PART FOUR

Enabling Operations

Part Four discusses operational-level enabling operations. Commanders direct enabling operations to support offensive, defensive, stability, and support operations. Enabling operations are usually shaping or sustaining; they may be decisive in some military operations other than war.

Chapter 11 addresses how Army forces conduct operations to gain and maintain information superiority. It describes the necessity for Army forces to be able to see their battlespace, understand the situation in their battlespace, and act before their opponent. It outlines the characteristics of information superiority and the information environment. It discusses the contributors to information superiority: intelligence, surveillance, and reconnaissance operations; information management; and information operations, to include its related activities. It describes the aspects of the operations process important to achieving information superiority. It concludes by outlining the impact of technology on the contributors to information superiority.

Chapter 12 addresses combat service support (CSS). It presents the purpose and characteristics of CSS and lists the CSS functions. It describes the factors that affect conducting CSS operations to support the four types of Army operations. The discussion addresses the support provided by national providers, CSS operations in joint and multinational environments, and the factors affecting operational reach and sustainability. Chapter 12 ends by describing the effect of technology on CSS operations.

Directing enabling operations is an intrinsic function of command and the art of operations. Alone, enabling operations cannot assure success; however, neglecting them can result in mission failure.

Chapter 11

Information Superiority

To guess at the intention of the enemy; to divine his opinion of yourself; to hide from both your intentions and opinion; to mislead him by feigned manoeuvres; to invoke ruses, as well as digested schemes, so as to fight under the best conditions—this is and always was the art of war.

Napoleon

CONTENTS

11-1. The side possessing better information and using that information more effectively to gain understanding has a major advantage over its opponent. A force that achieves this advantage and effectively uses it to affect enemy perceptions, attitudes, decisions, and actions has exploited information superiority. ***Information superiority* is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.** Commanders exploit information superiority to accomplish missions. Information superiority is not static. During operations, all sides attempt to secure its advantages and deny them to adversaries and enemies. The operational advantages of information superiority can take several forms, ranging from the ability to create a better operational picture and understand it in context, to the ability to shape the environment with offensive information operations (IO).

11-2. At its essence, information superiority is about Army forces being able to see first, understand first, and act first. Army forces cannot develop information superiority if they are constantly reacting to enemy operations. Information superiority requires commanders who are proactive, view information as an element of combat power, trust their subordinates to provide relevant information, and conduct (plan, prepare, execute, and continuously assess) operations accordingly. To achieve information superiority,

commanders synchronize and target information as intensely as they do fires and maneuver. They seek to make better use of their information and information systems than adversaries or enemies do of theirs. These information systems include the analysis, procedures, and training necessary to extract and exploit intelligence and other critical information from raw data, and present it in a form in which it can be quickly understood. Successful commanders are those who see, understand, and then exploit the situation.

CHARACTERISTICS OF INFORMATION SUPERIORITY

11-3. Gaining and exploiting information superiority demands effective doctrine, training, leadership, organization, materiel, and soldiers. It puts a premium on the commander's ability to visualize, describe, and direct operations. Effective use of advanced information systems, procedures, and training allows commanders to achieve and maintain situational understanding. Modern information technologies help commanders lead more effectively and consistently make better decisions than those opposing them.

11-4. Commanders manage their information resources, combine their judgment with the knowledge of their staffs and subordinates, and use information systems to understand their battlespace better than their adversaries or enemies do. Commanders require relevant information about the factors of METT-TC to exercise effective command and control (C2). From the initial warning order to completion of redeployment, Army forces use every means, including force, to acquire that information. At the same time, they attempt to deny adversaries and enemies information about friendly forces and actively degrade their ability to collect, process, store, display, and disseminate information. Effective friendly use of information, complemented with active measures that prevent enemies from using information effectively or countering friendly information use, creates conditions for achieving information superiority. Army forces use the qualitative advantages of information superiority as a springboard for decisive operations.

11-5. The operational and tactical implications of information superiority are profound. Rapid seizure and retention of the initiative becomes the distinguishing characteristic of all operations. Information superiority allows commanders to make better decisions more quickly than their enemies and adversaries. Unable to keep pace, enemies and adversaries must deal with new problems before they can solve current ones. In combat, a rapid tempo—sustained by information superiority—can outpace enemy's ability to make decisions contribute to his destruction. In stability operations and support operations, information superiority helps deploying forces anticipate problems and requirements. It allows commanders to control events and situations earlier and with less force, creating the conditions necessary to achieve the end state.

11-6. Adversaries and enemies pursue their own relative information advantages, very likely in asymmetric ways, while continually attempting to deny information superiority to friendly forces. Because opposing forces constantly adapt and situations continually evolve, information superiority is relative and transitory. Absolute information superiority is not possible. Commanders

assess the quality of their information against their decision making requirements. Against that assessment, they estimate the quality of the enemy's operational picture. Commanders avoid any complacency associated with relative levels of military technology. They are aware that their enemy may, by chance or countermeasures, uncover the sources of friendly informational advantage, block them, or use them to deceive.

11-7. Commanders recognize that unless they envision and direct operations designed to achieve and maintain information superiority, they may lose it. Commanders exploit any advantages in information capability and intelligence to increase the effects of combat power. They constantly seek to improve their situational understanding and to assess that of their enemy. They know that losing information superiority may result in losing the initiative.

> *Nations do not go to war because they think war is safe. They go to war because they think they will win.*
>
> Richard M. Swain
> *Lucky War*

THE INFORMATION ENVIRONMENT

11-8. The information environment is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. The climate, terrain, and weapons effects (such as electromagnetic pulse or blackout) affect the information environment but are not part of it. The information environment includes the C2 systems of friendly and enemy forces and those of other organizations and groups. Commanders consider the explosive growth of information and the pervasive nature of the information environment when they visualize an operation. They include that part of the information environment that affects their operation in their battlespace.

11-9. Most of the information environment is not under military control, adding to the challenges commanders face. While they cannot control the entire information environment, they must be prepared to operate within it. Interaction with the information environment increases the complexity of Army operations. More than ever, commanders consider how factors outside their area of operations (AO) may affect their operations. IO often requires coordination with governmental and nongovernmental agencies. Legal limitations on IO vary according to the situation. This interaction may affect the impact of tactics on operations and strategy. Military actions that are tactically or operationally insignificant may influence strategy, or even national policy, when highlighted by the media. Therefore, operational commanders consider more than the military conditions of the end state of a campaign. They consider the comprehensive diplomatic, political, and social aspects of it as well.

11-10. Army forces increasingly rely on the unrestricted use of the information environment. Commanders and staffs need to understand its effects on operations and develop C2 systems that support their operational needs and intelligence requirements. Distance has little meaning in the information environment. Army information systems are "in contact" with enemy information systems before any operation starts. They remain in contact after the

operation ends. Commanders understand that there is no sanctuary for friendly information. Before Army forces arrive in theater, the battle for information superiority begins. Commanders and staff conduct operations accordingly.

Information Superiority in the Gulf

In the opinion of many observers, the Gulf War emphasized integrating information systems, operations, and management in ways that heralded a new form of warfare. Air operations struck C2 nodes throughout Iraq and occupied Kuwait, disabling the air defense network and slowing operational and tactical response. Until the air operation started, Third Army restricted preparations to areas well south of the border. Under cover of intense air bombardment, Saudi and French units secured areas along the border while the powerful US forces shifted west. Even as the Third Army's VII and XVIII Corps moved into attack positions, the US Central Command conducted military deception operations at sea and on land, culminating with the feint by 1st Cavalry Division in the Wadi al-Batin area.

As the ground offensive neared, tactical reconnaissance and surveillance confirmed that the Iraqi Army had its right flank exposed to the west of Kuwait. Special Operations Forces and tactical air reconnaissance complemented these efforts. By 23 February 1991, both corps had secured the border area and extended ground and air reconnaissance well inside Iraq. Intense air attacks fixed and decimated the Iraqi army. The Marine deception and 1st Cavalry Division feint continued to draw Iraqi attention eastward. Third Army moved to attack positions west of the Wadi al-Batin to exploit the Iraqi mistake. At 0400 hours on 24 February 1991, coalition ground forces struck into Kuwait and Iraq. They ended their offensive four days later, having decisively defeated the once fourth-largest army in the world.

Speaking after the war, LTG S. Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies of the former Soviet Union, stated, "Iraq lost the war before it even began. This was a war of intelligence, electronic warfare, command and control, and counterintelligence. Iraqi troops were blinded and deafened…."

CONTRIBUTORS TO INFORMATION SUPERIORITY

11-11. Commanders direct three interdependent contributors to achieve information superiority (see Figure 11-1, page 11-6):

- Intelligence, surveillance, and reconnaissance (ISR).
- Information management (IM).
- IO (to include related activities).

These contributors enable and complement full spectrum operations. Specific objectives that contribute to information superiority include the following:

- Develop and maintain a comprehensive picture of enemies and adversaries; forecast their likely actions.
- Deny enemies and adversaries information about friendly forces and operations.

- Influence enemy and adversary leader perceptions, plans, actions, and will to oppose friendly forces.
- Influence noncombatants and neutrals to support friendly missions or not to resist friendly activities.
- Inform noncombatant and neutral organizations so they can better support friendly policies, activities, and intentions.
- Protect friendly decision making processes, information, and information systems.
- Continually provide relevant information (including intelligence) to the commander and staff in a useable form.
- Destroy, degrade, disrupt, deny, deceive, and exploit enemy decision making processes, information, and information systems, and influence those of adversaries and others.

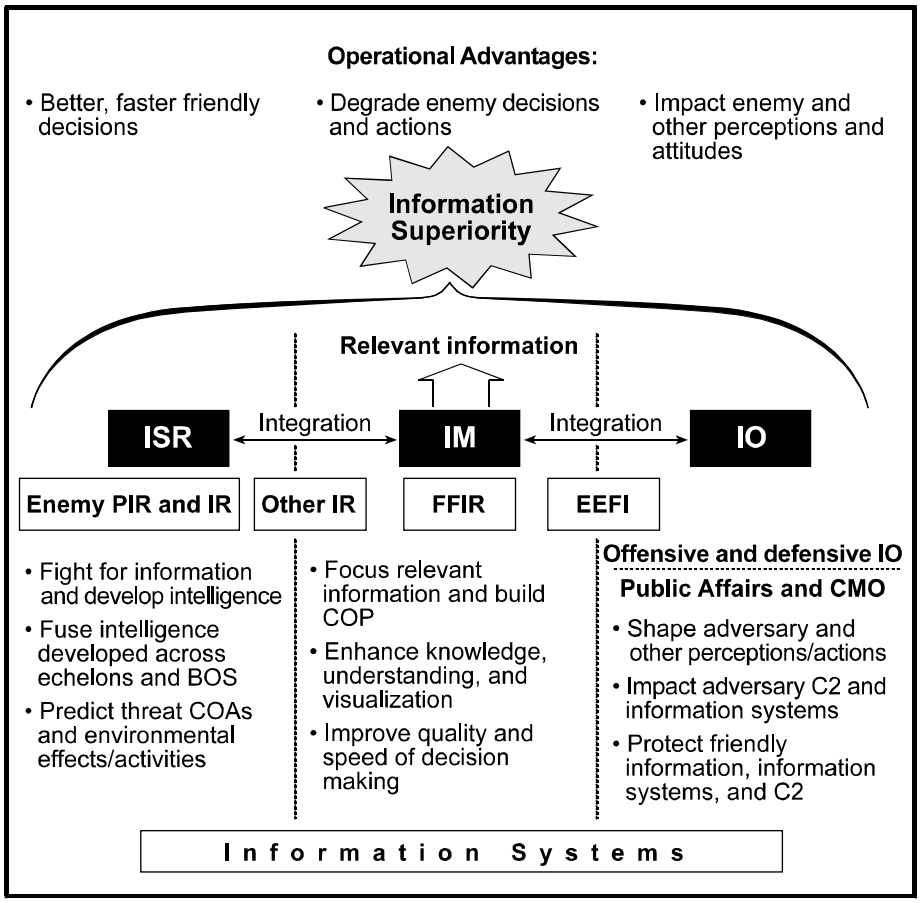

Figure 11-1. Information Superiority

11-12. Commanders wage the struggle for information superiority throughout the information environment, not only in the AO. Superiority in one contributor alone does not ensure information superiority. For example, Army forces may have better IM than a less sophisticated enemy. However, superior intelligence and better security may give the enemy commander more information about Army forces than they have about the enemy. Uncoordinated

actions within single contributors are ineffective. Information superiority results when commanders synchronize all three contributors. Figure 11-2 illustrates the nature of the struggle for information superiority.

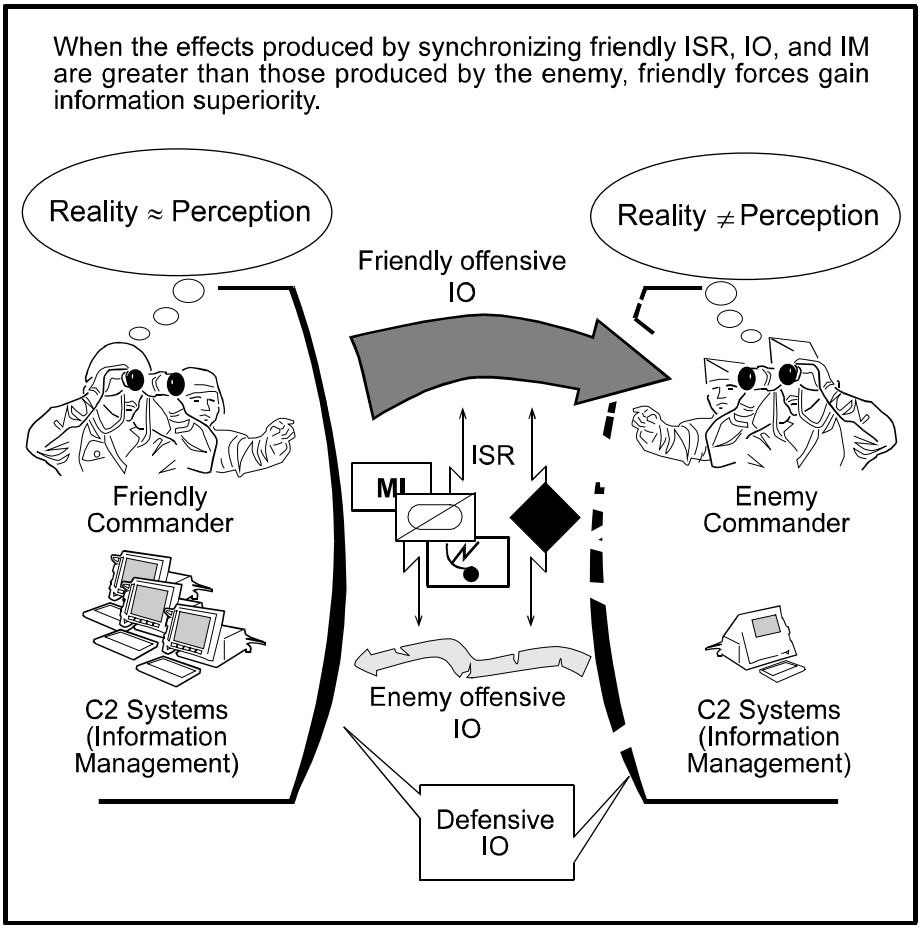

Figure 11-2. Information Operations and Information Superiority

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

11-13. ISR integration is fundamental to information superiority. Thoroughly integrated ISR operations add many collection sources. ISR integration eliminates unit and functional "stovepipes" for planning, reporting, and processing information and producing intelligence. It provides a common mechanism for all units to conduct ISR operations in a coordinated, synergistic way.

11-14. ISR operations allow units to produce intelligence on the enemy and environment (to include weather, terrain, and civil considerations) necessary to make decisions. This intelligence answers requirements developed throughout the operations process. Timely and accurate intelligence encourages audacity and can facilitate actions that may negate enemy superiority in soldiers and materiel. Normally, timely and accurate intelligence depends on aggressive and continuous reconnaissance and surveillance.

Intelligence

> ***Intelligence*** **is (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.**

11-15. The complexity of the operational environment requires sharing intelligence from the national level to the tactical level and among headquarters at each level. Analysis is a complex task that requires fusing information and intelligence from each ISR discipline and asset into an all-source product. Analysis is increasingly distributed and collaborative. Analysts who are closest to the point of collection enter data and perform initial processing one time for the entire force. Modern information systems allow analysts to collaborate on the overall analysis without degrading support to their own commanders, regardless of their geographic dispersion. This distributed, collaborative analysis process starts with the initial intelligence preparation of the battlefield (IPB) and continues throughout operations.

11-16. The commander drives the intelligence system. Managing the ISR effort entails—

- **Requirements visibility**. Intelligence personnel use procedures and information systems to monitor and display the status of information requirements.
- **Asset visibility**. Intelligence personnel use procedures and information systems to monitor and display collection asset status, location, and activities.
- **ISR assessment capability**. Intelligence personnel use procedures and information systems to assess the effectiveness of the ISR effort and the operational impact of ISR results (such as its success or gaps in collection), and to task collection assets.

> ***Intelligence preparation of the battlefield*** **is a systematic approach to analyzing the enemy and environment (for example, weather, terrain, and civil considerations) in a specific geographic area. It integrates enemy doctrine with the weather, terrain, and civil considerations as they relate to the mission and the specific environment. This is done to determine and evaluate enemy capabilities, vulnerabilities, and probable courses of action.**

11-17. Intelligence provides critical support to all operations, including IO. It supports planning, decision making, target development, targeting, and protecting the force. It is a continuous process for any operation. Surveillance and reconnaissance are the primary means of collecting information used to produce intelligence. A thorough understanding of joint ISR capabilities allows commanders to prepare complementary collection plans. Surveillance and reconnaissance assets focus primarily on collecting

information about the enemy and the environment to satisfy the priority intelligence requirements (PIR). In the end, the art of intelligence and its focus on supporting the commander are more important than any information system. This art includes an understanding of intelligence, analysis, the enemy, operations, and the commander's needs.

11-18. IPB is the first step toward placing an operation in context. It drives the process that commanders and staff use to focus information assets and to integrate surveillance and reconnaissance operations across the AO. IPB provides commanders with information about the enemy and environment, and how these factors affect the operation. In most cases, IPB allows commanders to fill gaps in information about the enemy with informed assessments and predictions. IPB is also the starting point for situational development, which intelligence personnel use to develop the enemy and environment portions of the common operational picture (COP). As such, IPB is important to the commander's visualization. The commander drives IPB, and the entire staff assists the intelligence staff with continuous updates. All staff officers develop, validate, and maintain IPB components relating to their areas of expertise. For example, the engineer contributes and maintains current mobility and countermobility situation overlays.

Surveillance

11-19. Surveillance involves continuously observing an area to collect information. Wide-area and focused surveillance provide valuable information.

> ***Surveillance*** **is the systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic or other means.**

11-20. Army forces at all echelons receive intelligence based on information from national, joint, Army, and commercial surveillance systems. National and theater surveillance systems focus on information requirements for combatant commanders and provide information to all services for theater-wide operations. Continuous theater surveillance helps analysts determine the location and approximate dispositions of enemy land forces. When available, near real-time surveillance platforms—such as the joint surveillance, target attack radar system (JSTARS)— provide moving target indicators. Additionally, long-range surveillance units can provide extremely accurate and valuable information.

11-21. Although the US may enjoy an advantage in surveillance assets, commanders should assume that enemies also have adequate surveillance means. For example, an enemy may purchase high-resolution imagery from commercial space-based systems. Alternatively, the local populace may report Army force actions through the civilian police to enemy intelligence agencies.

Reconnaissance

11-22. Reconnaissance collects information and can validate current intelligence or predictions. Reconnaissance units, unlike other units, are designed to collect information.

> ***Reconnaissance*** **is a mission undertaken to obtain by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.**

11-23. Information collected by means other than reconnaissance has great operational and tactical value. However, those assets may not be able to meet some requirements or collect information with adequate accuracy and level of detail. Operational priorities within the theater may limit ground commanders' ability to task theater surveillance systems. Therefore, Army commanders complement surveillance with aggressive and continuous reconnaissance. Surveillance, in turn, increases the efficiency of and reduces the risk to reconnaissance elements by focusing their operations.

11-24. In some situations, the firepower, flexibility, survivability, and mobility of reconnaissance assets allow them to collect information where other assets cannot. Reconnaissance units obtain information on adversary and potential enemy forces as well as on the characteristics of a particular area. Reconnaissance missions normally precede all operations and begin as early as the situation, political direction, and rules of engagement permit (see FM 5-0). They continue aggressively throughout the operation. Reconnaissance can locate mobile enemy C2 assets, such as command posts, communication nodes, and satellite terminals for neutralization, attack, or destruction. Commanders at all echelons incorporate reconnaissance into the conduct of operations (see FM 3-90).

> *You can never do too much reconnaissance.*
>
> General George S. Patton Jr.
> *War As I Knew It*

11-25. Continuous and aggressive reconnaissance does more than collect information. It may also produce effects or prompt enemy actions. The enemy may take forces needed elsewhere to counter friendly reconnaissance efforts. Hostile forces sometimes mistake reconnaissance units for the decisive operation and prematurely expose their dispositions or commit their reserves. Friendly commanders may exploit opportunities revealed by friendly reconnaissance, often using the reconnaissance force as the spearhead. Information from reconnaissance missions allows commanders to refine or change plans and orders, preclude surprises, and save the lives of soldiers.

11-26. Reconnaissance elements may have to fight for information. However, the purpose of reconnaissance is to gain information through stealth, not initiate combat. Reconnaissance operations that draw significant combat power into unplanned actions not in line with the commander's intent may jeopardize mission accomplishment.

11-27. Commanders integrate ISR missions into a single plan that capitalizes on their different capabilities. They synchronize reconnaissance and surveillance missions that employ maneuver units with both the ISR plan and scheme of maneuver.

INFORMATION MANAGEMENT

11-28. ***Information management*** **is the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making. It uses procedures and information systems to collect, process, store, display, and disseminate information** (see FM 6-0). IM is far more than technical control of data flowing across networks. It communicates decisions that initiate effective actions to accomplish missions and fuses information from many sources. Successful IM adds meaning to information as it is processed, so decision makers can focus on achieving understanding instead of processing or evaluating information. IM consists of two supporting components: information systems and relevant information.

11-29. Successful IM includes processing. Processing adds meaning to relevant information through progressively higher-level and complex cognitive methods to create a COP. Among other aspects, processing includes lower-level mechanical and mechanistic methods, such as organizing, collating, plotting, and arranging. However, effective processing requires analysis and evaluation (higher-level cognitive methods) to convert information into knowledge and knowledge into understanding. This aspect of processing depends on the insight and flexibility of well-trained and adaptive analysts.

11-30. Commanders and staffs assess the effectiveness of IM by considering how information contributes to lessening the "fog of war." First, untimely information or unusable data has the same effect as not having the information. It either arrives too late or cannot be understood in time to affect the commander's decision. Second, incomplete or imprecise information is better than no information. While not perfect, it contributes to the commander's grasp of the situation and may assist decision making. Finally, irrelevant or inaccurate information is worse than no information. Irrelevant information distracts and delays; inaccurate information may lead to an inappropriate decision. Computers and software cannot make these qualitative distinctions; making them requires soldiers with good judgment.

Information Systems

11-31. ***Information systems*** **are the equipment and facilities that collect, process, store, display and disseminate information. These include computers—hardware and software—and communications, as well as policies and procedures for their use**. Information systems are integral components of C2 systems. Effective information systems automatically process, disseminate, and display information according to user requirements. IM centers on commanders and the information relevant to C2. Commanders make the best use of information systems when they determine their information requirements and focus their staffs and organizations on meeting them.

Relevant Information

11-32. ***Relevant information*** **is all information of importance to commanders and staffs in the exercise of command and control**. To be relevant, information must be accurate, timely, usable, complete, precise, and reliable. Relevant information provides the answers commanders and staffs

need to successfully conduct operations, that is, all elements necessary to address the factors of METT-TC. The intelligence system, for example, provides intelligence that constitutes relevant information on the enemy, terrain and weather, time available (to the enemy), and civil considerations.

11-33. Relevant information results from assigning meaning to data to assist understanding. Processing changes raw data into information by assigning meaning to it. Analysis and evaluation transform information into knowledge, which is presented to commanders as relevant information. When commanders apply judgment to knowledge, it becomes understanding. Understanding enables making informed decisions with less-than-perfect data. Combined with will, understanding generates effective action.

11-34. Relevant information is perishable. If not delivered and acted upon quickly, it may become outdated (no longer relevant) and distort the commander's situational understanding. Masses of data and information may overwhelm the command post. Without effective IM, critical information will be misrouted, delayed, or buried in routine data and overlooked. Information systems can assist in managing volumes of data, but will not do so unless commanders define their information requirements, tie them to their intent, and update them as execution unfolds.

Categories of Information

11-35. IM narrows the gap between available information and information commanders require. Effective IM facilitates rapid dissemination of relevant information. IM assigns information into four categories: specified requirements, implied requirements, gaps, and distractions.

- **Specified requirements**. Specified requirements are requirements the commander specifically identifies. This information may take the form of facts, estimates, or assumptions.
- **Implied requirements**. Implied requirements are important pieces of information that commanders have not specifically requested. Full spectrum operations may place Army forces in situations that lie outside the commander's experience. Commanders may not know to obtain some elements of information. They may not know that they need a piece of information or may not recognize its importance. Effective staffs develop and recommend these additional information requirements. Commanders encourage intellectual versatility and agility within their staff and examine recommendations carefully.
- **Gaps**. Gaps are elements of information commanders need to achieve situational understanding but do not have. Ideally, analysis identifies gaps and translates them into specified requirements. To fill gaps, commanders and staffs make assumptions, clearly identifying them as such. There may be circumstances when commanders and staffs fail to identify a gap. Such circumstances are especially dangerous, particularly when facing an asymmetric threat. The commander not only does not have a piece of relevant information, but also does not know he needs it. This situation may result in the commander being surprised. Commanders and staffs remain adaptive and examine circumstances as they are, rather than fitting circumstances into preconceived notions.

- **Distractions**. Distractions include information commanders do not need to know but continue to be told. Excessive distractions result in information overload.

11-36. Information is further classified as facts, estimates, and assumptions. *Facts* are information commanders want to know and can know with certainty. A fact must be confirmed or come from a reliable source. *Estimates* and *assumptions* are information commanders want to know but cannot know with certainty. Commanders and staffs must use discipline in separating fact from assumption; otherwise they are vulnerable to deception or risk inaccurate situational understanding. Estimates and assumptions primarily include information about the enemy, the future, or factors over which commanders have little or no control.

11-37. Facts, estimates, and assumptions can be either relevant information or distractions. They are relevant information if the commander both wants and needs to know the information. They are distractions if the commander wants to know but does not need to know the information. Photographs, for example, can be distractions. Unless the commander clearly understands the imagery, demands for photos only clog overloaded information systems. Effective IM filters distractions from relevant information.

Quality of Information

11-38. Sources of information are imperfect and susceptible to distortion and deception. Soldiers processing information use these qualities to evaluate it:

- **Accuracy**. The information conveys the actual situation; in short, it is fact.
- **Timeliness**. The information has not been overtaken by events.
- **Usability**. The information is easily understood or displayed in a format that immediately conveys the meaning.
- **Completeness**. The information contains all required components.
- **Precision**. The information has the required level of detail, no more and no less.
- **Reliability**. The information is trustworthy, uncorrupted, and undistorted.

Effective IM keeps commanders and staffs aware of the quality of their information as they use it to build situational understanding.

Commander's Critical Information Requirements

11-39. Commanders channel information processing by clearly expressing which information is most important. They designate critical information that derives from their intent—the commander's critical information requirements (CCIR). **The *commander's critical information requirements* are elements of information required by commanders that directly affect decision making and dictate the successful execution of military operations**. The key to effective IM is answering the CCIR.

11-40. When commanders receive a mission, they and their staffs analyze it using the military decision making process. As part of this process, commanders visualize the battlefield and the fight. CCIR are those key elements

of information commanders require to support decisions they anticipate. Information collected to answer the CCIR either confirms the commander's vision of the fight or indicates the need to issue a fragmentary order or execute a branch or sequel. CCIR directly support the commander's vision of the battle—commanders develop them personally. Once articulated, CCIR normally generate two types of supporting information requirements: friendly force information requirements (FFIR) and PIR.

> ***Priority intelligence requirements*** **are those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making.**
>
> ***Friendly force information requirements*** **are information that the commander and staff need about the forces available for the operation.**

11-41. CCIR must be focused enough to generate relevant information. Unfocused requests, such as "I need to know if the enemy moves," may provide data but not much useable information. However, "I need to know when the enemy lead brigade reaches Named Area of Interest 2" or "I need to know if the multinational unit on our right flank advances beyond Phase Line Blue" are examples of CCIR specific enough to focus collection and IM priorities.

Essential Elements of Friendly Information

> ***Essential elements of friendly information*** **are the critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from enemy detection.**

11-42. Although essential elements of friendly information (EEFI) are not part of the CCIR, they become a commander's priorities when he states them. EEFI help commanders understand what enemy commanders want to know about friendly forces and why (see FM 6-0). They tell commanders what cannot be compromised. For example, a commander may determine that if the enemy discovers the movement of the reserve, the operation is at risk. In this case, the location and movement of the reserve become EEFI. EEFI support defensive IO, and as such may become information requirements. EEFI provide a basis for indirectly assessing the quality of the enemy's situational understanding: if the enemy does not know an element of EEFI, it degrades his situational understanding.

Common Operational Picture

11-43. **An *operational picture* is a single display of relevant information within a commander's area of interest**. By collaborating, sharing, and tailoring relevant information, separate echelons create a COP. **A *common operational picture* is an operational picture tailored to the user's requirements, based on common data and information shared by more than one command**. The COP is displayed at a scale and level of detail that meets the information needs of the command at a particular

echelon. C2 systems fuse information from a variety of sources, while information systems facilitate its rapid distribution in usable displays that facilitate understanding.

11-44. Different echelons require different information at different levels of precision and detail. The presentation of information in meaningful images assists its assimilation. IM provides relevant information as meaningful displays rather than masses of data. The COP allows collaborative interaction and real-time sharing of information among commanders and staffs without providing them with too much or too little information.

11-45. The Army continues to invest in technologies and develop procedures that increase commanders' ability to understand their battlespace. These modernizing efforts will increase the capability of Army forces to share a full-dimensional, highly accurate COP and rapidly disseminate guidance, orders, and plans. Technological applications that help visualize, illustrate, brief, and rehearse options contribute to a common understanding of the commander's intent and concept of operations. Increasing the speed of analysis, compilation, and communication leaves more time for synthesis—assigning meaning to information and generating potential options.

Situational Understanding

11-46. ***Situational understanding*** **is the product of applying analysis and judgment to the common operational picture to determine the relationships among the factors of METT-TC** (see FM 6-0). It enhances decision making by identifying opportunities, threats to the force or mission accomplishment, and information gaps. It helps commanders identify enemy options and likely future actions, the probable consequences of proposed friendly actions, and the effects of the environment on both. Situational understanding based on a COP fosters initiative in subordinate commanders by reducing, although not eliminating, uncertainty (see Figure 11-3, page 11-16).

11-47. Situational understanding has limits. It is imperfect, particularly with respect to the enemy situation. It requires constant verification. Situational understanding focuses on the current situation. It can reduce the friction caused by the fog of war. However, achieving accurate situational understanding depends at least as much on human judgment as on machine-processed information—particularly when assessing enemy intent and combat power. Simply having a technologically assisted portrayal of the situation cannot substitute for technical and tactical competence. Additionally, portions of the force will not be modernized for some time. The level of situational understanding between modernized and less modernized units may vary over time. Commanders recognize the disparity between organizations and adjust procedures and subordinate unit missions accordingly.

Information Management in Full Spectrum Operations

11-48. IM is a command responsibility. IM plans establish responsibilities and provide instructions for managing information. The IM plan is the commander's "concept of operations" for handling information. Effective IM plans cover the entire scope of operations. Designated staff elements refine the IM plan and provide overall management of information.

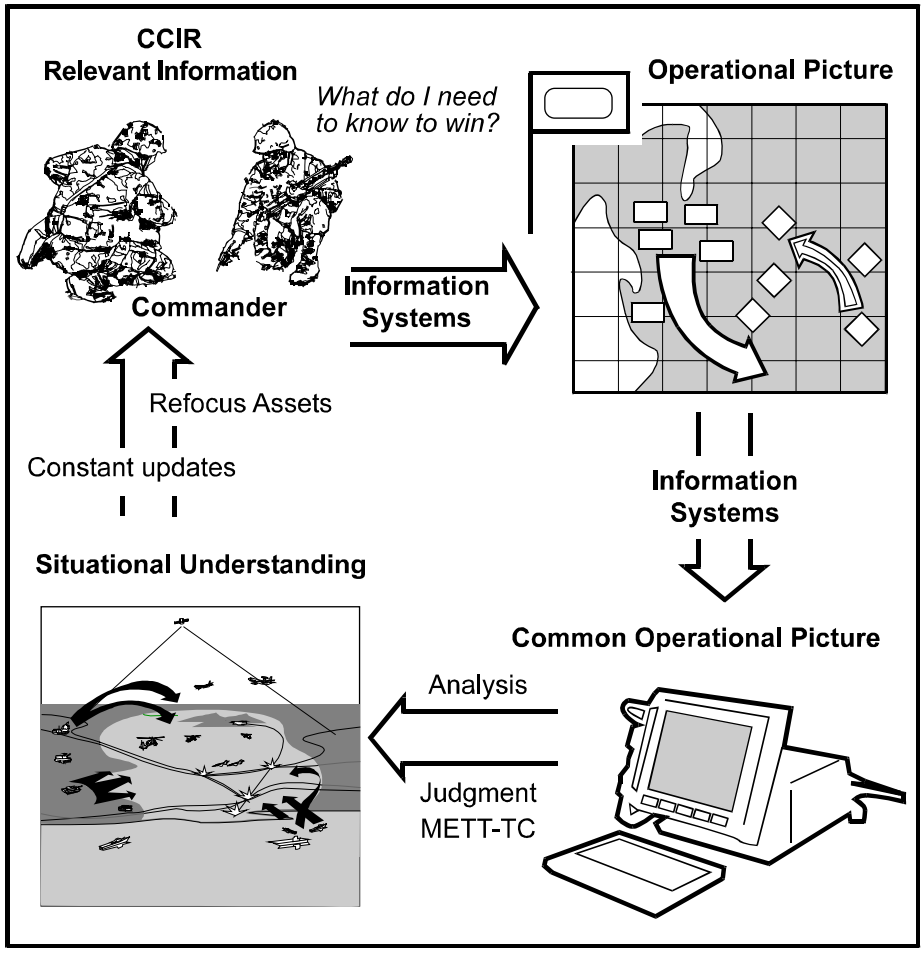

Figure 11-3. Situational Understanding

INFORMATION OPERATIONS

11-49. IO are primarily shaping operations that create and preserve opportunities for decisive operations. IO are both offensive and defensive. Related activities—public affairs and civil-military operations (CMO)—support IO.

Information operations **are actions taken to affect adversary, and influence others', decision making processes, information and information systems while protecting one's own information and information systems.**

11-50. The value of IO is not in their effect on how well an enemy transmits data. Their real value is measured only by their effect on the enemy's ability to execute military actions. Commanders use IO to attack enemy decision making processes, information, and information systems. Effective IO allow commanders to mass effects at decisive points more quickly than the enemy. IO are used to deny, destroy, degrade, disrupt, deceive, exploit, and influence the enemy's ability to exercise C2. To create this effect, friendly forces attempt to influence the enemy's perception of the situation.

11-51. Similarly, IO and related activities affect the perceptions and attitudes of a host of others in the AO. These include the local population, displaced persons, and civilian leaders. IO are shaping operations that help commanders create favorable conditions for not only decisive operations but also sustaining operations. Commanders use IO and related activities to mitigate the effects of enemy IO, as well as adverse effects stemming from misinformation, rumors, confusion, and apprehension.

Offensive information operations **are the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives.**

Defensive information operations **are the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.**

11-52. Successful IO require a thorough and detailed IPB. IPB includes information about enemy capabilities, decision making style, and information systems. It also considers the effect of the media and the attitudes, culture, economy, demographics, politics, and personalities of people in the AO. Successful IO influences the perceptions, decisions, and will of enemies, adversaries, and others in the AO. Its primary goals are to produce a disparity in enemy commanders' minds between reality and their perception of reality and to disrupt their ability to exercise C2 (see FM 3-13).

11-53. Offensive and defensive operations use complementary, reinforcing, and asymmetric effects to attack enemies, influence adversaries and others, and protect friendly forces. On a battlefield where concentrating forces is hazardous, IO can attack enemy C2 systems and undermine enemy capabilities and will to fight. It can reduce friendly vulnerabilities and exploit enemy weaknesses. Where the use of force is restricted or is not a viable option, IO can influence attitudes, reduce commitment to a hostile cause, and convey the willingness to use force without actually employing it. Information used in this manner allows friendly forces to accomplish missions faster, with fewer casualties.

Offensive Information Operations

11-54. The desired effects of offensive IO are to destroy, degrade, disrupt, deny, deceive, exploit, and influence enemy functions. Concurrently, Army forces employ elements of offensive IO to affect the perceptions of adversaries and others within the AO. Using the elements of IO offensively, Army forces can either prevent the enemy from exercising effective C2 or leverage it to their advantage. Ultimately, IO targets are the human leaders and human decision making processes of adversaries, enemies, and others in the AO.

Defensive Information Operations

11-55. Defensive IO protect friendly access to relevant information while denying adversaries and enemies the opportunity to affect friendly information and information systems. Defensive IO limit the vulnerability of C2 systems.

Information Operations Elements

11-56. Integrating offensive and defensive IO is essential to success. Many activities or operations comprise IO. Each element may have offensive or defensive applications (see FM 3-13).

Information Operations Elements

- Military deception
- Counterdeception
- Operations security
- Physical security
- Electronic warfare
  - Electronic attack
  - Electronic protection
  - Electronic warfare support
- Information assurance
- Physical destruction
- Psychological operations
- Counterpropaganda
- Counterintelligence
- Computer network attack
- Computer network defense

11-57. **Military Deception**. Military deception includes measures designed to mislead adversaries and enemies by manipulation, distortion, or falsification. Its aim is to influence the enemy's situational understanding and lead him to act in a manner that favors friendly forces.

11-58. **Counterdeception**. Counterdeception includes efforts to negate, neutralize, or diminish the effects of, or gain advantage from, a hostile deception operation. Counterdeception supports offensive IO by reducing harmful effects of enemy deception. Defensively, counterdeception identifies enemy attempts to mislead friendly forces.

11-59. **Operations Security**. Operations security (OPSEC) denies the enemy information critical to the success of friendly military operations. It contributes to the security of Army forces and their ability to surprise enemies and adversaries. OPSEC identifies routine activities that may telegraph friendly intentions, operations, capabilities, or military activities. It acts to suppress, conceal, control, or eliminate these indicators. OPSEC includes countersurveillance, signal security, and information security.

11-60. **Physical Security**. Physical security prevents unauthorized access to equipment, installations, and documents. It safeguards and protects information and information systems.

11-61. **Electronic Warfare**. Electronic warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW can cause an enemy to misinterpret the information received by his electronic systems. EW includes—

- **Electronic attack**. Electronic attack involves actions taken to degrade, neutralize, or destroy enemy electronic combat capabilities. Actions may include lethal attack, such as antiradiation missiles and directed energy weapons, and nonlethal electronic attack, such as jamming.

- **Electronic protection**. Electronic protection involves actions taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or enemy EW. Actions may include radio silence and antijamming measures.
- **Electronic warfare support**. Electronic warfare support involves detecting, identifying, locating, and exploiting enemy signal emitters. It contributes to achieving situational understanding, target development and acquisition, damage assessment, and force protection.

11-62. **Information Assurance**. Information assurance protects and defends information systems. Threats to information systems include physical destruction, denial of service, capture, environmental damage, and malfunctions. Information assurance provides an enhanced degree of confidence that information and information systems possess the following characteristics: availability, integrity, authentication, confidentiality, and nonrepudiation. Computer network defense is part of this element.

11-63. **Physical Destruction**. Physical destruction applies combat power against IO-related targets. Targets include information systems, EW systems, and command posts. Physical destruction that supports IO is synchronized with other aspects of the operation. For example, when deciding whether to destroy an enemy command post, the friendly commander weighs the advantages gained from disrupting enemy C2 against those gained from collecting information from the command post's radio traffic.

11-64. **Psychological Operations**. Psychological operations (PSYOP) are planned operations that influence the behavior and actions of foreign audiences by conveying selected information and indicators to them (see JP 3-53; FM 3-05.30). The aim of PSYOP is to create behaviors that support US national interests and the mission of the force. PSYOP are closely integrated with OPSEC, military deception, physical destruction, and EW to create a perception of reality that supports friendly objectives.

11-65. **Counterpropaganda**. Counterpropaganda includes activities directed at an enemy or adversary conducting PSYOP against friendly forces. Counterpropaganda can contribute to situational understanding and expose enemy attempts to influence friendly populations and military forces. Preventive actions include propaganda awareness programs that inform US and friendly forces and friendly populations about hostile propaganda.

11-66. **Counterintelligence**. Counterintelligence consists of activities that identify and counteract threats to security posed by espionage, subversion, or terrorism. It detects, neutralizes, or prevents espionage or other intelligence activities. Counterintelligence supports the commander's requirements to preserve essential security and protect the force.

11-67. **Computer Network Attack**. Computer network attack consists of operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks. It may also target computers and networks themselves. Although theater or national elements normally conduct computer network attack, the effects may be evident at corps and below.

11-68. **Computer Network Defense**. Computer network defense consists of all measures to defend computers and other components that are

interconnected in electronic telecommunications networks against computer network attacks by an adversary. Such measures include access controls, detection of malicious computer code and programs, and tools to detect intrusions. Army forces use inherent capabilities and accomplish specific computer network defense actions to defend computer networks from unauthorized users.

Related Activities

11-69. Public affairs and CMO are activities related to IO. Both communicate information to critical audiences to influence their understanding and perception of military operations. Related activities are distinct from IO because they do not manipulate or distort information; their effectiveness stems from their credibility with the local populace and news media. Public affairs and CMO—prime sources of information—link the force, the local populace, and the news media. They also provide assessments of the impact of military operations on civilians, neutrals, and others within the battlespace.

11-70. **Public Affairs**. Public affairs operations influence populations by transmitting information through the news media. They fulfill the Army's obligation to keep the American people and the Army informed. Public affairs help to establish conditions that lead to confidence in the Army and its readiness to conduct operations in peace, conflict, and war. Disseminating this information is desirable and consistent with security. Information disseminated through public affairs counters the effects of propaganda and misinformation.

11-71. **Civil-Military Operations**. CMO applies civil affairs to military operations. It encompasses activities that commanders take to establish, maintain, influence, or exploit relations between military forces and civil authorities—both governmental and nongovernmental—and the civilian populace. Commanders direct these activities in friendly, neutral, or hostile AOs to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur before, during, or after other military actions. They may also occur as standalone operations. CMO is the decisive and timely application of planned activities that enhance the relationship between military forces and civilian authorities and population. They promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. CMO range from support to combat operations to assisting countries in establishing political, economic, and social stability (see JP 3-57).

PLANNING AND PREPARING TO ACHIEVE INFORMATION SUPERIORITY

11-72. Information superiority requires extensive planning and preparation. It cannot be an afterthought. As an element of combat power, information requires the same attention as the other elements.

11-73. The foremost information superiority planning requirement is vertical and horizontal integration of ISR, IO, and IM. Army force plans support joint force commander (JFC) objectives and receive support from the JFC. In

particular, offensive IO follow a common theme and are directed against supporting objectives. If not integrated, IO at different echelons may counteract each other.

11-74. Preparation focuses on IM and deploying the right ISR assets to support the force. Because Army forces are in varying states of modernization, the integration of information systems requires not only careful planning but also rehearsal and testing, whenever time permits. IM planning ensures that Army forces are able to disseminate relevant information vertically and horizontally. Commanders assess their information requirements against collection capabilities and tailor the force accordingly.

CONTINUOUS COORDINATION

11-75. Continuous coordination distinguishes effective C2. The impact of information technologies increases the importance of coordination. There is an unfortunate tendency to accept everything that appears on a computer screen. Coordination, focused by CCIR, verifies information. Constant coordination identifies friction in IM and develops solutions. Coordination between humans becomes the lubricant that drives IM within each headquarters. Commanders emphasize the necessity of coordination between higher and lower units as well as adjacent and supporting units. Commanders coordinate with other commanders; they understand that coordination, while primarily the task of the staff, is not solely a staff responsibility.

INFORMATION SUPERIORITY AND STRATEGIC RESPONSIVENESS

11-76. Deploying forces may not have information superiority at deployment. The commander's information needs, coupled with an understanding of METT-TC, influence force tailoring and the deployment sequence. ISR assets deploy to the theater ahead of or with initial-entry forces, depending on enemy. In areas where Army forces are already deployed and surveillance systems are established and collecting, available information may be adequate. However, crises often occur where forces are not forward deployed and intelligence is relatively sparse. In those cases, getting additional surveillance and reconnaissance assets immediately into theater becomes critical. Commanders deploy ISR and information systems with habitually supported forces. Assets assigned to early deploying units reinforce assets already deployed to or covering the theater.

11-77. The available intelligence on potential AOs may have limited tactical use. Commanders and staffs often find they must develop intelligence on an AO while their units are deploying there. To answer some specified and implied requirements, commanders may use subject matter experts. Subject matter experts understand the terrain, culture, enemy capabilities, and civil considerations of the AO and can help staffs develop estimates. Contingency operations in response to unanticipated crises are usually conducted under time constraints. It is critical that commanders and staffs consult subject matter experts familiar with the AO while developing the commander's vision, establishing CCIR, and refining situational understanding.

11-78. As intelligence is refined and IPB continues, commanders focus surveillance and reconnaissance assets to collect additional information or verify

existing intelligence. Persistent gaps may require additional collection assets. In a low-threat environment, host nation assets may provide significant augmentation and reduce requirements for US assets. In a high-threat environment, extensive reconnaissance and surveillance may be required before the main body deploys. All these factors influence how commanders tailor their forces (see Figure 11-4).

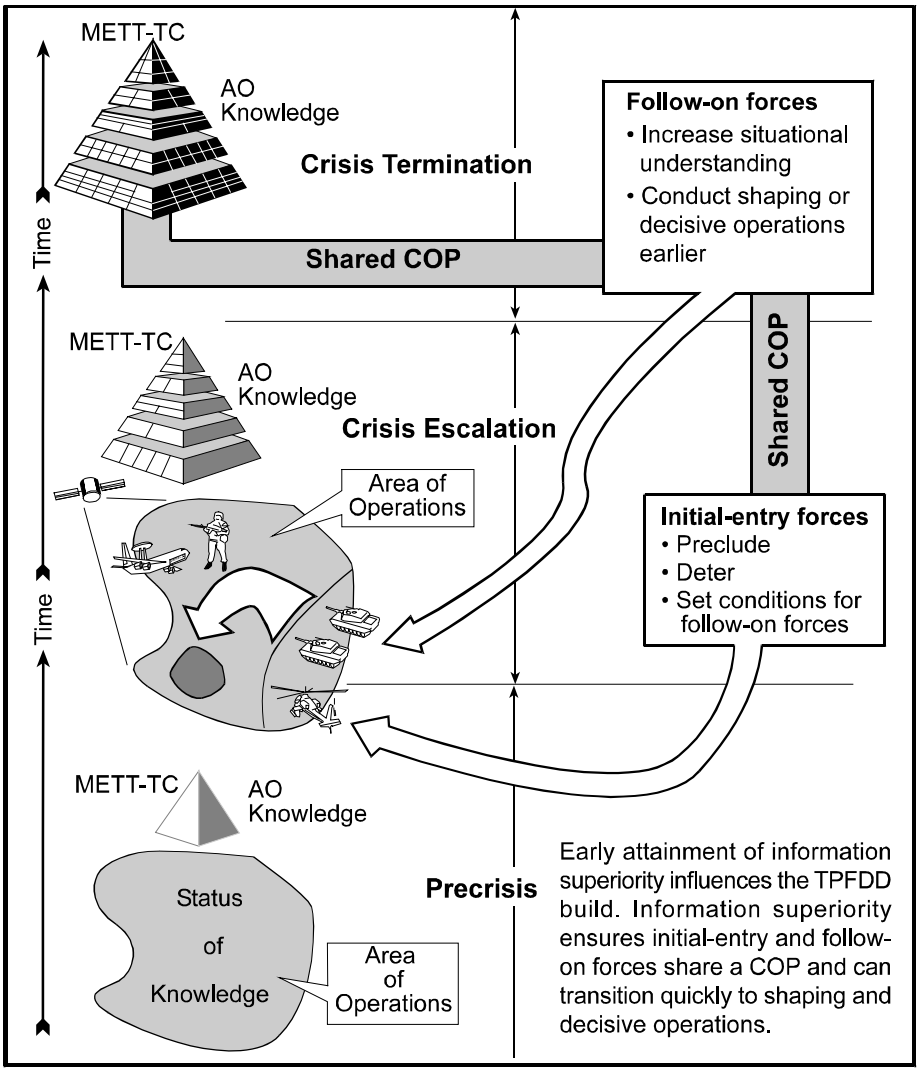

Figure 11-4. Information Superiority and Strategic Responsiveness

INFORMATION SUPERIORITY EXECUTION

11-79. Information superiority enables decisive action and is, in turn, complemented by that action. IO achieve greatest effect when complementing other operations. Effective jamming, for example, is a nuisance to an enemy force postured for defense but not facing assault. Confronted with swiftly maneuvering Army forces, however, effective jamming that degrades enemy C2 and synchronization can significantly disrupt enemy operations.

OPERATIONS IN NONCONTIGUOUS AREAS OF OPERATIONS

11-80. Noncontiguous areas of operations challenge commanders to use intelligence elements, reconnaissance units, and surveillance systems efficiently and imaginatively. When operating in noncontiguous AOs, commanders focus collection operations on areas between formations. Surveillance and reconnaissance assets cover areas between noncontiguous AOs. When the area requiring coverage exceeds the capabilities of reconnaissance units, commanders coordinate for additional coverage, with joint elements if available. When necessary, commanders task other forces to complement surveillance and reconnaissance assets.

SUBORDINATE INITIATIVE

11-81. Commanders depend on subordinate initiative to accomplish missions, even in the absence of orders or a COP. Information technology enhances Army operations but does not govern them. Inevitably, some information systems will fail—either of their own accord or because of enemy action. Commanders develop and communicate their vision to subordinates with enough clarity to allow them to act when this happens. Subordinates complement initiative with constant coordination and by keeping their higher commanders informed. Because Army forces must be able to execute in the absence of a COP, senior commanders avoid the temptation to overcontrol subordinates.

11-82. The capabilities of new information systems encourage subordinates to exercise disciplined initiative. A COP gives subordinates access to the same information as their commanders and tailors it to subordinate needs. Subordinates who know their commander's intent can act based on the COP, confident that their commander will understand what they are doing and why. More complete information allows well-trained leaders to make better decisions. A force in which commanders make good decisions at the lowest level will operate faster than one where decisions are centralized. Such a force is agile and can exploit opportunities as soon as they occur. As subordinates report their actions, those reports become part of the COP. Elements of the force affected by the action learn of it and can synchronize their actions with it. Properly used, modern information systems allow commanders to issue mission orders and control the battle through empowered subordinates. These subordinates can make decisions that fit both their immediate circumstances and the mission of the force as a whole.

THE IMPACT OF TECHNOLOGY

11-83. The increased range and lethality of weapons systems, faster tempo, shorter decision cycles, and extended battlespace all serve to increase confusion and the volume of information. The key to achieving situational understanding and avoiding information overload is identifying relevant information and filtering out distractions. Although emerging user-friendly technologies will facilitate coordinating, fusing, sharing, and displaying relevant information, these functions remain very human. The extended battlespace places increased emphasis on the initiative, judgment, and tactical and technical competence of skilled subordinate leaders. Current information technology is no substitute for small unit training and aggressive leadership.

11-84. Information technology helps commanders lead by allowing them more freedom to move around the battlefield while remaining connected electronically to the command post. This capability allows commanders to add their personal observations and feel for the ongoing operation to the synthesized information in the COP. Commanders can increase face-to-face contact with subordinates at decisive points without losing sight of the overall situation.

11-85. Technology is creating new techniques for displaying and disseminating information. Imagery, video, color graphics, digital maps and overlays all present relevant information faster and more precisely than analog methods. These new capabilities allow greater understanding by different audiences. Today, for example, commanders use collaborative planning across data networks to link subordinates with commanders throughout the operations process. Displays of information tailored to suit the audience, reduce acronyms, and eliminate jargon are particularly important when dealing with joint, multinational, and interagency participants. Technology allows staffs to quickly produce such tailored displays.

11-86. Modern technology provides a variety of means for commanders to see and engage the enemy in depth. Sensor-to-shooter links used with precision weapons enable forces to strike multiple targets simultaneously in near real-time with little regard for distance or geography. What these systems hit and when they hit it are important decisions. The results are in the effects they create, not solely in the targets they destroy. Systematic lethal attacks on enemy C2 systems provide leverage for air and ground forces and help create the conditions for success. By their nature, these effects are temporary; commanders must exploit them with maneuver to make them permanent.

11-87. Information technology can reduce, but not eliminate, uncertainty. It gives commanders windows of opportunity that, with quick and decisive action, help them seize the initiative. Commanders may lose opportunities if the quest for certainty leads them to centralize control and decision making. Technologically assisted situational understanding may tempt senior leaders to micromanage subordinate actions. This is not new; the telegraph and the command helicopter created similar tensions. Senior commanders need to develop command styles that exploit information technology while allowing subordinates authority to accomplish their missions. Exploiting the capabilities of information technology demands well-trained leaders willing to take risks within the bounds of the commander's intent. An understanding of the capabilities and limitations of information technology mitigates those risks.