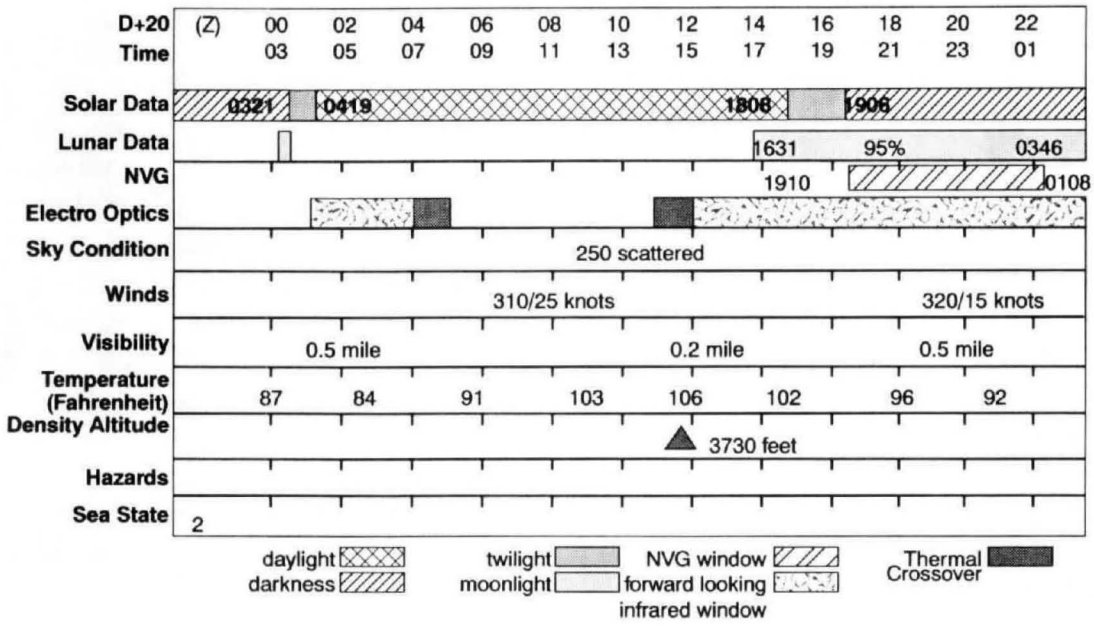

Figure 6-2. Weather Forecast Graphic.

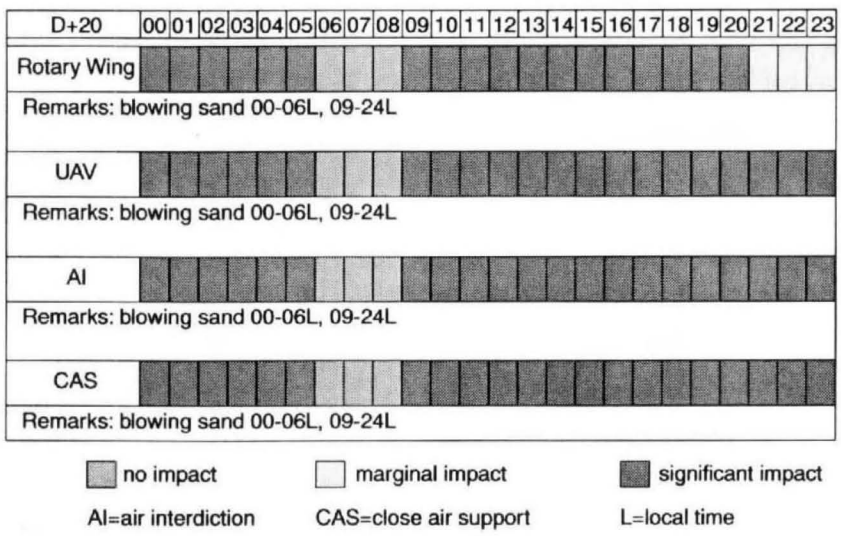

Figure 6-3. Weather Effects Matrix.

SECTION VII. INFRASTRUCTURE ANALYSIS

The infrastructure of a potential AO is a key element of information in an expeditionary environment. Points of entry, transportation systems, economic infrastructure, and social infrastructure, impact how friendly forces enter into, move through, and sustain themselves in the

AO. Infrastructure also impacts a potential threat's ability to conduct operations. The importance of particular facilities depends on the units involved and the type of operations envisioned. The study of a target area's infrastructure must focus on factors that are crucial to mission accomplishment. Most commands, particularly lower level tactical commands, must rely on other organizations and agencies to conduct infrastructure analysis and to provide accessible information.

Sources of Information

Detailed infrastructure analysis can be resource and time intensive, thus identification of analytical requirements prior to conflict or crisis helps ensure the availability of the information when needed. The intelligence staff must be familiar with all sources of infrastructure information that can be rapidly accessed when needed. Infrastructure analyses are performed by—

- Theater joint intelligence centers (JICs).
- U.S. Transportation Command.
- NIMA.
- Defense Intelligence Agency (DIA).
- Service intelligence centers (e.g., National Ground Intelligence Center, MCIA).
- Nonintelligence organizations (e.g., Marine Corps and Army civil affairs units).

Transportation System

In preparing intelligence studies, all transportation facilities must be carefully evaluated to determine their effect on the proposed operations. At higher levels of command, each major facility may be the subject of a detailed study by unit intelligence analysts or by external agencies such as theater JICs, U.S. Transportation Command JIC, or DIA.

Highway or Road Network

For intelligence purposes, a highway means roads, trails, multilane super highways, pack trails, and footpaths. Associated structures and facilities necessary for movement and for protection of routes, such as bridges, ferries, snowsheds, tunnels, and fords are integral parts of the highway system. An adequate highway system is required to conduct a major military operation. Military interest in highways of a given area or country covers physical characteristics of the existing system and various administrative and operational aspects pertaining to construction and maintenance.

Transportation studies should provide information on existing routes, major repair or rehabilitation requirements, and locations of new routes needed to support planned operations. The terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation. When evaluating the road network, analysts should consider—

- Routes in the combat zone should meet minimum standards.
- Roads in rear areas near water terminals, airfields, and supply installations must be well surfaced and capable of carrying heavy traffic without excessive maintenance.
- Operations on a wide front require a large number of secondary routes in forward and rear areas. The information presented in a terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation.
- Large volumes of heavy traffic severely abuse roads.
- Important bridges, intersections, and narrow passes are primary targets for enemy fires or unconventional operations.

- Maintenance should be conducted only on necessary routes.
- Construction of new routes must be held to a minimum.

Railroad Network

A railway includes fixed property belonging to the line. The fixed property includes land, facilities, bridges, tunnels, snowsheds, galleries, ferries, and other structures necessary for the movement of traffic. Railroad studies cover information pertaining to the development, construction, maintenance, and physical characteristics of the existing system. The network's physical characteristics information is necessary for determining capacities and maintenance requirements. Physical characteristics include the railroad's critical features, component parts (e.g., roadbed, ballast, track, rails/gauge), and horizontal and vertical alignment.

When evaluating railroad networks, analysts must consider the following factors:

- Railways are often the main transportation system in countries without an extensively developed road system.
- Suitability for mass movement and low susceptibility to weather effects make railroads useful for logistic support.
- Secondary and feeder railway lines are important to maneuver warfare with its emphasis on dispersal and the requirement for more and smaller rear installations.
- Railways and their associated facilities are highly vulnerable to enemy attack (e.g., sabotage, guerrilla operations).
- Keeping a railroad operational requires trained security forces and extensive protective measures.

Port and Harbor Facilities

Information and intelligence on ports, naval bases, and shipyard facilities is essential for estimating their capacities, capabilities, vulnerability, and other items of military significance. In wartime, principal and secondary ports and bases are prime targets for destruction. A port normally consists of a harbor plus terminal facilities. When natural, improved, or artificial harbors are developed for transactions between ship and shore, they become part of a port. Analysts classify these harbors as coastal, bay and estuary, and river. When evaluating port and harbor facilities, analysts are interested in harbor works, depths, navigable fairways, and anchorage.

Harbor Works

Structures designed to provide shelter, to control water flow, and to regulate erosion for the improvement of the navigability of a harbor are protective or harbor works. Harbor works do not include port facilities that are designed specifically for the transfer of cargo and the servicing of ships. The principal types of structures are—

- Breakwaters.
- Jetties.
- Groins.
- Sea walls.
- Bulkheads.
- Dikes.
- Locks.
- Moles.

Depths

Analysts compute depths of harbors, entrances, anchorages, wharves, and dry docks in reference planes based on tidal levels. When reporting depth, analysts must clearly indicate the reference plane or chart datum on the hydrographic chart. Datum established for ports is the basis for soundings.

Navigable Fairways

The approach, entrance, and the harbor itself frequently determine the size of ships that can

be accommodated in the port. Analysts must evaluate these fairway dimensions and describe any limitations on a ship's navigation (e.g., draft, length, beam, height above water). In addition, analysts should report ships' experiences entering the fairway.

Anchorage

Analysts show anchorage data on large scale charts and plans. Operational information reported includes—

- Anchorage designations.
- Berth assignments.
- Anchoring practices.
- Ships' experiences.

Airfields

Whether military or civilian, airfields are of vital importance to military combat situations. The size and features of an airfield determine its combat and reconnaissance capabilities.

Types

Installations termed airfields include—

- Air bases.
- Airports.
- Airstrips.
- Landing strips.
- Air depots.
- Heliports.
- Helipads.
- Seaplane stations.

Characteristics

Analysts conduct geographic studies to identify the airfield's—

- Type.
- Physical dimensions.
- Construction materials.
- Field condition.
- Support facilities.

Considerations

When evaluating the airfield, analysts report answers to the following questions:

- Is it serviceable?
- Is it occupied?
- Is it under construction?
- Is it in full or partial operations?

Structures and Crossings

Structures and crossings on highways or railways may reduce or interrupt the flow of traffic on a transportation route. Detailed information on structures and crossings is essential to a battlespace analyst and to an engineer, who may be required to repair or restore a structure. These structures and crossings include bridges, culverts, tunnels, galleries, snowsheds, retaining walls, ferries, fords, cableways, and tramways.

Bridges

Highway and railway bridges are vulnerable points on a LOC. Timely preservation, destruction, or repair of a bridge may be the key to an effective defense or to the successful penetration of an enemy area. A bridge seized intact has great value in offensive operations; even a small bridge facilitates the movement of forces over a river or stream.

Analysts obtain bridge information from reconnaissance or from the NIMA-produced planning terrain tactical data base. Using aerial photographs, analysts can determine bridge length, width, clearance, and height above water. Basic information requirements reported on a bridge include—

- Summary of its structural characteristics.
- Critical dimensions (length, usable width, overhead clearance).

- Capacity estimation.
- General conditions.

Tunnels, Galleries, and Snowsheds

Features on a transportation route where it would be relatively easy to block traffic or that affect the traffic capacity of the road, are considered to be critical features of the road. Such features include tunnels, snowsheds, galleries, mountain passes, terrain gaps, gorges and defiles, deep cuts, steep grades, and sharp curves. Any obstructions to traffic flow, which limit the physical dimensions of vehicles utilizing a specific route, are important aspects of route studies. Reductions in traveled way widths, such as narrow streets in built-up areas, drainage ditches, embankments, and war damage limit vehicular movement. Underpasses and other covered traveled ways may restrict traffic flow not only as to width but also as to height.

A tunnel is an underground section of the route that has been made by cut-and-cover or bored for the passage of a route. It consists of the bore(s), a liner (optional), and portals. Common shapes of tunnel bores are semicircular, elliptical, horseshoe, and square with arched ceiling. Bores may be unlined or lined with brick, masonry or concrete. Some long tunnels are artificially ventilated by blowers at the portals or in ventilating shafts above the bore. Alignment of tunnels may be straight or curved.

Snowsheds and galleries are protective structures built in rugged mountainous terrain. These are not as common as bridges or tunnels. Snowsheds offer protection against snow accumulations as well as drifts and slides on exposed sections of the permanent way. Galleries offer protection against snow and rock avalanches. They may be cut into the side of a cliff and have a natural overhang, or the cover may be a concrete slab, either of which guides the avalanche across the track or road. One side of a gallery is usually open.

Retaining walls are built to support embankments, either on the uphill or downhill side of the roadway. Retaining walls also are necessary where an embankment requires support against the pressure of water.

Ferries

A ferry site is that place where traffic and cargo are conveyed across a river or other water barriers by a vessel called a ferry or ferryboat. Ferryboats or vessels vary widely in physical appearance and capacity depending on the depth, width, and current of the stream and the characteristics of traffic to be moved. Propulsion of ferries may be by oars, cable and pulleys, poles, stream current (trail and flying ferries), or by steam, gasoline, and diesel engines. Analysts report the capacity of a civil ferryboat in tons and total number of passengers. In addition, it is often assigned a military load classification number. Ferry slips or piers are generally provided on the shore to permit easy loading of passengers, cargo, and vehicles. The slips may vary from simple log piers to elaborate terminal buildings. A distinguishing characteristic of a ferry slip is often the floating or adjustable approach ramp, which accommodates variations in the ferry deck level.

The limiting characteristics of ferry sites includes the width of the water barrier from bank to bank, the distance and time traveled by the ferryboat from one side to the other side, and the depths of the water at each ferry slip. Climatic conditions have a marked effect on ferry operations. Fog and ice substantially reduce the total traffic moving capacity and increase the hazard of the water route. Therefore, data on tide fluctuations, freezing periods, floods, excessive dry spells, and their effects on ferry operation are important considerations. Ferry slips are often optimal places for grounding displacement landing craft or as exit points for amphibious vehicles.

Fords

A ford is a location in a water barrier where the physical characteristics of the current, bottom, and approaches permit the passage of personnel or vehicles and other equipment under their own propulsion. Analysts assess a ford site for use as a bridge bypass.

Ford approaches may be paved with concrete or bituminous surface material but are usually unimproved. The composition of the stream bottom determines its trafficability. In some cases, the natural river bottom of a ford may have been improved to increase load-bearing capacity and to reduce the water depth. Improved fords may have gravel or concrete surfacing, layers of sandbags, metal screening or matting, timber or wooden planking. Bottom conditions are determined by checking the stability and composition of the bed. Known and suspected ford sites are key information when assessing the ability of a bridge to be bypassed.

Basic information requirements reported on a ford include—

- Trafficability.
- Approaches.
- Bottom composition.
- Current.

Cableways and Tramways

Cableways and tramways may be encountered in rugged mountainous regions and beach areas or used as connections between two primary supply routes. Cableways and tramways are considered obstacles to low flying aircraft.

Inland Waterways

The term inland waterways is applied to rivers, streams, canals, lakes, and inland seas which are used as avenues of transport. It also includes the intercoastal waterways, usually running parallel to the coastline of a landmass and sheltered to permit the navigation of small vessels. When evaluating inland waterways, analysts must consider the following factors:

- Inland waterways provide an economical form of transportation for bulk supplies, freeing faster modes for shipments of a higher priority.
- Depths of rivers and streams fluctuate with maximum and minimum rainfall.
- Falls and rapids commonly interrupt streams with fairly direct courses.
- Streams of low and uniform gradients are usually slow moving and their channels shift constantly, creating sandbars, which are a menace to navigation.
- Traffic is halted completely during a freezing period unless ice-breaking operations can be conducted.
- Thaw following a freeze may cause floods.
- Periods of drought may result in insufficient water for the movement of vessels.
- Waterway locks, bridges, cuts, dams, and other fixed facilities are vulnerable to enemy action.

Supply Systems

Utilities, services, facilities, and construction resources comprise the essential internal supply systems and installations used to protect and maintain the life of a region or city. Military interest in this field is primarily logistical, although these facilities take on greater importance during urban operations, particularly operations other than war. Analysts must report the adequacy and quality of the petroleum and natural gas facilities, as well as power, water, and telecommunications systems, to ensure their maximum use by military forces.

Power System or Grid

Electricity is essential to the life of modern regions and cities. Destruction of electrical generation and distribution facilities in most

cities would bring industrial production and most utilities and services to a halt.

Petroleum, Oils, and Lubricants Facilities

Information on a nation's petroleum and natural gas resources provides a means for evaluating the capacity of a nation to produce, process, and supply fluid or gaseous hydrocarbons for military purposes. Analysts also evaluate the petroleum supply system's vulnerability to attack.

Water

Water is the most extensively used commodity in both urban and rural habitats. Water supply systems maintain and control the quality and quantity of water in urban areas. Analysts evaluate an area's water supply system to ensure there is an adequate supply of quality water for military purposes.

Telecommunications

Analysts evaluate an area's civil and military telecommunications systems, services, facilities, and equipment for use by military forces. Governmental and commercial organizations that regulate and operate the area's systems are also evaluated. Telecommunications services evaluated include—

- Telephone.
- Telegraph.
- Teleprinter.
- Facsimile.
- Data transmission.
- Radio broadcast.
- Television broadcast.

Urban Areas

The ever-increasing urbanization of the world's population dictates that urban areas will increasingly be the AO for war and operations other than war. Urban area geospatial studies are important in the planning of operations, targeting, and logistical support for operations.

Characteristics

Knowledge of the characteristics of urban areas is essential to the conduct of civil affairs and counterintelligence operations. Urban areas are significant as military objectives, targets, and bases of operations. Often they will be the focal point for internal ethnic, class, religious, or cultural conflict. Urban areas may be one or a combination of—

- Power centers (e.g., political, economic, military).
- Industrial production centers.
- Population centers.
- Transportation centers.
- Service centers (e.g., distribution points for fuels, power, water, raw materials, food, manufactured goods).
- Cultural and scientific centers (e.g., seats of learning, modern technological developments).

Urban Area Classification

An important aspect in the classification of cities is the determination of construction type. Rarely is a city of one type of construction; instead there will be a mixture of everything from shantytowns to skyscrapers. The analyst should attempt to determine what the predominant construction type is as well as what percentages of the city are composed of varying types. Urban areas or cities are classified according to their—

- Population size and density.
- Position in the country's society, economy, and defense establishment (strategic, secondary, or minor).
- Function.
- Construction type (e.g., shantytowns, skyscrapers).

Evaluation Factors

Line of sight considerations in cities are crucial, thus the urban area must be assessed in ground-level, above-ground, and below-ground dimensions. Since urban operations are manpower intensive and generally conducted at low unit levels, the information required is usually very detailed. The MCIA-1586-005-99, *Urban Generic Information Requirements Handbook*, discusses the components of urban area analysis. The primary factors evaluated in urban area GEOINT studies include—

- Physical characteristics.
- Building construction type.
- Accessibility.
- Utilities.
- Civil facilities.
- Industrial facilities.
- Military and other important installations.
- Underground facilities (e.g., subways, sewers, underground rivers, utility tunnels).

Construction Resources

Analysts conduct construction resource studies to evaluate a foreign area's capability to support friendly military operations. To determine construction capabilities, analysts compare area construction types to the work carried out by the U.S. Army Corps of Engineers. These studies include data on—

- Available construction materials.
- Construction industry organization.
- Major construction firms, including data on the firm's—
  - Size.
  - Capital assets.
  - Organization.
  - Amount of equipment.
  - Personnel skills.
  - Experience.
  - Specialization.

SECTION VIII. POLITICAL, ECONOMIC, AND SOCIOLOGICAL ANALYSIS

The current and historical setting of a country is an important and integral part of intelligence analysis. Most of the analysis effort is expended on armed forces and GEOINT, but the factors that can make a difference in many operations, especially operations other than war, involve political, economic, and sociological aspects of the target area.

Political Intelligence

Political intelligence begins with an assessment of the internal political dynamics of a country to include its leadership, internal political stability, economic position, labor supply, physical resources, and relative military power. The first consideration is the distribution of political power—is it a democracy, an oligarchy, a dictatorship, or has political power devolved to multiple interest groups such as tribes, clans, or gangs?

Consideration must be given to the sources of political power: authority based on a legitimate constitution and the will of the people, political magnetism, skill and competence of the leaders, or brute force. It is particularly important for western-trained analysts to understand nonwestern political institutions. In other countries, institutions that on the surface are western in nature may in fact operate quite differently. For example, civil and military bureaucracies may not be neutral agents of policy but may operate almost entirely in their own self interest. Armies

may function as political parties or administrators rather than as guardians of the national security. Parliaments may have a developmental or honorary role rather than a legislative role.

The analyst must evaluate the political system as it really operates, not the way it is supposed to operate. Political analysis of a foreign country begins with an assessment of the basic principles of government, governmental operations, foreign policy, political parties, pressure groups, electoral procedures, subversive movements, as well as criminal and terrorist organizations.

Basic Governmental Principles

The starting point of political analysis is the formal political structure and procedure of a foreign nation. Analysts must evaluate—

- Constitutional and legal system.
- Legal position of the legislative, judicial, and executive branches.
- Civil and religious rights of the people.
- People's national devotion to constitutional and legal procedures.

Governmental Operations

Governments are evaluated to determine their efficiency, integrity, and stability. Information about how the government actually operates and changes in the method of operation give the intelligence user clues about the probable future of a political system. When assessing governmental operations, analysts should consider the following:

- Marked inefficiency and corruption, which differs from past patterns, may indicate an impending change in government.
- Continued inefficiency and corruption may indicate popular apathy or a populace unable to effect change.
- Increased restrictions on the electoral process and on the basic social and political rights of the people may mean the government is growing less sure of its position and survivability.

Foreign Policy

Analysis of a target country's foreign policy addresses the country's public and private stance toward the United States, foreign policy goals and objectives, regional role, and alliances. Analysts gather foreign policy data from various sources, to include—

- Diplomatic and military personnel.
- Technical collection systems.
- Official foreign government statements.
- Press releases.
- Public opinion polls.
- International businessmen.
- Academic analyses.

Political Parties

Analysts study special interest parties and groups, (e.g., labor, religious, ethnic, industry) to evaluate their—

- Aims.
- Programs.
- Degree of popular support.
- Financial backing.
- Leadership.
- Electoral procedures.

Pressure Groups

With few exceptions, most states have some type of formal or informal pressure groups. Examples include political parties, associations, religious or ethnic organizations, labor unions, even illegal organizations (e.g., banned political party). The analyst must identify these pressure groups and their aims, methods, relative power,

sources of support, and leadership. Pressure groups may have international connections, and in some cases, may be almost entirely controlled from outside the country.

Electoral Procedures

Elections range from stage shows of limited intelligence significance to a means of peaceful, organized, and scheduled revolution. In addition to the parties, personalities, and policies, the intelligence analyst must consider the circumstances surrounding the actual balloting process and changes from the historical norm.

Subversive Movements

In many countries there are clandestine organizations or guerrilla groups whose intention is to overthrow or destroy the existing government. When analysts report on subversive movements, they should include the organization's—

- Size.
- Character of membership.
- Power base within the society.
- Doctrine or beliefs system.
- Affiliated organizations.
- Key figures.
- Funding.
- Methods of operation.

Criminal and Terrorist Organizations

Criminal organizations in some countries are so powerful that they influence or dominate national governments. Analysts must examine the organization's influence or forceful methods of control. Most terrorist organizations are small, short-lived, and not attached to any government. Analysts should determine if external factors or even the area's government assists the terrorist group.

Economic Intelligence

The study of economics involves the production, distribution, and use of wealth. It analyzes the factors of production and how those factors are used to produce the things that people need and want. Economics focuses on production within nations and on relations between nations, especially on the competition for the world's scarce resources. That competition continues to be a major cause of international conflict.

Economic intelligence focuses on the use of natural and human resources, and especially on the functioning of national economies and economic relations between countries. Economic intelligence is vital to estimating the magnitude of military or other threats to ourselves and our allies. A nation can undertake and carry out only those operations, military or economic, that its economy is able to mount or sustain. In the short run, national strength consists of manpower that can be mobilized and weapons and supplies that have been manufactured or purchased.

The extraordinary expense of modern warfare means that anything beyond the briefest of campaigns will require the total economic resources of a nation. Despite the simplicity of the concept, this task is elusive and difficult.

A large nation's economic resources offer a wide range of possible actions. For example, efforts to increase military preparedness do not necessarily foretell military aggression. While it is possible to develop probability estimates based on key indicators, it would be unwise to think that analysis of economic information alone will yield completely dependable results.

Economic intelligence provides indications and warning of potential crisis or conflict. Economic failure often generates social unrest or disputes with neighboring nations. The resulting instability

may require United States or other national force intervention.

Sources of Economic Intelligence

Because nations and businesses often hide information to limit competition or to prevent the discovery of sensitive military-related technologies, the most reliable information may have to be obtained from more traditional intelligence methods such as informed reporting by attaches and officers on the scene. The most comprehensive and reliable sources of economic intelligence are printed and electronic trade and business publications. These open sources should be supplemented with reports from—

- Attaches and officers on the scene.
- Foreign broadcasts.
- Defectors.
- Commercial contacts.
- Clandestine sources.

Evaluation Factors

Analysts gather the following information for economic studies:

- Size of the area's economy.
- Sources of raw materials (e.g., minerals crucial to production of military weaponry).
- Products of the area manufacturers.
- Methods of production (e.g., advanced technologies).
- Profits from narcotics trafficking.
- Funds transfers by terrorist organizations.

Narcotics and Terrorism

Tracking profits from narcotics trafficking has been one of the most useful forms of intelligence activity against these organizations. Drugs enter the United States via a huge number of routes, but the profits exit by a more limited, and potentially traceable, number of routes. In some cases, narcotics are a country's prime resource and export. Terrorist organizations can also be tracked and studied using information on funds transfers, although the amounts tend to be smaller than those of narcotics traffickers.

Sociological Analysis

Analysts must study the way people organize their day-to-day living, including the study of groups within society, their composition, organization, purposes and habits, and the role of the individual in society. For intelligence purposes, analysts study seven sociological factors.

Population

Intelligence data derived from censuses and sample surveys describe the size, distribution, and characteristics of the population, including rate of change. Most countries now conduct censuses and publish detailed data. The U.S. Census Bureau and the United Nations are prime sources for detailed data on foreign populations. Analysts use censuses and surveys to evaluate an area's population in terms of—

- Location.
- Growth rates.
- Age and sex structure.
- Labor force.
- Military manpower.
- Migration.

Characteristics of the People

Analysts study social characteristics to determine their contribution to national cohesion or national disintegration. Social characteristics evaluated by analysts include—

- Social stratification.
- Number and distribution of languages.

- Prejudices.
- Formal and informal organizations.
- Traditions.
- Taboos.
- Nonpolitical or religious groupings and tribal or clan organizations.
- Idiosyncrasies.
- Social mobility.

Public Opinion

Key indicators of a society's goals may be found in the attitudes expressed by significant segments of the population on questions of national interest. Opinions may vary from near unanimity to a nearly uniform scattering of opinion over a wide spectrum. Analysts should sample minority opinions, especially of groups capable of pressuring the government.

Education

Analysts concentrate on the general character of education and on the quality of elementary through graduate and professional schools. Data collected for these studies include—

- Education expenditures.
- Relationship between education and other social and political characteristics.
- Education levels among the various components of society.
- Number of students studying abroad.
- Extent to which foreign languages are taught.
- Subjects taught in schools.

Religion

Religious beliefs may be a potentially dangerous friction factor for deployed U.S. personnel; this was experienced in the Middle East with fundamentalist Islamic sects. Understanding those friction factors is essential to mission accomplishment and the protection of friendly forces. Analysts evaluate data collected on an area's religions, which includes—

- Types.
- Size of denominations.
- Growth or decline rates.
- Cooperative or confrontational relationships between religions, the people they represent, and the government.
- Ways the government deals with religious organizations.
- Roles religious groups play in the national decisionmaking process.
- Religious traditions and taboos.

Public Welfare

To evaluate the general health of a population, analysts must identify—

- Health delivery systems.
- Governmental and informal welfare systems.
- Social services provided.
- Living conditions.
- Social insurance.
- Social problems that affect national strength and stability (e.g., divorce rate, slums, drug use, crime) and methods of coping with these problems.

Narcotics and Terrorism Tolerance

A population's level of tolerance for narcotics and terrorist activities depends on the relations between these organizations and the population as a whole. Analysts should determine if the tolerance is a result of the huge sums of money traffickers pump into the economy or a result of trafficker's use of force. Terrorists may be accepted and even supported by the local populace if they are perceived to be working for the good of the local people. The intelligence analyst must evaluate the way these organizations operate.

CHAPTER 7. THREAT ANALYSIS TECHNIQUES

Intelligence analysts make the greatest impact on plans and operations by conducting threat analysis. Using the IPB threat analysis techniques, analysts provide commanders and planners with paragraphs 3 through 5 of the intelligence estimate (see appendix A). To enhance the intelligence estimate, analysts use specialized analytical techniques. This chapter provides a detailed view of the knowledge essential in conducting threat analysis.

SECTION I. INTELLIGENCE PREPARATION OF THE BATTLESPACE TECHNIQUES

When conducting threat IPB, intelligence analysts evaluate the threat OOB, develop a threat model, and determine, evaluate, prioritize, and develop threat COAs.

Threat Order of Battle

An integral part of intelligence analysis, OOB is the identification, strength, command structure, and disposition of units, personnel, and equipment of foreign military forces, including irregular force units, auxiliary, insurgent, and criminal elements. The analyst must consider and integrate OOB intelligence with other METT-T factors to determine threat capabilities, vulnerabilities, intentions, and COAs.

Order of Battle Factors

The OOB analysis involves evaluating a threat force's composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, command and control warfare (C2W) data, and other supporting data.

Composition

The identification and organization of specific threat units or commands are keys to OOB intelligence. Through identification, the analyst develops a history of the threat unit's composition, tactics, training, and combat effectiveness. To determine a unit's composition, analysts identify the threat unit by—

- Name.
- Number.
- Type.
- Size or strength.
- Subordination.

Organization is the physical structure of a unit and the relationship of the various elements within that structure. The threat unit's identification within an organization alerts the analyst to the possible presence of other units in the same organization. With knowledge of the threat's organization, analysts can develop accurate intelligence on current strength and combat efficiency.

When analyzing composition, intelligence personnel should consider the unit's self-sufficiency. Units subordinate to a self-sufficient tactical unit, although capable of limited independent action, cannot sustain themselves over relatively long periods of time. These subordinate units are seldom employed independently or separately from the basic self-sufficient tactical unit. For example, a new threat battalion is reported to be operating in the AO. Knowing that the threat normally organizes and operates in brigades composed of three

to five battalions and that those battalions are normally not employed independently, analysts determine it is probable that the remaining elements of the threat brigade are in or near the AO.

Disposition

The threat unit's disposition consists of the unit's location and tactical or administrative deployment method. When evaluating a threat unit's disposition, analysts include the unit's current and projected movements to determine the capabilities of the enemy force and its effect on friendly mission accomplishment. A threat that has moved, is moving, or is planning to move may become capable of a number of actions (e.g., attacking, reinforcing, replacing, withdrawing). Analysts must continually monitor threat movements to integrate the threat unit's disposition with terrain analysis into doctrine and situation templates. When assessing a threat unit's disposition, analysts should consider—

- Predetermined doctrinal deployment, which may lead to an accurate appraisal of probable threat COAs.
- Knowledge of the threat's echelon arrangement may indicate which units will be employed in supporting and reserve roles.
- Patrol activity may indicate planned movement (but in itself is not movement).

Strength

A threat unit's strength is described in terms of personnel, weapons, and equipment. Information concerning enemy strength provides the commander with an indication of threat capabilities and helps determine the threat commander's probable COA. When assessing a threat's strength, analysts should consider—

- Lack of strength lowers the threat force's capabilities estimate, while superiority of strength raises the force's capabilities estimate.
- Marked concentration or buildup of units in an area may indicate a probable COA and threat objectives.
- Changes in strength of potential threat forces during peacetime may indicate the threat's intention to wage conflict.

Tactics

In OOB intelligence, tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the threat's accepted organization and employment principles, tactics refer to the threat's conduct of operations. From tactical doctrine knowledge, the analyst can determine how the threat may employ his infantry, mechanized, armor, and artillery units in the offense and defense under various conditions. Analysts integrate tactics in doctrinal templates and other intelligence products.

Training

Individual and unit training can significantly contribute to the combat effectiveness of any military organization. Analysts assess the thoroughness, degree, and quality of individual training received by the threat's recruit, specialist, noncommissioned officer, and officer to determine the overall efficiency of its armed force. When evaluating the threat's training, analysts should consider—

- Small unit exercises to large scale training maneuvers conducted in seasonal cycles are an essential part of the training necessary for a unit to operate at its full potential.
- Each type or phase of training accomplished by a unit adds to its capabilities and effectiveness.
- Crew training for weapons systems (e.g., tanks, artillery, and aircraft) increases weapons systems effectiveness.

Logistics

The threat's adoption of a COA depends on the ability of the logistical system to support that action. With knowledge of the threat's logistic capabilities, analysts can accurately evaluate the threat's capabilities, strength, and combat effectiveness. The location of a threat unit's logistical support structure elements aids analysts in determining the disposition of maneuver formations. Logistic information critical for effective intelligence analysis includes—

- Classes and types of supply.
- Lines of communication.
- Logistical requirements.
- Procurement methods.
- Distribution priorities and procedures.
- Transportation networks and modes.
- Installations and terminals.
- Evacuation and salvage procedures.
- Maintenance.

Combat Effectiveness

The abilities and fighting qualities of a unit are affected by numerous tangible and intangible factors. Analysts are expected to rate threat combat effectiveness by analyzing the following factors:

- Personnel strength, including estimated losses.
- Conditions and amounts of weapons and equipment.
- Status of training.
- Quality of leadership.
- Individuals' combat experience.
- Length of time a unit has been exposed to combat.
- Efficiency and training of the officer and noncommissioned corps.
- Past performance and traditions.
- Commander's personality traits.
- Morale, esprit, health, discipline, and political reliability (belief in the cause).
- Status of technical and logistical support of the unit.
- Adequacy of military schooling.
- Socioethnic characteristics of the people.
- Geographic area in which committed.

For each unit of interest, analysts must define, evaluate, and assign a color value to each applicable factor. This assessment is highly subjective; the experience and knowledge of the analyst and the scope of available intelligence will determine its validity.

Example: Assessment Values

When evaluating the length of time a unit has been exposed to combat, analysts use the following values:

- *Green*—Sporadic to intermittent limited combat (small arms fire, fire fights).
- *Amber*—Constant limited combat to sporadic intense combat (artillery barrage, heavy weapons).
- *Red*—Sustained intense combat (deliberate attack or defense).

Where a factor has elements, analysts assign a value to each element and then synthesize an overall value for that factor. After assigning a value to each factor, analysts assign an overall combat effectiveness rating to the unit. This process is highly subjective, and allowances can be made for prioritizing or weighting the individual factors. The values assigned to factors and the definitions of the effectiveness rating may be adjusted as the situation dictates.

The values and definitions should be understood by personnel using the information and should be marked on summaries or reports disseminated outside the command.

Example: Combat Effectiveness Values

Threat unit combat effectiveness can be expressed as a color corresponding to the following example definitions. The following associated percentages are not indicators of T/O and table of equipment (T/E) strength, but are shown to indicate a relative range for each definition:

- *Green:* Combat Effective (80-100%)—The unit possesses the required resources to undertake the wartime mission for which it is organized or designed. Few, if any, negative factors exist. The unit does not require any compensation for deficiencies.
- *Amber:* Marginally Combat Effective (60-79%)—The unit possesses the required resources to undertake most of the wartime missions for which it is organized or designed. Some negative factors are present. The unit would require little, if any, compensation for deficiencies.
- *Red:* Limited Combat Effectiveness (40-59%)—The unit possesses the required resources to undertake some, but not all, of the wartime mission for which it is organized or designed. Significant negative factors are present. The unit would require significant compensation for deficiencies.
- *Black:* Combat Ineffective (less than 40%)—The unit is not prepared to undertake its wartime mission. Numerous debilitating negative factors are present.

Electronic OOB and Technical Data

Electronic OOB and other electronic technical data are required to plan and execute SIGINT, electronic warfare, CIS, C2W, and other operations against the threat. This data includes threat communications and noncommunications equipment parameters, modulation, multiplex capability, pulse duration, pulse repetition, frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. The data also includes critical threat C2 nodes such as command posts, air defense operations centers, and communications relay sites.

With sufficient data, analysts can template threat emitters, which can be used to locate and develop the disposition of forces based on the forces' electronic emission assets. With electronic technical data, a more accurate evaluation of the threat's vulnerabilities to friendly EA and deception can be determined. Additionally, signals intercept and direction finding for SIGINT production are made easier and enhance support to electronic protection.

C2W Data

Analysis of C2W provides the commander with an assessment of the threat's ability to interfere with the friendly force's C2. The C2W data includes threat assets and capabilities to conduct electronic warfare, deception operations, psychological operations, and information warfare. Of increasing importance is the ability of any enemy to penetrate and disrupt friendly C2 and information systems or to deceive or jam friendly position locating devices (e.g., the global positioning system). This requires knowledge of a threat's deception capabilities, EA systems and protection measures, and monitoring capabilities.

Supporting Data

Analysts need supporting information to develop other OOB elements and comprehensive intelligence estimates. Basic intelligence describes the enemy and includes personalities' biographic data, unit history, uniforms and insignia, vehicle numbers, and other information important to mission accomplishment. Biographic data contains information on characteristics and attributes of a threat force's members. Knowledge of personalities is important in identifying units and, in some

cases, predicting a unit's COA. Personality data is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In MOOTW, supporting data may include tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat force.

Analytical Considerations

When assessing OOB factors, analysts should consider that—

- OOB factors must be analyzed as a whole.
- Changes in training status, command personality, strength, or any other OOB factors may affect a unit's tactics.
- The OOB factors form a framework for evaluation of any force.
- Extended family ties of suspected traffickers should be included when evaluating composition during a counternarcotics operation.
- The insurgent political structure and its relationship to the military elements should be included when evaluating an insurgent force.
- Composition analysis of a local terrorist organization would identify the support infrastructure among the local population.
- The OOB evaluation framework should be adapted to the mission and a unit's needs.
- An aviation unit's evaluation of composition would focus more on threat units that contain air defense assets; the equipment evaluation would focus on vulnerabilities of threat targets and technical characteristics of threat air defense systems.
- Properly maintained OOB files are sources of information on the threat's operations, capabilities, and weaknesses. See chapter 2 for a discussion of OOB files.

Threat Model Development

The threat model is a method of synthesizing information into a coherent evaluation of threat intentions and capabilities and predicting COAs. See chapter 5 for a discussion of doctrinal templates, description of preferred tactics and options, and identification of type HVTs.

Doctrinal Templates

When evaluainge doctrinal templates, analysts must—

- Determine how the threat normally organizes for combat and how he deploys and employs his maneuver units and various supporting assets.
- Look for patterns in task organization of forces, timing, distances, relative locations, groupings, or use of terrain and weather.

Doctrinal templates can also portray the threat's normal organization for combat, typical supporting elements available from higher commands, frontages, depths, boundaries, engagement areas, objective depths, and other control measures. The amount of this detail available will vary from situation to situation or may not exist at all. In the latter case, the analyst will need to rely on basic principles of war and tactics to develop an initial doctrinal template. Doctrinal templates are tailored to the needs of the unit creating them.

Description of Tactics and Options

Like the template, the description of the threat's tactics and options is developed from an evaluation of his doctrine and previous and current operations. Analysts include a description of the branches and sequels available to or preferred by the threat should the depicted operation succeed or fail. For example, the threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, his preferred branches might

include committing reserves, reinforcement, or shifting the main effort. Should the attack fail, his preferred sequel might be a hasty defense.

Analysts include decision criteria revealed in the data base that cause the threat to prefer one option over another. This intelligence will aid in wargaming threat and friendly COAs, targeting, and deception planning. When developing a threat model, analysts use the following techniques to describe tactics and options:

- Start with the scheme of maneuver and examine how each battlespace function provides support.
- Use time-event charts to describe how the threat normally conducts operations. These are particularly useful for describing large-scale air operations, which are difficult to depict graphically. With a time-event chart the time relationship between various echelons and their normal composition can be described easily.
- Make marginal notations on the graphic template and combine words with pictures to enhance understanding. Marginal notes are particularly effective when tagged to key events or positions on the template.
- Use a battlespace or warfighting function synchronization matrix (see fig. 7-1) to dissect threat operations and relate particular actions to time for threats with well-developed tactics and complex combined-arms organizations.

Time	H-10	H-1	H	H+4	H+7	H+8.5	H+10
Friendly Action	Begin move to attack position	Prepare fires	Cross line of departure	Engage 1st echelon	Defeat 1st echelon		
Enemy Decision Point					☆1		
Enemy Maneuver				Local counterattack	Close air support and attack helicopters to counterattack objective	Reserves begin move	Reserves pass NAI 9
Enemy Fire Support		Counterbattery	Engage HPTs	Defensive fires	Countermobility fires	Support reserve in engagement areas 7, 8, and 9	
Enemy Intelligence	Locate main effort	Locate artillery, identify main effort	Locate reserve, HPTs				
Enemy C2					Commit reserve to counterattack option 1 or block options 2 and 3		
Enemy Engineers	Continue counter-mobility in main battle area						

Figure 7-1. Threat Synchronization Matrix.

Identification of Type High-Value Targets

Analysts use the following techniques to identify type (e.g., air defense, engineer) HVTs for the threat model:

- Use tactical judgment when evaluating the data base, the doctrinal template, and its supporting narrative to identify HVTs.
- Mentally war game the threat operation under consideration to determine how the threat will use battlespace assets and to identify those assets critical to the operation's success.
- Identify assets necessary to satisfy decision criteria or initial adoption of the branches and sequels listed in the description and option statements.
- Determine the threat's reaction to the loss of each identified HVT. Consider his ability to substitute other assets and to adopt branches to the operation.
- Rank the set of HVTs in order of their relative value to the threat's operation, record sets as part of the threat model, and note value changes by phase of operation.
- Use a target value matrix to annotate identified HVTs in the margins of the doctrinal template. Figure 7-2 is a threat model depicting a doctrinal template, tactics and options description, and target value matrix.

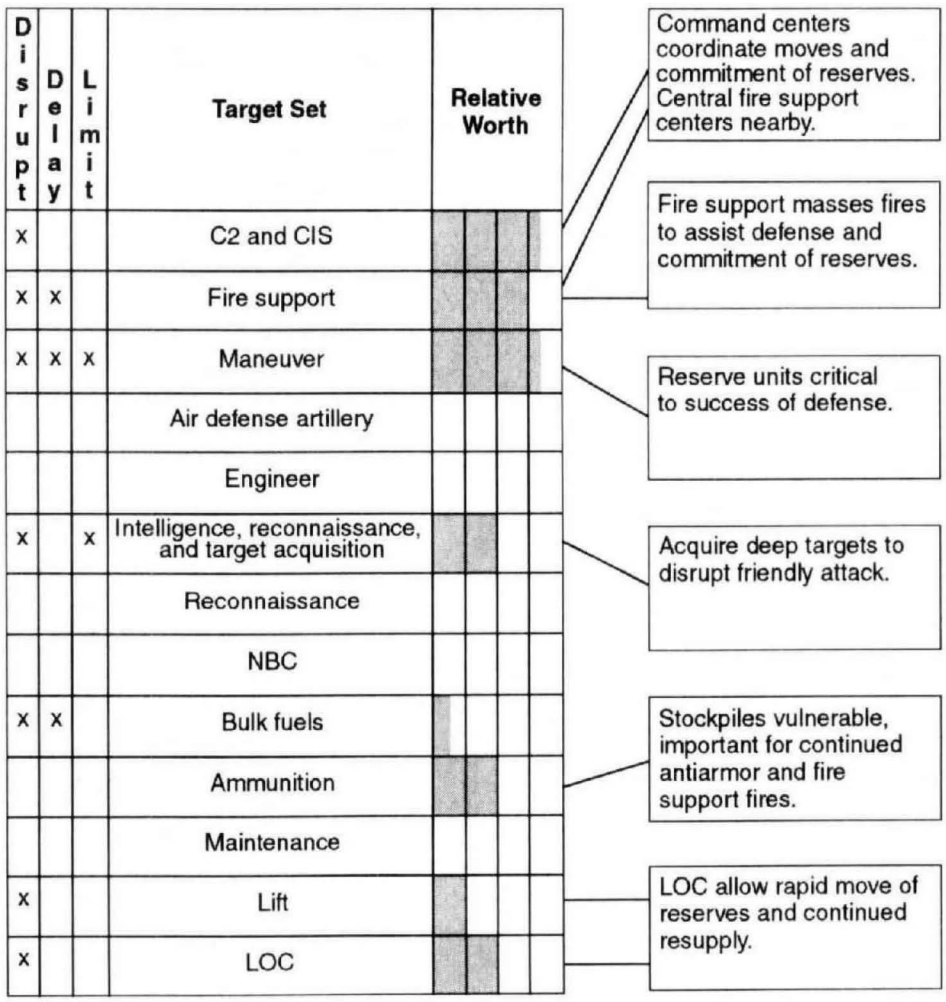

Figure 7-2. Threat Model with Target Value Matrix.

Threat Courses of Action Determination

To determine threat COAs, analysts start with general COAs open to the threat, such as deliberate attack, defend, and delay. They further define each general COA as a set of specific COAs by integrating the threat models developed in IPB process step 3 with the description of the battlespace effects from IPB process step 2.

Criteria for Testing Threat Courses of Action

Analysts must test each enemy COA using the criteria of suitability, feasibility, acceptability, uniqueness, and consistency with doctrine.

Suitability

When determining the suitability of a threat COA, analysts must evaluate the COA's potential for accomplishing the threat's objective.

Feasibility

Analysts evaluating the feasibility of a threat COA must answer the following questions:

- Are the time and space required to execute the COA available?
- Does the threat have the physical means required to make the COA a success?
- What radical measures can he take to create the conditions for success?

Acceptability

In determining the acceptability of a threat COA, analysts must consider the amount of risk involved by answering the following questions:

- Will threat forces accept the amount of risk entailed in adopting the COA?
- Can they afford the expenditure of resources for an uncertain chance at success? (This is a subjective judgment based on knowledge of the threat and his doctrine. In some instances, the threat might undertake otherwise unfavorable COAs, particularly if they are the only means to accomplishing his objective.)

Uniqueness

To determine the uniqueness of each threat COA, analysts must use their experience and training to answer the following questions:

- How will the COA affect the friendly mission?
- Will the threat use reserves or a second echelon?
- Where is the threat's main effort?
- What is the threat's scheme of maneuver?
- How is the threat task-organized?

Consistency with Doctrine and Recent Activities

When evaluating a threat COA's consistency with doctrine and recent activities, analysts must answer the following questions to be consistent with the threat's doctrine and recently observed activities, practices, and patterns.

- Is the COA consistent with the threat's written doctrine and past application of doctrine observation, as revealed in the intelligence data base?
- Will the threat achieve surprise by deviating from its known doctrine?

Considerations

To determine the COAs the threat believes are available, analysts should—

- Consider the effect of friendly dispositions or the threat's perception of friendly dispositions on the threat's COA.
- Conduct reverse IPB or replicate the process the threat is employing to discern friendly COAs.
- Consider the intelligence and reconnaissance assets available to the threat, their ability to collect information and produce intelligence, and the picture that intelligence will give threat commanders.

- Focus on threat COAs that will affect accomplishment of the friendly mission and include those indications that the threat might adopt a COA that favors accomplishment of the friendly mission. This prepares the commander to take advantage of opportunities that might arise.

Example: Threat COA That Favors Friendly Mission Accomplishmentp

If the friendly mission is to attack to destroy the threat, interfering threat COAs could be defend (including counterattacks), reinforce, and withdraw. If the friendly mission is to seize a terrain objective, interfering threat COAs could be defend (including counterattacks) and reinforce. Threat withdrawal would favor the accomplishment of this friendly mission and should also be included in the set of COAs if there are indications the threat might actually withdraw.

- Identify less likely but viable threat COAs by considering the threat's—
  - Superior understanding of the political, cultural, or information characteristics of the battlespace.
  - Ignorance of the military arts and sciences.
  - Immature decisionmaking.
  - Uncertainty as to friendly dispositions or intent.
  - Unexpected objectives or desired end states.
  - Cultural definitions of defeat and victory.
  - Willingness to sustain defeat at the tactical or operational level to achieve victory at the strategic or political level.
  - Desperation.
  - Bureaucratic inefficiency.
  - Audacity.

Course of Action Evaluation and Prioritization

The resulting set of COAs developed should depict the full set of options available to the threat. At this point the analyst should remember that the threat COAs identified are assumptions about the threat, not facts. For this reason, the analyst cannot predict with complete accuracy which of the COAs the threat will employ. However, the commander and staff still need to develop a plan that is optimized to one of the COAs, while allowing for contingency options if the threat chooses another COA. Therefore, the analyst must evaluate, analyze, and form an estimate for each COA and prioritize it according to how likely it is that the threat will adopt that option. The analysts must establish an initial priority list to allow the staff to plan for friendly COAs. Once the commander selects a friendly COA, the analyst may need to reorder the list of threat COAs and consider changes in the threat's perception of friendly forces.

Course of Action Development

Once the complete set of threat COAs has been identified, analysts develop each COA into as much detail as the situation requires and time allows. Analysts base the order in which each COA is developed on its probability of adoption and the commander's guidance. Each COA must answer the following five questions:

- **What**—The type of operation (e.g., attack, defend, reinforce, conduct retrograde).
- **When**—The time the action will begin is usually stated in terms of the earliest time that

the threat can adopt the COA under consideration.

- **Where**—The sectors, zones, axis of attack, AAs, and objectives that make up the COA.
- **How**—The method by which the threat will employ his assets (e.g., dispositions, location of main effort, the scheme of maneuver, and support required).
- **Why**—The objective or end state the threat intends to accomplish.

Course of Action Parts

Analysts consider threat forces available to at least one level of command above their own command when developing each COA. This helps to ensure accountability for possible reinforcing forces and the higher command's own objectives and intent. Each developed threat COA should contain a—

- Situation template.
- Description of the COA and options.
- Listing of HVTs.

Considerations

When considering an attacking threat, less detail is required. For example, depending on the situation, a friendly battalion might need only to work to a level of detail of threat companies. Considering the possible variations in the threat's COA based on the details of employment of individual platoons adds a tremendous amount of effort to the process, perhaps for little gain.

When considering a defending threat, a greater level of detail generally is required. For example, an attacking friendly battalion might be concerned with individual crew-served weapons positions given their relative contribution to the threat's defense.

Operations other than war will generally require a greater level of detail. The situation template may address such things as locations and movements of potential evacuees, displaced persons, or protesters as well as threats such as individual air defense systems and irregular forces. Analysts must focus on what is essential to accomplishing the friendly mission.

Course of Action Key Elements

The key elements of each COA are indicators, NAIs, and HVTs. These key elements will drive the collection and production efforts to determine which COA the threat will actually adopt. The art of identifying initial ICRs and IPRs revolves around—

- Predicting specific areas and activities which, when observed, will reveal the COA the threat has chosen.
- Determining the type intelligence products, formats, and who needs them.

As a threat force is visualized executing a COA during situation templating, analysts identify places where activity must occur if that COA is adopted. The NAIs facilitate intelligence collection, reconnaissance and surveillance, and analysis because—

- Attention is focused on areas where the enemy force must appear if the enemy has selected a particular mobility corridor or AA.
- Military significant events can be framed by time and location within the NAI.
- Events in one NAI can be compared to events occurring in the NAI of other mobility corridors as the basis for determining enemy intentions.
- Events within NAIs can be analyzed for indicators and HVTs against which intelligence and target acquisition resources can be directed.

SECTION II. SPECIALIZED ANALYTICAL TECHNIQUES

While IPB provides the overall framework and techniques for analyzing the threat, situations may dictate the use of more specialized techniques to enhance the overall product. Discussed below are a few of the more common techniques used by intelligence analysts.

Subsystem Threat Analysis

Subsystem analysis plays a major role in determining the overall posture of a threat force. Most of the products prepared during the IPB process will only partially satisfy the requirements of other staff sections and subordinate units. The targeting process may require focus on a particular aspect of the threat force. The intelligence analyst must be aware of the important threat analysis factors that specialized staff sections and units use in their IPB responsibilities. Intelligence analysts serve as the focal point for supplying information and data on a specific subsystem to other staff sections and units. Intelligence personnel assigned to specialized units discussed below will tailor their IPB efforts to the needs of their unit.

Air Defense

Evaluation

When air defense units and staffs evaluate the threat, they focus on threats posed by UAVs, cruise and ballistic missiles, fixed- and rotary-wing aircraft, and airborne and air assault forces. In addition to the broad range of OOB factors and threat capabilities, air defense staffs and units must evaluate—

- Flight operations tactics.
- Ordnance types and availability.
- Ordnance delivery techniques (e.g., standoff ranges, release speeds and altitudes, guidance systems).
- Technical capabilities of aircraft (e.g., all-weather or night, maximum and minimum speeds, ceilings, range, payloads, aerial refueling).
- Target selection priorities for air strikes or attack by air assaults.
- Air strike allocation procedures.
- C2 and supporting CIS procedures and techniques.
- Navigation capabilities.
- Threats to friendly air defense artillery (ADA) assets, including threat ground forces and electronic warfare assets.

COA Determination

The threat's air activities will be a part of his overall operation. Intelligence personnel begin determining the threat's air COAs by acquiring the supported command's basic IPB products, to include situation templates. Analysts evaluate the general COAs that situation templates portray and determine how the threat might support COAs with air power. When determining air COAs, analysts must consider the maneuver forces the COAs support. The employment flexibility of modern aircraft makes the determination of specific threat COAs extremely difficult. When determining the threat's air COAs, analysts should answer the following questions:

- Where will the threat locate FARPs?
- When will the threat's air strikes or air assault operations occur?
- What are the threat's targets and objectives?
- What are the threat's likely air corridors and air AAs?
- What are the threat's strike package composition, flight profiles, and spacing in time and space, including altitudes?

- Where do friendly air defense assets fit into the threat COA?
- Will the threat ground COAs require movement of friendly ADA assets?

Artillery

Evaluation

When evaluating the threat, the artillery unit personnel or staff should—

- Refine standard threat models to focus on HVTs.
- Evaluate the threat's ability to fight the counterfire battle by—
  - Identifying the threat's target acquisition assets and describing their normal deployment patterns and tactics.
  - Describing the accuracy and timeliness of each threat target acquisition system.
  - Identifying CIS that moves target acquisition information to decision-makers or weapons systems, and describing the system in terms of efficiency and timeliness.
- Describe the threat's ability to locate and destroy friendly target acquisition assets.
- Use techniques associated with the rear battle to evaluate rear area threat to artillery units.

COA Determination

When determining threat COAs, analysts—

- Refine the threat COA models to reflect—
  - HVTs.
  - Dispositions and activity of threat fire support.
  - Dispositions of threat target acquisition assets.
  - Rear area threats to friendly units.
- Focus on COAs that primarily deal with counterfire against friendly assets, other aspects of force protection, and threat activities that will require friendly units to displace.

Aviation

Evaluation

When evaluating the threat, aviation unit personnel identify—

- Units supported by ADA assets.
- Types of ADA systems and their capabilities, such as—
  - Ranges.
  - Altitudes.
  - Engagement times.
  - Fusing systems.
  - Radars.
  - Countermeasures.
  - Range capabilities.
  - Altitude restrictions.
- Other threats such as lasers or artillery fire zones.
- Artificial illumination effects on target acquisition and night vision devices.
- Target characteristics, such as—
  - Normal deployment patterns.
  - Capability to detect attacking aircraft.
  - Typical reactions.
  - HVTs within each formation.

COA Determination

When refining the higher command's threat COA model, analysts—

- Include air defense system range fans.
- Determine where radars and weapons systems are masked by terrain.
- Identify areas with the least amount of air defense coverage.
- Identify likely threat air approaches to friendly engagement areas and battle positions.
- Develop situation templates for threat actions within the engagement area and include reactions to aviation attack.

- Identify threat units along flight paths, consider threat units' reactions, and develop appropriate situation templates.
- Consider threat reactions to downed pilots.

Counterintelligence

Evaluation

When assessing the threat, counterintelligence personnel—

- Describe the threat decisionmaking process and include descriptions of the threat's—
  - IPB process.
  - Command estimate and wargaming methods.
  - Techniques for selecting intelligence requirements.
  - Collection planning and collection management.
  - Asset reporting system.
  - Intelligence processing architecture.
  - Dissemination procedures.
- Estimate the standard lengths of the threat decision cycle for both anticipated and unanticipated decisions by answering the following questions:
  - How long does it take the threat staff to plan and execute a new mission?
  - How long does it take the threat staff to plan and execute changes to the current mission?
  - What is the length of time between acquisition of key indicators by collection assets and execution of that decision?
- Identify the collection systems available to each threat unit, develop doctrinal templates and descriptions for the standard employment of these systems, and rank each collection system in relative order of importance to standard threat operations.

COA Determination

When formulating threat COAs, the analyst should—

- Determine threat intelligence requirements by using the basic maneuver COA model and by answering the following questions:
  - What does the threat need to know to make operations successful?
  - Where are the decision points?
  - When does the threat need to know?
- Estimate the threat's intelligence requirements and attempt to recreate his version of the event template, matrix (NAIs and indicators), and collection plan.
- Develop products that show the employment of each collection system and the ensuing coverage by—
  - Depicting range fans for each system.
  - Describing the type of activity that can be collected within each range fan.
  - Highlighting the strengths and weaknesses of the threat collection plan.
- Develop a friendly event template to support counterintelligence and counterreconnaissance.
- Identify locations (NAIs) and activities (indicators) that confirm or deny key elements of the threat collection assumptions.

Command and Control Warfare

Threat analysis in support of C2W can be divided into areas of threat capabilities to conduct C2W and threat vulnerabilities to C2W.

Evaluation of Capabilities

When evaluating threat C2W capabilities, the analyst should consider the threat's—

- Ability to locate and intercept our C2 centers and agencies and supporting CIS.
- Targeting speed and accuracies of threat intelligence collection systems and capabilities of its production elements.

- EA equipment and techniques effectiveness, to include capabilities against space-based systems and computer networks.
- Ability to link collection systems to indirect fire systems.
- Range capabilities of supporting indirect fire systems.
- Ability to conduct deep strikes or special operation forces operations.
- Deception doctrine, tactics, techniques, procedures, and effectiveness.
- Psychological operation capabilities and effectiveness.
- Deployment patterns and tactics of SIGINT collection systems and EA assets, as depicted on the threat model.
- Deployment patterns, tactics, and range capabilities of long-range indirect fire systems, as depicted on the threat model.
- Techniques of intrusion or electronic deception, as depicted on the threat model.

Evaluation of Vulnerabilities

When evaluating threat vulnerabilities to C2W, analysts consider the threat's—

- C2 structure and CIS, with emphasis on locating key C2 nodes.
- Decisionmaking process and speed.
- Command personalities.
- Intelligence, reconnaissance, and target acquisition assets and their vulnerability to jamming or deception.
- Communications security procedures and their ability to work through or around EA.
- Counterintelligence effectiveness.
- Operations security procedures and effectiveness.
- Effectiveness of electronic protective measures and computer network protection.
- Susceptibility to psychological operations and ability to conduct counterpsychological operations.

COA Determination

When developing threat COAs, analysts consider threat C2W capabilities and how those capabilities will be used to support specific operations. The threat command, control, and communications posture and associated vulnerabilities are considered during the identification of COGs and HVTs and contribute to development of HPTs and targeting strategies.

Engineer

Evaluation

Analysts conducting threat analysis in support of engineer planning should evaluate the threat's—

- Engineer units' organization, standard operations, equipment, and employed tactics for conducting mobility, countermobility, survivability, obstacle placement, and breaching operations.
- Engineering capabilities required to lay each type of obstacle system, to breach obstacles, to entrench a type unit, and to bridge different size rivers and streams.
- Logistical system ability to sustain engineer operations.
- Weapons capabilities to penetrate friendly survivability measures and systems.
- Survivability techniques (e.g., use of chain-link fence to defeat antitank rounds and missiles).
- Engineer capabilities of threat infantry, armor, and other nonengineer units.

COA Determination

When determining threat COAs, analysts should include engineering factors in threat models and templates. To develop situation templates for engineers, analysts use the maneuver situation

template of the supported unit and develop multiple threat engineer COAs that include—

- An engineer status estimate, which includes the percentage of combat vehicles with entrenched primary, alternate, supplementary, and deception positions and the extent of likely obstacle system measures.
- Likely locations and obstacle systems required to support, disrupt, turn, fix, or block defensive measures.
- A mobility support estimate, which includes the maneuver and supporting engineer detachments' breaching and fording capabilities.

Combat Service Support

Evaluation

When conducting threat analysis in support of CSS staffs and units, analysts should include—

- Regular threat formations, particularly reserves or second echelon units, that might penetrate main defenses or conduct counterattacks through CSS areas.
- Details on air assault, airborne, unconventional warfare, and light infantry forces and their means of infiltration (e.g., air, ground, and sea).
- Insurgent and partisan forces.
- Terrorist organizations.
- Criminal organizations.

COA Determination

When preparing threat models in support of CSS units, analysts include—

- Air assault, airborne, and light infantry techniques for deep attack.
- Unconventional warfare techniques for deep operations.
- Standard procedures for insurgent raids and ambushes.
- Typical procedures for terrorist attacks.
- Targets and methods of operations for criminal organizations.

COA Development

When evaluating threat COAs, the analyst should consider each maneuver COA available to the threat and develop multiple CSS COAs that include—

- Likely areas of penetration for ground forces.
- Likely objectives in the rear area that will facilitate the threat's main attack or defense.
- The HVTs and HPTs (e.g., key terrain, specified CSS activities) that the threat will identify to support their concepts of operations.
- Situation templates for air assault and airborne operations (e.g., air avenues to LZs and DZs, infiltration lanes, exfiltration lanes).
- Insurgent or partisan activities (e.g., assembly and hide areas, infiltration routes, objective actions, exfiltration).
- Terrorist and sabotage activities.

Pattern Analysis

Pattern analysis is the process of careful observation and evaluation of threat activities to deduce the doctrinal principals and techniques, tactics, and procedures that threat forces or groups prefer to employ. When faced by an opponent whose doctrine is unknown or undeveloped, the intelligence analyst must use pattern analysis to create or update threat models and doctrinal templates. This form of analysis is used in operations other than war, such as counterinsurgency, peacekeeping, or even humanitarian assistance operations. The coordinates register and pattern analysis plot sheet are used to develop threat models when it is necessary to determine threat operational patterns.

Coordinates Register

Sometimes referred to as an incident map, a coordinates register illustrates cumulative events that have occurred within the AO (see fig. 7-3). Coordinates registers focus on where an event occurred, but it can contain additional information as the situation dictates. The date and time of the incident are recorded next to the location. As reports of individual events or sightings are recorded, the analyst attempts to identify links between the location and time of those events. What may appear to be random events will often develop into coordinated actions. When time lined and illustrated, these events form patterns that provide the basis for developing threat models and doctrinal templates. Although the time of the event is normally recorded on the coordinates register, it should always be used with the pattern analysis plot sheet and the doctrinal template, if developed.

Pattern Analysis Plot Sheet

The pattern analysis plot sheet focuses on the time and date each incident occurs in the AO. In figure 7-4, the rings depict the days of the month and the radial segments depict the hours of the day. Events are recorded using the same alphanumeric designator as was used on the coordinates register to allow easy cross-referencing. Along the right side of the plot sheet, the events are recorded by the day and date they occurred. By organizing the events in this manner, it is possible to identify the times of the day and days of the

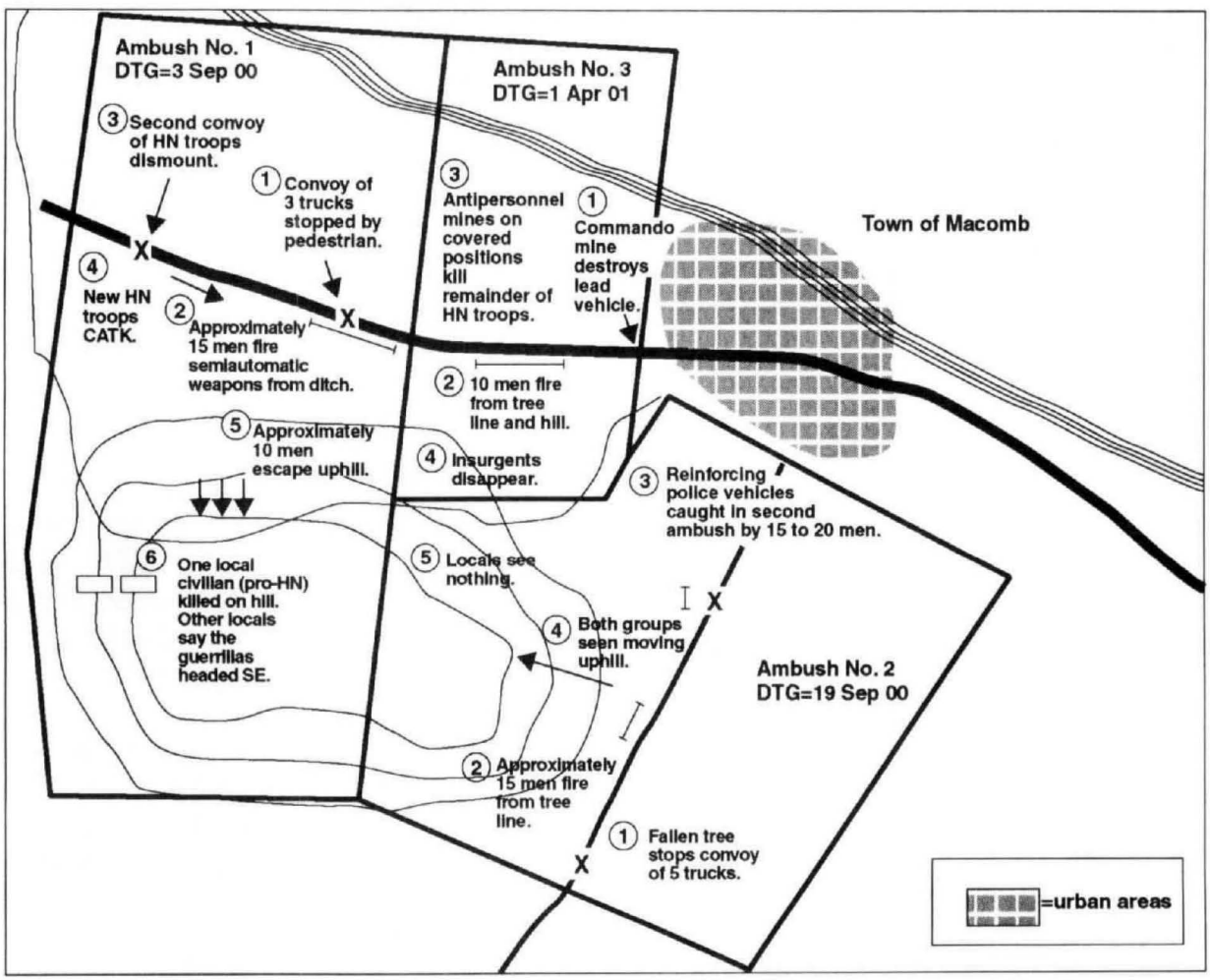

Figure 7-3. Coordinates Register.

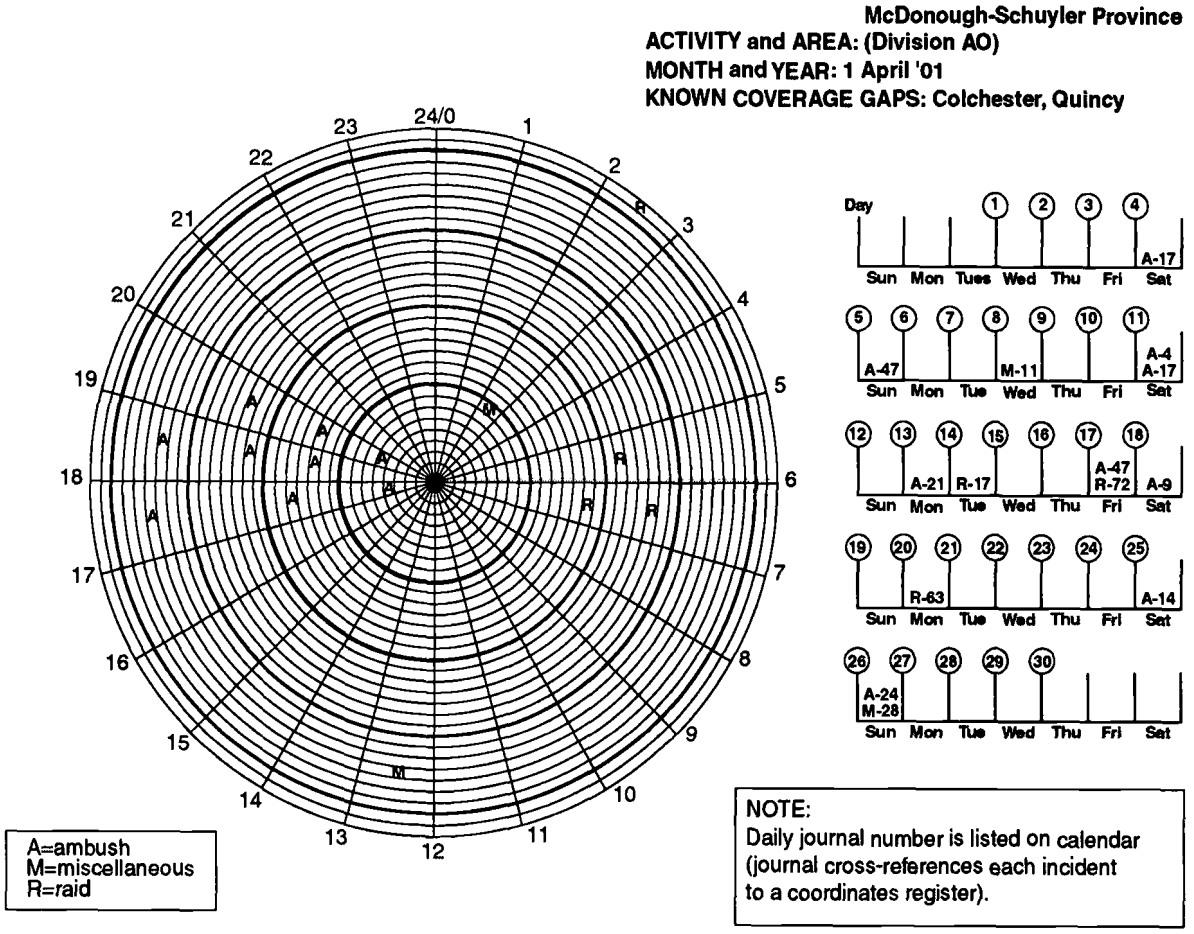

Figure 7-4. Pattern Analysis Plot Sheet.

week or month when threat activities occur. Used in conjunction with the coordinates register, the pattern analysis plot sheet identifies where, when, and how past actions occurred. This allows the analyst to use information derived from the coordinates register and pattern analysis plot sheet, to develop threat models and doctrinal templates, and to predict potential threat activity.

Matrix Analysis

Constructing a matrix is a simple, graphical way to organize a large volume of complex data. Matrices are used to show relationships between numbers of entities, such as people, incidents, organizations, weapons, locations, functions, and actions. Analysts use activities and association matrices to organize a large volume of complex data, particularly in cases where the tracking of individuals and organizations is emphasized. Activities and association matrices are useful in analyzing insurgent, terrorist, criminal or drug trafficking activity.

Activities Matrix

Analysts use the activities matrix to link people to events or organizations. An activities matrix quickly displays which notable personnel within the AO are related to a particular organization or type of activity. This matrix can also link certain activities or incidents within the AO with organizations or units.

In figure 7-5, individuals are listed down one side, with organizations listed across the top. Reported relationships are noted on an individual's row that intersects the appropriate organization's column. This example demonstrates the use of dots to signify the confirmed, possible, or probable certainty of the relationship. The absence of a dot indicates either no relationship or a lack of information. The system used must be explained in a legend. To complete this particular example, the analyst created a remarks column to record significant information regarding each individual.

● – confirmed ◍ – probable ○ – possible Remarks		Christian Reform Party (good guys)	Society for the Preservation of Order (SPO) (right wingers)	Farmer's Alliance (unknown peasant group)	People's Democratic Society (peaceful moderate)	Insurgent Company	New Liberation Movement (political front for New Metropolitan Edict (NME))	NME	Name of Individual	
Warrant Outstanding	Leader in the insurgent company. Possible platoon commander or company commander.					●	●	●	Johnston, S. D. alias "The Red"	Bandolph
	Possibly linked to death squad activities.	●	◍						Garra, N. A.	
	Mayor, ineffective due to war-torn town.	●							Mulvhill, P.	
	Possible platoon leader.	○		●	◍	○	○		Daniels, P.	
	Regional governor.	◍	○	◍	●				Jenkins, T. L.	Malcolm
Warrant Outstanding	Tactical genius, principal trainer of insurgent company.					●	●	◍	Cornier, J.	
				○		◍	◍	◍	Webb, C.	
					◍	○	○		Seipel, B.	
	Leader in the insurgent company. Platoon leader or executive officer.			○		◍	◍	◍	Trollinger, L.	Beards town
	Possible head of intelligence.					○	●	●	Ahearn, E.	
	Probable platoon leader.					◍	○		Timoney, J.	
Warrant						●	●		Thompson, J.	
Warrant	Probable heavy weapons platoon leader.					●	○	●	Bridgeford, R.	
	Possible liaison between insurgent company and the NME			◍	○	○		○	Halbleib, M.	Bushnell
	"Doctor of Death" leads the SPO.	●	●	○	○				Mueller, H.	
Warrant						●	◍	◍	Martinez, E.	

Figure 7-5. Activities Matrix.

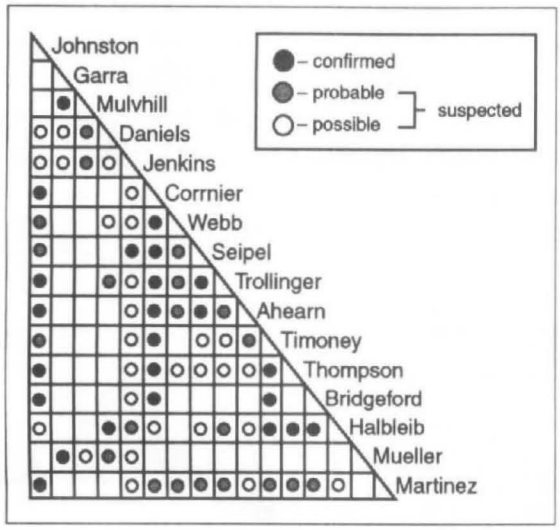

Figure 7-6. Association Matrix.

Association Matrix

The association matrix is used to show relationships between individuals. In figure 7-6, the individual names constitute both a column and a row. A dot indicates that a relationship exists. Through the use of the activities matrix, analysts note individuals that are members of the same organization and indicate the relationship on the association matrix.

Link Analysis

Link analysis is a method of evaluating and displaying relationships and activities information that has been organized into matrices. In link analysis, pictures or symbols are used to display intelligence data that depicts relationships between people or entities. Analysts assess the reliability and validity of the intelligence data and assemble a link diagram to gain greater insight into the construction of a relationship network.

In figure 7-7, the link analysis diagram uses circles to represent people, squares or rectangles to represent organizations, and lines to represent their connections. Solid lines represent confirmed or strong relationships, while dashed lines indicate suspected or weak relationships. When

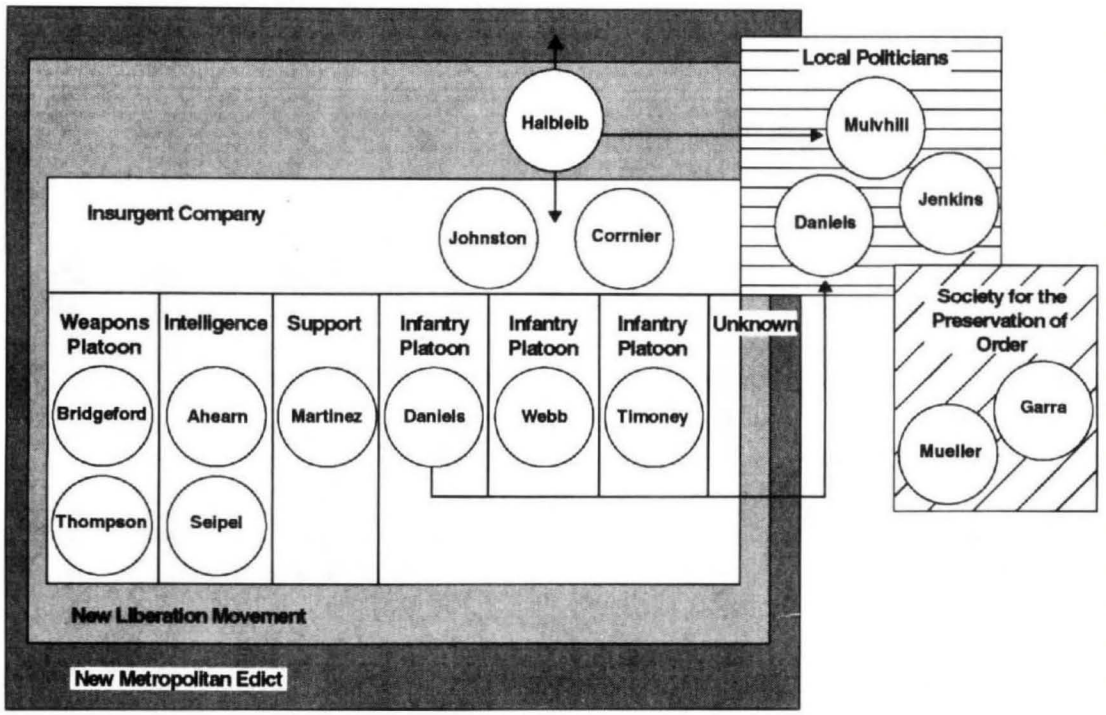

Figure 7-7. Link Diagram.