13TH ICCRTS
"C2 for Complex Endeavors"

An Analysis of Situation Development in the Context of Contemporary Warfare

Topic 1 - C2 Concepts, Theory, and Policy
Topic 4 -- Cognitive and Social Issues
Topic 7 – Network-Centric Experimentation and Analysis

Gerald M. Powell, Christopher J. Matheus, Brian Ulicny,
Robert Dionne, Mieczyslaw M. Kokar and David Lorenz

Point of Contact:
Christopher Matheus
VIStology, Inc.
5 Mountainview Drive
Framingham, MA 01701 U.S.A.
508 788-5088
cmatheus@vistology.com

Abstract. This paper is the result of an analysis of the Situation Development process as carried out today by the US Army in both conventional and unconventional (e.g., asymmetric, counterinsurgency and urban) warfare. Definitions of situation development in current field manuals and other doctrinal documents are almost exclusively confined to its application to conventional warfare in which the enemy is clearly defined, its operational strategies and tactics are well understood, the activities occurring on the battlefield can be finely monitored with deployed sensors and observers, and situations unfold over hours or days. In confrontations faced by today's military the enemy is often poorly defined and hard to differentiate from civilians, its modes of operation are evolving and lack a standardized military doctrine, its activities must be gleaned primarily from human intelligence, and situations develop over months or years. The analysis outlined in this paper attempts to define situation development in a way that accounts for the new face of contemporary warfare. In addition, we present a breakdown of the situation development process to help elucidate various aspects of the problem that make it particularly challenging in the context of unconventional warfare.

Keywords: situation development, situation awareness, contemporary warfare, asymmetric warfare, military intelligence

1 Introduction

We have studied the Situation Development process as carried out today by the US Army in both conventional and unconventional (e.g., asymmetric, counterinsurgency and urban) warfare. Definitions of situation development in current field manuals and other doctrinal documents are almost exclusively confined to its application to conventional warfare in which the enemy is clearly defined, its operational strategies and tactics are well understood, the activities occurring on the battlefield can be finely monitored with deployed sensors and observers, and situations unfold over hours or days. In confrontations faced by today's military the enemy is often poorly defined and hard to differentiate from civilians, its modes of

operation are ill defined and constantly changing, its activities must be gleaned primarily from human intelligence, and situations develop over months or years. The analysis outlined in this paper attempts to define and describe situation development in a way that accounts for the new face of modern warfare. The paper begins with a review of existing definitions of situation development and then proposes a new definition. We then discuss a number of analyses of the problem from the literature before proposing a breakdown of the problem along several dimensions, ultimately coming to a process decomposition, which we explore in detail.

2 Situation Development Definition

Situation Development is mentioned throughout US military doctrine but it tends to be rather loosely and inconsistently defined and very little is said about "how" it is done. Furthermore, most definitions and uses of the term occur in the context of conventional warfare and as such do not address some of the nuances encountered in asymmetric warfare and complex operational environments.

As a basis for comparison we consider first two definitions for situation development as provided by U.S. Army FM 2-0 "Intelligence":

> *Situation development is a process for analyzing information and intelligence about the enemy and environment during current operations. The process helps the intelligence officer recognize and interpret the indicators of enemy intentions, objectives, combat effectiveness, and potential ECOAs. Situation development*
> - *Confirms or denies threat COAs.*
> - *Provides threat locations.*
> - *Explains what the threat is doing in relation to the friendly force operations.*
> - *Provides an estimate of threat combat effectiveness.*

And Army FM 34-3 "Intelligence Analysis":

> *Situation development enables commanders to see and understand the battlefield in sufficient time and detail to make sound tactical decisions. It helps locate and identify enemy forces; determine their strength, capabilities, and significant activities; and predict their probable courses of action. Situation development helps the commander to effectively employ available combat resources where and when the decisive battles will be fought. Also, it helps prevent the commander from being surprised.*
>
> *… Analysis in support of situation development continues the IPB process and portrays significant aspects of the enemy, weather and terrain in support of the decision-making process.*

In these definitions the focus is on the identification of the *enemy*, their location, capabilities and likely courses of action. In short, the intent is to provide a best estimate of what the enemy is doing and what they might do next. This can be summarized as ***hypothesizing*** the *current* and *projected enemy courses of action* (ECOA). Since there are an overwhelming number of possible ECOAs in any situation it is necessary to filter out all but the most likely and or threatening.

In complex operational environments situation development needs to be concerned with more than just the enemy; the identity, locations, dispositions, capabilities and potential actions of the local populaces and host nation governments also require attention. Again this amounts to the generation of hypotheses concerning their current and future courses of action.

Taking these issues and concerns into consideration, we propose the following working definition of situation development that treats it as a multi-step process while encompassing conventional warfare, asymmetric warfare and complex operational environments:

Situation Development is an ongoing process carried out by a team led by intelligence analysts to estimate current and future threats to friendly forces, the local populace and host nation government interests within

a unit's area of operation and with respect to the current and planned friendly-force missions; and to communicate the essential aspects of the outcome of this process (i.e., most dangerous and/or likely ECOAs and IRs) to commanders and key personnel.

Inputs to the situation development process come from the output of other intelligence processes such as IPB, PIR Answering, Collection Management, etc. These inputs include existing ECOAs, intelligence reports, combat information reports, TTPs/doctrine, PIR/IRs, METT-TC and DIME/PMESII/ASCOPE information, and assessments of recent activities and events.

The output of situation development is a collection of descriptions of the most likely and/or threatening ECOAs to be disseminated to the immediate commander as well as to commanders on down to the lowest level echelons. Additionally, new intelligence requirements (IR) may be generated that if answered would help to identify which ECOAs are being carried out or planned.

3 Breakdowns from Military Literature

In this section we consider three breakdowns based on field manuals and military literature pertaining to ECOA development in asymmetric and counterinsurgency environments. More specifically, these breakdowns are:

1) a breakdown based on the dimensions used in the Asymmetric Threat Matrix approach to ECOA identification and ranking

2) a breakdown according to the process of determining Threat Course of Action in the field manual on Intelligence in Counterinsurgency

3) a breakdown based on the adaptive methodology for developing ECOAs developed by Col. Jack Kem

3.1 Asymmetric Threat Matrix Breakdown

The "Asymmetric Threat Matrix" (ATM) is an Excel spreadsheet program with an accompanying descriptive whitepaper and PowerPoint presentation by Capt. Adam S. Talkington, then at Ft. Leonard Wood, MO. It was developed in late 2001 and early 2002. The purpose of the Matrix was:

> To identify most probable, feasible, dangerous and likely Enemy Courses of Action (COAs) in order to prioritize force protection effort in the Area of Operations.

As such, this threat matrix originates in force protection, rather than in a more forward-operating perspective.

The Matrix specifies each threat ECOA as a complex of four factors: enemy group, goal, avenue of approach (AoA), and delivery system.

- Each enemy group (e.g., Criminals, Foreign Terrorists) is assigned a rank from 20 (most) to 1 (least) by order of prevalence of threat. Enemy groups are denoted by Roman numerals. The threat group characterizes the group that would carry out the attack, not the sponsor of the attack.

- Each enemy goal (e.g., Disrupt activities, Harm individuals, Damage facilities) is assigned a rank (from 20 to 1, most to least) by order of likelihood for the group. Goals are denoted by capital letters. The characterized goal refers to the immediate goal of the ECOA, not the long-term goal of the group.

- Each Avenue of Approach (Air, Road, Water, Cyber, etc.) is assigned a rank from 20 to 1 by order of the number of people likely to be potentially reachable by an attack using that Avenue of

Approach. Avenues of Approach are denoted by Arabic numerals.

Each Delivery System is then ranked from 20 to 1 by order of ease of acquisition and use. Delivery systems are denoted by lowercase letters. Alternatively, this is the most proliferated means for carrying out the attack. This characterization is made at the potential point of impact: A pedestrian who drives onto an installation, gets out of his/her car and places a satchel charge near a water tower would be considered a Pedestrian, not a Car with respect to Delivery System.
Examples:

1. IV, F, 1, a. = (Foreign Terrorist) x (Intending to Harm the Lives of the US Military & Family Community) x (by using the Air Corridor) x (to fly a plane) into a building/crowd/MEVA. = 17 x 16 x 18 x 6 = 29,376

2. IV, F, 1, l. = (Foreign Terrorist) x (Intending to Harm the Lives of the US Military & Family Community) x (by using the Air Corridor) x (release particles of bio/chem. hazard) into the Area of Operations/MEVA. = 17 x 16 x 18 x 13 = 63,648

Discussion: The ATM is essentially a Risk Assessment (RA) approach to ECOA ranking, like the CARVER method discussed below. In RA, risk is characterized by two quantities:

1. the magnitude (severity) of the possible adverse consequence(s), and

2. the likelihood (probability) of occurrence of each consequence.

Consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time). The total risk is the sum of the products of the consequences multiplied by their likelihoods. The ATM model represents a slightly more sophisticated application of these ideas.

The numerical values assigned in the ATM are quite subjective. This technique seems possibly effective at producing a ranking of threats, but the numerical assessment of risk is questionable due to the subjectivity in assigning numerical values. More realistic metrics for each coefficient could be imagined. For example, group prevalence could be expressed in terms of percentage of total enemy; likeliness of group goal could be measured in terms of likelihood that enemy fighters mention the goal in interrogations or documents (open source and captured). The ranking of avenues of approach in terms of number of potential victims might be adequate, but why rank delivery systems in terms of only their ease of acquisition and use rather than the number of potential victims as well as their ease of acquisition and use? According to this system, the threat of car bombs would be calculated as dependent upon the number of potential car bomb victims multiplied by some factor representing the ease of acquiring and using a car bomb, whatever that is. But the correct representation of the ECOA should be in terms of the total number of attacks possible by that means, not a single attack. A car bomb can kill, say, 200 people maximum, but given the relative cheapness of producing car bombs, the total number of victims is much higher.

Additionally, there is a problem of incommensurability between types of damage. Avenues of approach are ranked in terms of the number of people affected, but there is no ranking for the severity of the effect. The same number of people might be inconvenienced by a power outage or phone disruption as a radiological weapon, but the degree of the effect is quite different and important. For example, how would one characterize the number of people affected by the bombing of an empty mosque, for example? As the number of local Muslims of that sect? All Muslims of that sect? All Muslims? There are many questions of commensurability here.

In the ATM, every possible ECOA is assigned a coefficient of 1 or 0 if it is feasible/unfeasible to use this avenue of approach and delivery system to achieve the goal of the ECOA. Since the feasibility factor is

multiplied through, saying something is unfeasible is equivalent to saying that it is impossible. Unfeasibility judgments could just be a failure of imagination, however. It might be worthwhile to assign every ECOA some small degree of possibility, however unlikely.

Finally, no attempt is made to factor historical or geographical patterns into the analysis. The fact that an ECOA has been used numerous times before plays no part, nor does the fact that an ECOA was successfully or unsuccessfully used in another area. This seems to be a deficiency as well.

3.2 Intelligence in Counterinsurgency

FM 3-24 (Counterinsurgency) contains a section called "Determine Threat Courses of Action" in chapter 3 "Intelligence in Counterinsurgency" (written by Kyle Teamey, apparently). The entire manual contains no mention of Situation Development.

The relevant paragraphs are these:

3-114. The purpose of this IPB step is to understand insurgent approaches and tactics so they can be effectively countered. The initial determination of threat courses of action focuses on two levels of analysis. The first is determining the overall approach, or combination of approaches, the movement leaders have selected to achieve their goals. The second is determining tactical courses of action used to execute that approach.

115. The insurgents' approach is based on their objectives, desired end state, and requirements of the operational environment. The approach and the tactics used to execute it set the conditions for the insurgents to achieve their desired end state. Insurgents can accomplish this goal by maintaining preexisting adverse conditions or by creating those conditions.

116. Approaches may have the following indicators:

Table 3-6. Potential indicators of insurgent approaches

- **Conspiratorial**
  - Absence of overt violent or informational actions.
  - Large cadre relative to the number of combatants in the organization.
  - Small mass base or no mass base at all.
- **Military-focused**
  - Presence of leaders and combatants, but little, if any, cadre or mass base.
- **Urban**
  - Terrorist attacks in urban areas.
  - Infiltration and subversion of host-nation government and security forces in urban areas.
  - Organization composed of small, compartmentalized cells.
  - Cadre and mass base small relative to the number of combatants.
- **Protracted popular war**
  - A large mass base.
  - Overt violence.
  - Heavy use of informational and political activities.
  - Focus on building popular support for the insurgency.
- **Identity-focused**
  - Presence of a resistance movement.
  - Presence of an "us-and-them" gap between the government and one or more ethnic, tribal, or religious groups.
  - Large mass base of passive and active supporters built around preexisting social networks.
  - Many auxiliaries.
  - Small cadre composed primarily of traditional authority figures.
  - Large numbers of part-time combatants.

Insurgents base their tactical courses of action on their capabilities and intentions. Evaluating the support, information, political, and violent capabilities of insurgent organizations was discussed in paragraphs 3-95 through 3-106. The intentions come from goals, motivations, approach, culture, perceptions and leadership personalities. Insurgents may pursue many different courses of action in an AO at any time. Their tactical courses of action change with both time and location. People and their attitudes, both within the nation and often outside it, are the ultimate targets of the insurgents. Therefore, commanders pay special attention to the effects insurgent actions have on the populace and how the insurgents achieve those effects. Finally, tactical actions can have strategic effects. This is because insurgent propaganda and media reporting can reach a global audience, multiplying the effects of insurgent tactical actions. Insurgents can employ a wide variety of tactics. (See table 3-7.)

So, essentially, the COIN manual provides the following guidance:

1. Determine the threat capabilities. This includes:
    - Threat support
    - Information/communication capabilities
    - Political capabilities
    - Violent capabilities
    - Insurgent organization
2. Determine threat intentions:
    - Goal
    - Motivation
    - Approach
    - Culture
    - Perception
    - Leadership Personality

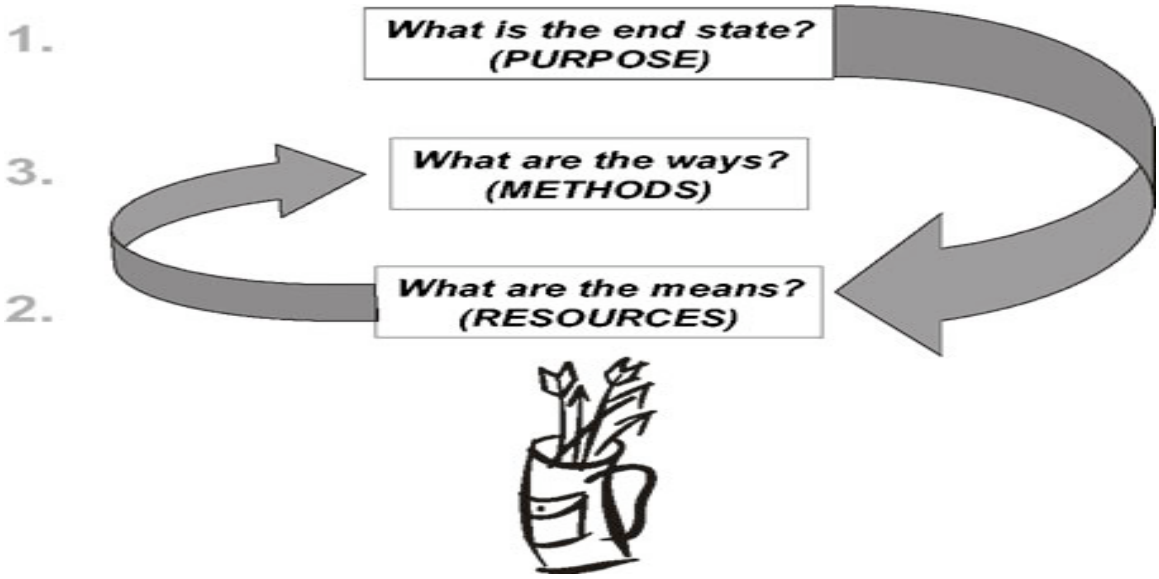
From these, the S2 is supposed to identify and rank the most likely and most dangerous ECOAs. That is as far as the manual goes, however. It does not say HOW one is to use these factors to identify the most likely and most dangerous ECOA, it only specifies that these are the inputs that should be considered. For each tactic, one must ask:

> Is this tactical COA consistent with/probable given the threat's capabilities?
>
> Is this tactical COA consistent with/probable given the threat's intentions?
>
> What effect would this tactical COA have on the local populace?
>
> What effect would this tactical COA have on global opinion?

Beyond these, the manual does not provide guidance on how to rank the most likely or most dangerous ECOAs, or even how to enumerate all the possible (tactical) ECOAs. Admittedly, FM 3-24 is not an intelligence manual, so this is not too surprising. It does, however, provide an account of social network analysis and link analysis methods and tools that are crucial for understanding the structure of the threat organization in a counterinsurgency.

3.3 Kem Methodology Breakdown

"An Adaptive Methodology for Developing Enemy Courses of Action" was published in the Military Intelligence Professionals Bulletin (Jan-Mar 2005), authored by Jack Kem (Colonel, U.S. Army, Retired), an Associate Professor in the Department of Joint and Multinational Operations at the U.S. Army Command and General Staff College (CGSC) at Fort Leavenworth, Kansas.



Kem says "we have no standard methodology for developing ECOAs that is adaptable and assists in maintaining a "running estimate" of the enemy once operations begin." He therefore proposes a methodology consisting of the following steps:

1. Complete a detailed "enumeration of enemy capabilities" paragraph in the intelligence estimate.
2. Develop the "ends": the end state, the Centers of Gravity, and the Decisive Points from the enemy's perspective.
    A. Purpose: What is the enemy's mission (goal?)? What is the end state the enemy wishes to achieve?
    B. Define Centers of Gravity (CoGs): What Center of Gravity is the enemy trying to effect
    C. Identify Decisive Points associated with each Center of Gravity.

Clausewitz defined the center of gravity (COG) as the "hub of all power and movement, on which everything depends."[1] The current approved joint definition is "those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight."[2] The evolving joint definition is "A source of power that provides moral or physical strength, freedom of action, or will to act."[3]

A Decisive Point is defined as "a geographic place, specific key event, critical system or function that, when acted upon allows commanders to gain a marked advantage over an enemy or contribute materially to achieving success." (JP 1-02).

Kem doesn't say how to identify the Centers of Gravity the enemy is concerned with, but another MIPB articles outlines four steps in analyzing an enemy's Centers of Gravity.[4]

a. Determine the enemy's (here, blue forces) critical capability, the absolutely essential function the enemy's system performs. The system might have several capabilities but not all are critical in every situation

b. Identify the enemy's critical capability's source of power, which is the enemy's center of gravity

c. Identify the center of gravity's critical requirements.

d. Identify the critical requirements or components that are vulnerable to attack or disruption.

This leads to Step 3:

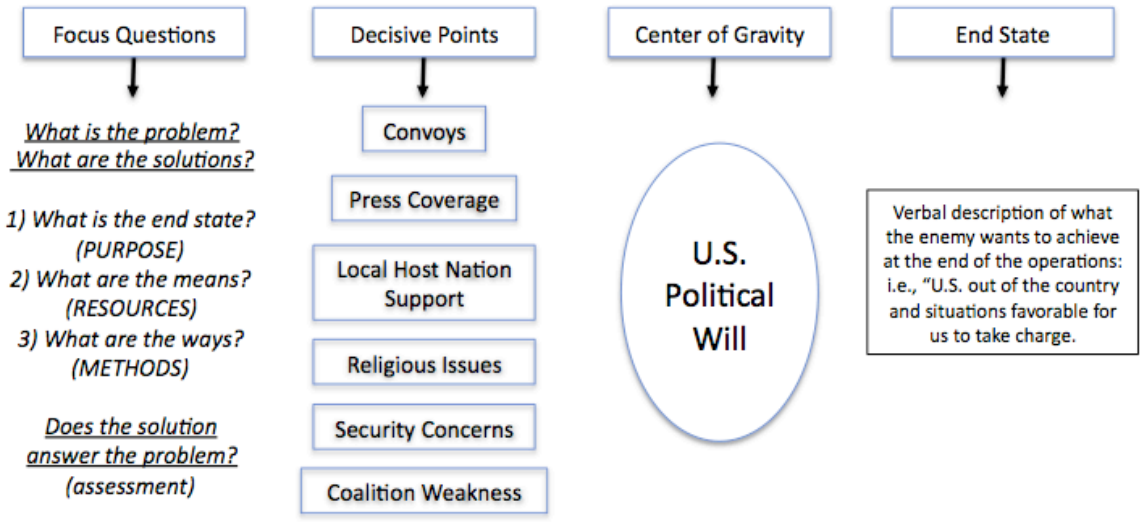
3. Develop the "ways"—reassess the enemy capabilities and resources available. What tasks can accomplish this purpose? (i.e. What can be done to advance the mission?) Kem suggests that this is done by essentially evaluating each combination of capabilities paired with a decisive point: if the enemy is capable of x, y, and z, and applies it to decisive point D, what would the effect be? How likely is the enemy to enact this combination of capabilities and decisive points? As output, then, we must:

Determine most likely ECOA as tactic that embodies "way enemy would prefer to fight. His comfort zone."

Determine most dangerous ECOA as tactic that "causes us most problems".

Step 4. Continually reassess. "Did I get this right?"

Example: Kem then provides an example illustration:



Discussion:

Kem's discussion is at a pretty high level. He does provide a method for enumerating possible ECOAs as pairs of (*capability*, *decisive point*), where the capabilities are a subset of the enemy's current total capabilities. No quantitative methodology is provided for assessing the likelihood or dangerousness of these ECOAs, however.

4 A Process Breakdown of Situation Development

In this section we break the situation development process down into its constituent subprocesses, incorporating as appropriate key aspects of the breakdowns reviewed above. From our definition we take the situation development process to be one in which information from other intelligence processes – which we call "intelligence artifacts" -- are taken in as input and the resulting output is a collection of descriptions of ECOAs that are deemed most likely and or threatening and possibly a set of discriminating IRs. This high level process is depicted graphically in Figure 1.

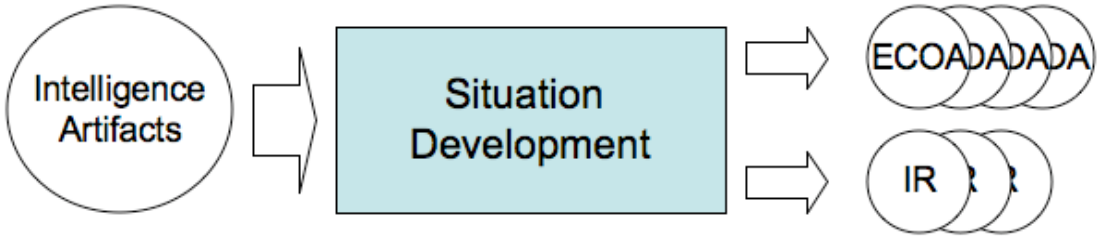


Figure 1: High Level Situation Development Process

A top-level process breakdown based on what we have identified as the fundamental subprocesses is shown in Figure 2. This breakdown consists of the five sequential subprocesses[1]:

1) Analyze Organizations
2) Develop ECOA Hypotheses
3) Evaluate ECOA Hypotheses
4) Generate Discriminating IRs and
5) Describe and Disseminate.

These processes take place within the context of all of the intelligence artifacts generated through other intelligence processes, in particular IPB steps 1 and 2, PIR Answering and Collection Management. This does not mean that all intelligence artifacts are relevant to all subprocesses of situation development; a significant part of the Analyze Intelligence subprocess is in fact the identification of what artifacts are relevant to the generation and evaluation of ECOA hypotheses as they are pulled into the process of developing models of the enemy.

4.1 Analyze Enemy

The "Analyze Enemy" subprocess operates upon intelligence artifacts, many of which resulted from other forms of intelligence analysis. What takes place in this subprocess is the analysis that establishes an understanding of the perceived enemy including their makeup, capabilities, patterns of operation, and possible objectives. The goal is to develop sufficiently accurate models of the enemy to explain their current activities and predict possible future actions. These models may be mental models in the minds of the analysts, computational models executed on computers or a combination of the two (e.g., mental models facilitated through computer based tools for capturing, representing and/or simulating information about the enemy).

[1] These same steps would apply to Neutral COAs and Neutral elements that had the ability to impede our mission, as well.

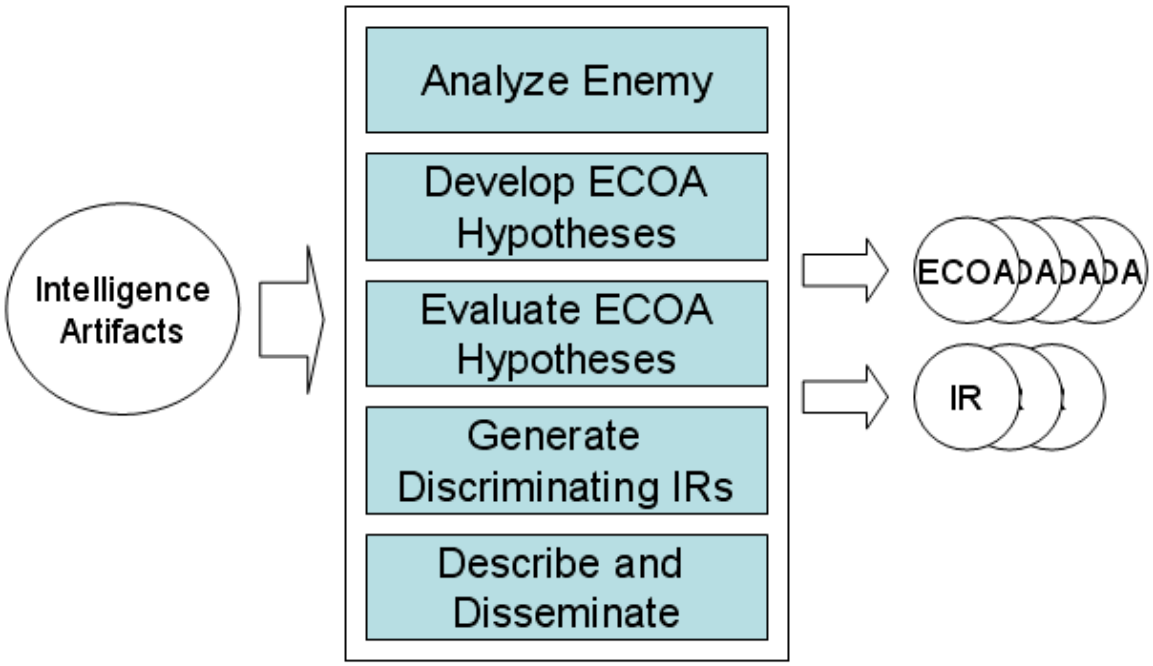


Figure 2: Situation Development Top Level Process Breakdown

Since the Analyze Enemy process is the most complex of the five situation development subprocesses, we have broken it down into more manageable pieces as shown in Figure 3. This diagram also makes it clear the result of this analysis process is a collection of models of the enemy that will be used by subsequent subprocesses. The processes that go into the analysis of the enemy are: Identify Organizations, Identify Capabilities, Identify Methods, Identify Patterns and Hypothesize Objectives. These processes occur in parallel with the products that they produce (models or pieces of models) feeding into and being expanded upon by the sibling processes.

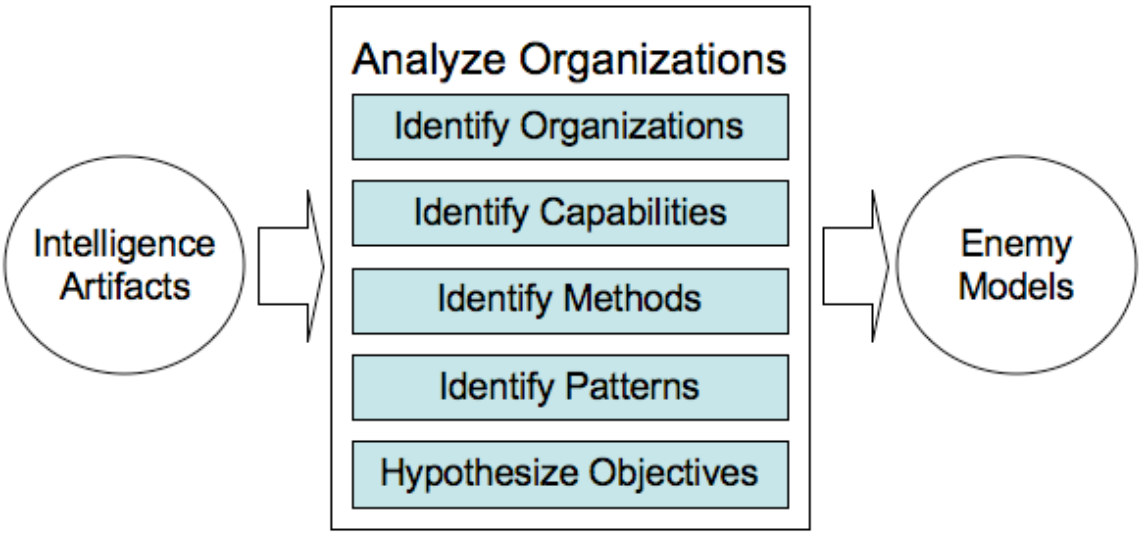


Figure 3: Sub Processes of Analyze Organizations

4.1.1 Identify Organizations

The "Identify Organizations" process seeks to identify and structurally characterize candidate enemy organizations. As shown in Figure 4, this process can be decomposed into separate subprocesses for identifying individuals and roles, identifying the relationships among the organization's parts and identifying affiliations with other organizations. In a conventional context this information traditionally exists within the Threat Order of Battle prepared as part of the initial IPB process and is updated as the conflict evolves. In unconventional environments the enemy is not always as well defined and its supposed organization and affiliations may change frequently. The threat may not even have a hierarchical structure; it may be best described in terms of social network analysis.

Within an organization we need to be able to identify and describe individuals when possible and if not at least be able to postulate roles that some yet to be identified individuals fill. For an individual we would like detailed information about their names and aliases, assumed roles, historical activities, and possible whereabouts. Also important is the relationships between the individuals or roles.

What results from this subprocess is the development of the structural make up and inter-relationships among relevant organizations including not just the enemy but also governmental, societal and NGO organizations. These organization models serve as the basic framework off of which the other elements of the evolving enemy models are associated. Note that not all identified organizations need be "enemy" organizations; some organizations may be identified that are friendly, supportive or hostile to an enemy organization without themselves being an enemy.

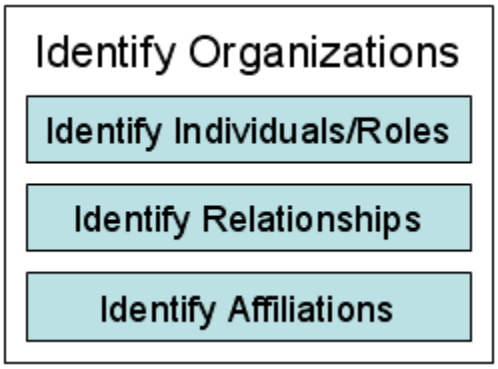


Figure 4: Subprocesses of Identify Organizations

4.1.2 Identify Enemy Capabilities

As in Kem's methodology, identifying the enemy's capabilities is a crucial part of the Analyze Enemy subprocess in which an enemy's resources are characterized. These resources are traditionally a part of the Threat Order of Battle which includes things such as available equipment, systems of delivery, weapons supply and general disposition and levels of training of its members; in asymmetric/counterinsurgency contexts, additional key pieces of information includes sustainability factors such as funding sources, recruitment sources and weapons suppliers. These factors are catalogued in Chapter 3 of FM 3-24.

4.1.3 Identify Enemy Methods

It is important to understand the enemy's preferred and possible patterns of operating (what Kem refers to as the enemy's "method"). This knowledge has been traditionally captured by doctrinal templates that represent the enemy's well-studied operational maneuvers and practices. In unconventional warfare the enemy's modes of operation are typically less well known, can change frequently and are captured more loosely using descriptions of commonly observed tactics, techniques and procedures (TTP). A key challenge in the case of asymmetric/counterinsurgency conflicts is how to anticipate possible new TTPs before they start occurring, or barring that, how to rapidly capture new TTPs from just a small number of incidents.

4.1.4 Identify Enemy Patterns

While doctrinal templates and TTPs capture known enemy methods of operation they do not usually contain information about where or when such methods are likely to be used. Trend analysis of patterns of enemy activities based on recent historical data has become an important part of the problem of understanding how the enemy behaves and how they are likely to behave in the future.

4.1.5 Identify Enemy Objectives

In Kem's methodology emphasis is placed on understanding the enemy's purpose or "ends", i.e., the end state, centers of gravity and decisive points. This amounts to first understanding the enemy's intent (purpose) and then identifying how it might be achieved by influencing various forces (centers of gravity) through leveraging actions focused on specific places, events or functions (decisive points). Unfortunately it is not always possible to know with any certainty the enemy's ultimate intent, and sometimes the intent only becomes evident after some time and experience in observing the enemy's actions or noticing the types of CoG the enemy is trying to affect. For this reason we view the process of Hypothesizing the Enemy's Objectives not as a strict sequence of steps but as a process involving three intertwined subprocesses of Hypothesizing Intent, Identifying CoGs, and Identifying Decisive Points.

4.1.5.1 Hypothesize Intent

The intent of the enemy is a succinct statement of the highest-level objectives that they would like to see achieved in a specific area of operation. For example (returning again to Kem), the intent of the insurgents in Iraq might be "U.S. out of the country". This intent might be refined into sub-objectives, such as for example, "U.S. troops out of Baghdad" and "U.S. troops out of Fallujah". In many cases these intents will exist as "hypotheses" rather than verifiable statements, although intelligence analysis may serve to confirm enemy intents from communication intercepts, interrogations, document exploitation, and so on. In either case the important aspect of intent is how it relates to Centers of Gravity and the Decisive Points that can be used to achieve the desired objectives.

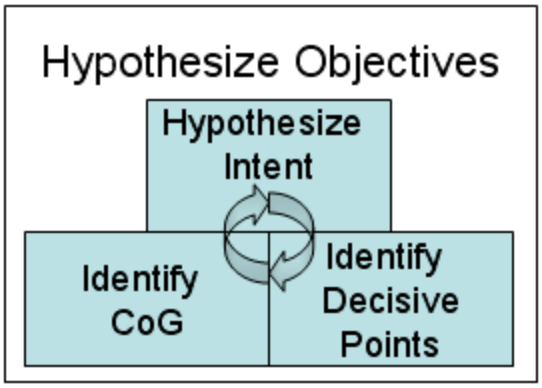


Figure 5: Subprocess of Hypothesize Objectives

4.1.5.2 Identify Centers of Gravity

To achieve their objectives the enemy will need to influence key forces at play in and around the area of operation. These forces are defined as Centers of Gravity (see definition above in Section 3.3) and may be tangible characteristics of a physical entity or infrastructure (e.g., military force, transportation network, power grid) or more intangible forces (political will, civilian support). The CoG can be identified by a simple statement ("U.S. political will") but as such they are not very useful unless their connection to the enemy's objectives is understood (i.e. how/why would a change in a CoG help achieve the enemy's objectives?) and unless specific decisive points can be identified that would enable the enemy to affect a change in the CoG. An understanding of these connections relating CoGs to intents and decisive points requires a behavioral model that can accurately represent how changes in one part of the model result in changes in other parts. Such models may be purely "mental models" in the minds of the analyst or they may be computational models that capture the key behavioral interdependencies among the conceptual elements (or some combination of the two).

The problem of developing CoG models is perhaps the most daunting of all the situation development analysis problems because of the wide variety and complexity of the forces/powers that may be involved, particularly in unconventional, complex operational environments (e.g., asymmetric, counterinsurgency, urban). It is no longer sufficient to understand the military and political powers alone; complex intertwined cultural, societal, governmental, tribal, and infrastructural forces may all be at play. This is the focus of the DIME[2] and PEMSII[3] factors that now play a major role in the IPB Process. Developing, verifying, maintaining and employing complex models based on these factors is an overwhelming challenge that cannot be fully or objectively achieved by the unaided mental capacity of a group of human analysts.

In his Military Review article, Eikmeier recommends the following steps for developing CoGs (see Section 3.3 for more details):

1) Determine the enemy's critical capability,

2) Identify the enemy's critical capability's source of power

3) Identify the center of gravity's critical requirements

4) Identify the critical requirements or components that are vulnerable to attack or disruption

The last step is more closely aligned with Kem's use of decisive points.

4.1.5.3 Identify Decisive Points

To affect a change in a CoG the enemy must have a decisive point (or what might be called a "leverage point"). A decisive point is some tangible entity, event or function that an enemy can take action against or for that will in turn shift the CoG in a favorable direction (from the perspective of the enemy). A decisive point can be given a label (e.g., "U.S. convoys") but again it is only useful if the (possibly complex) relationship it has with the CoG is understood, i.e., a model is developed for how the concepts are interrelated. It also becomes important for this model to be tied into the models of the enemy's organization, capabilities, and practices because a decisive point cannot be employed if the enemy does not have the means or ways for doing so.

4.2 Develop ECOA Hypotheses

At some point in the process the development of enemy models in the Analyze Enemy subprocess must be interrupted in order to generate ECOA hypotheses. This subprocess aims to search a space of candidate hypotheses for consideration in the next step (Evaluation). So what is the nature of this search space?

An ECOA describes to the extent possible 1) **who** the enemy is (e.g., local Al Qaeda), 2) **what** actions they are taking or planning (e.g., attack) 3) **what** (if any) are their targets (e.g., US convoys), 4) **how** they are executing or planning to execute the action (e.g., use roadside IEDs), 5) **when** they intend to execute the action (e.g., weekday afternoons), 6) **where** the action is to take place (e.g., NAI 34, 56, 77, etc), and possibly 7) **why** they are executing or planning such actions (e.g., to erode US civilian support for the war effort). One way to breakdown the process of Developing ECOA Hypotheses is to consider what is required to answer these seven questions. If we take each of these questions as representing a separate dimension we have a multi-dimensional space in which candidate ECOA hypotheses must reside. This approach is similar to those proposed by the Asymmetric Threat Matrix (which proposed 4 fixed dimensions) and Kem's Methodology (which proposes a two dimensional space using capabilities and decisive points). In addition to the larger number of dimensions, our proposed search space has dimensions that that are unfixed in the sense that the set of values that a dimension will represent can change (for

[2] Diplomatic, Informational, Military, and Economic instruments of power.
[3] Political, Military, Economic, Social, Informational, Infrastructural

example, the "who" dimension will have a set of possible values based on the current set of enemy organizations that have been identified).

Let us now consider how each of these questions can be answered using the products of the Analyze Enemy subprocess described above. While we consider each question sequentially and have ordered them in a way that each tends to build upon earlier ones, we do not intend to that there is a rigid order to the answering of these questions and it certainly is the case that some are necessarily answered together. In particular, as Kem suggests, identifying the enemy's goals helps focus one's thinking about the means they might employ.

4.2.1 Who is the enemy?

The Identify Organizations process developed the set of enemy organizations that are used to answer this question. Each one can be considered in turn as the enemy component for a set of ECOA hypotheses that will be fleshed out by the remaining questions.

4.2.2 What is the enemy's target?

Candidate targets for enemy actions described in ECOA hypotheses can come for several different sources. First, the models of organizations may identify groups towards which the enemy is hostile, making them candidate targets. Second, the pattern of historic activity that the enemy has participated in may identify not only groups that they target but also specific aspects of those groups that they target, for example Shiite mosques or U.S. convoys. Third, the models of the enemy's objectives may identify broad targets in the forms of CoGs or more specific targets owning to identified decisive points.

Targets can be identified at various levels of abstraction from large populations (e.g., the state of Israel) to very specific objects and events (e.g., the lead vehicle in a convoy). While it is generally more useful for targets to be identified as specifically as possible, the level of specificity will naturally depend upon the detail and completeness of the models at hand. In some situations, targets may be identifiable only as a class, not as individuals: e.g., the enemy will target Shiites (it doesn't matter to them which ones, particularly) or Sunni mosques (whichever ones are accessible) or electrical power stations (attacking any of which can disrupt the entire system).

4.2.3 What is the enemy action and how will it be carried out?

We group these two questions "what is the enemy action" and "how is it to be carried out?" together because they are so closely related, the former being more general and the latter focusing more on specifics.

For a given enemy organization and a given target there will be a set of actions or operations they can perform based on the enemy's identified methods and available resources as well as on the vulnerabilities and characteristics of the target.

4.2.4 Where will it occur?

The location of an enemy's action in an ECOA may be evident from the way in which it was derived and the nature of the action. Clearly if the model of the enemy's intent includes details about a specific place or entity it may be possible to derive the specific location directly from the model, or the model may a collection of likely locations (e.g., markets within the AO). Historical data can also be used to identify likely locations. Knowing the environmental requirements of a specific TTP employed by an enemy (e.g., a bridge based IED attack) may permit the identification of plausible locations for this attack even in the absence of historical data.

4.2.5 When will it occur?

The time element in an ECOA will vary in its nature depending upon several factors. If the ECOA Is motivated by a specific event, say a religious holiday, it might be possible to identify a period of time when some activity is most likely (e.g., during the holy week of Ramadan or during Election Day). If the basis for the ECOA is historical reports of recurring types of actions (e.g., repeated IED attacks at the same location) there may be a pattern that shows specific times of the day or week when they are more likely. In

many cases however a specific time or date may not be identifiable at all due to lack of information or the random nature of the enemy's activities.

4.2.6 Why might the enemy want to do this?

This question gets at the issue of enemy intent. If a detailed model of the enemy's objectives, COGs and decisive points has been developed and used to support the generation of the ECOA then answering this question should be deducible from the model. If however the ECOA was developed without a clear understanding of the enemy's intent then the best answer may simply be "because this is what the enemy has been doing recently".

There is value in providing as much information about the enemy's intent as possible. If an ECOA accurately identifies the enemy's intent but gets some of the details wrong about how it is going to take place, it becomes possible for the recipients of the ECOA to see how the enemy's actions are consistent with the ECOA because they achieve the same objectives.

4.3 Evaluate and Select ECOA Hypotheses

After a candidate set of ECOA hypotheses has been developed the next step is to rank them according to some metrics and select those that will be included in the final set of ECOAs. This step is necessary because of the sheer number of possible ECOAs and the desire to keep the working set to a manageable size. In practice this step occurs to some extent in parallel with the hypothesis generation process as decisions are made along the way as to which ECOAs are even worth developing as hypotheses. In any case, a key question becomes that of what metrics to use. The most commonly used metrics are of two types, those measuring likelihood and those measuring threat.

4.3.1 Evaluate and Select Most Likely ECOAs

In evaluating the likelihood of an ECOA there are two main determinants: 1) certainty in the supporting knowledge and data and 2) the enemy's ability and propensity to act as defined by the ECOA.

The matter of "certainty" (or its inverse "uncertainty") arises from the fact that our models and the data they are applied to are usually incomplete and seldom fully accurate. Certain types of computational models can incorporate uncertainty in the way they handle and propagate data (e.g., Bayesian models, Dempster-Shafer[4] models) but they are much less capable of managing the uncertainty associated with the models that are manually constructed with them (systems that learn models from data often provide an indication of the model's reliability, but these require large amounts of training data that are often not readily available – see below). The models constructed by humans, either mentally or using some tool, will be deemed to have some degree of validity based on the modelers confidence in the models ability to reflect reality; this unfortunately is very subjective and relies more often on "gut feelings" or speculation than hard facts. Even when the models are accurate, the lack of complete data may require the postulation of the existence of certain entities or forces, which if present would perfectly explain the enemy's actions or intents; the likelihood of the prediction in such cases is no more likely than that of the truth of the postulations.

The other aspect of judging the likelihood of an ECOA (and the one emphasized in Kem's methodology) is determining the relative degree to which the enemy is able and willing to act according to the ECOA. Is it a way the enemy would "prefer to fight"? In reality this type of reasoning is exactly what the models of the enemy are intended to capture. The stronger your models and the more accurately they reflect the true way the enemy "prefers to fight" the better they will be at reflecting likely behavior. Unfortunately a distinguishing characteristic of enemies faced in unconventional warfare is their tendency to abruptly change their behavior; this too must therefore be part of the model of the enemy, although it is much more difficult to model by design. A system based entirely on training or historical data makes one vulnerable to

[4] Dempster-Shafer theory is a mathematical theory of evidence based on *belief functions* and *plausible reasoning*, which is used to combine separate pieces of information (evidence) to calculate the probability of an event. The theory was developed by Arthur P. Dempster and Glenn Shafer.

surprise by an enemy reacting to our countermeasures. This is the fundamental nature of asymmetric warfare.

4.3.2 Evaluate and Select Most Threatening ECOAs

In evaluating the threat of an ECOA the main determinants are 1) the potential damage to tangible entities such as troops, civilians, equipment, infrastructure and 2) the degree of shift in non-tangible forces and centers of gravity.

In the first cases the degree of damage can be quantitatively measured such as when estimating troop casualties, civilian casualties, equipment loss, infrastructure repair costs, etc, although making these quantities commensurable for evaluating the most threatening is a problem, as we have seen with the ATM: which is more damaging, loss of electricity to 1000 homes or tainting 1000 lbs of food entering the food chain? The process of comparing the relative threat of two or more ECOAs can be like comparing apples and oranges.

Estimating the degree of damage done to an intangible CoG such as "US will to support the war" is that much more difficult and highly subjective, even if some quantification can be made (e.g., number of unfavorable stories on Al Jazeera, etc.).

4.4 Develop Discriminating Intelligence Requirements

When dealing with more than one ECOA it is valuable to have a way to determine which of them (if any) are actually occurring as soon as possible. One of the products of the fourth IPB process step is a list of IRs that can be used to confirm or deny the candidate ECOAs. Ideally one would like to be able to identify IR's that represent leading indicators that identify when an ECOA is about to occur rather than IRs that indicate an ECOA is already underway.

4.5 Describe and Disseminate ECOAs and IRs

In the final step of the situation development process the ECOAs and IRs need to be described such that they can be effectively communicated to their respective end users. IRs can be readily shared simply as written questions with perhaps references to the ECOAs they relate to. ECOAs, being more complex benefit from additional representation formats such as map overlays, situation templates, event matrices, timelines, and other such charts/diagrams.

4.6 Process Refinement: A Meta Process

Situation development is a continuous process that in contemporary warfare may span months or years of time. As analysts become more familiar with an enemy they may develop a keener understanding of what factors are important to consider (e.g., airplanes as bomb delivery devices). In some case this might result in fundamental changes in the very nature of the models that they develop to represent the enemy. The overall process of analyzing the enemy and developing ECOA may not change but the tools and the ways in which they are employed may under go modification. This "process refinement" is not a part of the situation development process itself; rather it is a meta process that operates on the situation development process. As such it may be open to the application of computational methods aimed at improving its results.

4.7 Process Breakdown Task Identification

To tie the separate subprocesses into a comprehensive picture of the tasks that go on during situation development we have constructed a diagram (shown in Figure 6) that relates the various modeling tasks to the generation of candidate ECOAs on through the evaluation and selection of ECOAs and IRs for dissemination. The models that are developed – be they mental models, computational models or some combination of the two – can be very complex, are intimately intertwined and can only be expected to present an imperfect description of the enemy. As a result of these characteristics it is clearly impossible for all of the intricate details of such a model to be maintained in the mind of an analyst alone. In addition to developing, verifying and maintaining the enemy model, the analyst must be able to use it to generate

(from a vast search space of potential candidates) and evaluate a set of likely and threatening ECOAs. The potential for computational tools to facilitate and in some cases enable this type of analysis is undeniably immense.

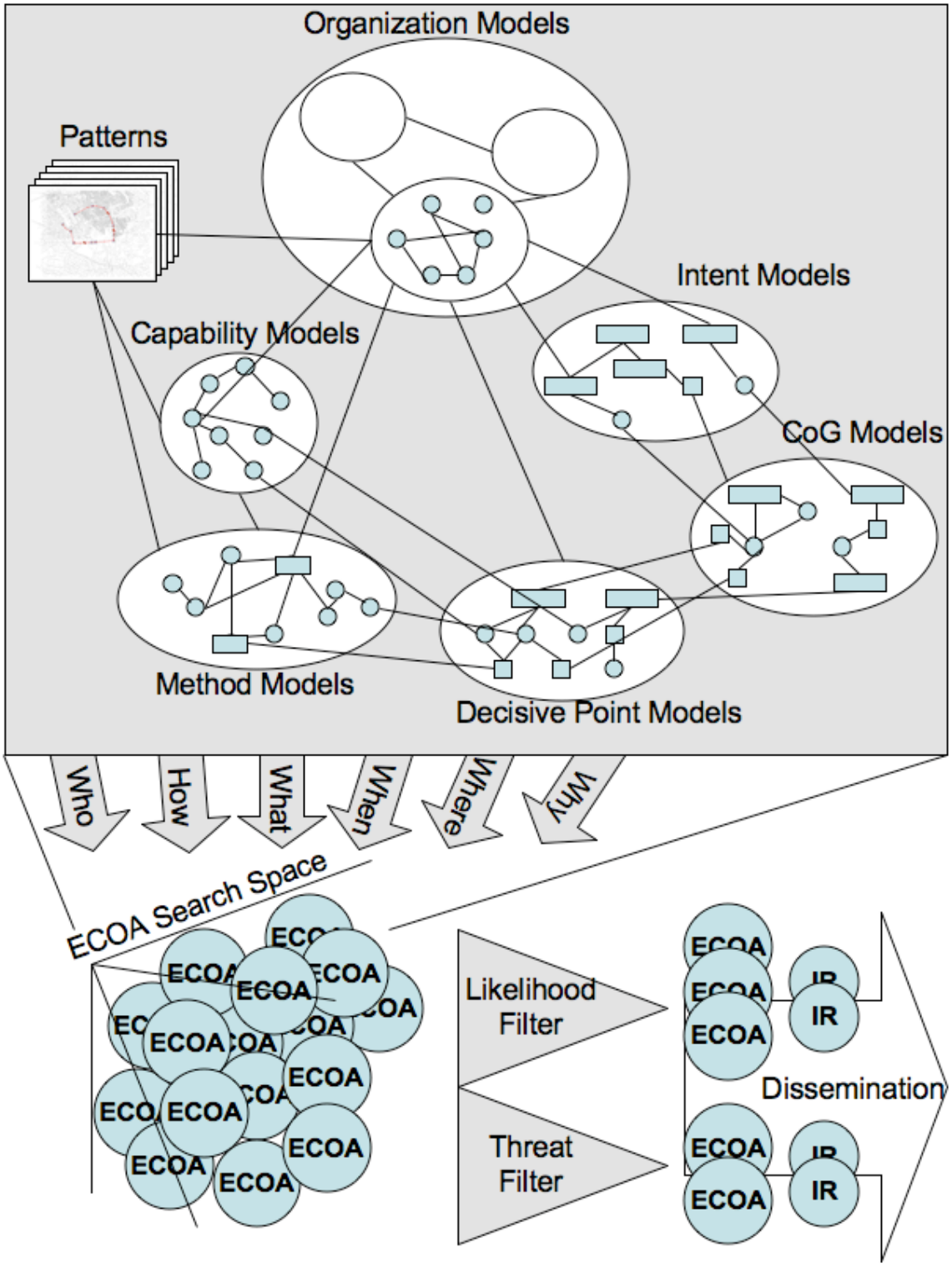


Figure 6: A Comprehensive Picture of Situation Development Tasks

5 Discussion

In this paper, we have analyzed the component processes of situation development in order to develop an analysis of situation development in unconventional warfare that also coheres with the conventional warfare context that is most often assumed in its presentations of military doctrine. To this end, we have presented and discussed three previous process breakdowns of situation development: the first, as embodied in the Asymmetric Threat Matrix tool, the second, as expressed in the "Intelligence in Counterinsurgency" chapter of FM 3-24, and the third as expressed in Jack Kem's article "An Adaptive Methodology for Developing Enemy Courses of Action". From these, it is clearly our contention that the output of situation development is primarily an account of what the enemy is likely to do next expressed in terms of most likely and most dangerous ECOAs and information requirements distinguishing between various ECOAs, and an account of what the enemy is doing now.

Unlike conventional warfare, the likely targets of enemy actions include the local populace, the host-nation government, and global public opinion, in addition to friendly forces. Second- and third-order effects of enemy actions may be more important than the first-order effects in this context, and the effects of enemy action may not be local. Therefore, the dangerousness of an ECOA can't be evaluated primarily in terms of the local, first-order effect on friendly forces. As emphasized by Kem, evaluation of ECOAs requires a higher-order analysis of center of gravity and enemy ends against which to evaluate various threat scenarios for their ability to shift the center of gravity in ways unfavorable to our mission.

Our process breakdown involves capturing a great deal about the enemy's capabilities, intents, perception of the center of gravity, and so on. This leads to a large space of possible ECOAs that (potentially) would have to be evaluated for their dangerousness and likelihood. (In practice, many of these ECOAs may be immediately discounted; but it is worth investigating the reasons why they are not considered.) We have not suggested, nor do we have a methodology to provide for formally ranking the ECOAs for their dangerousness (understood as their effect on a center of gravity counter to our mission) nor for their likelihood (except to the extent that the threat scenario resembles previous incidents). Pattern-based observations might also allow one to infer when the enemy is likely to switch tactics in that the previously successful tactics, if overused, may lose their element of surprise. In order to quantify dangerousness, commensurable metrics for the first- and higher-order effects of a threat scenario with respect to friendly forces, the local populace, the host-nation government, and global opinion would have to be developed.

The purpose of the analysis presented in this paper is to help foster a better understanding of the problem of situation development and to encourage the design and development of the next generation of tools to assist human analysts to carry out the process.

References

1 *On War*, trans. Michael Howard and Peter Paret [New Jersey: Princeton University Press, 1976], 595-96.
2 Joint Publication [JP] 1-02, DOD Dictionary of Military and Associated Terms [Washington, DC: U.S Government Printing Office (GPO), as amended through 8 August 2006].
3 JP 5-0, Joint Operation Planning [Washington, DC: GPO, 26 December 2006), GL-6.
4 Dale C. Eikmeier, "Center of gravity analysis", Military Review, July-August, 2004).