

Joint Publication 2-01



Joint and National Intelligence Support to Military Operations



7 October 2004



EXECUTIVE SUMMARY COMMANDER'S OVERVIEW

- **Explains the Role of Intelligence in Military Operations**
 - **Describes Joint and National Intelligence Organizations, Responsibilities, and Support Mechanisms**
 - **Discusses Intelligence Operations and the Intelligence Process**
 - **Describes Intelligence Support to Joint Planning**
 - **Discusses Intelligence and the Global Information Grid**
-

Introduction

The objective of joint intelligence operations is to integrate Service and national intelligence capabilities into a unified effort that surpasses any single organizational effort and provides the most accurate and timely intelligence to commanders.

Joint intelligence is produced by elements of more than one Service and consequently relies heavily on the timely and integrated departmental intelligence afforded by national intelligence organizations. **This joint intelligence effort facilitates that degree of dominance in the information domain which permits the conduct of operations without effective opposition (i.e., information superiority).** In order to accomplish this, intelligence must provide the joint force commander (JFC) with as timely, complete, and accurate an understanding as possible of the battlespace. Intelligence staffs must anticipate and fully understand the intelligence requirements of their superior and subordinate commands and components, identify organic intelligence capabilities and shortfalls, access theater and/or national systems to alleviate shortfalls, and ensure that timely and appropriate intelligence is provided or available to the JFC and subordinate commands and components.

Intelligence Support to Military Operations

Intelligence plays a critical role across the range of military operations.

Commanders use intelligence to anticipate the battle, visualize and understand the full spectrum of the battlespace, and influence the outcome of operations. Intelligence enables commanders at all levels to focus their combat power and to provide full-dimensional force protection across the range of military operations. **In war,** intelligence focuses on adversary military capabilities, centers of gravity (COGs), and potential courses of action to provide operational and tactical commanders the information they need to plan and conduct operations. **Short**

of war, joint operations are normally very sensitive to political considerations and can be governed by rules of engagement requiring the adoption of a new and complex set of operational responses. The intelligence directorate of a joint staff (J-2) must modify and tailor intelligence support to meet the unique challenges presented in each operation.

Joint Intelligence Organizations

Joint intelligence organizations are directly responsible for providing the combatant command and subordinate joint force with a common, coordinated intelligence picture by fusing national and theater intelligence and law enforcement/counterintelligence information into all-source estimates and assessments.

Joint intelligence activities focus on determining the joint force's intelligence needs based on the mission and commander's guidance; prioritizing intelligence requirements; developing an optimal collection plan and strategy; identifying collection or production shortfalls that may require resource augmentation, intelligence federation, or direct national-level analytic support; and then evaluating satisfaction of needs and requirements and adjusting intelligence services and support accordingly.

The combatant command J-2 assists the commander and staff in developing strategy, planning theater campaigns, and organizing the command relationships of theater intelligence assets for effective joint, interagency, and multinational operations and to facilitate interagency coordination. Additionally, the J-2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort supporting the commander's objectives.

The combatant command joint intelligence center (JIC) is the focal point for intelligence analysis and production effort, and is organized in a manner best suited to satisfy the combatant commander's intelligence requirements. If the JIC cannot meet the combatant commander's requirements, the JIC forwards a request for information to the National Military Joint Intelligence Center or to subordinate command levels using the community on-line intelligence system for end-users and managers.

The organizational structure of a subordinate joint force's intelligence element is determined by the JFC based on the situation and mission. All subordinate joint force J-2s, however, will at a minimum require a core element of analytical and administrative capabilities. Most situations will require augmentation of joint force intelligence capabilities through the deployment and integration of theater intelligence elements into a joint intelligence support element (JISE). Capabilities of the JISE include order of battle analysis, identification of adversary

COGs, analysis of adversary command, control, communications, and computers, targeting support, collection management, and maintenance of a 24-hour watch.

National Intelligence Organizations

National intelligence organizations conduct extensive collection, processing, analysis, and dissemination activities.

National intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. These organizations routinely provide support to the JFC while continuing to support national decision makers. However, **the focus of these national organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements.**

The Intelligence Community (IC) refers in the aggregate to those Executive Branch agencies and organizations that are funded in the National Foreign Intelligence Program. The IC consists of 15 member organizations:

The **Defense Intelligence Agency (DIA)** has oversight of the Department of Defense Intelligence Production Program (DODIPP), under which all-source intelligence is produced for use by both policymakers and commanders. Under DODIPP, DIA's Armed Forces Medical Intelligence Center is assigned responsibility for medical intelligence and DIA's Missile and Space Intelligence Center is responsible for missile and space intelligence. Additionally, DIA's Defense Human Intelligence (HUMINT) Service provides a full range of HUMINT and HUMINT-related intelligence collection services to combatant commanders and other Department of Defense (DOD) and national-level consumers. DIA also provides intelligence support in areas such as: counterintelligence, counterterrorism, counterdrug operations, computer network operations, personnel recovery, proliferation of weapons of mass destruction and the means of delivery, United Nations peacekeeping and coalition support, measurement and signature intelligence (MASINT), noncombatant evacuation efforts, indications and warning, targeting, battle damage assessment, current intelligence, collection management, intelligence architecture and systems support, and document and media exploitation capability.

The National Security Agency/Central Security Service is a unified organization structured to provide for the signals intelligence mission of the United States and to ensure the

protection of national security systems for all departments and agencies of the United States Government.

The National Geospatial-Intelligence Agency provides timely, relevant, and accurate geospatial intelligence support to include imagery intelligence, geospatial information, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic data and information.

The National Reconnaissance Office is responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering, development, acquisition and operation of space reconnaissance systems and related intelligence activities.

The Service Intelligence Organizations provide intelligence support for Departmental missions related to military systems, equipment, training, and national intelligence activities. The Services also provide support to DOD entities, including combatant commands and their components.

The Central Intelligence Agency's (CIA's) primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political and economic intelligence.

The Department of State (DOS) Bureau of Intelligence and Research performs intelligence analysis and produces studies on a wide range of political and economic topics essential to foreign policy determination and execution.

The Federal Bureau of Investigation (FBI) has primary responsibility for counterintelligence (CI) and counterterrorism operations conducted in the United States. FBI CI operations overseas are coordinated with the CIA.

The Department of Treasury analyzes foreign intelligence related to US economic policy and participates with the DOS in the overt collection of general foreign economic information.

The Department of Energy analyzes foreign information relevant to US energy policies and nonproliferation issues.

The Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection analyzes the

vulnerabilities of US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to the Homeland Security Advisory System.

The United States Coast Guard (USCG), a component of the Department of Homeland Security, operates as both an armed force and a law enforcement organization. The USCG's Maritime Intelligence Fusion Centers Atlantic and Pacific serve as the central hub for collection, fusion, analysis and dissemination of maritime intelligence and information to Coast Guard operating units, Department of Homeland Security and all members of the IC including DOD and key decision makers at the national level.

Intelligence Operations

Intelligence supports joint operations by providing critical information and finished intelligence products to the combatant command, the subordinate Service and functional component commands, and subordinate joint forces.

Commanders at all levels depend on timely, accurate information and intelligence on an adversary's dispositions, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities and critical vulnerabilities. **The intelligence process is comprised of a wide variety of interrelated intelligence operations.** These intelligence operations (planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback) must focus on the commander's mission and concept of operations.

The intelligence process describes how the various types of intelligence operations interact to meet the commander's intelligence needs.

The intelligence process provides a useful model that, albeit simplistic, nevertheless facilitates understanding the wide variety of intelligence operations and their interrelationships. There are no firm boundaries delineating where each operation within the modern intelligence process begins or ends. Intelligence operations are not sequential; rather they are nearly simultaneous. Additionally, not all operations necessarily continue throughout the entire intelligence process. The increased tempo of military operations requires an unimpeded flow of automatically processed and exploited data that is both timely and relevant to the commander's needs. This unanalyzed combat information must be simultaneously available to both the commander (for time-critical decision making) and to the intelligence analyst (for the production of current intelligence assessments). Likewise, the analysis, production, and dissemination of intelligence products must be accomplished in time to support the commander's decision-making needs.

Planning and direction.

Joint intelligence operations begin with the identification of a need for intelligence regarding all relevant aspects of the battlespace especially the adversary. These intelligence needs are developed by the J-2 in coordination with other staff elements, and are formalized as intelligence requirements early in the planning process. **Those critical pieces of intelligence the commander must know by a particular time to plan and execute a successful mission are identified as the commander's priority intelligence requirements (PIRs).** PIRs are identified at every level and are based on guidance obtained from the mission statement, the commander's intent, and the end state objectives.

Collection.

The collection portion of the intelligence process involves **tasking appropriate collection assets and/or resources to acquire the data and information required to satisfy collection objectives.** Collection includes the identification, coordination, and positioning of assets and/or resources to satisfy collection objectives. Finally, collection involves gaining electronic, physical, spectral, or visual access to a target and searching for, discovering/sensing, and gathering characteristics, data, equipment, or phenomena to process and exploit.

Processing and exploitation.

Once the data that might satisfy the requirement is collected, it must undergo processing and exploitation. **Through processing and exploitation, the collected raw data is transformed into information that can be readily disseminated and used by intelligence analysts to produce multidiscipline intelligence products.** Relevant, critical information should also be disseminated to the commander and joint force staff to facilitate time-sensitive decision making. Processing and exploitation time varies depending on the characteristics of specific collection assets.

Analysis and production.

The analysis and production portion of the intelligence process involves **integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product.** The demands of the modern battle require intelligence products that anticipate the needs of the commander and are timely, accurate, usable, complete, relevant, objective, and available.

Dissemination and integration.

Properly formatted intelligence products are disseminated to the requester, who integrates the intelligence into the decision-making and planning processes.

Evaluation and feedback.

Intelligence operations, activities and products are continuously evaluated. Based on these evaluations and the resulting feedback, remedial actions should be initiated, as required, to improve the performance of intelligence operations and the overall functioning of the intelligence process.

Intelligence Support to Joint Planning

In today's global threat environment, rigid sequentially-structured intelligence support to planning must yield to a more dynamic process involving overlapping and simultaneous activities.

Military planners and decision makers require a faster, more accurate flow of information and intelligence. Intelligence support in this environment requires increased agility to quickly identify requirements, collect and disseminate information, and analyze and produce predictive intelligence to support the planning process. Intelligence support to the joint planning effort must be focused to ensure that it fully anticipates and dynamically responds to the commander's requirements and the requirements of subordinate units and/or elements.

Intelligence support to joint operation planning includes a single integrated set of policies, activities, and procedures applicable to both deliberate planning and crisis action planning (CAP). Deliberate plans include operation plans in complete format, operation plans in concept format with or without time-phased force and deployment data, and functional plans. CAP is conducted for the actual commitment of allocated forces, based on the current situation, when a contingency response is imminent. This planning results in time-sensitive development of campaign plans and/or operation orders for execution.

Intelligence and the Global Information Grid

The Global Information Grid is the end-to-end integrated set of information technology capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to commanders, policy makers and support personnel in a globally interconnected environment.

The Global Information Grid (GIG) includes **all DOD-owned and leased communications and computing systems software, data, security services, and other associated services necessary to achieve information superiority.** This environment supports all DOD and IC missions and functions (strategic, operational and tactical), in war and peace, at all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

The communications networks and information processing, storage, and management systems that comprise the GIG provide the basic framework for the timely transfer of data and information to support military operations. The GIG also provides the means for the timely

dissemination of information and finished intelligence to commanders and other key decision makers, thereby facilitating information superiority. The GIG architecture implements common procedures, standards, and streamlined support, and continues to evolve. **The intelligence portion of the GIG is designed to provide an architecture that can be individually tailored to the specific needs of a joint force, ensures survivability and flexibility through distributed operations, and can be rapidly reconfigured to accommodate changing demands and responsibilities including facilitating relationships among federated intelligence partners.** This tailorable, distributed, and rapidly reconfigurable joint architecture provides all relevant available battlespace information to the user in the form of a common operational picture. **Within the GIG, the Department of Defense Intelligence Information System (DODIIS) is the aggregation of personnel, procedures, equipment, computer programs, and supporting communications of the military IC.** DODIIS defines the standards for intelligence system and application interoperability. The system concept provides an integrated strategic, operational, and tactical user environment for performing identical intelligence support functions on compatible systems. DODIIS provides a robust and flexible intelligence capability for subordinate joint forces as long as supporting communications lines are available. DODIIS tools support the movement of intelligence between DIA, the combatant commands, the Services, and other intelligence production and customer activities worldwide.

*Intelligence-Related
Communications
Infrastructure.*

The joint intelligence communications subarchitecture encompasses collection, processing, exploitation, analysis, and dissemination nodes. These nodes are supported by a robust communications infrastructure and automated systems equipped with tailored applications to meet the broad array of intelligence activities. Command, Service, and combat support agency intelligence processes rely on a communications backbone consisting of the Joint Worldwide Intelligence Communications System and the Secret Internet Protocol Router Network. This infrastructure is supplemented by a distributed, common exploitation and dissemination system, tactical data links, and intelligence broadcast services.

CONCLUSION

This publication establishes doctrinal guidance on the provision of joint and national intelligence products, services, and support to military operations. It describes the organization of joint intelligence forces and the national IC, intelligence responsibilities, command relationships, and national intelligence support mechanisms. It provides information regarding the fundamentals of intelligence operations and the intelligence process, discusses how intelligence supports joint and multinational planning, and describes intelligence dissemination via the GIG.

Joint Publication 2-01.3



Joint Intelligence Preparation of the Operational Environment



16 June 2009



CHAPTER IV SPECIAL CONSIDERATIONS

“Not a Frenchman then doubted that such rapid victories must have decided the fate of the Spaniards. We believed, and Europe believed it too, that we had only to march to Madrid to complete the subjection of Spain...The wars we had hitherto carried on had accustomed us to see in a nation only its military forces and to count for nothing the spirit which animates its citizens.”

Napoleonic soldier on the French occupation of Spain and subsequent Spanish insurgency, 1808

1. Introduction

In its most basic sense, the JIPOE process simply combines an understanding of the constraints and influences imposed by the operational environment with the normal *modus operandi* of an adversary in order to forecast that adversary’s future actions. This basic JIPOE process is relevant throughout the range of military operations. However, some types of missions, operations, and situations may require a more tailored JIPOE approach that places greater emphasis on specific aspects of the operational environment. For example, stability operations require an approach that places far greater emphasis on understanding the civil population and critical infrastructure. Likewise, the contribution of the JIPOE effort to countering asymmetric approaches requires techniques and products that are specifically tailored to the types of joint operations capable of defending against and defeating asymmetric threats. Finally, some situations (particularly crisis response operations) will require JIPOE analysts to adopt a nontraditional, broad view of what constitutes an “adversary” (e.g., disease, starvation, floods). This chapter discusses *some* of the special considerations, procedures, and types of products that JIPOE planners and analysts may find useful in specific situations. The discussion is intended only as a point of departure for JIPOE analysts to further develop specific techniques and products based on their initiative, imagination, and innovation.

SECTION A. SUPPORT DURING STABILITY OPERATIONS AND IRREGULAR WARFARE

2. Overview

JP 1, *Doctrine for the Armed Forces of the United States*, describes both traditional war (a confrontation between nation states or coalitions/alliances of nation-states) and IW. Traditional war typically involves small-scale to large-scale, force-on-force military operations in which adversaries employ a variety of conventional military capabilities against each other. By contrast, IW, which has emerged as a major and pervasive form of warfare, typically involves a less powerful adversary that seeks to disrupt or negate the military capabilities and advantages of a more powerful, conventionally armed military force, which often represents the nation’s established regime. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary’s power, influence, and will. What makes IW

“irregular” is its focus— a relevant population – and its strategic purpose – to gain or maintain control or influence over, and the support of that relevant population through political, psychological, and economic methods. Friendly forces may also engage in stability operations to restore order in the aftermath of an irregular or traditional war or a natural disaster. Stability operations encompass various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. Stability operations likely will be conducted in coordination with and in support of HN authorities, OGAs, NGOs, IGOs, and the private sector. The long-term goal is to help develop indigenous capacity for securing essential services, developing a viable economy, establishing a legal process that conforms to local cultural norms, and restoring civil society with functioning institutions. JIPOE support during operations that focus on the civil population as a COG requires a different mindset and different techniques than a JIPOE effort that focuses on defeating an adversary militarily. The following discussion identifies some of the special considerations relevant to applying the JIPOE process in support of nontraditional missions. Appendix B, “Somalia 1992-1993– A Case Study of Support to Stability Operations and Irregular Warfare,” illustrates many of the constructs discussed in this section.

3. Increased Emphasis on Sociocultural Factors

JIPOE support during stability operations and IW requires a more detailed understanding of the relevant area’s sociocultural factors than is normally the case during traditional war. JFCs, subordinate commanders, and their staffs must understand the cultural landscape in which they operate in order to make sound decisions concerning force protection and the deployment of forces. JIPOE products must describe the impact of ethnic groups and religions, to include their associated leadership, the locations of places of worship and cultural/historical significance, languages being spoken, population density, age, living conditions, allocation of wealth, and means of income. This information provides the backdrop against which an analysis of social and political factors will allow for successful stability operations to include, when necessary, establishing the process for initiating elections and establishing government. The key social and political factors revolve around understanding previous political systems, parties, formal and informal leaders, affiliations, political grievances, loyalty to former local, regional, and national government officials, patterns of political tolerance or violence, and the education system. This information will provide an appreciation of the nation’s cultural landscape, its previous and potential future leaders, and its expectations of governance and civil institutions. In order to accomplish this, JIPOE analysts must develop a comprehensive understanding of the following factors:

a. **Society.** A society is a population whose members are subject to the same political authority, occupy a common territory, have a common culture, and share a sense of identity. Every society has social structure and culture; however, societies are dynamic and heterogeneous. JIPOE must consider societies or societal links to groups

outside the operational area and the impact of society on the overall operational environment.

b. Social Structure. Social structure refers to the relations among groups of persons within a society and involves the arrangement of the parts that constitute society, organization of social positions, and distribution of people within those positions. Understanding social structure provides insight into how a society functions. Groups may be based on racial, ethnic, religious, or tribal identities. Group identity is more than being aware of what the societal make up is by percentage or group. The JIPOE assessment of ethnic breakdown must explore its relationship to any dislocated civilian problems, religious affiliations, historic grievances and conflict, loyalty to formal and informal leaders, points and dates of cultural significance, and language. Even in a society that is seemingly devoid of any coherent social system, the reality is that a system still does exist. For example, a clan-based society that is made up of entities struggling to seize and maintain power is a system in itself. Failure to conduct detailed analysis creates the risk of new or renewed tensions and violence, thereby undermining any effort towards a safe and secure environment or enduring institutions.

(1) Races and ethnic groups are key aspects of social structure. A race is a human group that is different by virtue of innate physical characteristics. An ethnic group is a community whose learned cultural practices, language, history, ancestry, or religion distinguish them from others. Religious groups may be subsets of larger ethnic groups. Racial or ethnic groups are often key sources of friction within societies.

(2) Networks may be an important aspect of a social structure as well as within the insurgent organization. Common types of networks include elite networks, prison networks, worldwide ethnic and religious communities, and neighborhood networks. JIPOE must determine what networks exist, what their purpose is, who is involved, how they operate, and how they adapt.

(3) Groups collectively engaged to complete a common task are called institutions. Institutions are the long-term building blocks of societies. Organizations are institutions with bounded membership, defined goals, established operations, fixed facilities or meeting places, and means of financial or logistic support. Organizations may be communicating, religious, economic, social, or any combination of the previous four categories, and they may control, direct, restrain, or regulate the local populace. It is important to determine which members of what groups belong to each organization and how their activities may affect the local populace, whose interests they fulfill, and what role they play in influencing local perceptions.

(4) JIPOE analysts must understand the dynamic interaction among social groups to include formal relationships (such as treaties or alliances), informal relationships (such as custom or common understanding), divisions or cleavages, and cross-cutting ties (such as religious alignments that cut across ethnic differences).

(5) Another factor that must be assessed by the JIPOE analyst is the means in which the subgroups within the cultural landscape communicate and receive information. On the surface, it may seem obvious for the joint force to communicate to the populace through established media such as newspapers or broadcast. However, in some societies the populace may not have broad access to these sources of information, or may even have a cultural or historical mistrust of established media sources of information.

(6) JIPOE analysts must also understand the importance of roles, status, and norms within the society. Members of a society interact with social positions, and these social positions are referred to as status. For example, most societies associate particular statuses with particular social groups, such as family, ethnicity, or religion, and every social status has a corresponding cluster of expected behaviors (roles) that dictate how a person is expected to think, feel, or act. The standard of conduct for given roles and status is known as a social norm. A social norm is what people are expected to do or should do, rather than what people actually do. Norms may be either moral or customary. When a person's behavior does not conform to social norms, it will result in social disapproval. Social status and roles dictate social norms that may significantly impact stability operations.

(7) JIPOE products should inform the planning process by identifying historical patterns of crime in local areas as well as locations of police stations and jails. The JIPOE effort should also address the relationship between the population and police, the current or past methods of justice, how stability operations may drive criminal activity, and who will be the perpetrator or victim of crimes.

c. **Culture.** Once the social structure has been thoroughly assessed, the JIPOE effort should identify and analyze the culture of the society as a whole and of each major group within the society. Culture is a system of shared beliefs, values, customs, behaviors, and artifacts that members of a society use to cope with their world and with one another. Culture is habitual and perceived as “natural” by people within the society. Culture conditions an individual's range of action and ideas; influences how people make judgments about what is right, wrong, important or unimportant; and dictates how members of a society are likely to perceive and adapt to changing circumstances. Where social structure comprises the relationships within a society, culture provides meaning within the society. JIPOE should identify and analyze the culture of the society as a whole and of each major group within the society.

(1) **Identity.** Primary identities can be national, racial, and religious (specific examples could be tribe and clan affiliation). Secondary identities include past times or personal preferences. Individuals belong to multiple social groups which determine their cultural identities. Furthermore, people tend to rank order these identities depending on the importance they place on different groups. As a result, an individual's cultural identities may conflict with one another, such as when tribe loyalty may conflict with political affiliation.

(2) **Beliefs.** Beliefs are concepts and ideas accepted as true. Core beliefs are part of an individual's primary cultural identity and are highly resistant to change. Examples include religious beliefs, the importance of individual and collective honor, and the role of the family. Attempts to change the central beliefs of a culture may result in significant unintended second and third order consequences.

(3) **Values.** A value is an enduring belief that a specific mode of conduct is preferable to an opposite or converse mode of conduct. Values include beliefs concerning such topics as toleration, stability, prosperity, social change, and self-determination. Each group to which an individual belongs inculcates that person with its values and their ranking of importance. Since individuals are affiliated with multiple groups, their associated values are sometimes in conflict. For example, religious values may conflict with generational values or gender values.

(4) **Attitudes and Perceptions.** Attitudes are affinities for and aversions to groups, persons, and objects. Attitudes affect perception, which is the process by which an individual selects, evaluates, and organizes information from the external environment.

(5) **Belief Systems.** The totality of the identities, beliefs, values, attitudes, and perceptions that an individual holds (and the ranking of their importance) constitutes that person's belief system. Belief systems act as filters through which individuals process and adapt to new information.

(6) **Cultural Forms.** Cultural forms are the concrete expression of the belief systems shared by members of a particular culture. These forms include language, rituals, symbols, ceremonies, myths, and narratives and are the medium for communicating ideologies, values, and norms that influence thought and behavior. A culture's belief system can be decoded by observing and analyzing its cultural forms.

(a) **Language.** Language is a learned element of culture. Communication requires more than just grammatical knowledge; it requires understanding the social setting, appropriate behaviors towards people of different statuses, and nonverbal cues, among other things.

(b) **Rituals.** A ritual is a stereotyped sequence of activities involving gestures, words, and objects. Rituals can be either religious or secular.

(c) **Symbols.** Institutions and organizations often use cultural symbols to amass political power or generate resistance against external groups.

(d) **Ceremonies.** Ceremonial behavior can follow rigid etiquette or a prescribed formality. Just like rituals, it is vital to understand not only the ceremony, but the context in which they take and the meaning thereof.

(e) **Myths.** Myths serve to explain some phenomenon which to the populace can have a great influence on the perceived truth. The counterinsurgent must understand that some myths are as resilient as the truth, and can influence the target audience either negatively or positively.

(f) **Narratives.** Narratives are the means through which ideologies are expressed and absorbed by members of a society. The most important cultural form for counterinsurgents to understand is the narrative.

d. **Power and Authority.** The JIPOE effort should identify how both formal and informal powers are apportioned and used within a society. Often in stability operations, informal power holders, such as ethnoreligious groups, social elites, and religious figures are more important than formal power holders. Often, the key power holders with connections and influence in a society operate behind the scenes, and are therefore difficult to identify and assess. JIPOE products should identify these key individuals and assess their motivations and strategies. The JIPOE effort should also identify current and emerging parties; formal and informal leaders; party and leader influence on local, regional, and national levels; ties to threat or religious entities; facilities; and financial means of support. The JIPOE process also identifies previous actors and influencers as well as current political parties and their agendas; analyzes the local, regional, and national concept of what constitutes a legitimate government, and determines any political grievances that the population may have had locally, regionally, or nationally. A complete JIPOE analysis will inform not only the potential timing for establishing a civil government, but also the nature of the government that should be established and the political personalities who should (or at least should not) establish it and occupy key offices. For example, conducting elections in Bosnia prior to the establishment of viable institutions resulted in the return of officials who were tied to or were of like mind to those who had initiated the conflict. JIPOE analysts must understand the types of power each group has, what it uses that power for, and how it acquires and maintains power. Four major forms of power in a society include coercive force, social capital, economic power, and authority.

(1) **Coercive Force.** Coercion is the ability to compel a person to act through threat of harm or by the use of physical force. Coercive force can be positive or negative. Groups may use coercive means for a variety of purposes such as protecting their community, carrying out vendettas, and engaging in criminal activity. One essential role of government is providing physical security for its citizens by monopolizing the use of coercive force for legitimate purposes.

(2) **Social Capital.** Social capital refers to the power of individuals and groups to use social networks of reciprocity and exchange to accomplish their goals. In many societies, patron-client relationships are an important form of social capital. In a system based on patron-client relationships, an individual in a powerful position provides goods, services, security, or other resources to followers in exchange for political support or loyalty, thereby amassing power.

(3) **Economic Power.** Power may be based on the ability of a group or individual to use formal or informal economic incentives and disincentives to change people's behavior. Economic systems can be formal, informal, or a mixture of both. In weak or failed states, the formal economy may not function well. The informal economy refers to such activities as smuggling, black market activities, barter, and exchange. For example, in many societies, monies and other economic goods are distributed through tribal or clan networks through patronage systems. JIPOE must analyze how groups use economic power with the operational environment and how that power can be exploited.

(4) **Authority.** In some societies substantial power stems from the authority associated with a social position. Authority may be grounded in law and contract and codified in impersonal rules. Alternatively, authority may be exercised by leaders who have unique, individual charismatic appeal, whether ideological, religious, political, or social. Authority may also be invested in a hereditary line or particular office by a higher power.

e. **Interests.** Interests refer to the core motivations that drive behavior. These include physical security, basic necessities, economic well-being, political participation, and social identity. During times when the government does not function, groups and organizations to which people belong satisfy some or all of their interests that the government does not. The interests of civil populations usually include physical security, essential services, economic well-being, and political participation.

(1) **Physical Security.** During any period of instability, people's primary interest is physical security for themselves and their families. When the US, HN, or multinational forces fail to provide security or threaten the security of civilians, the population is likely to seek security guarantees from insurgents, militias, or other armed groups. JIPOE analysts should determine the extent to which the population is safe from harm, whether there is a functioning, fair, and nondiscriminatory police and judiciary system, and who provides security in the absence of a functioning state apparatus.

(2) **Essential Services.** Essential services provide those things needed to sustain life and include items such as food, water, clothing, shelter, electricity, waste removal, and medical treatment. People pursue their essential needs until they are met and tend to support any group that provides such services. Stabilizing a population requires meeting these needs.

(3) **Economy.** A society's individuals and groups satisfy their economic interests by producing, distributing, and consuming goods and services. How individuals satisfy their economic needs depends on the society's level and type of economic development. For instance, in a rural-based society, land ownership may be a major part of any economic development plan, while in urban societies public and private sector jobs may be of greater concern. Real or perceived economic disparities among social groups can contribute to political instability and insurgents may attempt to exacerbate such disparities by attacking the economic infrastructure of a society. JIPOE analysts

help identify economic disparities and assess the vulnerabilities and capabilities of economic infrastructure.

(4) **Political Participation.** Another common interest of civil populations concerns the right to effective political representation and participation. Groups that have been denied participation in the political process often support insurgencies or organizations that promise enfranchisement. Very often, such groups rally around traditional or charismatic authority figures.

4. Increased Importance of Infrastructure Analysis

a. Infrastructure analysis takes on added importance as the focus of military operations shifts from target development during traditional war to the reconstruction of facilities and reestablishment of services during stability operations. Infrastructure analysis should emphasize what currently exists and what is a critical shortfall locally, regionally, and nationally. JIPOE analysts should also assess the vulnerability of critical infrastructure to sabotage, direct attack, or other interference by the adversary. JIPOE infrastructure analysis must be tailored to orient commanders and planners on the priorities for US military, interagency, NGO, and IGO relief immediately and over time so as to prevent humanitarian crises and to reinforce a secure and stable environment.

b. From an infrastructure perspective, it is imperative to understand the current state of the previous and remaining government services, associated civilian expertise, transportation nodes, lines of communications, hospital and medical facilities and public utilities as well as what is projected to remain. An accurate portrayal of the infrastructure status will potentially prevent or help eliminate humanitarian crises. JIPOE analysts should focus not only on what infrastructure is available, but also what is missing and the means by which it may be obtained. Subsequent to the initial needs, an assessment must be conducted in terms of the industrial, financial, and import/export systems within the country. Enduring institutions will require operating expertise, potential rebuilds or enhancement, security, monetary assistance, and resource inputs to not only restart but also to expand the inherent or existing capabilities and institutions. Doing so will allow the gradual build up of the enduring institutions necessary for immediate assistance and long-term success. For example, during Operation JUST CAUSE, US forces gradually subdued looting crowds and secured the 142 sites that provided Panama City's sanitation, power, water, telephone, and other public services after three days of anarchy, initiating the rebuilding of Panama's infrastructure and an economy racked by years of corruption.

5. Heavier Emphasis on Detailed Knowledge

JIPOE analysts must use information from a variety of intelligence and non-intelligence sources and methods and use appropriate analytical strategies to develop the type of detailed knowledge required during stability operations. Determining the cultural landscape of the operational area requires a heavy reliance on information from open sources, civilian academic centers of excellence, and local officials and law enforcement. Although the JIPOE effort will require input from all intelligence disciplines, HUMINT

and GEOINT assume increased importance in stability operations. In combination, HUMINT, GEOINT, and other sources enable the creation of products invaluable during stability operations and IW. For example, US and multinational forces operating in an urban environment will require the ability to correctly orient their forces against specific street addresses based on local tip-off information. Operations directed against the wrong building or dwelling may have unintended and/or undesired consequences. In many situations, however, street addresses in foreign urban areas do not use conventional numbering or structured identification systems. In these situations, HUMINT and information derived from open sources and local postal officials may be combined with GEOINT to produce accurate street address maps. Likewise, local law enforcement officials are crucial sources of information regarding criminal organizations, individuals, activities, areas, and methods. Mapping relevant sociocultural and environmental factors utilizes information and intelligence from multiple sources (intelligence disciplines, police units, military patrols, civil affairs units, provincial reconstruction teams, etc.) to produce network analysis diagrams and corresponding geospatial products. Figure IV-1 depicts using reported data, a network perspective, and a geospatial perspective to understand the sociocultural and environmental factors of the operational environment.

a. **Geospatial Intelligence.** GEOINT applies to all spatially referenced functions, data, and activities within the JIPOE process, and GEOINT data and processes provide the foundation for all fusion, analysis, and visualization activities. It is essential that GEOINT support be coordinated in advance between the joint force, national agencies, combatant commands, and allied and HN forces in order to form a common point of reference and framework for JIPOE. The accuracy and scale of foreign maps and charts may vary widely from US products. Additionally, release of US geospatial and JIPOE products and information may require foreign disclosure approval. While joint operations graphics are often used as the standard scale for joint plans and operations, stability operations require extremely accurate geospatial products and information with significantly greater detail. The JFC must ensure that all subordinate commands utilize compatible GEOINT products, data, and standards to ensure JIPOE processes and products developed by the joint force J-2 adequately support the mission. The joint force GEOINT staff officer will assist all units and activities participating in stability operations to acquire all GEOINT products prescribed by the JFC.

b. **Human Intelligence.** Due to the emphasis placed on understanding the civil population, HUMINT assumes increased importance during stability operations and IW and often provides the most valuable sources of information. However, a HUMINT infrastructure may not be in place when US forces initially arrive. Appropriate liaison channels need to be established as quickly as possible with multinational partners and appropriate elements within the HN while HUMINT operations are established. This will require early planning and release authority for exchanging intelligence with the HN and other multinational partners. Operational circumstances may also require the insertion of HUMINT personnel into the operational area ahead of a joint force. HUMINT can provide route reconnaissance, ground truth reporting, intentions, and enabling support for other intelligence disciplines. In addition, HUMINT and CI operations provide information on foreign intelligence services and terrorist activities in the operational area

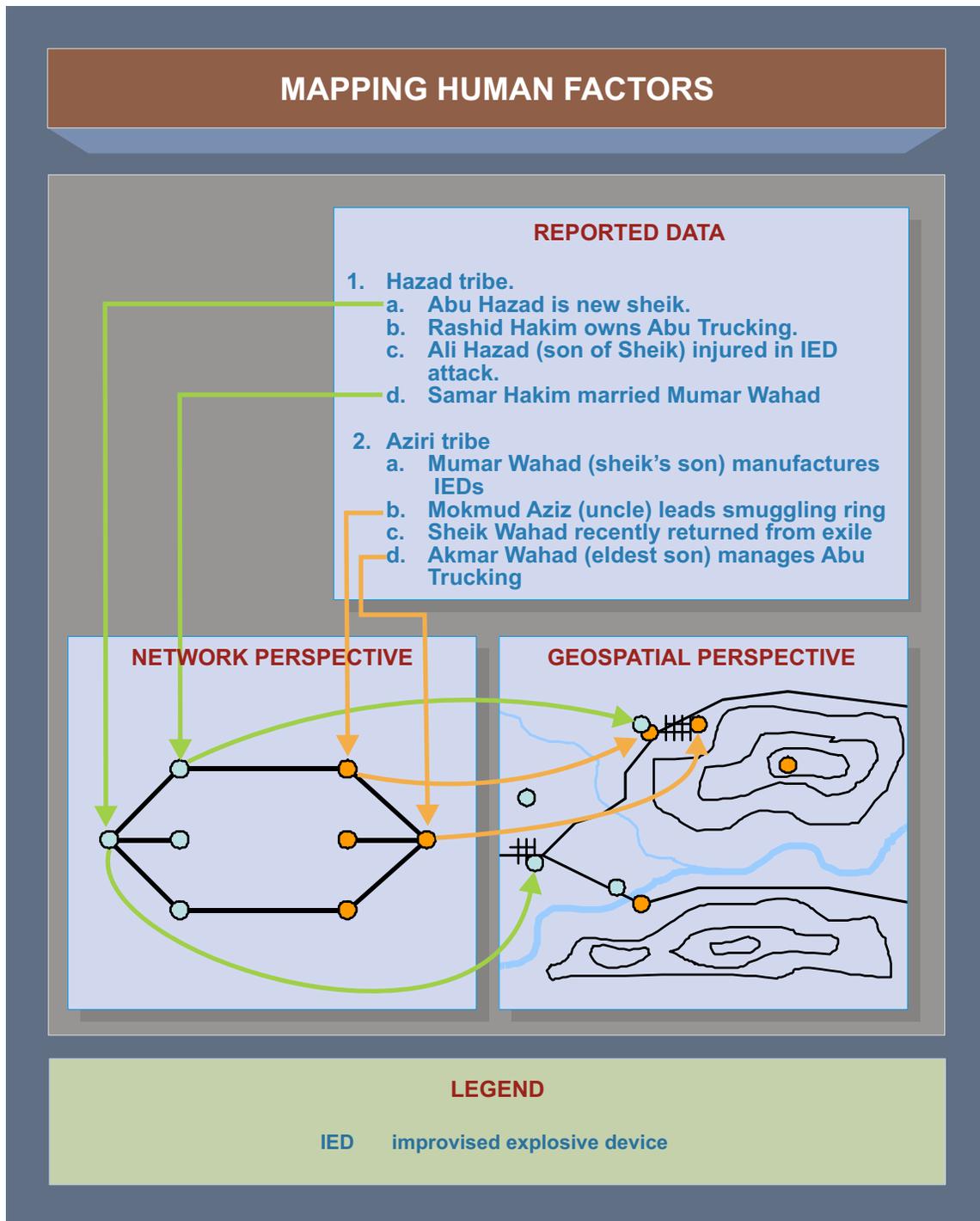


Figure IV-1. Mapping Human Factors

that allow CI assets to identify, exploit, or neutralize an adversary's capabilities and initiative. HUMINT can also be a critical element in supporting special operations.

6. Increased Need for Collaboration and Information Sharing

a. During stability operations and IW, the joint force will usually operate in a complex international environment alongside other important actors that will have a need for JIPOE products. They are also likely to possess valuable information they can provide the joint force that is unique to their own mission and sources. The J-2 must have a process in place to exchange information with external sources and assess the validity of information supplied by mission partners. This process should include foreign disclosure officers, delegated with the proper authority to disclose classified military information to foreign government and international organizations in accordance with legal and policy guidelines. Mission partners may include USG interagency members, UN organizations, allied coalition military and security members, local indigenous military and security forces, NGOs, and private companies and individuals providing contract services within the operational area. Although the joint force may have organic ISR capabilities assigned, the aforementioned mission partners may, in fact, provide the bulk of information for analyzing the operational environment during stability operations and IW. The J-2 will find the information coming from these disparate entities just as valuable, or more so, for assessing the overall situation than traditional intelligence sources. Therefore, a robust information sharing process will be required with individuals operating at multiple classification levels. Wherever possible, consistent with DOD Directive 5530.3 *International Agreements*, the J-2 should establish routine procedures to foster a cross-flow of information. Information from mission partners may not arrive in standard DOD or IC formats, and will require validation to assess veracity prior to inclusion in JIPOE assessments. Nonetheless, the information provided by the mission partners is critical for the JIPOE effort to produce a comprehensive picture of the operational environment.

b. Support to stability operations will require JIPOE planners to collaborate closely with IC elements to obtain expertise and materials that do not exist at the JTF level. This will occur to a greater extent during stability operations due to a reduced ISR support structure and a less clearly defined adversary. In some cases, external support for analyzing sociocultural factors or tracking the financial activities of potentially threatening individuals, groups, or activities may be required. In other contingencies, a majority of the JIPOE output will be GEOINT products. This may be the case when the primary adversary is terrain or weather factors. Other products deemed of interest may be obtained or provided by producers external to the JTF or combatant command. For example, MIPOE products can be obtained from the National Center for Medical Intelligence (NCMI), which serves as the DOD focal point for medical intelligence. Requests for external support should be coordinated through the combatant command JIOC or joint force JIPOE coordination cell (when formed).

7. Focused Process and Tailored Products

The primary difference between the basic JIPOE process during traditional war and the JIPOE effort during stability operations and IW is one of focus; particularly in the high degree of detail required, and the strong emphasis placed on demographic analysis

“Imagine cartography in three dimensions, as if in a hologram. In this hologram would be the overlapping sediments of group and other identities atop the merely two-dimensional color markings of city-states and the remaining nations, themselves confused in places by shadowy tentacles, hovering overhead, indicating the power of drug cartels, mafias, and private security agencies. Instead of borders, there would be moving ‘centers’ of power, as in the Middle Ages. Many of these layers would be in motion. Replacing fixed and abrupt lines on a flat space would be a shifting pattern of buffer entities... To this protean cartographic hologram one must add other factors, such as migrations of populations, explosions of birth rates, vectors of disease. Henceforward the map of the world will never be static. This future map – in a sense, the ‘Last Map’ – will be an ever-mutating representation of chaos.”

**SOURCE: Robert D. Kaplan, “The Coming Anarchy,”
The Atlantic Monthly, Feb 1994**

of the civil population. JIPOE products must be tailored to the situation and focus on analyzing the vulnerabilities of critical infrastructure, understanding the motivations of the adversary, and identifying any shared aspirations, values, or outlooks that link the adversary to the general population. Due to the fluid and dynamic nature of stability operations, commanders and their staffs are often overwhelmed with details and can quickly reach information overload. The JFC and supporting units, multinational forces, and local officials and law enforcement personnel must have access to continuously updated situational depictions of the operational environment in order for them to be effective. In this type of environment, written products are less likely to be used unless they are of critical importance. Therefore, the JIPOE effort in support of stability operations will be graphic intensive and use techniques that can easily and rapidly update and summarize *relevant* aspects of the operational environment. The following discussion describes some of the specific types of information relative to stability operations and IW that should be considered during the JIPOE process. Techniques for graphically depicting this information are illustrated in Appendix D, “Specialized Products.”

a. **Defining the Operational Environment.** The transition from traditional war to nontraditional missions may be blurred in that the stability phase may begin in some liberated areas under US or coalition control prior to conclusion of hostilities. Therefore, stability operations can and will occur across the range of military operations. They can also occur in response to natural or man-made disasters, outside the context of any political or military conflict.

(1) JIPOE in support of stability operations and IW places a heavy emphasis on the identification and evaluation of unforeseen obstacles to mission accomplishment. In addition to establishing a secure environment, a mission of the joint forces during stability operations may be to help set the conditions for effective governance. There may be numerous obstacles presented by the operational environment to setting

conditions conducive to effective governance that do not involve use of violence against the joint force or the civilian authorities. Nonetheless, these obstacles must be identified by JIPOE analysts and considered by the JFC during operation planning.

(2) During stability operations and IW, the single most important aspect of the operational environment will usually be the civil population. The role of the JIPOE analyst is to anticipate natural and human impediments to fulfilling the joint mission. There are instances in which the mission will be opposed by groups or individuals using political or violent means of resistance. In other cases, the population will welcome outside assistance but the geography, climate, infrastructure, or nature of the mission itself will present challenges that must be anticipated and overcome. The JIPOE process in support of nontraditional missions will necessarily involve the identification and complex examination of all relevant factors – environmental and human – that help define the operational environment.

b. Describing the Impact of the Operational Environment. The JIPOE effort during stability operations should be focused on detailed analysis of all the relevant cultural aspects previously described, and should portray the current state of government services, transportation system, LOCs, public utilities, finance, communication, agriculture and food distribution, healthcare, and commerce. In doing so JIPOE analysts are able to determine what exists versus what does not exist. The analyst can then recommend what is most critical immediately and over time, and enable commanders to tailor operations according to the situation. In addition to the types of templates and overlays discussed earlier, JIPOE products supporting stability operations may include graphic depictions of infrastructure status and demographic/cultural characteristics of the operational environment. These graphic products are a key visualization aid for commanders and their staffs, and should be designed with the perspective of the joint force mission in mind. For instance, during a mission in support of a natural disaster, such as a flood or earthquake, overlays should be produced depicting the condition of existing road and rail infrastructure and locations of displaced persons.

c. Evaluating the Adversary. The term “adversary” must be understood to mean a party, groups or individuals, potentially hostile, who may interact with the joint force and could potentially hamper mission accomplishment. During stability operations and IW, the adversary may range from loosely organized networks or entities with no discernible hierarchical structure to highly structured organizations with centralized C2. Regardless of structure, the adversary must usually rely on the civil population for its sustainment – a critical vulnerability that may be exploited within the country’s interconnected systems. This type of adversary often wages a protracted conflict in an attempt to break the will of the nation-state and sometimes employs tactics (such as terrorism) that may alienate the civil population. During stability operations, threats to completion of the mission can also come from a variety of physical, environmental, or sociocultural factors.

(1) In an effort to create a secure and stable environment it is imperative to be able to identify and understand the characteristics of the remaining military threat in the realm of conventional military forces, unconventional military forces, local militias,

weapons, facilities and sustainment means being used, evolving chains of command, and influence on the local population. The JIPOE process must articulate the hostile forces both internal and external to the targeted country, to include their tactics, objectives, and key leaders.

(2) The identity and general uniformity of a military threat is often absent in a stability operation. When potential violent groups exist in the operational area, the environment becomes even more complex with rapidly shifting, self-proclaimed group titles, multiple memberships by individual terrorists or cells, and blurred connections between groups, political movements, and communities. In many cases, the adversary is described in terms of individuals or small cells that are disaffected and prone to violence. These individuals may be hybrid terrorists and criminals that use illicit activities to finance terrorist activities in support of political goals. The roles of private organizations, such as contract security personnel, NGO service providers, indigenous neighborhood associations, religious communities, and other local actors must also be assessed.

(3) In addition, the potential criminal threat must be assessed. JIPOE analysts must determine who the criminals are, how they are organized, where they are located, and what their historical patterns of activity were. Beyond organized crime and its associated hierarchy, methods, and focus, the JIPOE effort should address what the environment will look like for crime following combat operations. For example, what are the needs and shortages of the local population that will drive crime and who are the likely targets? What will be the likely targets of looting? What are the capabilities of local police?

d. Determining Adversary Courses of Action. The weaker opponent that exists in most IW and stability situations will usually seek to avoid large-scale combat and will focus instead on small, stealthy, hit-and-run engagements and possibly suicide attacks. The weaker opponent also could avoid engaging the superior military forces entirely and instead attack nonmilitary targets in order to influence or control the local populace. An adversary using IW methods typically will endeavor to wage protracted conflicts in an attempt to break the will of their opponent and its population. IW typically manifests itself as one or a combination of several possible asymmetric approaches including insurgency, terrorism, disinformation, propaganda, organized criminal activity (such as drug trafficking), strikes and raids, and the use of WMD. The specific form will vary according to the adversary's capabilities and objectives. IW focuses on the control of populations, not on the control of an adversary's forces or territory. Adversary COAs may not be solely directed against US, coalition, or HN *military* forces, but may be directed more toward the sociological, governance, economic, and technological elements of a nation. Discerning these types of nonmilitary COAs presents a unique challenge to JIPOE analysts and requires a comprehensive appreciation for how all the relevant aspects of the operational environment interact with one another.

SECTION B. COUNTERING ASYMMETRIC APPROACHES

“Asymmetric warfare—attacking an adversary’s weaknesses with unexpected or innovative means while avoiding his strengths—is as old as warfare itself. In the modern era, many forms of asymmetric attack are possible—to include ... terrorism, guerilla operations, and the use of WMD [weapons of mass destruction]. Because of our dominant military position, we are very likely to be the focus of numerous asymmetric strategies...”

Lieutenant General Patrick M. Hughes, US Army
Global Threats and Challenges: The Decades Ahead, 1998

8. Overview

Adversaries are likely to use asymmetric approaches as a method of degrading or negating support for military operations or the military dominance of friendly forces. Adversary asymmetric approaches may include activities such as camouflage and concealment, MILDEC, hardening and burying targeted infrastructure, CNA, propaganda, terrorism, insurgency, and the use or threatened use of WMD, theater missiles, and innovations such as improvised explosive devices. Several types of joint force activities and operations are applicable to deterring, mitigating, or countering an adversary’s use of asymmetric approaches. JIPOE support to these types of joint force activities may require a slightly different focus than that described in previous chapters. Although the basic four-step JIPOE process remains the same, each activity will require detailed information relating to its own unique set of requirements. The following information, although not all inclusive, provides examples of some of the factors that should be considered when applying the JIPOE process in support of joint force activities capable of countering asymmetric approaches (see Figure IV-2).

9. Adversary Measures to Avoid Detection

The adversary may use asymmetric means to counter friendly ISR capabilities and complicate friendly targeting efforts through MILDEC, camouflage and concealment, frequent repositioning of mobile infrastructure, and the selective use of air defense systems to force airborne ISR assets to less than optimum flight profiles. For example, Serbian forces in Kosovo made extensive use of camouflage, concealment, and decoys to mitigate the effectiveness of allied air strikes during Operation ALLIED FORCE. JIPOE helps to counter the effectiveness of these asymmetric techniques by supporting the joint force’s ISR and targeting efforts. JIPOE support to ISR is designed to optimize the employment of ISR and target acquisition assets by forecasting the times and locations of anticipated adversary activity. Additionally, ISR collects the information required to update the joint force’s JIPOE products. ISR is therefore both a consumer and provider of JIPOE data.

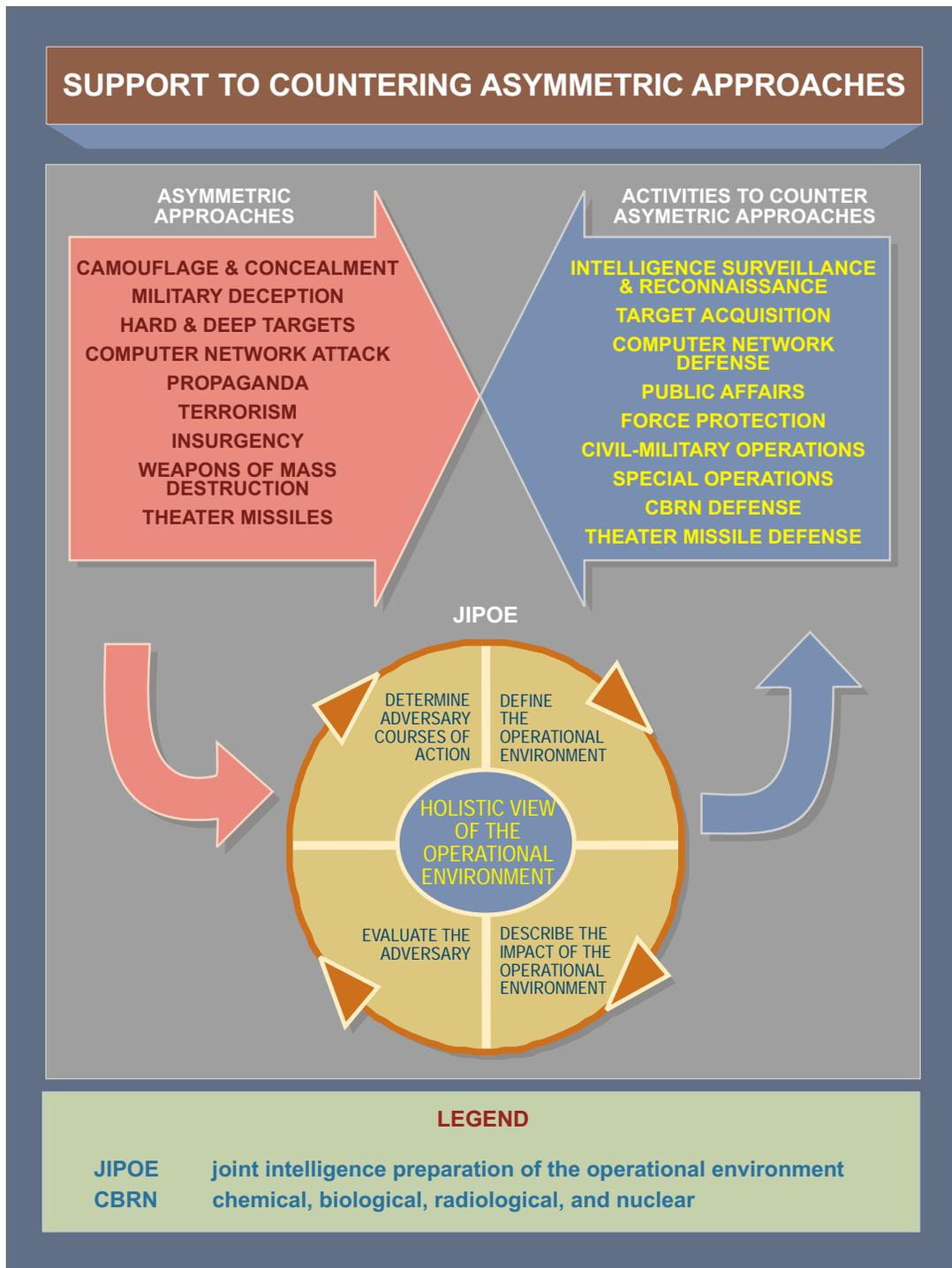


Figure IV-2. Support to Countering Asymmetric Approaches

a. **Define the Operational Environment.** The operational environment must encompass all aspects relevant to adversary capabilities to counter friendly ISR and target acquisition efforts. Conversely, the JIPOE effort must also include all aspects and measures that would increase the efficiency of friendly ISR and target acquisition assets. In addition to the locations of all adversary military forces, the operational environment should include the following:

(1) Potential airfields, supporting infrastructure, and optimum locations in the operational area capable of supporting friendly ISR and target acquisition operations.

(2) Adversary or third-nation air defense envelopes and antisatellite launch locations;

(3) Areas of known or probable underground facility construction.

(4) Actual and potential sources of intelligence or information (e.g., third party nations, internet sites) available to the adversary regarding friendly ISR capabilities, schedules, and flight profiles.

b. Describe the Impact of the Operational Environment

(1) Identify and analyze potential deployment locations for land-, air-, and sea-based ISR assets. Consider factors such as:

(a) Location of ISR targets vice the range of ISR assets;

(b) Accessibility to the ISR site;

(c) Optical and radio line of sight from the ISR site to adversary locations;

and

(d) Defense against rear area threats.

(2) Locate obstacles to ISR operations such as:

(a) Areas with good natural camouflage and concealment;

(b) Objects that may interfere with ground, airborne, and naval ISR operations, such as high power transmission lines, jungle vegetation, buildings, mountains, reefs, sandbars, defensive obstacles, and barriers; and

(c) Widespread non-adversary military, commercial, and civilian use of radio frequencies.

(3) Evaluate how environmental conditions will affect both friendly and adversary ISR systems. Consider how extreme temperatures, winds, humidity, dust, cloud cover, atmospheric conditions, and electromagnetic storms will affect:

(a) Sensitive electronic equipment and antennas;

(b) Flight operations of ISR airborne platforms;

(c) Line of sight observation for optical, infrared, millimeter wave, and other sights and sensors; and

(d) Imagery resolution and radio frequency propagation.

(4) Assess the adversary's capability to relocate underground, or disperse to remote areas, critical infrastructure and military assets (e.g., factories, storage depots, aircraft, theater missiles).

(5) Determine those areas where the effectiveness of adversary air defense systems is optimized.

(6) Identify areas where adversary air defense systems are least effective due to factors such as terrain masking or ground clutter.

(7) Locate all subsurface facilities (subways, tunnels, mines, overpasses) of potential use to the adversary in relocating or hiding mobile targets.

c. **Evaluate the Adversary.** Analyze the standard OB factors for each adversary unit, concentrating on how the adversary will appear to friendly ISR systems.

(1) Identify signatures for specific adversary units and items of equipment.

(2) Analyze the adversary's capability, techniques, and procedures for conducting camouflage, concealment, and MILDEC.

(3) Assess the adversary's normal state of OPSEC.

(4) Analyze the adversary's potential use of air defense assets in new or innovative ways to locate and destroy friendly ISR assets.

(5) Construct adversary templates identifying locations where the adversary is most likely to deploy military HVT and HPT at each phase of specific COAs.

(6) Analyze hard and deeply buried targets for points of vulnerability to precision munitions.

d. **Determine Adversary Courses of Action.** Identify and analyze adversary COAs that could directly affect friendly ISR operations, such as:

(1) Attacks on friendly ISR assets located in the JSA;

(2) Specific types of lethal and nonlethal operations to counter friendly ISR (e.g., SOF, global positioning system denial, CNA, lasers, CBRN); and

(3) Reallocation of adversary air defense units or MILDEC assets to areas previously vulnerable to friendly ISR operations.

10. Adversary Use of Information Operations

An adversary is likely to use information-related approaches to counter US advantages in C2, information processing, and decision making, and to reduce public and international support for military operations. JIPOE supports IO and activities by identifying adversary capabilities, vulnerabilities, and strategies and influencing friendly public opinion and decision making.

For further information regarding IO and public affairs see JP 3-13, Information Operations and JP 3-61, Public Affairs.

a. Define the Operational Environment. The general characteristics of the operational environment, as it pertains to IO, will vary depending on factors such as the following:

- (1) The capabilities and geographic reach of the friendly and adversary information gathering systems;
- (2) The sources of information upon which friendly and adversary forces base significant decisions;
- (3) The capabilities of friendly and adversary information processing, transmission, reception, and storage systems; and
- (4) The strategic goals, political motivations, and psychological mindset of the targeted country or group.

b. Describe the Impact of the Operational Environment. The physical, informational, and cognitive dimensions of the information environment could impact both friendly and adversary forces and should be analyzed in order to:

- (1) Evaluate existing and potential impediments to the flow of information required to support the decision-making process.
- (2) Identify and evaluate critical nodes in information collection, processing, and dissemination systems.
- (3) Determine the characteristics and vulnerabilities of specific C2 and ISR systems.
- (4) Evaluate the level of adversary and friendly OPSEC and communications security discipline.

(5) Assess to what degree the values, beliefs, and motivations of key adversary population groups and military forces coincide or conflict with those of political leaders or may influence decision making.

(6) Identify potential vulnerabilities of friendly forces to specific types of adversary propaganda themes or disinformation.

(7) Assess the effectiveness of PSYOP products in the operational environment.

c. Evaluate the Adversary

(1) Identify and assess adversary capability to conduct computer network operations to include defense, exploitation, and attack.

(2) Identify adversary propaganda themes and techniques for exploiting friendly and international public opinion.

(3) Identify potential “key communicators” that could be used by the adversary to influence friendly public opinion or decision making.

(4) Identify and prioritize significant sources of information and decision-making criteria used by friendly decision makers.

(5) Analyze friendly IO related vulnerabilities with attention to factors such as:

(a) C2 network structure vulnerabilities and redundancies;

(b) The susceptibility of friendly ISR systems to MILDEC;

(c) Procedures for shifting to backup systems or making use of another nation’s assets or networks; and

(d) Frequency allocation techniques.

(6) Assess the potential for adversary exploitation of friendly perceptions regarding the political situation, military objectives, and general morale.

d. Determine Adversary Courses of Action

(1) Identify which friendly information systems are most likely to be targeted by adversary information capabilities. Correlate specific adversary information capabilities with indicators of other likely adversary activity (e.g., special operations, sabotage, conventional attacks).

(2) Postulate how the adversary will exploit any loss or degradation of specific friendly information systems at critical junctures during an operation.

(3) Identify likely adversary propaganda messages and/or themes (e.g., misinformation, disinformation, or other public information disseminated to negatively influence public opinion about US and partner/coalition operations).

11. Terrorism

Adversaries may commit terrorist acts against US Service members, civilian employees, family members, facilities, and equipment in an attempt to demoralize US forces and counter public support for military operations. JIPOE helps combat terrorism by supporting force protection measures, CI, and other security related activities. Combating terrorism consists of actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (actions taken directly against terrorist networks and indirectly to influence and render global environments inhospitable to terrorist networks), taken to oppose terrorism throughout the entire range of possible threats.

a. **Define the Operational Environment.** The operational environment, relative to combating terrorism, may involve an area larger than that associated with traditional types of operations. Since the operating area for some terrorist groups may not be restricted geographically, the AOI pertaining to the terrorist threat to the joint force may be worldwide.

(1) Identify the locations and communications networks of adversary terrorists and supporting nations, groups, or organizations, as well as the likely targets of such forces (such as friendly military housing units, transportation networks, and rear area installations).

(2) Consider which terrorist groups are most likely to attack friendly personnel, equipment, and assets. Determine where they are normally based, and what third parties may provide them with sanctuary and support (training, logistics, etc.).

(3) Anticipate how additional missions such as a noncombatant evacuation operation (NEO) may affect force protection.

b. Describe the Impact of the Operational Environment

(1) Identify the stated and unstated strategic goals or desired end state of terrorist leaders.

(2) Determine the demographic issues that make protected areas or personnel attractive as potential terrorist targets.

(3) Evaluate the potential for terrorist attack on infrastructure targets such as local sources of drinking water, stockpiles of supplies, arms depots, transportation systems, communications infrastructure, and electrical power facilities.

(4) Assess the vulnerability of specific targets to attack. Consider both physical security issues and time constraints that might limit the availability of a target to terrorist attack.

(5) Identify probable avenues of approach as well as infiltration and exfiltration routes.

c. Evaluate the Adversary

(1) Analyze the strengths and weaknesses of terrorist ISR capabilities against force protection-related targets. Determine all available sources of the adversary's information.

(2) Assess the degree of risk the terrorist group is willing to take in order to attack various types of force protection targets. Determine which types of targets the adversary considers most valuable.

(3) Identify the goals, motivations, political or social grievances, dedication, and training of terrorist groups. Evaluate how these factors may affect target selection.

(4) Identify the adversary's preferred methods of attack such as bombing, kidnapping, assassination, arson, hijacking, hostage taking, maiming, raids, seizure, sabotage, or use of WMD.

(5) Assess any variations in terrorist organization, methods, and procedures that may be unique to specific types of terrorist actions (e.g., ambushes, assassinations, bombing, hijackings).

(6) Determine how and from where the adversary receives external support.

d. Determine Adversary Courses of Action

(1) Identify the adversary's most likely targets by matching friendly vulnerabilities against adversary capabilities, objectives, and risk acceptance.

(2) Assess the status of specific types of terrorist support activities that may indicate the adoption of a specific COA.

(3) Identify likely terrorist activity along infiltration routes, assembly areas, and surveillance locations near each of the adversary's likely objectives.

12. Insurgency

In order to counter US advantages in conventional forces, an adversary may support insurgencies in other countries or in response to an occupation of their country. Insurgents may use tactics ranging from terrorism to small or intermediate size

unconventional attacks. In addition to supporting conventional forces, JIPOE analysts help support specialized joint force counterinsurgency activities such as special operations and CMO. Special operations encompass the use of specially organized, trained, and equipped units to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. Special operations can be used to counter asymmetric threats by attacking or neutralizing adversary targets that may be inappropriate for engagement by conventional means alone. Due to the high level of physical and political risk involved, special operations require extremely detailed JIPOE products. CMO are the activities of a commander that establish, maintain, influence, or exploit relationships between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile operational area to facilitate military operations and consolidate operational objectives. Effectively executed CMO are capable of countering potential asymmetric threats, such as attempts by the adversary to incite hostility toward friendly forces, or to use crowds, demonstrations, or dislocated civilians (DCs) to hinder friendly military operations.

a. **Define the Operational Environment.** The AOI for special operations and CMO should encompass:

- (1) Infiltration and exfiltration routes and corridors;
- (2) Insurgent communications means and methods;
- (3) Areas or countries that provide military, political, economic, psychological, or social aid to the target forces or threats to the mission;
- (4) Military, paramilitary, governmental, and NGOs that may interact with the friendly force;
- (5) The extent to which international law constrains special operations and CMO activities both during and after hostilities;
- (6) Sources of food and water, pattern of population distribution, and locations of critical infrastructure; and
- (7) The attitudes of the population toward US and friendly forces and toward civil government in general.

b. **Describe the Impact of the Operational Environment**

(1) Evaluate how METOC affects SOF capabilities to conduct infiltration and exfiltration operations, with particular attention to factors such as the following:

- (a) Surface and upper air winds on SOF airborne, aerial leaflet, and loudspeaker operations;

(b) Benefits of clouds and low visibility on SOF air operations and special reconnaissance;

(c) Extreme temperatures, humidity, or sand on SOF personnel, aircraft, and other equipment;

(d) Tides, currents, and sea state as well as water temperature and bioluminescence on waterborne operations; and

(e) Illumination.

(2) Analyze the electromagnetic environment for its effect on SOF communications.

(3) Assess how the attitudes, values, and motivations of the civil populace will facilitate or constrain CMO activities. For example, nationalism or religious beliefs may cause the population to resent or resist certain types of CMO activities.

(4) Analyze the attitude of the local populace toward the existing or pre-hostilities civil government. Assess how this may affect CMO activities conducted through or in conjunction with local civil officials.

(5) Survey the extent of damage to local infrastructure, estimate the level of infrastructure capacity required to support the populace (including additional DCs), and determine if local sources of repair materials are sufficient.

(6) Estimate how and where the weather and environment might help or hinder insurgent forces. For example, drought may exacerbate food shortages, while flooding may increase the number of DCs and create shortages of shelter. These factors may help insurgents recruit additional members but could also reduce their access to necessities.

c. Evaluate the Adversary

(1) Assess the capabilities and procedures of the insurgent's military, political, and internal security forces.

(2) Evaluate the organizational structure and procedures of all groups supporting the insurgents.

(3) Identify the motivations and potential sources of discord within the insurgent force.

d. Determine Adversary Courses of Action

(1) Identify how the adversary will attempt to counter special operations or CMO missions. Determine to what degree the adversary's likely response will include political, economic, social, or military countermeasures.

(2) Assess the insurgent's capability to secure all identified infiltration and exfiltration routes. Determine to what degree the adversary's strengthening of internal security in one area will detract from security in a different area.

(3) Postulate how the civil populace is likely to respond to various types of CMO activities, and how insurgents may attempt to leverage or exploit such responses. For example, the adversary may attempt to use propaganda against a vaccination program or try to gain control over food distribution centers.

(4) Consider the effect that the insurgent's perception of friendly forces may have on COA selection. If friendly forces appear overwhelmingly powerful, non-confrontational COAs may be preferred, whereas the appearance of weakness may invite insurgents to pursue higher risk COAs.

13. Actual or Threatened Use of Weapons of Mass Destruction

The actual or threatened development, proliferation, or employment of WMD by an adversary can impact friendly forces by causing those forces to prepare for or conduct WMD nonproliferation, counterproliferation, or consequence management operations. JIPOE analysts help mitigate this threat by assessing the adversary's potential proliferation or employment of WMD, characterizing the consequences of a WMD-related activity, and supporting the joint force's WMD defense effort. The potential for accidental or deliberate release of CBRN agents within the operational area is also a major JIPOE analytic concern.

a. Define the Operational Environment. With regard to WMD, the operational environment should encompass the following:

(1) All adversary countries or groups as well as potential belligerents known or suspected of possessing a WMD capability and their intent or commitment to using it;

(2) All current and potential locations of adversary and potential belligerent WMD delivery systems (e.g., missiles, artillery, aircraft, mines, torpedoes, and forces).

(3) All adversary known and suspected CBRN agents, nuclear capabilities, and their storage and production facilities;

(4) Nontraditional threats and targets;

(5) Unconventional weapons or materials capabilities (e.g., nanotechnology, biotechnology, advanced genetics, space-based capabilities, and advances in computing that allow actors more efficient access to information or production techniques); and

(6) Proliferation of WMD material, capabilities, expertise, and sensitive technologies.

b. Describe the Impact of the Operational Environment

(1) Identify and assess the vulnerability of key friendly logistic facilities and infrastructure to WMD attack.

(2) Identify all known and suspected chemical and biological agents.

(3) Identify critical weather and terrain information needed to determine the effects of weather on the use of WMD. Analyze the seasonal or monthly normal variations in weather patterns that might affect the use of WMD.

(4) Analyze the land and maritime surface dimensions to identify potential target areas for WMD attack, such as chokepoints, key terrain, and transportation nodes.

(5) Identify state and non-state actors of proliferation concern.

(6) Identify WMD material, capabilities, expertise, and sensitive and dual-use technologies.

c. Evaluate the Adversary

(1) Analyze adversary capabilities and will to proliferate and/or employ specific types of WMD. Determine the locations, volume, and condition of adversary WMD materials and stockpiles.

(2) Identify the specific types and characteristics of all adversary WMD delivery systems, with special attention to minimum and maximum ranges.

(3) Evaluate adversary doctrine to determine if WMD employment is terrain oriented, force oriented, or a combination of both.

(4) Assess the level and proficiency of adversary WMD training and protective measures.

(5) Assess the practicality and timeliness of an adversary's exploiting a new or different technology to develop a WMD capability and delivery means.

d. Determine Adversary Courses of Action

(1) Identify friendly assets that the adversary is most likely to target for WMD attack.

(2) Determine those locations where the adversary is most likely to deploy WMD delivery systems. These locations should be within range of potentially targeted friendly assets, yet still consistent with the adversary's deployment doctrine.

(3) Evaluate those characteristics of the adversary's WMD stockpile that may dictate or constrain WMD weapons use. These may include factors such as the quantity and yield of nuclear weapons, the age and shelf-life of stored chemical munitions, and the production and handling requirements for biological agents.

(4) Determine types and quantities of CBRN agent likely to be employed by an adversary.

14. Theater Missiles

An adversary may use theater ballistic missiles, unmanned aircraft, and cruise missiles to directly threaten friendly forces or to provoke political situations that may have strategic ramifications. For example, Iraqi Scud missile launches against Israeli targets during Operation DESERT STORM were intended to provoke an Israeli attack that could have had negative consequences for the coalition. Theater ballistic missile defense and counterair operations help protect the force from these types of asymmetric threats.

a. **Define the Operational Environment.** The operational environment for theater ballistic missile defense and counterair operations should incorporate portions of the air, land, maritime, and space domains. Consider factors such as the following;

(1) Areas likely to be targeted by adversary theater ballistic or cruise missiles.

(2) Theater ballistic and cruise missile launch locations, potential hide sites, forward operating locations, related locations, garrison locations, and associated infrastructure.

(3) Locations of operational and potentially operational airfields and launch locations.

(4) Range characteristics and flight profiles of adversary theater ballistic and cruise missiles.

(5) Bases, normal operating areas, and ranges of adversary SLCM-capable naval forces.

b. Describe the Impact of the Operational Environment

(1) Determine the locations of targets within range of specific adversary missile launch sites or airfields. Analyze the geography between the target and adversary base to determine potential missile trajectories and air avenues of approach for unmanned aircraft and cruise missiles.

(2) Identify areas for likely standoff attack orbits, SLCM launch locations, and aircraft carrier operating areas.

(3) Determine optimal times on target based on weather patterns, adversary launch and attack cycles, and light data.

(4) Determine line of sight from friendly air and missile defense systems and radar.

c. Evaluate the Adversary

(1) Assess the adversary's launch procedures, resupply operations, and target selection priorities.

(2) Consider the adversary's demonstrated capabilities, level of training and readiness status, operational cycles, and C2 regime, as well as actual equipment and hardware capabilities.

(3) Evaluate the threat to friendly air defense systems, to include adversary artillery, unconventional forces, and EW assets.

(4) Determine the adversary's requirements for air and missile base infrastructure, navigation aids, and communications system support equipment.

(5) Analyze the characteristics, availability, and quantity of specific types of warheads and launch platforms.

(6) Analyze the adversary's will to launch missiles.

d. Determine Adversary Courses of Action. Although the employment flexibility of mobile missiles and modern aircraft make the determination of specific COAs difficult, the JIPOE analyst should postulate how missile operations will support the adversary's joint campaign. Consider factors such as the following:

(1) Likely timing of missile strikes;

(2) Likely targets, objectives, and cruise missile avenues of approach;

(3) Occupation or preparation of forward launch locations;

(4) Strike package composition, ballistic missile flight profiles, distance between launch platforms, and time intervals between strikes; and

(5) Friendly air defense locations and coverage, and their likely effect on adversary missile operations.