Chapter 2

Information Environment Analysis

INTELLIGENCE PREPARATION OF THE BATTLEFIELD AND INFORMATION OPERATIONS

2-1. The information environment is the aggregate of three components—individuals, organizations, and systems—that collect, process, disseminate, or act on information. Understanding this environment requires an analyst—chiefly the IO officer or designated representative—to analyze each component of the environment as well as their aggregate. The analyst determines how the components interrelate.

2-2. The information environment also has three dimensions: physical, informational, and cognitive. All are important. The physical dimension consists of what users see—the physical content of the environment. This dimension contains observable behavior. This behavior enables the commander and staff to measure the effectiveness of their efforts to influence enemy and adversary decision making and the attendant actions that must occur across all audiences in the area of operations (AO). The informational dimension is the code that captures and organizes information that occurs in the physical dimension so that it can be stored, transmitted, processed, and protected. This dimension links the physical and cognitive dimensions. The cognitive dimension consists of the perspective of those who inhabit the environment; their individual and collective efforts to give context to what is happening or has happened and make sense of it. In this dimension, sense making occurs. If conflict is ultimately a contest of wills and victory is achieved by defeating the enemy or adversary psychologically, then achieving effects in the cognitive dimension can be decisive. The cognitive dimension is the hardest to understand. Therefore, the better that units operate in and exploit the physical and informational dimensions, the more they can overcome the challenges associated with the cognitive dimension. Table 2-1 on page 2-2 explores the three dimensions.

2-3. One purpose of IO involves affecting an adversary's ability to make sense of unfolding events. Affecting the adversary's perception of an event can indirectly impair, disrupt, or disable the adversary's ability to lead and direct operations. At the same time IO affects those perceptions, it attempts to preserve friendly commanders' ability to lead their forces and understand, visualize, describe, and direct operations. IO uses social media—a dominant aspect of the information environment—across and among all three dimensions. Messages, images, graphics, and sounds transmitted via social media affect perceptions and behaviors in real time and with profound impact.

2-4. Actions that occur in an operational environment almost always create effects in all three dimensions of the information environment. Through effective, proactive planning, units account for intended primary, secondary, and tertiary effects to support the commander's intent and concept of operations, while mitigating unintended effects. Precise effects across all three dimensions are only possible if the unit commander analyzes, understands, and visualizes the information environment and operational environment as a whole. Even the most prepared staff cannot anticipate all potential effects; however, understanding the information environment enables the staff to prepare for and react to unintended effects and determine why they occurred.

2-5. The mechanics of analyzing the information environment and enemy or adversary operations in the information environment are generally the same as those established to support intelligence preparation of the battlefield (IPB) for other military planning. IPB is a critical component of the military decisionmaking process (MDMP). It provides a systematic approach to evaluating the effects of significant characteristics of an operational environment for missions (for a full discussion of IO and the MDMP, see FM 3-13). IPB to support IO refines traditional IPB to focus on the information environment. Its purpose is to gain an understanding of the information environment in a geographic area and determine how the enemy or adversary will operate in this environment. The focus is on analyzing the enemy's or adversary's use of information to gain positions of relative advantage. The end state is the identification of threat information capabilities in the information environment against which friendly forces must contend and threat vulnerabilities that friendly forces can exploit with IO.

Table 2-1. Information environment dimensions

Types	*Affects*	*Examples*
Physical	Content	• The physical world and its content, particularly that which enables and supports exchanging ideas, information, and messages. • Information systems and physical networks. • Communications systems and networks. • People and human networks. • Personal devices, handheld devices, and social media graphical user interface. • Mobile phones, personal digital assistants, and social media graphical user interfaces.
Informational	Code	• Collected, coded, processed, stored, disseminated, displayed, and protected information. • Information metadata, flow, and quality. • Social media application software, information exchange, and search engine optimization. • The code itself. • Any automated decision making.
Cognitive	Context	• The impact of information on the human will. • The contextualized information and human decision making. • Intangibles, such as morale, values, worldviews, situational awareness, perceptions, and public opinions. • Mental calculations in response to stimuli, such as liking something on a social media application.

2-6. In addition to the running estimate, IPB to support IO results in producing a graphic or visualization product known as the combined information overlay. This overlay results from a series of overlays that depict where and how information aspects such as infrastructure, content, and flow potentially affect military operations. In certain instances, staffs may need more than one combined information overlay to capture the full complexity of the information environment (see paragraph 2-50 for a discussion on combined information overlay).

2-7. During mission analysis, the IO officer or representative ensures that IPB addresses the information environment and supports the planning and execution of operations. The intent is to better visualize the impact of the information environment on unit operations and to identify potential threat capabilities and vulnerabilities that the unit can protect against or exploit. This analysis involves four substeps that mirror the steps discussed in ATP 2-01.3:

- Define the information environment.
- Describe the information environment’s effects.
- Evaluate the threat’s information situation.
- Determine threat courses of action in the information environment.

STEP 1: DEFINE THE INFORMATION ENVIRONMENT

2-8. During the first step of mission analysis, the IO officer or representative coordinates with other staff officers and elements, particularly the intelligence staff section. Defining the information environment begins by clearly delineating the AO, as well as areas of interest, including contiguous areas to the AO that may affect information flow and decision making. Once delineated, the IO officer identifies the significant characteristics of the information environment within this defined area in all three dimensions (physical, informational, and cognitive) that can affect friendly and threat operations, as well as influence friendly courses of action and command decisions. These significant characteristics can include, but are not limited to, the following:

- Terrain (and weather).
- Populace.
- Societal structures.
- Military or government information and communications infrastructure.
- Civilian information and communications infrastructure.
- Media.
- Third party organizations.

TERRAIN (AND WEATHER)

2-9. One characteristic that the IO officer identifies is the terrain (and weather). The IO officer looks at the various ways physical, geographical, and atmospheric aspects of the AO impact information content and flow. These aspects can include compartmentalization, canalization, signal attenuation, radio wave propagation, and atmospheric and environmental limits on employing information systems.

POPULACE

2-10. Populace is another characteristic that the IO officer identifies. This characteristic involves identifying the human composition of the AO or area of interest in all its diversity to determine factors that impact information flow, receipt, and understanding. These factors tend to be static and non-voluntary; they are enduring traits or patterns of behavior that are innate or culturally ingrained to the point they are habitual and non-reflexive. Often IO officers study demographic and linguistic factors such as age, gender, education level, literacy, birth rate, ethnic composition, family structure, employment or unemployment rates, and languages.

SOCIETAL STRUCTURES

2-11. Societal structures affect friendly and threat operations. IO officers identify human networks, groups, and subgroups that affiliate along religious, political, or cultural lines, including commonly held beliefs and local narratives. These affiliations are voluntary and varied—over time, over space, and among individuals. IO officers focus their analysis on preferred means, methods, and venues that each social affiliation uses to interact and communicate and the ways each collectively constructs reality. Analysis examines biases, pressure points, general leanings, and proclivities, especially as they pertain to support or opposition of friendly and adversarial forces. Analysis also explores how these networks, groups, and subgroups express themselves and their commonly held beliefs through written and spoken narratives, stories, and messages.

MILITARY OR GOVERNMENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

2-12. The IO officer identifies another characteristic: the military or government information and communications infrastructure. Details of this characteristic involve understanding informational networks and communications systems that move information through the information environment to support military and governmental activities and facilitate decision making. Key networks and systems include special or enclave telecommunications means, methods, and capacity, such as telecommunications towers, fiber-optic networks, telephone networks (wired or wireless), microwave, satellite, and internet. IO officers understand the type and volume of information passed over or through these systems. These officers also benefit from knowing military or governmental authorities (leaders, decision makers, and military and civilian workforce) who use, manage, and control these systems.

CIVILIAN INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

2-13. A related characteristic that the IO officer identifies is civilian information and communications infrastructure. This characteristic involves understanding informational networks and communications systems servicing the general population that move information throughout the information environment. Key systems include telecommunications towers, fiber-optic networks, telephone networks (wired or wireless), microwave, satellite, internet, and cellular networks. IO officers identify these systems and the informational content moved on them before understanding ways that forces—friendly or adversarial—can exploit these systems to influence indigenous populations.

MEDIA

2-14. Characteristics of media can affect friendly and threat operations. Media includes physical, informational, and cognitive means by which local populations (including the adversary) receive and have their thinking shaped by information. Examples of the media's characteristics include radio and television broadcast facilities; print production facilities; news reporting, production, and dissemination sources; and outlets servicing the AO and areas of interest. Other examples include the primary and backup information systems used to move information from point to point, the information reported in terms of volume and content, the media's range and distribution capabilities, the audiences being marketed to and affected by the media, and the observed bias of the media and its cognitive effect on government, military, and civilian leaders, decision makers, and the general population.

THIRD-PARTY ORGANIZATIONS

2-15. Third-party organizations also have characteristics that affect operations. These organizations that simultaneously message in the information environment vary from nongovernmental and private organizations to other government agencies and international organizations. IO officers place analytical emphasis on identifying these organizations, determining their audiences, discerning their agendas, and estimating their impact on friendly operations.

2-16. Identifying and defining the significant aspects of the information environment helps to focus the IPB to support IO on those characteristics that will influence friendly courses of action (COAs) and command decisions. This focus thereby prevents unnecessary analysis and wasted effort. The initial analysis in this step determines the resources and time the IO officer or element commits to the detailed analysis that occurs in Step 2.

STEP 2: DESCRIBE THE INFORMATION ENVIRONMENT EFFECTS

2-17. In this step, the IO officer examines the significant characteristics or features of the information environment identified in Step 1 and determines their potential effects or impacts on friendly and threat operations in each dimension. As with IPB in general, this step focuses on how the threat, terrain and weather, and civil considerations can affect operations.

DESCRIBE HOW THE THREAT CAN AFFECT FRIENDLY OPERATIONS

2-18. The enemy or adversary is part of an operational environment and information environment. The threat's physical posture alone influences friendly decisions and operations, as well as the decisions and actions of the populace in the AO in ways that benefit the threat commander's intent.

2-19. For many adversaries, the information environment is decisive terrain. Adversaries actively seek to shape it to their advantage, often well before hostilities begin. Although a detailed analysis of enemy forces occurs during Step 3 and Step 4 of the IPB process to support IO, Step 2 defines the type of enemy forces and their general information capabilities. This is done to place the existence of these forces and their capabilities in context with other variables to understand their relative importance to the information environment. Sometimes the mere presence of a threat force is the most important characteristic in the information (as well as operational) environment. This force presence is the chief locus of influence. In other instances, the presence or absence of communications infrastructure or other feature will be the predominating characteristic.

2-20. The results of this substep are typically reflected in threat and situational overlays, which are visual depictions of doctrinal and current physical dispositions of all potential threat information forces or capabilities in the AO and area of interest. In addition to locations, these graphics include the identity, size, strength, AO, and coverage or reach for each potential threat information unit or capability. The IO officer often supplements these overlays with a threat description table that describes the threat's broad information capabilities (see Steps 3 and 4 of the IPB process for additional information about these overlays).

DESCRIBE HOW TERRAIN AND WEATHER CAN AFFECT FRIENDLY AND THREAT OPERATIONS

2-21. *Terrain analysis* is the collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations (JP 2-03). Just as terrain can canalize friendly or threat movement and maneuver, it can canalize the flow of information, thereby affecting the timeliness and effectiveness of decision making. Weather analysis is the evaluation of the direct and indirect effects of weather and climate on operations in the information environment. These effects can be as simple as directly affecting the employment of capabilities, such as EC-130J Commando Solo, or as complex as indirectly affecting AO-wide efforts to inoculate the local populace against enemy propaganda.

2-22. Terrain analysis involves identifying obstacles and key terrain, but IPB to support IO analyzes these features in terms of how they will affect the employment of IRCs, the flow of information, and decision making. Similarly, IPB to support IO analyzes weather patterns, forecasts, and climate data to determine their impact on IRC's employment, information flow, and decision making.

DESCRIBE HOW CIVIL CONSIDERATIONS CAN AFFECT FRIENDLY AND THREAT OPERATIONS

2-23. An understanding of civil considerations enhances the selection or formulation of IO objectives, the weighting of IO efforts (attack, defend, or stabilize), the appropriate mix of IRCs, and their employment, among other aspects. Such understanding begins even before deployment and leverages the entire staff, as well as outside agencies and unified action partners, who has relevant regional knowledge and expertise in civil considerations.

2-24. One method to discern significant civil consideration characteristics is depicted in table 2-2 on page 2-6, which crosswalks civil considerations with operational variables. Operational variables are known by the acronym PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time). Civil considerations, a subset of mission variables—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (known as METT-TC)—comprise areas, structures, capabilities, organizations, people, and events (known as ASCOPE). Staffs use operational variables to develop a comprehensive understanding of operational and information environments. Civil considerations refine this understanding so that staffs can visualize and describe operational and information environments in a manner that fosters shared understanding. This crosswalk helps the IO staff refine its understanding of what is relevant to missions and operations from its perspective. The staff can complete it with any single mission variable to the operational variables (see appendix A of FM 6-0 for information about operational variables; see chapter 4 ATP 2-01.3 for information on specific civil considerations in the IPB process).

Table 2-2. Examples of operational variables crosswalked with civil considerations

	Political	*Military*	*Economic*	*Social*	*Information*	*Infrastructure*
Areas	• Enclave, province, district • National boundaries • Shadow government influence area	• Areas of influence and interest • Area of operations • Safe haven • Local nation base or training area	• Commercial • Fishery • Industrial • Markets • Mining • Smuggling routes • E-commerce	• Refugee camp • Ethnic, social, tribal enclave • School district • Online group	• Broadcast coverage area • Social media reach or penetration • Word of mouth • Graffiti	• Road system • City limit • Power grid • Irrigation network • Suburb, exurb, urban core
Structures	• Court house • Government center • Capitol building • Meeting hall	• Base and base buildings • Training facility • Known leader house	• Banking • Fuel • Factory • Warehousing • Online store • "Wall Street" versus "Main Street"	• Club • Jail • Library • Religious building • Restaurant • Social media platform	• Cell tower • Broadcast facility • Physical internet structure • Postal service • Print shop	• Emergency shelter • Public building • Airfield, bridge, railroad • Construction sites • Electric station
Capabilities	• Civil authority, practices and rights • Executive, legislative, and judicial functions • Dispute resolution	• Doctrine • Organization • Training • Materiel • Leadership • Personnel • Facilities • Civil-military relationship	• Currency • Food security • Market or black market • Raw material • Tariff • BITCOIN • Imports or exports	• Social network • Nonprofit support to disasters • Social services	• News operation • Newspaper • Social media platform • Literacy rate • Intelligence service • Internet access	• Law enforcement • Fire fighting • Maintenance • Transportation • HVAC (heating, ventilation, and air conditioning)
Organizations	• Major political party • Nongovernmental organization • Host government • Court system • Insurgent group affiliation	• Host-nation forces • Insurgent group or network • Terrorist • Military lobbying group	• Bank • Business organization • Guild • Labor union • Landowner • Cooperative	• Clan • Online or in-person affinity group • Patriotic or service organization • Familial	• Media group • Public relations firm • Social media information group • News organization	• Construction company • Trade union • Cooperative

Table 2-2. Examples of operational variables crosswalked with civil considerations (*continued*)

	Political	*Military*	*Economic*	*Social*	*Information*	*Infrastructure*
People	• United Nations representative • Political leader • Governor • Elder • Legislator, judge, and prosecutor	• Key leader • Thought leader	• Banker • Employer or employee • Employment rate • Merchant • Smuggler	• Community leader • Teacher • Entertainer • Criminal • Migration patterns	• Decision maker • Elder • Religious leader • Internet personality	• Builders • Local development council • Road repairers • Police, fire fighter
Events	• Election • Council meeting • Treaty signing • National parade • Speech • Significant legal trial	• Combat • Military parade • Unit relief • Loss of leadership	• Drought, yield • Labor migration • Market day • Payday • Business opening	• Celebration • Civil disturbance • Funeral • Online forum • Social media livestream	• Censorship • Publishing dates • Online launch • Press briefing • Interview • Disruption of service	• Scheduled maintenance • School construction • New bridge opening • Disaster, man-made or natural

2-25. Due to the complexity and volume of data involving civil considerations, no simple or single model exists for presenting this analysis. It typically comprises a series of products, such as data files, overlays, and assessments.

2-26. IO officers and planners often use one common technique to present analysis. They prepare an overlay (graphical depiction) for each significant characteristic that visually displays its salient features and identifies gaps in intelligence or information that are subsequently refined into requirements for collection (requests for information, requests for collection). Figures 2-1 and 2-2 on pages 2-8, 2-9, and 2-10 provide example overlays. The first focuses on population centers and the second focuses on communications infrastructure. Both examples are based on the Decision Action Training Environment or DATE scenario as employed at the Joint Readiness Training Center.

Note. These overlays depict "a" way, not "the" way. IO officers or representatives must adapt their products to the situation at hand, their units' standard operating procedures, and commander's preference.

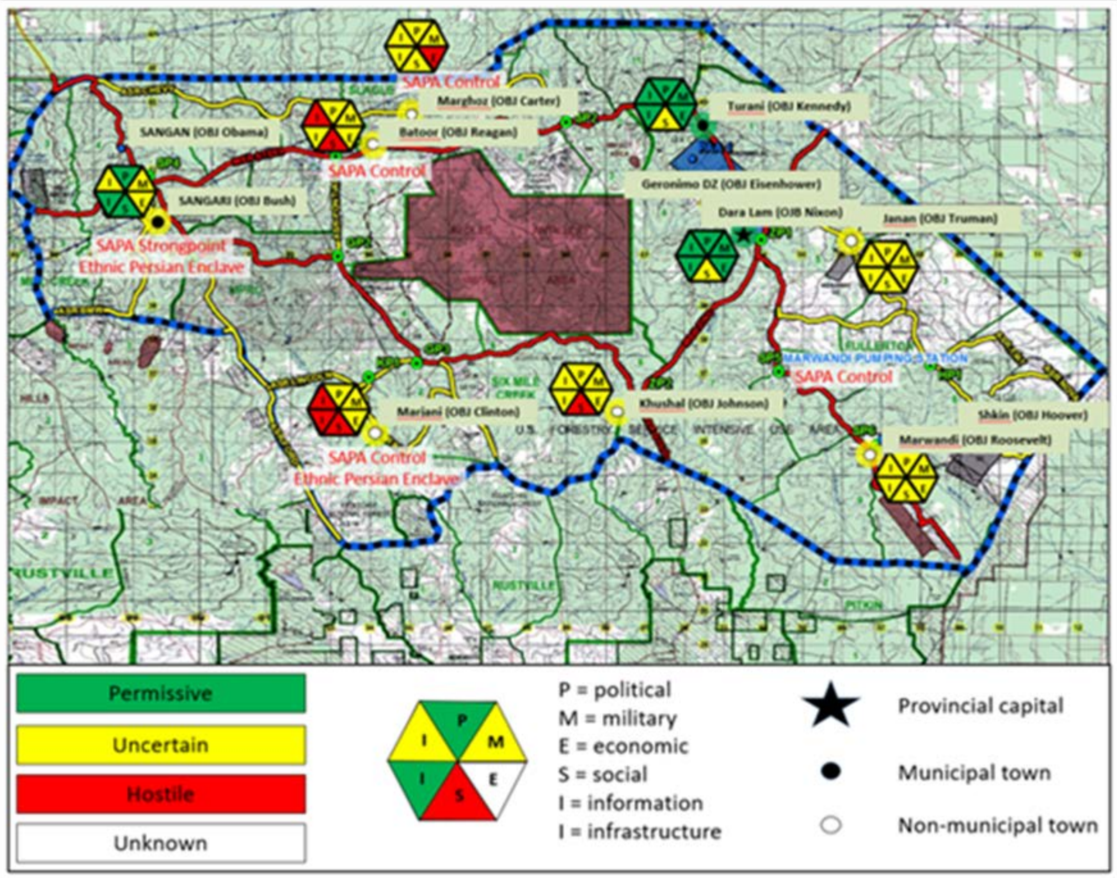


Figure 2-1. Example overlay that depicts relevant information about the populace in the area of operations

Sangari: • 2nd largest town in Kirsham • Strong allegiance to ROA (pre-SAPA) • Active municipal gov. (pre-SAPA) • ROA/U.S. built 'Model City" • Regular access to school, medical facility, and emergency services • Many businesses • Majority ethnic Persian; minimal ethnic tension pre-SAPA • SAPA restricts information flow	***Turani:*** • Joint municipality with Dara Lam • Strong allegiance to ROA • Strong economic growth • Majority ethnic Atropian • Moderate inter-ethnic friction • Adequate transportation • USAID and NGO activity • Clinic funded and operated by town (USAID rehabilitation project)	***Janan:*** • Small rural village • Dependent on NGO/IGO for essential services • Agricultural economy; minimal growth • Majority ethnic Atropian; dislike SAPA/likely support anti-SAPA activity • Ethnic unrest; Persian residents likely support insurgents/resent U.S. presence • Inadequate transportation
Batoor: • Small rural village • Active local gov. (pre-SAPA) • Majority ethnic Atropian strongly dislike SAPA/support anti-SAPA activity • Ethnic groups polarized; Persian residents likely resent U.S. mil. • Subsistence agriculture (pre-SAPA); some work for pipeline company • Atroprian-funded medical clinic; mobile NGO medical/food aid (pre-SAPA) • SAPA severely restricts information • Provincial water treatment facility	***Dara Lam:*** • Kirsham Provincial Capital and largest most prosperous town • U.S. Consulate • Strong allegiance to ROA • Strong economic growth • Majority ethnic Atropian • Moderate inter-ethnic friction • Adequate transportation • Access to schools, medical, emergency services • Sadvol enclave	***Khushal:*** • Small rural village • Active local government • Majority ethnic Atropian; strongly dislike SAPA/support anti-SAPA activity • Polarized population; Persian-Atropian tensions actively exploited by SAPA • ROA funded med clinic/school; mobile med/food aid (NGOs) • Subsistence agriculture/livestock; some work for pipeline company
Marghoz: • SAPA long operated in/around • Small rural village • Active local government (pre-SAPA) • Minority ethnic Atropian; strongly dislike SAPA/support anti-SAPA • Some inter-ethnic friction; majority Persian residents likely resent U.S. • Majority dissatisfied with food, health, and economic conditions. • Shrinking economy, rising unemployment, increasing poverty • Pipeline laborers, farmers, and seasonal agricultural labor • Basic educational/medical available to most; sporadic electricity	***Marjani:*** • Small rural village • Depend on NGO/IGO for essential services (pre-SAPA) • Some residents may support SAPA • Majority Ethnic Persian; clear ethnic tension (pre-SAPA) likely exacerbated by SAPA • Agricultural economy; minimal growth • Small businesses provide necessities • Limited access to schools, medical facilities, and emergency services NGOs medical support diminished under SAPA • Severely restricted information under SAPA	***Marwandi:*** • Small rural village • Active local government • SAPA activity due to Marwandi Pumping Station's importance • Majority ethnic Atropian; strong dislike of SAPA/likely support anti-SAPA activity • Some Persian-Atropian tension • ROA funded school • Primary occupations farmers, rural labor, and pipeline/pumping station workers.

AO	area of operations	OA	operational area
ASR	alternate supply route	ROA	Republic of Atropia
MSR	main supply route	SAPA	South Atropian People's Army
IGO	intergovernmental organization	USAID	United States Agency for International Development
NGO	nongovernmental organization		

Figure 2-1. Example overlay that depicts relevant information about the populace in the area of operations (*continued*)

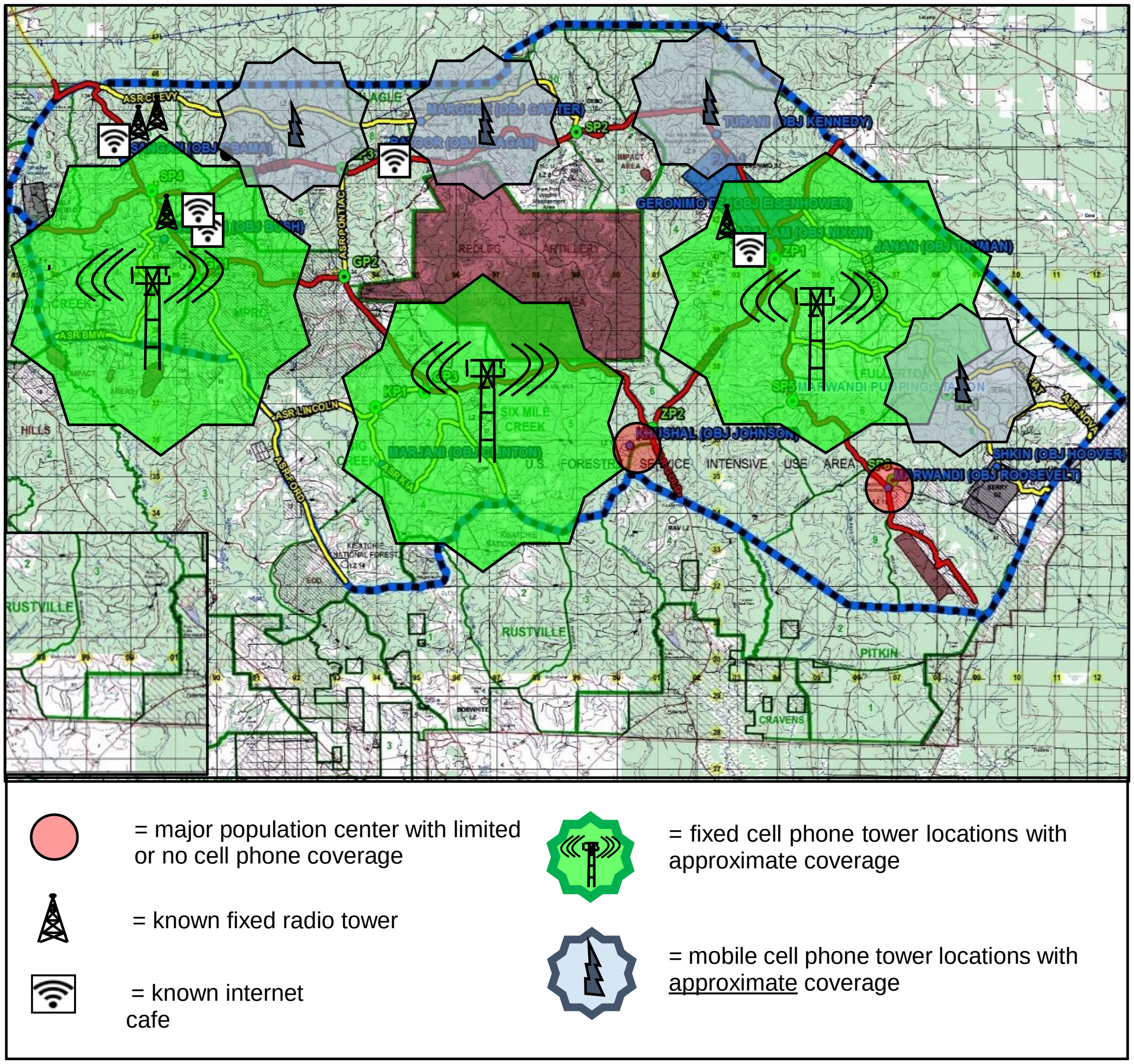


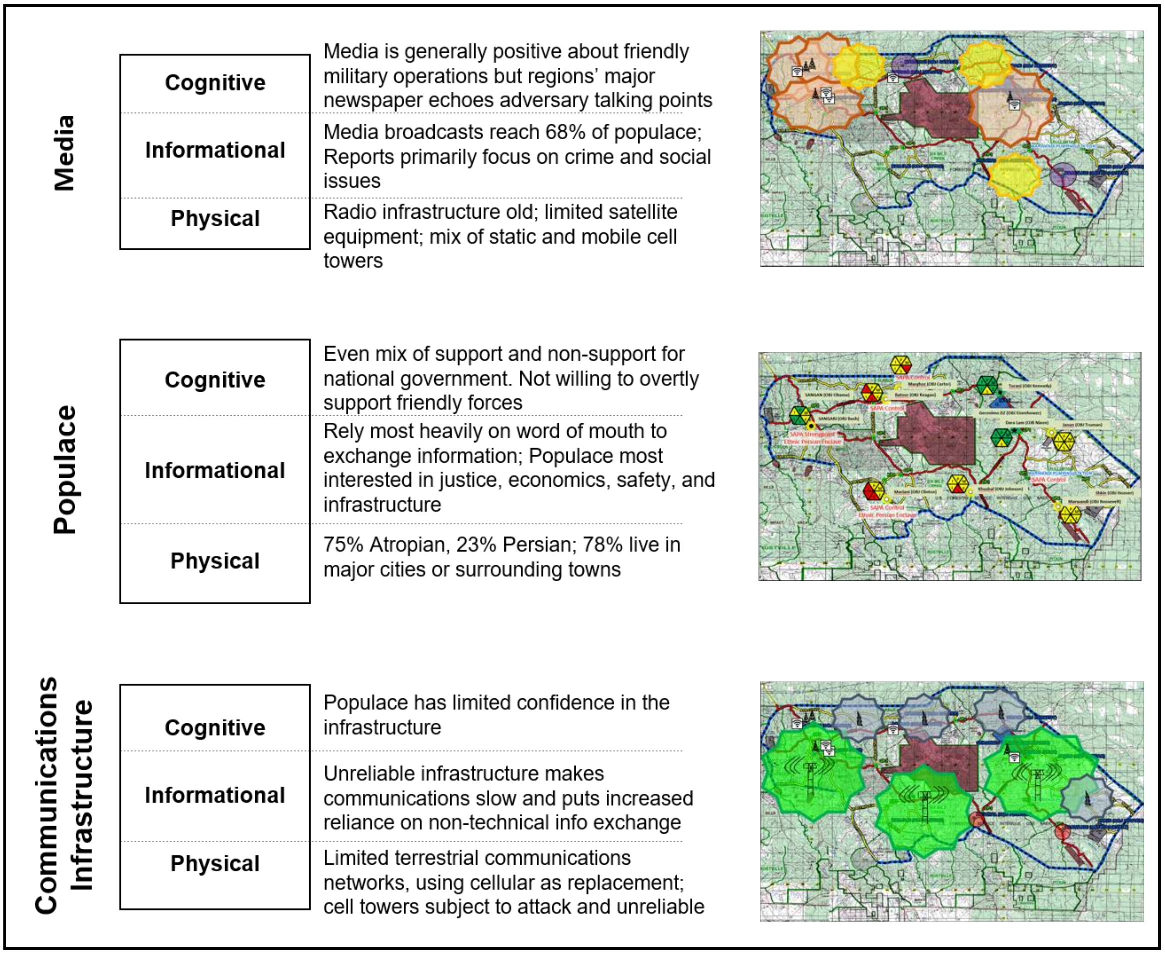
Figure 2-2. Example overlay that depicts relevant information about communications infrastructure in the area of operations

2-27. Next, the IO officer or planner refines the information overlays to produce a “so what” statement for each. Put another way, IO officers iteratively refine information overlays to capture and display those features and impacts that most affect mission accomplishment. The information environment is complex. While oversimplifying it can lead to faulty conclusions and decisions, staffs must competently represent it in a few products that enable commanders to visualize and understand it sufficiently to make informed decisions.

2-28. Once IO planners have generated an information overlay for each significant characteristic, they determine the aggregate impacts across all significant characteristics, mindful of these questions, among others:

- How will each significant characteristic impact the others?
- How does the interaction among significant characteristics impact employing IRCs and the content and flow of information?
- What slow-go or no-go areas in the information environment constrict, restrict, or prevent information flow; what areas facilitate or hasten its flow?

Figure 2-3 illustrates possible impacts among significant characteristics across the three information environment dimensions.



Media	Cognitive	Media is generally positive about friendly military operations but regions' major newspaper echoes adversary talking points
	Informational	Media broadcasts reach 68% of populace; Reports primarily focus on crime and social issues
	Physical	Radio infrastructure old; limited satellite equipment; mix of static and mobile cell towers
Populace	Cognitive	Even mix of support and non-support for national government. Not willing to overtly support friendly forces
	Informational	Rely most heavily on word of mouth to exchange information; Populace most interested in justice, economics, safety, and infrastructure
	Physical	75% Atropian, 23% Persian; 78% live in major cities or surrounding towns
Communications Infrastructure	Cognitive	Populace has limited confidence in the infrastructure
	Informational	Unreliable infrastructure makes communications slow and puts increased reliance on non-technical info exchange
	Physical	Limited terrestrial communications networks, using cellular as replacement; cell towers subject to attack and unreliable

Figure 2-3. Sample description of the information environment effects

STEP 3: EVALUATE THE THREAT'S INFORMATION SITUATION

2-29. Opposing forces use the information environment just as they use the physical domains of air, land, maritime, and space. They aim to gain positions of relative advance, place their enemy at a disadvantage, dominate the information environment, and achieve their objectives. In this step, the staff determines threat capabilities; doctrinal principles; and tactics, techniques, and procedures that threat forces prefer to employ. The IO staff identifies how enemies or adversaries view and use the information environment, including how they array their forces and employ capabilities to create effects in this environment.

2-30. The IO staff applies critical thinking to avoid confirmation bias, groupthink, and other biases. A common mistake is presuming that the adversary views and, therefore, uses the information environment in the same way as U.S. forces—that they are bound by the same constraints or limited by the same means. To avoid mirror-imaging the friendly concept of IO upon the enemy or adversary and prevent mismatching U.S. capabilities and vulnerabilities, the IO staff views adversary operations in the information environment in terms of activities to collect, protect, and project information. These three functions are universal to any armed force's ability to use information as combat power regardless of its organization, capabilities, and mission. As such, these functions form the basis of a threat's capabilities (and vulnerabilities) in the information environment (see table 2-3 on page 2-12 for a description of adversary functions).

Table 2-3. Adversary functions

Term	*Definition*
Collect	To plan and execute operations, the adversary must collect accurate and timely information
Protect	To ensure its ability to make timely and informed decisions, the adversary must protect its critical information from collection and maintain its means of communication
Project	To further its goals and objectives, the adversary must project the information into the information environment to influence the perceptions of its target audiences

2-31. Depending on the threat, the means used can be as simple as direct human observation and open sources (collect); couriers and intimidation (protect); and public broadcasts, printed materials, graffiti, or lethal action. When taken together, these means create a cohesive narrative (project). Ideally, analysis of how the adversary operates in the information environment is based on modeling or templating. Two common tools to conduct this analysis are threat templates and center of gravity (COG) analysis.

2-32. The resulting analysis is an understanding of threat capabilities and vulnerabilities under unconstrained conditions in the information environment. IO planners then refine this understanding using the actual, constrained conditions identified in the information environment analysis and depicted in information overlays and the combined information overlay (for more information on threat templates and center of gravity analysis, see JP 2-01.3 and ATP 5-0.1, respectively).

THREAT TEMPLATES

2-33. Threat templates graphically portray how the threat might use its capabilities to perform the functions required to accomplish its objectives when not constrained by the effects of an operational environment. Threat templates are scaled to depict the threat's disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping). Threat templates are the result of careful analysis of a threat's capability, vulnerabilities, doctrinal principles, and preferred tactics, techniques, and procedures that, in turn, lead to developing threat models and situation templates (see ATP 2-01.3). When possible, IO planners place these threat templates on a terrain product (such as a paper or digital map), adjusting time and distance relationships as necessary, but without violating the threat's fundamental doctrinal precepts. When not practical to overlay these templates on a terrain product, templates nonetheless depict doctrinal interrelationships of threat information warfare forces, key personnel, capabilities, and assets.

2-34. In terms of threat information warfare, threat templates seek to depict doctrinal information usage and flow, decision-making nodes, and locating IRCs, informational systems, sub systems, and associated assets. IO planners typically use three templates:

- Decision-making or information exchange template.
- Information infrastructure template.
- Information tactics template.

2-35. IO planners coordinate with the intelligence staff officer to incorporate information-related threat templates into the threat model. This coordination creates accurate situation templates and subsequent COAs in Step 4 of IPB. Threat templates allow the staff to fuse all relevant combat information and identify intelligence gaps. Further, they enable the staff to predict threat activities—in this case, in the information environment—and adopt COAs, as well as synchronize information collection.

Decision-Making Template

2-36. Also termed an information exchange template, this model considers and then depicts who makes or supports decisions and how they exchange information to support their decision making. It reveals human nodes and links that a threat organization uses to exchange information, with particular emphasis on ways the threat commander receives and disseminates information. Developing this template requires an understanding of threat organizational structures, critical links and interrelationships, and key personnel affecting the decision-making process.

Information Infrastructure Template

2-37. This template considers and then depicts the assets and means the threat employs to exchange information. If the decision-making template focuses on *who* is involved with information exchange, the infrastructure template focuses on *what* enables them to exchange that information. It depicts known infrastructure to exchange information internally and externally. Examples include satellite uplinks or downlinks, radio antennas, cell towers, couriers, and face-to-face interactions.

Information Tactics Template

2-38. The tactics template models how the threat arrays or employs its information assets and capabilities. While the first two templates do not necessarily have to be overlaid on terrain, the tactics template works best depicted as an overlay, so that staffs can clearly see and understand time and distance relationships. Not every adversary will have formal organizations or doctrine for employing information assets and capabilities; thus, the IO officer carefully avoids mirroring U.S. doctrine, capabilities, and methods onto the threat.

THREAT CENTER OF GRAVITY ANALYSIS

2-39. An IO planner uses a COG analysis to identify threat capabilities, requirements, and vulnerabilities. The IO officer does not conduct a separate COG analysis but participates in and contributes to the staff COG effort, led by the intelligence staff officer. The IO officer brings to this effort expertise in the information environment.

2-40. COG analysis, with an emphasis on the information environment, is used to—

- Identify potential threat COGs.
- Identify critical capabilities.
- Identify critical requirements for each critical capability.
- Identify critical vulnerabilities for each critical requirement.
- Prioritize critical vulnerabilities.

Identify Potential Threat Centers of Gravity

2-41. In this step, the staff visualizes the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and uses its physical and psychological strengths and weaknesses, the staff selects the threat's primary source of moral or physical strength, power, and resistance. Depending on the level (strategic, operational, and tactical), COGs may be tangible entities or intangible concepts. To test the validity of the COG, the staff asks: "Is the COG capable of achieving the threat's objective?" The COG is supported, not supporting; if something provides support or contributes to a function that ultimately achieves the threat's objective, then it is a capability or a requirement, not a COG. Typically, a threat COG in the information environment is the threat's information position, which is a way of describing the quality of information the threat possesses and its ability to use that information.

Identify Critical Capabilities

2-42. The IO planner analyzes each COG to determine what primary abilities (functions) the threat possesses in the context of the operational area and friendly mission that can prevent friendly forces from accomplishing the mission. Critical capabilities are not tangible objects; rather, they are threat functions. To test the validity of a critical capability, the staff asks: "Is the identified critical capability a primary ability in context with the given missions of both threat and friendly forces? Is the identified critical capability directly related to the COG?" A critical capability is a crucial enabler for a COG to function and, as such, is essential to accomplishing the adversary's specified or assumed objectives.

> ***Note.*** The threat's critical capabilities relate to the functions in the information environment—collect, protect, and project.

Identify Critical Requirements for Each Critical Capability

2-43. The IO planner analyzes each critical capability to determine what conditions, resources, or means enable threat functions or mission. To test validity of a critical requirement, the staff asks: “Will an exploitation of the critical vulnerability disable the associated critical requirement? Does the friendly force have the resources to affect the identified critical vulnerability?” If either answer is no, then the IO planner must review the threat’s identified critical factors for other critical vulnerabilities or reassess how to attack the previously identified critical vulnerabilities with additional resources.

Note. Critical requirements usually are tangible elements such as communications means, nodes, or key communicators.

Identify Critical Vulnerabilities for Each Critical Requirement

2-44. The IO planner analyzes each critical capability to determine which critical requirements (or components thereof) are vulnerable to neutralization, interdiction, or attack. As a planner develops the hierarchy of critical requirements and critical vulnerabilities, the staff seeks interrelationships and overlapping between the factors to identify critical requirements and critical vulnerabilities that support more than one critical capability. When selecting critical vulnerabilities, a critical-vulnerability analysis is conducted to pair critical vulnerabilities against friendly capabilities.

Note. Critical vulnerabilities may be tangible structures or equipment, or intangible perception, populace belief, or susceptibility.

Prioritize Critical Vulnerabilities

2-45. A tool for prioritizing critical vulnerabilities is CARVER, which stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability. As a methodology or process, CARVER weighs and ranks six target criteria for targeting and planning decisions. The IO planner applies the six criteria against the critical vulnerability to determine impact on the threat organization as follows:

- **Criticality** is estimating the critical vulnerability’s or target’s importance to the enemy. Vulnerability will significantly influence the enemy’s ability to conduct or support operations. As applied to targeting, criticality means target value and relates to how much a target’s destruction, denial, disruption, and damage will impair the enemy or adversary’s political, economic, or military operations or how much a target component will disrupt the function of a target complex.
- **Accessibility** is determining whether the critical vulnerability or target is accessible to the friendly force; it is the ease with which a target can be reached.
- **Recuperability** is evaluating how much effort, time, and resources the enemy or adversary must expend if the critical vulnerability or target is successfully affected.
- **Vulnerability** is determining whether the friendly force has the means or capability to affect the critical vulnerability or target using available assets. A target is vulnerable if friendly forces can attack it.
- **Effect** is determining the extent of the effect achieved if the critical vulnerability is successfully exploited. Effect means the impact on the enemy or adversary decision maker or makers. A target should not be attacked unless it can achieve the desired military effect.
- **Recognizability** is determining if the critical vulnerability or target, once selected for an exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

2-46. The resulting analysis provides a prioritized list of objectives or targets that can then be discussed in context of each possible COA, aiding COA analysis. Each COA will dictate the capability to be employed (see ATP 3-05.20 for an overview of Army special operations forces targeting methodology that includes COG analysis and CARVER criteria; see ATP 2-33.4 and ATP 3-60 for the Army use of CARVER as a target value analysis tool).

Note. Planners also use COG analysis to identify friendly COGs, capabilities, requirements, and vulnerabilities and CARVER to identify friendly targets that are vulnerable to attack and for defensive purposes.

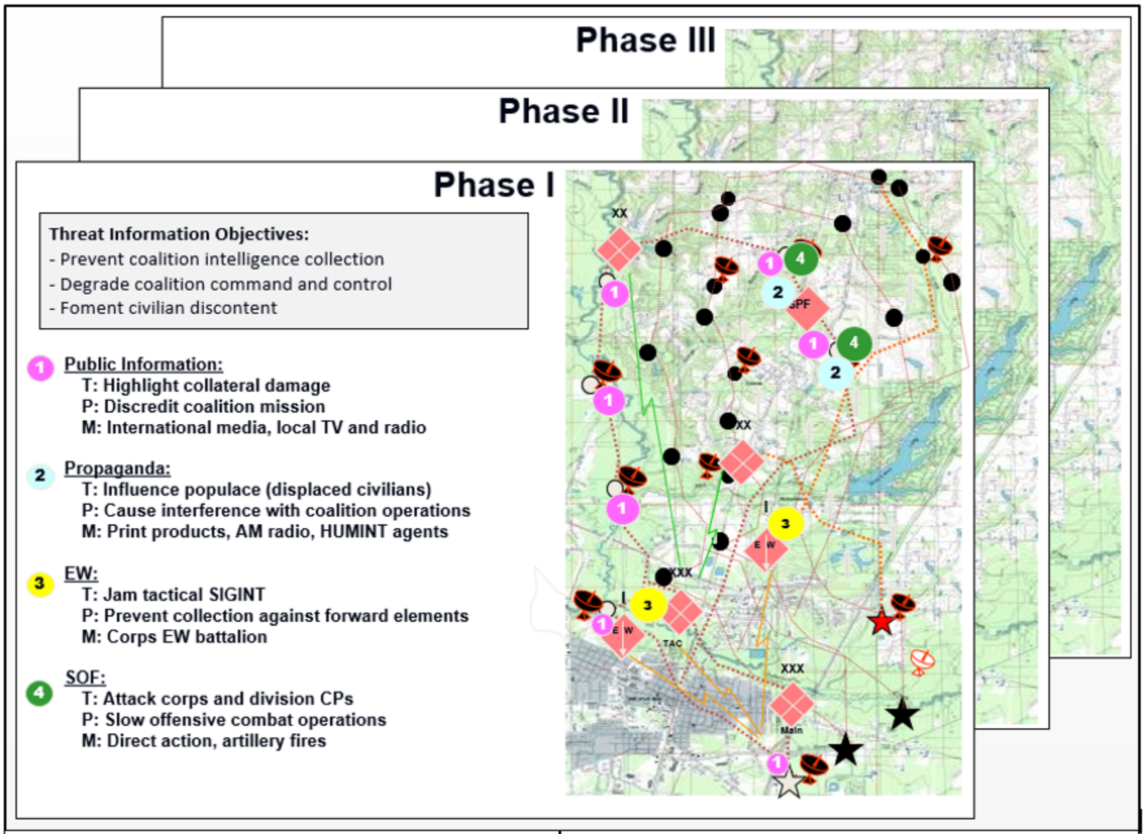
STEP 4: DETERMINE THREAT COURSES OF ACTION

2-47. Developing a threat COA is a six-step process that requires an understanding of the threat characteristics and the effects of terrain, weather, and civil considerations on operations (see ATP 2-01.3 for a detailed discussion on the threat). These steps include:

- Identify likely objectives and end state.
- Identify the full set of COAs available to the threat.
- Evaluate and prioritize each threat COA.
- Develop each COA in the detail that time allows.
- Identify high-value targets for each COA.
- Identify initial collection requirements for each COA.

2-48. The IO officer or planner filters each step of the process through an information lens, determining possible COAs that rely on the information environment to achieve an advantage. When developing each COA, the IO officer or planner coordinates closely with the intelligence staff officer to ensure each situation template depicts where, when, and why the threat employs its information systems and capabilities. The IO officer or planner develops IO-specific situation templates as a first step in the coordination process. These templates do not stand alone; instead, they contribute to the intelligence staff officer’s situation templates. Continual coordination during IPB ensures that the staff develops the most accurate threat COAs.

2-49. While threat templates reflect how the threat should operate based on doctrine or preferred methods, the situation template conveys how the threat actually operates and employs its forces and capabilities based on an operational environment. Figure 2-4 on page 2-16 provides an example information-focused situation template that the IO officer or planner uses to enhance staff coordination during IPB.



Threat Information Objectives:
- Prevent coalition intelligence collection
- Degrade coalition command and control
- Foment civilian discontent

1 Public Information:
T: Highlight collateral damage
P: Discredit coalition mission
M: International media, local TV and radio

2 Propaganda:
T: Influence populace (displaced civilians)
P: Cause interference with coalition operations
M: Print products, AM radio, HUMINT agents

3 EW:
T: Jam tactical SIGINT
P: Prevent collection against forward elements
M: Corps EW battalion

4 SOF:
T: Attack corps and division CPs
P: Slow offensive combat operations
M: Direct action, artillery fires

AM	amplitude modulation	P	purpose
CP	command post	SIGINT	signals intelligence
EW	electronic warfare	SOF	special operations forces
HUMINT	human intelligence	T	task
M	method	TV	television

Figure 2-4. Example information situation template

COMBINED INFORMATION OVERLAY

2-50. In addition to the running estimate, IPB to support IO results in producing a graphic visualization product known as the combined information overlay (CIO). The CIO results from the prior analysis conducted in Steps 1 through 4, aggregating the information, threat, and situation templates (or overlays) to depict where and how aspects—such as infrastructure, terrain, and populace—can affect military operations. In certain instances, the IPB may require more than one CIO to capture the full complexity of the information environment.

2-51. The CIO gives the commander and the staff a visual depiction of the ways in which information affects the AO. Similar to the modified combined obstacle overlay, which the intelligence staff officer develops during the IPB, the CIO is a simplified depiction of numerous interconnected variables. The CIO is a tool to visualize a collection of inputs that can never be completely synthesized. As such, it never becomes a final product; it is continually updated as new information arises and as time and staffing permits.

2-52. Reachback capabilities, such as provided by the 1st IO Command, sometimes provide a starting point for a CIO, but the IO working group must verify and refine these products with more localized analysis. The IO officer, aided by the IO working group, is ultimately responsible for the product. Although the CIO may include classified information, particularly when dealing with technical or military aspects of an operational environment or intelligence products, it primarily consists of open-source and publically available information that is useful once validated. With a request for information, the IO officer can obtain additional information about the threat from the intelligence staff.

Note. Using open-source and publically available information for other than intelligence purposes should not be confused with open-source intelligence (known as OSINT). Only intelligence personnel conduct open-source intelligence (see ATP 2-22.9 for more on this topic).

2-53. Figure 2-5 on page 2-18 illustrates a sample CIO. What appears in or on the CIO depends on the situation, mission, commander preferences, and the resulting analysis. Templates include a combination of narrative (descriptive) elements, pictorial elements, and graphical elements. Whether the “so what” statement appears on the template itself or in accompanying notes, it needs to be conveyed concisely to the commander. The proportion of one element to the others depends on the conclusions the IO officer reaches and a judgement call on the best way to convey these conclusions.

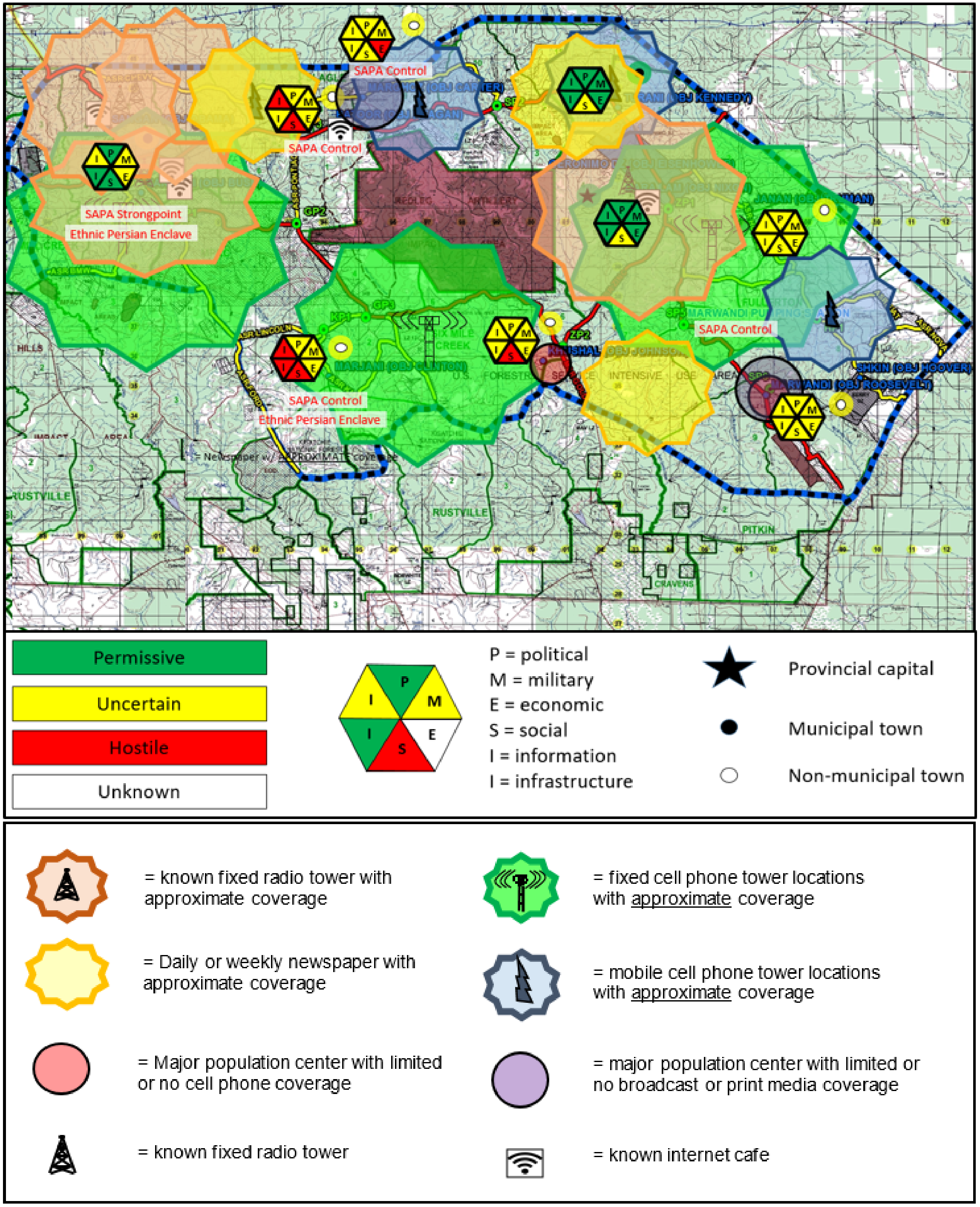

SAPA Control
SAPA Control
SAPA Strongpoint
Ethnic Persian Enclave
SAPA Control
SAPA Control
Ethnic Persian Enclave
= Newspaper w/ APPROXIMATE coverage
RUSTVILLE
PITKIN
CRAVENS
HILLS
GP2
GP3
KP1
ZP2
SP2
SP3
INTENSIVE USE
Permissive
Uncertain
Hostile
Unknown
P
M
E
S
I
I
P = political
M = military
E = economic
S = social
I = information
I = infrastructure
Provincial capital
Municipal town
Non-municipal town
= known fixed radio tower with approximate coverage
= fixed cell phone tower locations with approximate coverage
= Daily or weekly newspaper with approximate coverage
= mobile cell phone tower locations with approximate coverage
= Major population center with limited or no cell phone coverage
= major population center with limited or no broadcast or print media coverage
= known fixed radio tower
= known internet cafe

Figure 2-5. Example of combined information overlay