Develop the description of the COA in as much detail as time and situation requires using whatever ever tools or techniques best meet requirements.

5 Describe preferred tactics that accompany the threat templates.

6 Note when and where to expect the threat to take certain action or make a certain decision.

7 Record each event in the description of the COA.

8 Tie, when possible, each event or activity to time phase lines, timelines, or other specific geographical areas on the situation template.

9 Record threat force advances as they approach decision points.

10 Deter which COA the threat will eventually adapt.

11 Predict specific areas and activities that, when observed, to reveal which COA the threat has adapted.

12 Nominate specific areas where key events are expected as named areas of interest (NAIs).

13 Consider each war-fighting function and its role in making the threat COA successful.

14 Address the concept of operation of operations and how it is supported, not just the disposition of forces.

15 Determine the threat's capabilities, doctrinal principles, and TTPs that threat forces prefer to employ.

16 Develop threat models and the database.

17 Develop a threat model to portray the threat to allow the consolidation of information, identify gaps, predict threat activities and COA, and plan reconnaissance and surveillance in order to mitigate or negate operational risk.

18 Compare an existing model to current activity to identify patterns, trends, and activity levels.

19 Develop new models that include the operational environment, organizational structure of the threat, organizational structure of friendly force, population, and physical objectives variations.

20 Update new models by refining to maintain its validity.

21 Develop threat models that include: standard graphics control measures, description of typical tasks for subordinates, evaluate how the threat force is trained for the tasks, employment considerations, and discuss typical contingencies, sequels, failure options, and wildcard variations.

22 Advise the commander if time allotted is insufficient to complete the directed analysis and provides a recommended solution.

by: (c) The staff identified initial reconnaissance and surveillance requirements in order to have an effective plan

1 Develop event templates to guide the reconnaissance and surveillance synchronization planning.

2 Depict the NAIs where activity or lack of it will indicate which threat COA the threat has adapted.

3 Evaluate each threat COA to identify its associated NAI.

4 Compare and contrast the NAI and indicators associated with each threat COA against the other and identify their differences.

5 Focus on the difference that provides the most reliable indicators of a distinct threat COA.

6 Mark the selected NAI on the event template.

7 Identify which predicted threat COAs the threat has adapted.

8 Update and refine further the event template and its supporting matrix to support friendly decisions identified during staff war-gaming.

9 Identify times and places where the threat HVT's are employed or enter areas where they can be easily acquired and engaged.

10 Develop an event matrix to compliment the event template by providing details on the type of activity expected to occur at each NAI, the time the NAI is expected to be active, and its relationship to other events in the AO.

11 Include the following techniques to develop event matrices: examine the events associated with each NAI on the event template and restate them in the form of indicators, enter the indicators into the event matrix along with the times they are likely to occur, use the TPLs or timelines from either the situation template or the description of the COA to establish the expected times in the event matrix, refine the event matrix during staff war-gaming and the targeting process, assist in developing the decision support template (DST), which incorporates NAIs that support decisions by the commander and the tracking of high-payoff targets during staff war-gaming.

12 Disseminate the threat COA models as widely as possible.

13 Use the completed event template forms for planning intelligence synchronization strategy and synchronizing intelligence with friendly operations.

(Asterisks indicates a leader performance step.)

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. The staff, led by the Intelligence section applied the four steps of the IPB process to analyze and visualize the mission variables of: threat, terrain, weather, and civil considerations in the unit's area of operation (AO) for the current or future operation or mission.			
2. The entire staff participated in the IPB process and provided input to support the running estimate and the military decision making process (MDMP) by performing the following steps:			
a. Defined the Operational Environment (step1 of IPB) in order to conduct further analysis on specific features of the environment or activities within it and the physical space where they exist that may influence available courses of action (COA) or the commander's decision by:			
(1) Analyzed the terrain characteristics to assess the existing situation and developed the military aspects of the terrain to include: hydrological data, elevation data, soil composition and vegetation.			
(2) Described the weather (weather forecast) to support a planned future operation to include: visibility, wind, cloud cover/ceiling, temperature, humidity, atmosphere pressure (as required).			
(3) Identified the limits of the command's AO, to include: the extent of subordinate's area of influence when defining subordinate's AO, confirmed the AO is encompassed by the area of influence, and confirmed the area of interest (AOI) as specified by the operation order or operation plans from higher headquarters that defined the commander's mission.			
(4) Established the limits of the area of influence and the AOI.			
(5) Evaluated existing databases and identified intelligence gaps.			
(a) Examined national, multination partners, joint and higher echelon databases to determine if the information is already available.			
(b) Identified and prioritized gaps in the current holdings, using the commander's intelligence requirements and intent to set priorities.			
(c) Identified gaps that cannot be filled within the time allowed for IPB.			
(d) Discussed with the commander and the staff gaps not expected to be filled and formulated assumptions to fill them.			
(6) Initiated collection of information required to complete IPB by:			
(a) Initiated collection or requested information to fill intelligence gaps.			
(b) Included collection against all identified significant characteristics of the operational environment, not just threat forces, in priority order and continuously updated the IPB products as additional information is received.			
(c) Informed the commander if assumptions made during the initial mission analysis and IPB process were confirmed.			
(d) Informed the commander if any assumption made during the initial mission analysis must be reexamined.			
(e) Developed an understanding of the operational environment to completely match the actual situation on the ground.			
(f) Began developing databases once intelligence gaps were filled on the threat, terrain, weather, and civil considerations.			
b. Described Environmental Effects on Operations (step 2 of IPB) to determine how the environment affects both threat and friendly operations by analyzing the environment in accordance with mission variables (METT-TC) of terrain, weather and civil considerations.			
(1) Identified aspects of the environment that favor one type of operation (offense, defense or stability operations).			

(2) Collected, analyzed, and interpreted geographic information on natural and manmade features of the terrain, combined with other relevant factors to predict the effects of terrain on military operations.			
(3) The geospatial engineer element conducted the major portion of the terrain analysis by combining extensive databases with the results of reconnaissance.			
(4) The geospatial engineer element coordinated with the air force's staff weather officer to incorporate the effects of current and projected weather conditions for: engagement areas directed against aerial and ground targets, battle positions, infiltration routes, exfiltration routes, avenues of approach (AA), specific system or asset locations, observation posts, ambush sites or positions, and weapon system employment.			
(5) The geospatial engineer element coordinated with the G2/S2 to exploit imagery, reconnaissance information and reports, as well as other all-source data collected by the G2/S2 to supplement their standard terrain database and to provide direct support to the unit using following computer – generated applications to address: cross-country mobility, lines of communications (LOCs) (transportation, communications, and power), vegetation type and distribution, surface drainage and configuration, surface materials, subsurface (bedrock) materials, obstacles, infrastructures, flood zones, helicopter landing zones, and amphibious landing zones.			
(6) The entire staff evaluated the military aspects of terrain using observations and fields of fire, avenues of approach, key terrain, obstacles, and, cover and concealment (OAKOC).			
(a) Evaluated observation and fields of fire for potential engagement areas, defensible terrain and specific equipment or equipment positions, areas where friendly forces are most vulnerable to observation fires and areas of visual dead space.			
(b) Identified and evaluated air and ground AA mobility corridors in order to identify the suitability of access to key terrain and adjacent avenues, the degree of canalization and ease of movement, use of military aspect for terrain, sustainability (LOC support) and access to the objective.			
(c) Identified key terrain whose seizure, retention, or control affords a marked advantage to either combatant.			
1 Identified key terrain in an urban environment.			
2 Identified high ground in the AO.			
3 Identified draws and/or wadi in open and arid environments.			
4 Identified and recommended decisive terrain whose seizure and retention is mandatory to mission success.			
5 Developed a MCOO that identified: severely, restricted and unrestricted terrain.			
(d) Identified obstacles that disrupt, fix, turn or block the movement of threat forces and imposes additional losses in personnel, time, and equipment.			
1 Identified obstacles as natural, manmade or a combination of both.			
2 Identified other affect of obstacles on mounted and dismounted forces such as improvised explosive devises, alarms, anti-intrusive devises and tripwires.			
3 Determined the effects of each type of obstacles on the mobility of the friendly and threat forces.			
4 Combined the effects of individual obstacles into integrated products, such as the modified combined obstacles overlay (MCOO).			
5 Developed a MCOO that identifies: severely, restricted and unrestricted terrain.			
(e) Identified cover and concealment:			

<p>_1_ Identified protective concealment from observation and surveillance that include manmade and natural sources.</p>			
<p>_2_ Identified protective cover from the effects of fire, exploding rounds, flame, nuclear effects biological agents, and chemical agents.</p>			
<p>(f) Evaluated the terrain's effects on the COAs available to threat and friendly force by using one of the following techniques:</p>			
<p>_1_ Concentric rings.</p>			
<p>_2_ Belt.</p>			
<p>_3_ Avenue in depth.</p>			
<p>_4_ Box.</p>			
<p>(g) The air force weather team in coordination with the geospatial team and the intelligence section analyzed the weather's direct effects on terrain and other aspects of the environment by:</p>			
<p>_1_ Integrated climate, forecasts, and current weather data with terrain analysis and the overall analysis of the environment.</p>			
<p>_2_ Provided detailed descriptions of weather effects on each equipment systems and subsystems.</p>			
<p>_3_ Evaluated each aspect of the local climatology and then fine-tuned the evaluation with the most current forecasts available.</p>			
<p>_4_ Described the effects on the range of friendly and enemy personnel, weapon sensors, logistics and tactics.</p>			
<p>_5_ Described the effects on the range of friendly and enemy personnel, weapon sensors, logistics and tactics.</p>			
<p>_a_ The effects of visibility such as: begin morning nautical twilight (BMNT), begin morning civil twilight (BMCT), sunrise, sunset end, evening civil twilight (EECT), ending evening nautical twilight (EECT), moon rise and moon set.</p>			
<p>_b_ The effects of the wind.</p>			
<p>_c_ The effects of precipitation.</p>			
<p>_d_ Cloud cover.</p>			
<p>_e_ The effects of temperature.</p>			
<p>_f_ The effects of relative and absolute humidity.</p>			
<p>(h) Analyze civil consideration.</p>			
<p>_1_ The staff determined the impact on operations to include the selection of objectives, location, movement and control of forces, use of weapons, and protection measures.</p>			
<p>_2_ The staff used areas, structures, capabilities, organizations, people and events (ASCOPE) when analyzing civil considerations:</p>			
<p>_a_ Determined the effects of key civilian areas within the AO that may not be of any military significant but how they may affect the following areas: Political boundaries, such as districts within a city of municipalities within a region; location of government centers; social, political, religious, or criminal enclaves; agricultural and mining regions; trade routes; possible sites for the temporary settlement of displaced civilians or other civil functions.</p>			

<p>_b_ Determined the effects of existing structures such as: high-payoff targets, such as bridges, communication towers, power plants, and dams; cultural sites that international or other agreements generally protect, such as: churches, mosques, temples, national libraries, hospitals, and clinics; other facilities with practical applications such as: jails, TV broadcast stations, radio stations and print plants.</p>			
<p>_c_ Analyzed capabilities in terms of those required to save lives, sustain, or enhance life or the ability of local authorities (host nation) aggressor nations, that provide a populace with key functions such as: public administration, public safety, emergency services, food and technology.</p>			
<p>_d_ Analyzed how organizations (nonmilitary groups or institutions inside and outside of the AO) in the AO influence and interact with the populace, the force, and each other that include: church groups; fraternal organizations; patriotic or service organizations; labor unions; criminal organizations; community watch groups; multinational corporations; intergovernmental organizations (IGOs), such as United Nations agencies, and international organizations, such as the International Committee of the Red Cross; other government agencies, such as Central Intelligence Agency; nongovernmental organizations (NGOs), which are private, self-governing, not-for-profit organizations.</p>			
<p>3. Evaluated the Threat (step 3 of IPB). The staff, lead by the intelligence section evaluated the threat in order to portray the threat as accurately as possible in how they normally execute operations, how they've executed operations in the past, and what they are capable of doing giving the current situation.</p>			
<p>a. The staff identified the threat, which may include military forces, paramilitary, or small-cell-oriented organizations.</p>			
<p>b. Determined the maximum capabilities of the unit to acquire targets and physically dominate the threat.</p>			
<p>c. The staff identified and evaluated the threat to determine all factors to include: their capabilities or equipment, to understand their doctrine and tactics, techniques and procedures (TTP), and history.</p>			
<p>d. The staff, lead by the intelligence section focused on the two sub-steps of step 3, Evaluate the threat:</p>			
<p>(1) Updated or created threat models.</p>			
<p>(2) Identified threat capabilities.</p>			
<p>e. The intelligence section analyzed the commander's intelligence holdings to determine how the threat normally operates under similar circumstances or against a new or less-defined threat.</p>			
<p>f. The intelligence section developed or expanded intelligence data bases and threat models.</p>			
<p>g. The intelligence sections conducted threat characteristic (order of battle) for each group identified by identifying:</p>			
<p>(1) Composition- identified threat cells or forces, their affiliated political, religious, or ethnic organizations; for conventional forces identified the unit's equipment and personnel make up.</p>			
<p>(2) Disposition - identified the geographic location of threat elements and how they are deployed, employed, or located.</p>			
<p>(3) Training-identified the type and level of individual and group training that threat forces have received.</p>			
<p>(4) Operational Effectiveness – identified the ability of the threat to replace personnel losses and ability to conduct operations at various levels of expertise.</p>			

(5) Communications – identified how and what methods the threat uses to communicate their plans, orders or other information...high-frequency short wave radios, cellular phones, internet, mail, couriers, face-to-face meetings, citizen band sets, ham radios, etc.			
(6) Intelligence – identified how the threat conducts a variety of intelligence tasks in preparation for operations and understands the political and physical strengths/weaknesses of their intelligence capabilities.			
(7) Logistics - identified the effectiveness of threat's logistical capabilities.			
(8) Tactics - identified the threat's strategy, method of operation, and doctrine as well as political, military, psychological and economic considerations.			
(9) Recruitment – identified how the threat recruits people to become members of a cell and how they develop a network of supporters of the organization who may or may not claim membership.			
(10) Support – identified the various forms of support they may receive to further their operations or goals, such as:			
(a) Local support.			
(b) Regional support.			
(c) National support.			
(d) International support.			
(e) Popular support from the local, regional, national, and international levels that result in safe havens, freedom of movement, logistical support, financial support, intelligence support and new recruits.			
h. Anticipated future and on order missions.			
(1) Finance – identified how the threat pays for services, or items purchases and how the threat sustained and continued future support.			
(2) Reach – identified how the threat obtains data on friendly forces.			
(3) National agencies – identified the threat's ability to leverage national agencies to assist with their operations/goals.			
(4) Law enforcement agencies - identified how a national, regional, or local enforcement agencies may impact the threat's military capabilities by providing information or other support.			
(5) International, Intergovernmental, and Nongovernmental organizations – Identified the threat's ability to influence international, intergovernmental, and nongovernmental organizations to their advantage.			
(6) Personality – identified critical personalities, their interest and their group associations that are linked to know or unknown elements of threat organizations.			
(7) Other Threats - identified nonmilitary threats such as chemical, radiology material, biological material, diseases, natural threats, and toxic industrial materials.			
i. The intelligence sections updated or created threat models to piece together information, identify gaps, predict threat activities or COAs and plan information collection by: converting threat doctrine or patterns of operation to graphics, describing the threat's tactics and options, and identifying high-value targets (HVTs) and high-pay off targets (HPTs).			
j. The intelligence section converted threat doctrine or patterns of operation to graphics by:			
(1) Graphically templated how the threat might utilize its capabilities to perform the functions required to accomplish its objectives. (
(2) Scaled threat templates to depict the threat's disposition and actions for a particular type of operation (defense, offense, insurgent ambush, or terrorist kidnapping operation).			

(3) Depicted the template as an overlay, on a support system, or through some other means.			
(4) Constructed threat templates that analyze intelligence databases and evaluated the threats past operations.			
k. The intelligence section determined how the threat normally organizes for combat and how the threat deploy and employ their forces and assets by:			
(1) Continuously refined the threat patterns and practices.			
(2) Tailored threat templates to the needs of the unit or staffs creating them using the warfighting functions of intelligence, movement and maneuver, sustainment, mission command, fires, and protection.			
l. The intelligence section described the threat's tactics and options by:			
(1) Described the threat's preferred tactics.			
(2) Listed the options available to the threat should the operation fail or succeed.			
(3) Prevented the threat model from becoming more than a "snapshot in time" of the operation being depicted.			
(4) Mentally wargamed the operation over the duration and during the development of threat COAs and situational templates.			
(5) Addressed typical timelines and phases of operations, points where unit's transition from one form of maneuver to the next and how each warfighting function contributed to the success of the operation.			
(6) Described and made a determination of what goal or goals the threat is trying to achieve.			
(7) Identified HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE (size, activity, location, unit, time, equipment) reports.			
(8) Identified assets that were key to executing the primary operation or sequels.			
(9) Determined how the threat/adversary might react to the loss of each identified HVT.			
m. The intelligence section identified threat capabilities or COAs and supporting operations that influence accomplishing friendly missions by:			
(1) Described the threat's tactics and options.			
(2) Identified HVTs and HPTs.			
(3) Determined how the threat might react to the loss of each identified HVT. Considered the threat's/adversary's ability to substitute other assets as well as adopt branches or sequels.			
n. The staff, led by the intelligence section, determined if the amount of detail required is feasible within the time available by:			
(1) Defined the threats capabilities using capability statements.			
(2) Defined other capabilities to include attack, defend, reinforce, retrograde or specific types of operations, as well as operations that would allow the threat to use a COA that would not normally be available or would severely be hindered if the supporting operation were not conducted.			
(3) Reviewed the full set of threat models and considered the threats ability to conduct operations based on the current situation and the threat's own METT-TC conditions.			
(4) Considered cultural awareness that assist friendly forces in identifying groups or individual members of the population that may be friendly, somewhere in between, or both and what capabilities those personnel can bring into the existing or new COA.			

4. Determined threat courses of action (step 4 of IPB). The staff lead by the intelligence section determined the threat's COAs by:			
a. Identified the threat's likely objectives and desired end state.			
(1) Depicted the threat based on the commander's guidance.			
(2) Determined likely objectives and the desired end state.			
(3) Evaluated propaganda, graffiti, and gang symbols in order to determine likely propaganda objectives, propaganda campaigns, production sources, target audiences, themes, and desired end states.			
(4) Determined how the threat has conducted past operations.			
b. Identified the threat's likely objectives and desired end state.			
(1) Considered the threat COAs that the threat believes are appropriate to the current operation and the identified the threats likely objectives.			
(2) Understood the threats decisionmaking process as well as gained an appreciation for how the threat perceives the current situation.			
(3) Identified threat COAs that may go outside the boundaries of known threat doctrine or TTPs.			
(4) Identified recent activities and events that may determine current threat COAs.			
(5) Identified threat COAs that are distinct and evaluated each based on its effects on the friendly mission and protection.			
(6) Compared the consolidated list of threat capabilities identified in step 3 of the IPB process and eliminated any COA that the threat is incapable of executing.			
(7) Selected a threat model that has the potential to accomplish the threat's likely objectives.			
(8) Examined how the effects of the operational environment will influence applications of its COA.			
(9) Considered the effects of terrain, weather, and civil considerations on a set of threat COAs.			
(10) Defined each general threat COA as a set of specific threat COAs by integrating the threat models from step 3 of IPB with the description of the operational environment effects identified in this step.			
(11) Considered the following factors when defining the general threat COAs into specific threat COAs:			
(a) The threat's intent or desired end state.			
(b) Likely attack or counterattack objectives.			
(c) Effects of the operational environment on operations and COAs.			
(d) Threat vulnerabilities or shortages in logistics or personnel.			
(e) Location of main and supporting efforts.			
(f) Current disposition of forces, groups, or cells.			
(g) Threat perception of friendly forces.			
(h) Threat efforts to present an ambiguous situation or achieve surprise.			
(i) Threat perception of friendly forces.			
(j) Threat efforts to present an ambiguous situation or achieve surprise.			
(12) Used the same criteria for evaluating threat COAs; suitability, feasibility, acceptability, distinguishable, and completeness.			
(13) Determined the doctrinal requirements for each type of operation it is considering, included doctrinal tasks to be assigned to subordinate units.			
(14) Examined each (changed, added, or eliminated threat COAs as appropriate) to determine if it satisfies threat COA collective criteria.			

(15) Avoided the common pitfalls of presenting one good threat COA among several "throw away" threat COAs.			
(16) Accounted for the effects of friendly dispositions or threat perception of friendly disposition when determining the COAs the threat believes are available.			
(17) Determined which COA the threat will evenly adapt.			
c. Identified the amount of detail required on each area of the operation or each threat force to support planning.			
d. The commander and staff evaluated and prioritized each COA after developing a plan that optimized one of the COAs, while allowing for contingency options should the threat choose another COA.			
(1) The staff evaluated each threat COA and prioritized it according to how likely the threat will adopt that option by establishing an initial priority list to allow the staff to plan friendly COAs.			
(2) The staff may have had to reorder the list of threat COAs following the commander's selection of a friendly COA.			
(3) The staff prioritized each COA by considering the following:			
(a) Analyzed each COA to identify threat strengths, weaknesses, decision points and potential center of gravity.			
(b) Evaluated how each COA meets the criteria of suitability, feasibility, acceptability, distinguishable and completeness with threat doctrine, their previous operation, and TTPs.			
(c) Evaluated how well each COA takes advantage of the operational environment.			
(d) Analyzed the threat's recent activity to determine if there are indications that one COA has already been adapted.			
(e) Evaluated how the operational environment encourages or discourages selection of each COA.			
(4) The staff considered the possibility that the threat may or may not choose the predicted COA over another COA.			
(5) The staff compared each COA to the others and determined if the threat is more likely to prefer one over the other.			
(6) The staff used judgment to rank the threat COAs in their likely order of adaption, modified the list as needed to account for changes in the current situation.			
(7) The staff developed each threat COA once the complete set of threat COAs are identified in as much detail as the situation requires given time available.			
(8) To ensured completeness, each COA answered six basic questions:			
(a) Who the threat is and its makeup.			
(b) What type of operation is the threat conducting.			
(c) When the threat action occur, usually stated in terms of earliest time that the threat can adapt the COA under consideration.			
(d) Where are the objectives in the AO.			
(e) How or the method by which the threat will employ its assets such as disposition, location of the units main effort, scheme of maneuver, or time and place of an attack, and how it will be supported.			
(f) Why the threat intends to accomplish its objective or end state.			
(9) During a conventional fight, the staff considered forces to at least one level of command above and two below the friendly force when developing each COA.			
(10) The staff's developed COAs has three parts.			

(a) Situation templates that depict possible threat COAs that are part of a particular threat operation and consist of:			
1 Identified the threat model (conventional or asymmetric) representing the operation under consideration.			
2 Overlaid the threat template on the products that depict the operational environment effects on the operation, normally represented by the modified combined obstacle overlay (MCOO).			
3 Used analytical judgment and knowledge of threat TTP and doctrine, adjusted the dispositions depicted on the threat template to account for the operational environment's effects.			
4 Checked the situational templates to account for all the threat major assets and functions, and that none of them have been inadvertently duplicated.			
5 Ensured that the template reflects the main effort (conventional) or potential multiple targets (asymmetric) identified for the COA.			
6 Compared depicted dispositions to the threat's known doctrine.			
7 Considered the threat's desire to present an ambiguous situation and achieve surprise.			
8 Included as much detail on the template as time and the situation warrants or allow.			
9 Ensured the template depicts the location and activities of the HVTs listed in the threat models.			
10 Used the description of preferred tactics that accomplish the threat template as a guide.			
11 Mentally war-gamed the scheme of maneuver or scheme of activities from positions or locations depicted on the template through to the COA's success or failure.			
12 Developed threat models and the database.			
(b) Threat COA and options that consist of:			
1 Written narrative description of a detailed synchronization matrix depicting activities of each unit, warfighting function, or asymmetric activity in detail.			
2 Addressed the earliest time the COA can be executed, timelines and phases associated with the COA, and decisions the threat commander will make during execution of the CAO and afterwards.			
3 Used the COA description to support staff wargaming and to developed the event template and supporting indicators.			
4 Developed the description of the COA in as much detail as time and situation requires using whatever ever tools or techniques best meet requirements.			
5 Described preferred tactics that accompany the threat templates.			
6 Noted when and where to expect the threat to take certain action or make a certain decision.			
7 Recorded each event in the description of the COA.			
8 Tied, when possible, each event or activity to time phase lines, timelines, or other specific geographical areas on the situation template.			
9 Recorded threat force advances as they approach decision points.			
10 Determined which COA the threat will evenly adapt.			
11 Predicted specific areas and activities that, when observed, to reveal which COA the threat has adapted.			
12 Nominated specific areas where key events are expected as named areas of interest (NAIs).			

13 Considered each war-fighting function and its role in making the threat COA successful.			
14 Addressed the concept of operation of operations and how it is supported, not just the disposition of forces.			
15 Determined the threat capabilities, doctrinal principles, and TTPs that threat forces prefer to employ.			
16 Developed a threat model to portray the threat to allow the consolidation of information, identified gaps, predicted threat activities and COA, and planned IRS in order to mitigate or negate operational risk.			
17 Developed a threat model to portray the threat to allow the consolidation of information, identify gaps, predict threat activities and COA, and plan reconnaissance and surveillance in order to mitigate or negate operational risk.			
18 Compared an existing model to current activity it identified patterns, trends, and activity levels.			
19 Developed new models that include the operational environment, organizational structure of the threat, organizational structure of friendly force, population, and physical objectives variations.			
20 Updated new models by refining to maintain its validity.			
21 Developed threat models that include: standard graphics control measures, description of typical tasks for subordinates, evaluating how the threat force is trained for the tasks, employment considerations, and discussing typical contingencies, sequels, failure options, and wildcard variations.			
22 Advised the commander if time allotted is insufficient to complete the directed analysis and provided a recommended solution.			
(c) The staff identified initial reconnaissance and surveillance requirements in order to have an effective plan to include:			
1 Developed event templates to guide the reconnaissance and surveillance synchronization planning.			
2 Depicted NAIs where activity or lack of it indicated which threat COA the threat has adapted.			
3 Evaluated each threat COA to identify its associated NAI.			
4 Compared and contrasted the NAI and indicators associated with each threat COA against the other and identified their differences.			
5 Focused on the difference that provides the most reliable indicators of a distinct threat COA.			
6 Marked the selected NAI on the event template.			
7 Identified which predicted threat COAs the threat has adapted.			
8 Updated and refined further the event template and its supporting matrix to support friendly decisions identified during staff war-gaming.			
9 Identified times and places where the threat HVT's are employed or enter areas where they can be easily acquired and engaged.			
10 Developed an event matrix to compliment the event template by providing details on the type of activity expected to occur at each NAI, the time the NAI is expected to be active, and its relationship to other events in the AO.			

<p>_11_ Included the following techniques to develop event matrices: examined the events associated with each NAI on the event template and restated them in the form of indicators, entered the indicators into the event matrix along with the times they are likely to occur, used the TPLs or timelines from either the situation template or the description of the COA to establish the expected times in the event matrix, refined the event matrix during staff war-gaming and the targeting process, assisted in developing the decision support template (DST), which incorporates NAIs that support decisions by the commander and tracked of high-payoff targets during staff war-gaming.</p>			
<p>_12_ Disseminated the threat COA models as widely as possible.</p>			
<p>_13_ Used the completed event template that forms for planning intelligence synchronization strategy and synchronized intelligence with friendly operations.</p>			

TASK PERFORMANCE / EVALUATION SUMMARY BLOCK							
ITERATION	1	2	3	4	5	M	TOTAL
TOTAL PERFORMANCE MEASURES EVALUATED							
TOTAL PERFORMANCE MEASURES GO							
TRAINING STATUS GO/NO-GO							

ITERATION: 1 2 3 4 5 M

COMMANDER/LEADER ASSESSMENT: T P U

Mission(s) supported: None

MOPP: Sometimes

MOPP Statement: None

NVG: Never

NVG Statement: None

Prerequisite Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-5113	Develop Commander's Critical Information Requirements (Battalion - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5120	Prepare for Tactical Operations (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-5-0007	Analyze the Operational Environment	71 - Combined Arms (Collective)	Approved
	71-5-0009	Conduct Open Source Intelligence (OSINT) Analysis	71 - Combined Arms (Collective)	Approved
	71-5-0010	Conduct Human Factor Analysis (HFA)	71 - Combined Arms (Collective)	Approved

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	150-718-2300	Perform Information Collection	150 - Combined Arms (Individual)	Approved
	171-133-5003	Assist the S3 in Preparation of Operation Orders	171 - Armor (Individual)	Approved

Supporting Drill Task(s): None

TADSS

Step ID	TADSS ID	Title	Product Type	Quantity
No TADSS specified				

Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
No equipment specified			

Material Items (NSN)

Step ID	NSN	LIN	Title	Qty
No equipment specified				

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 FM 5-19, Composite Risk Management. Leaders will complete a DA Form 7566 COMPOSITE RISK MANAGEMENT WORKSHEET 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, NBC Protection, FM 3-11.5, CBRN Decontamination. .