AUGUST 1996

FM 100-6

Information Operations

DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.

HEADQUARTERS,
DEPARTMENT OF THE ARMY

Field Manual
No. 100-6

Headquarters
Department of the Army
Washington, DC, 27 August 1996

INFORMATION OPERATIONS

Contents

Preface

This manual addresses the operational context of information operations (IO), relevant terminology, and the environment of information operations. It supports battle command and provides guidelines for commanders that conduct IO to support all phases of the force-projection operating environment, including planning and executing early entry and force-projection operations in joint and multinational settings.

Military operations occur in peace and war. The traditional focus when discussing information and C^2 was electronic warfare (EW), electronic countermeasure (ECM), and electronic counter countermeasure (ECCM) operations that take place during war. The focus of this manual is on command and control warfare (C^2W), public affairs (PA), and civil affairs (CA). All are operations that the Army currently uses to gain and maintain *information dominance* as well as effective C^2. Successful operations require effective C^2 to transform military capabilities into applied military power. The more effective the force's C^2 system, the more completely its capabilities can be realized in peace or war.

As the Army's capstone doctrine for IO, this manual supports soldiers and leaders that execute IO to support military operations. Not only does the doctrine herein provide commanders and their staffs with guidance to conduct information operations, it also serves as the foundation for development of US Army tactics, techniques, and procedures (TTP) manuals. It is also the foundation to refine existing training support packages (TSPs), mission training plans (MTPs), training center and unit exercises, and service school curricula. The manual provides a basis to examine organizations and materiel developments applicable to IO.

This doctrine applies to the total Army—active and reserve components and Army civilians. It is specifically oriented at the operational and tactical levels of military operations. It may be useful to other services, nonmilitary agencies, and allies involved in such operations.

The proponent of this manual is HQ TRADOC. Send comments and recommendations on DA Form 2028 directly to Commander, US Army Combined Arms Center, ATTN: ATZL-SWW-L, Fort Leavenworth, Kansas 66027-1352.

Unless this publication states otherwise, masculine nouns or pronouns do not refer exclusively to men.

Introduction

The Army is embracing a new era characterized by the accelerating growth of information, information sources, and information dissemination capabilities supported by information technology. This new era, the so-called *Information Age*, offers unique opportunities as well as some formidable challenges. New technology will enhance the Army's ability to achieve situational dominance on land, where the decisive element of victory for our nation has always been critical. At the same time, it will enable adversaries to employ many of these same capabilities. This new technology also allows the Army to transform itself.

The Army is changing the way it does business in the foxhole; in its schools and training centers; and in its doctrine, training, leader development, organizations, materiel development, and soldier development. Responding to the challenges and opportunities of the Information Age, the Army is preparing the warfighter for operations today as well as in the twenty-first century. Information and the knowledge that flows from it empower soldiers and their leaders. When transformed into capabilities, information is the currency of victory.

Information operations integrate all aspects of information to accomplish the full potential for enhancing the conduct of military operations. Information operations are not new. In their simplest form they are the activities that gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities by whatever possible means. Effects of IO produce significant military advantage for forces conducting such operations.

Information is an essential foundation of knowledge-based warfare. It enables commanders to coordinate, integrate, and synchronize combat functions on the battlefield. To gain the relative advantage of position (maneuver) and massing of effects (firepower), commanders must act while information is relevant and before the adversary can react. Targeting an adversary's information flow to influence his perception of the situation or prevent him from having or using relevant information contributes directly to decisive operations. As the commander targets the adversary's information systems (INFOSYS), he protects his own. Realizing that absolute and sustained dominance of the information environment is not possible, commanders seek to achieve information dominance at the right place, the right time, and in the right circumstances. They seek information dominance that defines how the adversary sees the battlespace, creating the opportunity to seize the initiative and set the tempo of operations.

- The accuracy, lethality, and range of modern weapons have forced commanders to disperse their formations, decentralizing control and execution. Massing the effects of these dispersed systems depends on accurate information. Disruption of the flow of information or corruption of the information itself can negate the effects of weapons and systems. Instead of being limited to the physical destruction of people or war machines as the only path to battlefield success, armies now can target information or an adversary's INFOSYS to alter the battlefield chemistry and yield battlefield success.
- The speed and pervasiveness of data transmission in the Information Age are causing a revolutionary change in the nature of military operations and warfare. Targeting information extends beyond the battlefield and involves more than attacking an adversary's information flow while protecting the

friendly information flow. It also requires awareness of, and sensitivity to, information published by nonmilitary sources. These information sources are able to provide tactical-level information in near real time to audiences throughout the world, with the potential of profoundly influencing the context of those operations.

- IO define the operational situation by generating understanding, providing context, and influencing perceptions. They enable and protect friendly INFOSYS; synchronize force application; connect hierarchical and nonhierarchical systems; link sensors, shooters, and commanders; and degrade, disrupt, or exploit adversary operations by attacking the adversary's command and control (C^2). Units conduct IO across the full range of military operations, from operations in garrison, through deployment, to combat operations, to redeployment. IO greatly expand a commander's battlespace, including interaction with the media, industry, joint forces, multinational forces, and computer networks worldwide.
- Within the context of joint and/or multinational operations, the Army must be able to dominate the information environment in order to perform its missions in any contingency or conflict. The Army's force-projection capability is based upon accurate and timely information. IO can significantly enhance the Army's ability to deter aggression, to effectively execute the full range of operations, and to win decisively in combat.

Notwithstanding the synergy possible with the power of information and information technology, fog and friction will remain; the challenge of sorting out the signals from the noise amidst a mass of expanding data will also remain. Many solutions to the dilemma of uncertainty for the commander are technical. But there can be no *information revolution* without the human influence and understanding of soldiers and commanders who link and integrate information, technology, and action. IO do not offer any panaceas. Perfect knowledge is not the objective. The military objective remains—to enter an operational theater capable of achieving superior relative combat power against an enemy, or to establish situational dominance in operations other than war (OOTW).

The Army's keystone doctrine in FM 100-5 describes how the Army thinks about the conduct of operations. This manual, while designed to enhance and enable the operations in FM 100-5, reaches out to accommodate and leverage newly emerging information technologies, especially digitization.

As the Army's capstone publication for information operations, this manual supports the *National Military Strategy* and explains the fundamentals of IO for the Army. IO doctrine reflects, and goes beyond, the joint military strategy of command and control warfare (C^2W), which implements Department of Defense (DOD) information warfare policy. This manual—

- Identifies information as a major influence on operations at the tactical, operational, and strategic levels.
- Enables commanders to successfully integrate information, INFOSYS, and their effects across the full range of military operations. Such integration enables and enhances the elements of combat power.

- Creates synergy, which contributes to increased lethality, survivability, and tempo in combat, as well as highly credible and capable forces in OOTW.

This publication provides Army capstone doctrine and facilitates the transition to the Information Age.

Chapter 1

Operating Environment

Army forces today are likely to encounter conditions of greater ambiguity and uncertainty. Doctrine must be able to accommodate this wider variety of threats. In so doing, the Army is prepared to respond to these worldwide strategic challenges across the full range of possible operations as part of a joint and combined team.

FM 100-5

Commanders and their staffs operating in the Information Age face an increasingly complex environment. Commanders and staffs at all levels will encounter an expanding information domain termed the *global information environment* (GIE). The GIE contains those information processes and systems that are beyond the direct influence of the military or even the National Command Authorities (NCA), but nevertheless may directly impact the success or failure of military operations. The media, international organizations, and even individuals represent a partial list of GIE players.

This chapter describes the GIE domain and introduces the concept of *information dominance* as the key element for operating effectively within this new environment. To achieve information dominance, the commander must be able to dominate both the traditional maneuver-oriented battlefield and the *military information environment* (MIE), defined as that portion of the GIE relevant to his operation. To achieve the latter, the commander directs the acquisition, use, and management of friendly and enemy information and conducts command and control warfare (C^2W) attack and protect operations.

GEOSTRATEGIC AND TECHNOLOGICAL ENVIRONMENTS

Because of rapid advances in technology, especially in the information arena, the geostrategic environment of today has become increasingly complex and will become even more so in the future. Global communications accelerate and expand collective awareness of events, issues, and concerns. They ignite passions, spark new perspectives, crystallize deeply held beliefs, and compel people, nations, organizations and institutions everywhere to examine, define, and act on their interests. While many effects of this phenomenon may be benign and beneficial, others will create turbulence, confusion, chaos, and conflict. Such conflict may extend beyond the traditional battlefield to encompass espionage, sabotage, terrorism, economic competition, and efforts to shape public perceptions.

In the Information Age, the United States is in the forefront of exploiting modern information technology to harness the explosive potential of rapid dissemination and use of information. The US economy, social and civil structures, and federal, state, and local governments have become dependent upon the rapid and accurate flow of information. At the same time, America exerts extraordinary influence throughout the world through its multinational media and commercial and entertainment industries. To a

lesser degree, America is influenced by similar phenomena exerted from outside its borders. The global information infrastructure (GII) electronically links organizations and individuals around the globe and is characterized by a merging of civilian and military information networks and technologies.

Developments in information technology will revolutionize—and indeed have already changed—how nations, organizations, and people interact. The rapid diffusion of information, enabled by technological advances, challenges the relevance of traditional organizational and managerial principles. The military implications of new organizational sciences that examine internetted, nonhierarchical versus hierarchical management models are yet to be fully understood. Clearly, Information Age technology and the management ideas it fosters greatly influence the armed forces—organizations, equipment, how they train, how they fight, how they protect the force, or how they assist in resolving conflict.

Global Information Environment

The *global information environment* includes—

> All individuals, organizations, or systems, most of which are outside the control of the military or National Command Authorities, that collect, process, and disseminate information to national and international audiences.

All military operations take place within the GIE, which is both interactive and pervasive in its presence and influence. Current and emerging electronic technologies permit any aspect of a military operation to be made known to a global audience in near-real time and without the benefit of filters. With easy access to the global or national information network, suppression, control, censorship, or limitations on the spread of information may be neither feasible nor desirable (see Figure 1-1).

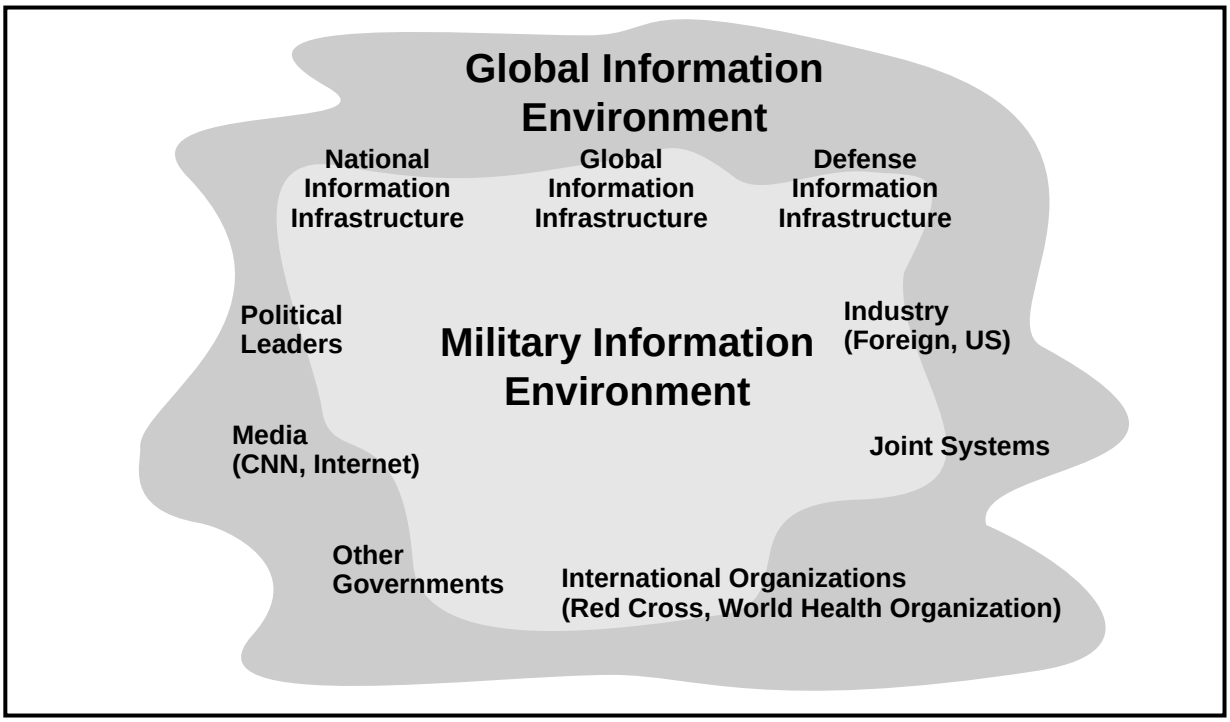

Figure 1-1. Information Environments (GIE and MIE)

Adversaries and other non-DOD organizations, including many actors, agencies, and influences outside the traditional view of military conflict, intrude into the MIE. Adversaries, perhaps supported by nonaligned nations, will seek to gain an advantage in the GIE by employing battlespace systems and organizations. In addition, the media, think tanks, academic institutions, nongovernment organizations (NGOs), international agencies, and individuals with access to the *information highway* are all potentially significant players in the GIE. These entities can affect the strategic and operational direction of military operations before they even begin. Independent of military control, their impact is always situationally dependent. Their activities may cause an unanticipated or unintentional effect on military operations. Such actors include—

- Government agencies such as the Department of State (DOS) or Federal Emergency Management Agency (FEMA).
- NGOs.
- Private voluntary organizations (PVOs).
- International agencies that provide a commercial service, such as the European Space Agency.
- Agencies that coordinate international efforts, such as the International Committee of the Red Cross or World Health Organization.
- Social and cultural elements, including religious movements and their leaders.
- Intelligence and military communications systems of other services, allies, and adversaries.
- Individuals with the appropriate hardware and software to communicate with a worldwide audience.

As technology enables ever greater numbers of individuals, groups, organizations, and nation states to be linked to the world through the GIE, these actors can be expected to pursue their interests by attempting to manipulate and control the content and flow of information within the MIE.

NEWS MEDIA

The role of the news media will continue to expand. The number of news organizations and their means to gather, process, and disseminate information is increasing exponentially. From the 147 reporters who accompanied the D-Day invasion in World War II, to the 800-plus reporters in Panama during Just Cause, to the 1,300 reporters in the Kuwaiti theater in Desert Storm, the ability and desire of the news media to cover US military operations is a given. Likewise, the demand by the US and international public to know what is happening, consistent with security and propriety, is also a given.

FM 100-5 observes that the impact of media coverage can dramatically affect strategic direction and the range of military operations. Clearly, the effect of written, and, more importantly, visual information displayed by US and international news organizations directly and rapidly influenced the nature of US and international policy objectives and our use of military force in Rwanda, Somalia, and in the former Yugoslavian republic.

INFORMATION INFRASTRUCTURES

Within the GIE, an intricate set of information infrastructures have evolved to link individuals, groups, and nations into a comprehensive network that allows for the increasingly rapid flow of information to all elements having access to the network. In practice, subelement labels are misleading as the information environment has no discrete boundaries. Each subelement is inextricably intertwined, a trend that will only intensify with the continuous application of rapidly advancing technology. This worldwide telecommunications web transcends industry, the media, and the military. It includes both government and nongovernment entities, the GII, the national information infrastructure (NII), and the defense information infrastructure (DII).

Global Information Infrastructure

An interconnection of communications networks, computers, data bases, and consumer electronics that puts vast amounts of information at the user's fingertips. The GII is a term that

encompasses all these components and captures the vision of a worldwide, seamless, dynamic web of transmission mechanisms, information appliances, content, and people. Global accessibility and use of information in the GII is especially critical, given the increasing globalization of markets, resources, and economies. The GII—

- Includes more than just the physical facilities used to store, process, and display voice, data, and imagery. It encompasses a wide array of ever-expanding capabilities, including cameras, scanners, keyboards, fax machines, and more.
- Electronically links organizations and individuals around the globe and is characterized by a merging of civilian and military information networks and technologies.

National Information Infrastructure

All nations' NIIs are an integral part of the GII. The composition of the NII mirrors the GII, but on a reduced scale. The NII is—

- A series of components, including the collection of public and private high-speed, interactive, narrow and broadband networks.
- The satellite, terrestrial, and wireless technologies that deliver content to home, businesses, and other public and private institutions.
- The information and content that flows over the infrastructure, whether in the form of data bases, the written word, television, or computer software.
- The computers, televisions, and other products that people employ to access the infrastructure.
- The people who provide, manage, and generate new information and those that help others to do the same.

Defense Information Infrastructure

DII encompasses transferring information and processing resources, including information and data storage, manipulation, retrieval, and display. The DII connects DOD mission support, command and control (C^2), and intelligence computers and users through voice, data imagery, video, and multimedia services. It provides information processing and value-added services to subscribers over the Defense Information Systems Network (DISN).

Military Information Environment

The sphere of information activity called the *military information environment* is defined as—

> The environment contained within the GIE, consisting of information systems (INFOSYS) and organizations—friendly and adversary, military and nonmilitary, that support, enable, or significantly influence a specific military operation.

The MIE, at a minimum—

- Reaches into space from the home station to the area of operation (AO).
- Reaches into time, from the alert phase through the redeployment phase.
- Reaches across purposes, from tactical missions to economic or social end states.
- Includes people, from deployed soldiers and families at home to local or regional populations and global audiences.

Within the context of the MIE, Army leaders exercising battle command will face many new challenges. They will also have many new operational opportunities. To realize these opportunities, information operations (IO) need to become an integral part of full-dimensional operations. The intertwined relationship between geopolitical strategic factors, technology, and management requires the adoption of a new perspective.

The proliferation of INFOSYS and the global information explosion brings more actors into the battlespace, implies new ways of

managing force and forces, compresses the traditional levels of war in time and space, and gives operations a simultaneous and continuous character. A commander's battlespace now includes global information connectivity. As a result, tactical military actions can have political and social implications that commanders must consider as they plan, prepare for, and conduct operations. *Know the situation* now requires additional focus on nonmilitary factors. Commanders can best leverage the effects of new technology on their organizations by employing new and emerging automated planning and decision aids and new or different methods and techniques of control and management.

THREATS TO THE INFORMATION INFRASTRUCTURE

The threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing. They come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, or personal/industrial gain. They come from information vandals who invade INFOSYS for thrill and to demonstrate their ability. The globalization of networked communications creates vulnerabilities due to increased access to our information infrastructure from points around the world. Threats against computers, computer systems, and networks vary by the level of hostility (peacetime, conflict, or war), by technical capabilities, and by motivation (see Figure 1-2). The bottom line is that threats to all forces, from strategic to tactical, exist from a variety of new and different sources, and they exist on a continuing basis even during periods of relative peace.

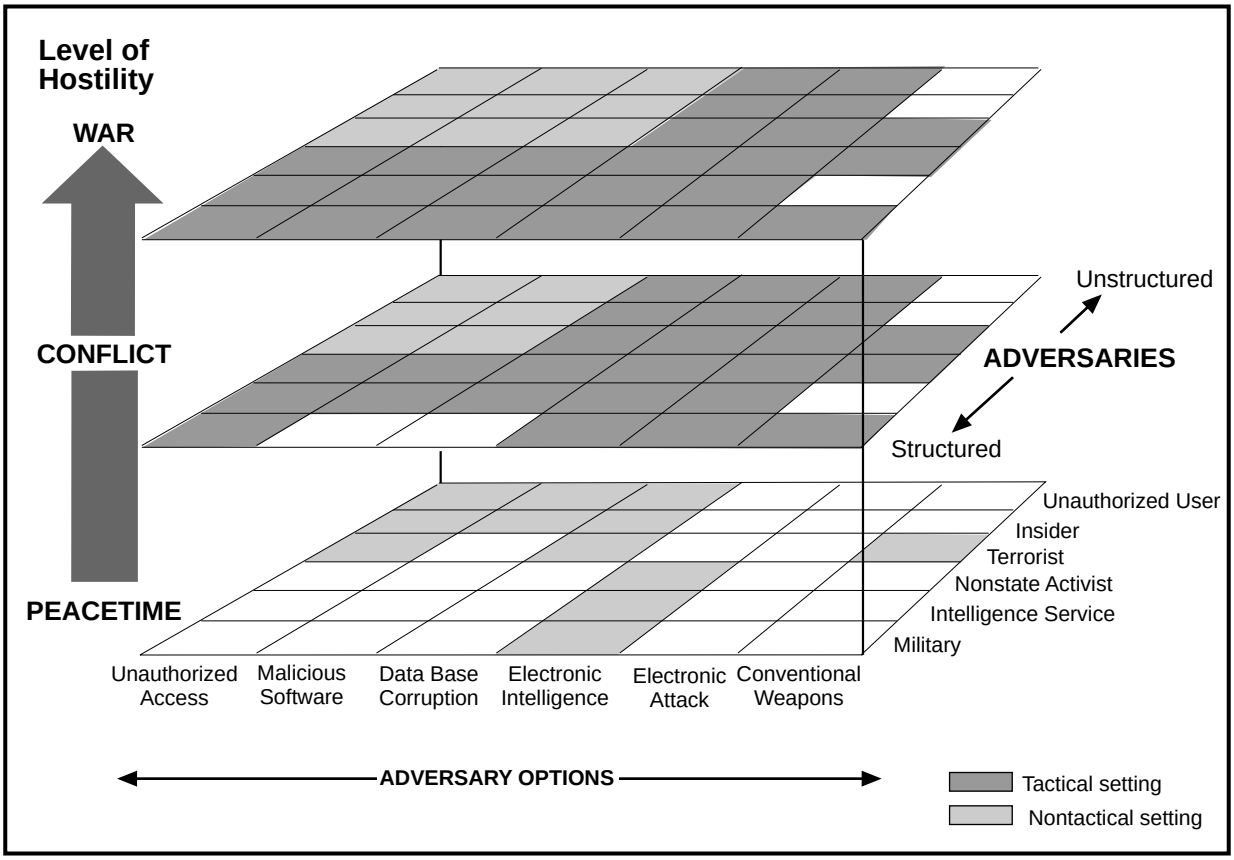

Figure 1-2. Threats to Information Systems

Adversaries have several options to influence or attack opposing INFOSYS and services. Attacks can be designed with a delayed effect, such as corrupting a data base or controlling program as well as immediate actions to degrade or physically destroy. Examples include—

- Unauthorized access, either to gain information or insert data.
- Inserting malicious software to cause a computer to operate in a manner other than that intended by its users. This category includes computer viruses, logic bombs, and programs designed to bypass protective programs.
- Corrupting data through use of malicious software, alteration of data, or use of electronic attack (EA) to make data misleading or useless.
- Collecting electronic intelligence, whether signals, radiation, or data.
- Conducting EA actions such as jamming, broadcasting false signals, or generating bursts of electromagnetic pulse (EMP).
- Using psychological operations (PSYOP) and deception to influence or oppose friendly INFOSYS.
- Attacking to physically destroy, degrade, or disrupt military communications and control networks or civilian systems upon which military operations rely. Weapons employed in such efforts range from terrorist bombs to artillery, missiles, and direct air attack.
- Using jamming and deceptive transmissions (EA) to attack commercial communications systems on which the Army relies. In such cases, more than communications can be disrupted. Sensors at all levels of operation can be jammed or triggered to produce misleading information. Both commercial systems and sensors are particularly vulnerable to the effects of EMP.

The effectiveness of military operations can be degraded if the user's confidence in the quality of the data can be eroded. Spurious data or false signals could be transmitted to erode confidence in the accuracy and effectiveness of such critical systems as the global positioning system (GPS).

Sources of Threats

Threats come from a range of sources—from individuals (unauthorized users or insiders) to complex national organizations (foreign intelligence services and adversary militaries). Boundaries between these groups are indistinct, and it is often difficult to discern the origins of any particular incident. For example, actions that appear to be the work of hackers may actually be the work of a foreign intelligence service. Sources include unauthorized users, insiders, terrorists, nonstate groups, foreign intelligence services, and opposing militaries or political opponents.

UNAUTHORIZED USERS

Unauthorized users such as hackers are the source of most of the attacks against INFOSYS in peacetime. While to date, they have mainly targeted personal computers, the threat they pose to networks and mainframe computers is growing.

INSIDERS

Individuals with legitimate access to a system pose one of the most difficult threats from which to defend. Whether recruited or self-motivated, the insider has access to systems normally protected against attack. While an insider can attack a system at almost any time during its lifetime, periods of increased vulnerability for a system include design, production, transport, and maintenance.

TERRORISTS

Terrorists are increasing their use of commercial INFOSYS. Their actions range from unauthorized access, to an information network, up to direct attacks against the infrastructure

(bombing, and so forth). Terrorist groups have also been identified using computer bulletin boards to pass intelligence and technical data across international borders.

NONSTATE GROUPS

New players, ranging from drug cartels to social activists, are taking advantage of the possibilities offered by the Information Age. They can acquire, at low cost, the capabilities to strike at their foes' commercial, security, and communications infrastructures. Moreover, they can strike with relative impunity from a distance. Besides attacking opponents directly, these actors use the international news media to attempt to influence global public opinion and shape perceptions of a conflict. They even attempt to inflame dormant issues into conflicts that otherwise would not arise.

FOREIGN INTELLIGENCE SERVICES

Active during periods of both peace and conflict, foreign intelligence services take advantage of the anonymity offered by computer bulletin boards to hide organized collection or disruption activities behind the facade of unorganized hackers. Their primary targets are often commercial and scientific networks rather than direct attacks on the military.

OPPOSING MILITARIES OR POLITICAL OPPONENTS

While the adversary's activities are more traditionally associated with open conflict or war, his manipulation of the news media during peacetime may help frame the situation to his advantage prior to the onset of hostilities.

Level of Hostility

The level of hostility generally reflects the scope and scale of an adversary's actions against friendly INFOSYS. In peacetime, unauthorized access to and use of computers, computer systems, and networks is the greatest current threat. Deliberate use of malicious software by an adversary could be used against communications, transportation, banking, power, and computation systems upon which both industry and the military might depend. We can expect an adversary to use malicious software to assess the vulnerability of our information networks.

As the crisis moves toward overt conflict or war, more direct and far-reaching attacks can arise against information and INFOSYS. Targets can include both units and their supporting infrastructures. Deployed tactical units may face the results of earlier intrusions and insertions, allowing embedded malicious software to cripple systems or degrade communications. By the time a unit is engaged in combat, it could have been subjected to a variety of overt and covert attacks against its INFOSYS.

On the battlefield, reliance on an extensive and potentially fragile communications infrastructure presents a vulnerability that entices exploitation. The initial candidates for attack could be vital information nodes or links such as CPs and communications centers. In addition to striking battlefield information nodes, adversaries can also strike the supporting infrastructure, both on and off the battlefield. Central system support assets such as power sources can be very difficult to repair or replace. Artillery, tactical ballistic missiles, and air power provide the major attack systems for most adversaries today. The ability of an adversary to strike will only grow as more capable systems, such as cruise missiles and precision-guided munitions, proliferate. This ability to strike with precision will be enhanced by the spread of such technologies as GPS, unmanned aerial vehicles (UAVs), and near-real time imagery satellites. If INFOSYS or facilities cannot be destroyed, they can be made untenable through contamination by chemical or biological weapons.

CHALLENGES

Commanders and national leaders face significant and interrelated challenges in dealing with and anticipating the effects of the global visibility of operations and rapid changes in information technology and their impacts in the GIE.

Information security

Two commonly recognized facts address why information security (INFOSEC) is an important challenge. First, the Defense Information Systems Agency (DISA) reports that over 95 percent of DOD communications during peacetime travel over the relatively unprotected public switch network (PSN) and are largely outside the direct control or influence of the military. In addition, a significant amount of open-source intelligence is carried by commercial means.

Continuous Operations

Because of the pervasive and intrusive nature of the MIE, preparation for dealing with IO must not wait until a unit receives a warning order to deploy. By that time, the commander and his staff must have already developed plans and procedures for dealing with the myriad aspects and influences in the MIE or risk being rapidly overcome by events.

Policy and Public Opinion

With global visibility, dramatic information displays and expert analyses of military operations in progress can rapidly influence public opinion and, therefore, policy related to the conduct of military operations. The population that receives and potentially reacts to this coverage includes the US public, decision makers, alliance or coalition partners, and other nations. It also includes potential or actual adversaries of the US. The news media will most likely provide 24-hour coverage of all perspectives on the operation.

Global visibility of operations can also affect a commander's decision-making. When the information in the GIE is inaccurate, incomplete, not presented in context, based on rumor or the result of purposeful misinformation or disinformation efforts, a commander may react in haste, make an emotional decision, or make choices that are inconsistent with the real situation, up to and including a termination of an ongoing operation. Effective commanders anticipate how the adversary might attempt to manipulate the news media in order to prevent a potential foe from setting the terms of the conflict in the public arena.

Morale

The global visibility of operations impacts a command's combat power by either enhancing or degrading soldier morale. Soldier spirit and perseverance, the will to win, dedication to the cause, and devotion to fellow soldiers and the unit can be rapidly undermined by what is being said in the GIE. The instant communications capabilities of these INFOSYS often disseminate information to soldiers—whether accurate or inaccurate—faster than the military chain of command. Bad news, misinterpretation, inaccurate information, and misinformation (or disinformation) impact families and communities as well as soldiers, affecting their morale and commitment to the objective at hand and potentially undermining the critically important human psychological dimensions discussed in FM 100-5. Nevertheless, Americans on and off the battlefield will continue to have free access to radio, television, and the press and be aware of events and circumstances.

Legal Considerations

Relatively few rules and laws govern the use of or access to many new INFOSYS or technologies. For that reason, IO confront legal challenges and other constraints such as rules of engagement (ROE) or status of forces agreements/status of mission agreements. Tension exists both in peace and during times of conflict. Collection of intelligence, or, simply,

information in peacetime, is often limited by policy and/or law. Many policies and laws for using nonmilitary computer systems and other information networks during peacetime are yet to be determined. For example, the control or regulation of access on the internet to protect sensitive information or critical network nodes is largely unaddressed. What are the ROE for the INFOSYS in peace? In war? Close coordination with the supporting judge advocate is critical in confronting IO challenges based on legal considerations.

Because many of the actors and influences in the MIE are outside friendly military control, contracts or legal restrictions may prevent the military from controlling or influencing the use of civilian assets by an adversary. As an example, during hostilities an allied coalition force may depend upon an international agency to change the access codes for an imagery satellite to protect critical information in the area of responsibility (AOR). Without the change, the imagery is available in the open market. An adversary could, under commercial contract, download critical satellite imagery of the geographic region in near-real time as the satellite passed over the ground station.

INFORMATION DOMINANCE: THE RESPONSE TO THE CHALLENGES

Information dominance is defined as—

> The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.

As we have come to recognize and depend on air superiority as a key condition for military success, information dominance has taken on a similar importance for military operations. This means that friendly knowledge and understanding of the situation must be more certain, more timely, and more accurate than the adversary's, revealing to the friendly commander the conditions that will lead to success. Creating information dominance has two equally important facets:

- Building up and protecting friendly information capabilities.
- Degrading enemy information capabilities.

The friendly commander achieves information dominance by gaining a *knowledge advantage* over an enemy

The knowledge advantage generated by commanders using innovative technical and human techniques permits the force to more readily seize or retain the overall initiative and increase its lethality and survivability. Building a knowledge advantage requires a highly developed sense of what information is required and an ability to manage the use and dissemination of that knowledge to the right place, at the right time, for the desired purpose.

Successful leaders use the knowledge advantage by combining technical and human information capabilities with a broad intent statement and a clearly articulated concept of operation. Like air power, a ground commander can enjoy levels of knowledge advantage ranging from *information supremacy* to *information parity.* An enemy can also achieve a knowledge advantage at our expense. Information also vary dominance can change over space and time; it can by echelon. An Army may achieve information dominance at the operational level but lose it at the tactical level. The notion of information dominance is not new. Throughout history, commanders have sought to leverage the temporary opportunity that comes from an information advantage, whether it comes from knowledge of terrain or satellite imagery.

HISTORICAL PERSPECTIVE

For nearly two hours a succession of young officers, of about the rank of major, presented themselves. Each had come back from a different sector of the front. They were the direct personal representatives of the Commander-in-Chief, and could go anywhere and see anything and ask any questions they liked of any commander, whether at the divisional headquarters or with the forward troops. In turn, they made their reports and were searchingly questioned by their chief to unfold the whole story of the day's battle. This gave Field Marshal Montgomery a complete account of what had happened by highly competent men whom he knew well and whose eyes he trusted. It afforded an invaluable cross-check to the reports from all the various headquarters and from the commanders. I thought the system admirable, and indeed the only way in which a modern Commander-in-Chief could see as well as read what was going on in every part of the front.

Sir Winston Churchill
Triumph and Tragedy, 1953

Directed Telescope

High-performing units are in large part distinguished from other units by their ability to effectively acquire and use information. Historically, high-performing units often gained the information advantage by using nontraditional means and methods. One such method is often referred to as the *directed telescope.* In concept, the directed telescope acquires information by supplementing the routine information flow, normally by—

- Going outside the traditional command and its hierarchical information channels.
- Using special operations units, reconnaissance teams or officers, and special communications networks.

These techniques are still valid and in use today. Modern technological innovations potentially make the advantages gained via the directed telescope technique almost routine. Innovations in sensors, processors, communications, and computers can give commanders immediate access to enemy and friendly situation information and thus a subsequent operational *knowledge advantage*.

Battlefield Visualization

Creation of an operational knowledge advantage supports the commander's battlefield visualization. *Battlefield visualization* is the process whereby the commander—

- Develops a clear understanding of his current state in relation to the enemy and environment.
- Envisions a desired end state that represents mission accomplishment.
- Visualizes the sequence of activity that will move his force from its current state to its end state.

A key step toward achieving information dominance is reached when one commander's level of battlefield visualization is significantly greater than his opponent's.

In the past, leveraging a knowledge advantage to decisively achieve a desired end state has been largely an intuitive process. Truly exceptional commanders have almost always possessed this trait; less successful commanders often have not. Information technologies now hold a potential for making this grasp of the battlespace, and the inherent opportunities it affords, more accessible to every leader, from field army to rifle platoon. The effect of these changes will be to enhance battlefield visualization by better supporting leaders with a deliberate and systematic information process

based upon building blocks of raw data parsed and collated by both man and machines, synthesized into a coherent whole, and focused upon drawing understanding from the chaos of battle. Additionally, by linking commanders at different echelons, this same technology will enhance situational awareness and promote synchronized operational planning and execution. Ideally, the command will see and think as one.

Situational Awareness

A critical aspect of achieving a knowledge advantage over your adversary is the achievement of a condition of situational awareness throughout the force. *Situational awareness* includes—

- A common understanding of the commander's assessment of the situation.
- The commander's intent.
- The commander's concept of operation, combined with a clear picture of friendly and enemy force dispositions and capabilities.

IO potentially assure situational awareness appropriate to every level of an organization, down to the individual soldier. Systems being tested and fielded today offer commanders at all levels the potential of a collective, shared understanding of the battlespace. The commander's assessment of the situation, his intent, and the concept of operation provide the framework that applies throughout the organization. This framework fosters increased cohesion and unity of effort in the execution of operations. Figure 1-3 illustrates this relationship.

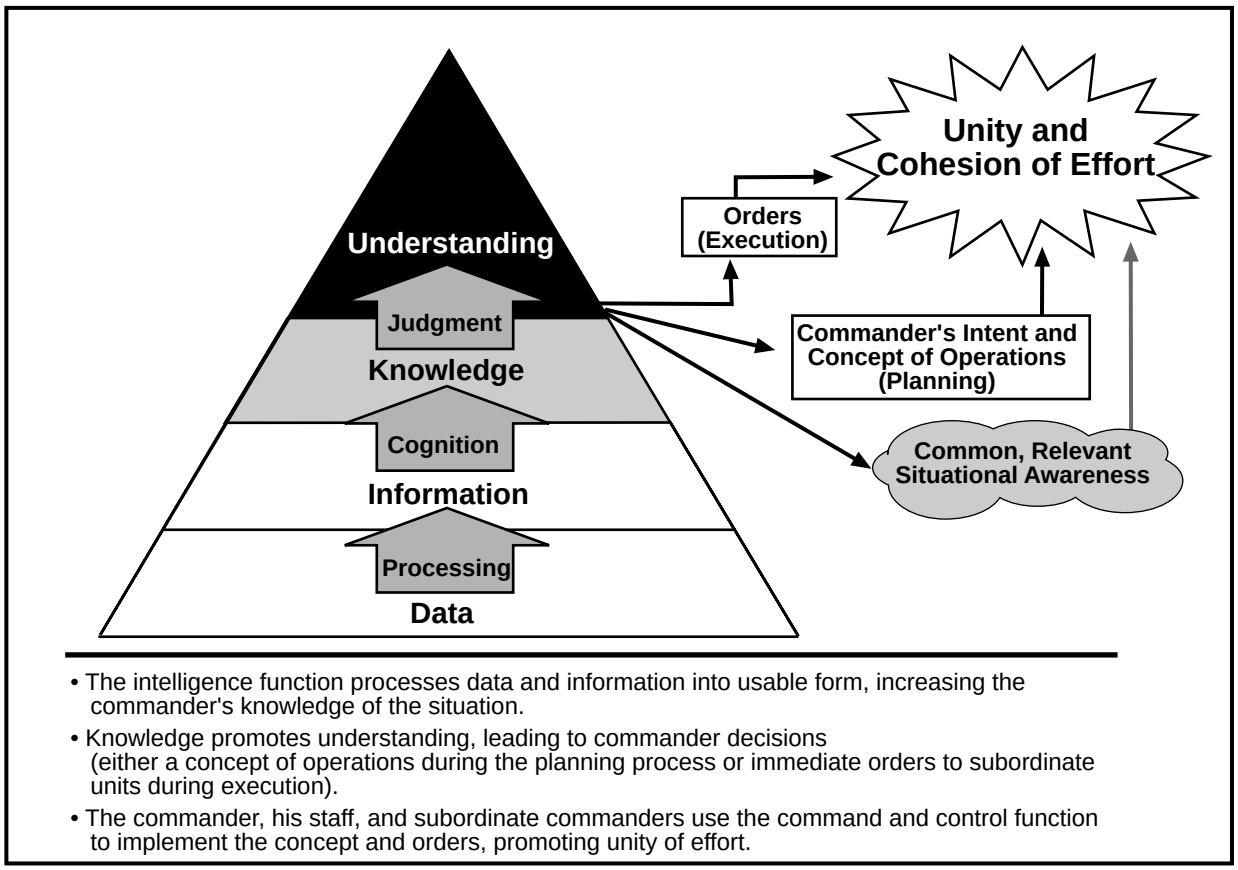

Figure 1-3. Situational Awareness

Situational awareness is inherently local, providing immediate context and relevance for the interpretation and use of new information as it is received by a soldier in a particular situation. The local situation relevant to each level and individual is developed within the common framework and shared vertically and laterally as appropriate. This situation not only retains the advantage of hierarchical structure (common framework and intent) but also adds the advantage of nonhierarchical INFOSYS that enable decentralized adaptation and action to local situations throughout the command.

Developing the flexibility of a nonhierarchical structure places a greater obligation on the commander to clearly articulate his intent and concept of operations. Traditionally, commanders ensured that both intent and concept were understood two echelons up and down in a hierarchical structure. Information technology now makes it possible for a senior commander's intent and concept to be relatively easily shared throughout the command whenever doing so will enhance the operation. The art of command requires clearly stating a common framework with sufficient freedom for local adaptation and application. Proliferation of that understanding, potentially to all leaders on the battlefield, gives the force a singular perspective and a clarity of focus that optimizes its combat power against an opponent or enables it to control a situation in other operations. Denying an adversary a similar capability, such as degrading his situational awareness, is an equally important objective and is addressed in Chapter 3 under C^2W.

Expanded Vision

Our traditional operational vision must expand to take full advantage of the potential contribution of IO to dominate the enemy while protecting friendly forces. Before any mental constraints are placed on intent or operational concept, commanders at every level assess those actors and elements that can affect upcoming operations, to include informational aspects. The commanders' assessments include actors and elements both within and outside of their control. The result of this process of thinking about the GIE is a manageable number of informational elements with which commanders decide to deal, which, by definition, constitutes the MIE for a particular operation. This expanded vision of the battlespace can include various combinations of space, time, purpose, and people.

The elements of an IO vision align with the combat functions associated with traditional operations. The MIE equivalent of the *tactical advantage* of high ground, or the flanking position, might be transformed into an information advantage of local and international recognition that the military operation is legitimate and has international support. Just as successful *maneuver* gives a commander more options than the enemy, a perception of credibility and support, or an ability to command and control, provides an advantage for informational maneuver. Maintaining this advantage requires constant assessment and adjustment. To this end, PSYOP-supported Special Forces (SF) teams in the countryside, civil affairs (CA) teams in urban areas, reports from PVOs, and media coverage provide a form of reconnaissance and surveillance, just as standard military reconnaissance and surveillance operations provide information that drives subsequent fire and maneuver.

The purpose of firepower in combat is the generation of destructive force against an enemy's capabilities and will to fight. The MIE equivalent of firepower, already included in doctrine, is the employment of lethal and nonlethal, direct and indirect capabilities through C^2W. C^2W uses deception, PSYOP, electronic warfare (EW), operations security (OPSEC), and destruction to attack an adversary's capabilities. At the same time, C^2W protects friendly operations. US armed forces have always employed these capabilities, but they were recently integrated into operations under C^2W. This integration improves the friendly targeting process by directing the power of traditional attack, deception, PSYOP, EW, and OPSEC at the adversary's decision cycle, thus gaining control of that cycle and helping generate information dominance.

While the 1993 version of FM 100-5 recognizes the impact of global news coverage on the scope, nature, and duration of major operations, recent events demonstrate that the GIE also affects operations at brigade, battalion, and company levels. Commanders at every level may now find that CA, military police (MP), public affairs (PA), PSYOP, and SF activities that support, enable, or influence operations have become integral to their decision process and operations and require careful coordination and synchronization to achieve maximum effect. Commanders must continue to carefully manage the separation of PA and PSYOP functions to preserve the integrity and credibility of PA operations. The methods of using C^2W, PA, and CA together to enhance operations is discussed in detail in Chapter 3.

Activities that affect how operations are seen and perceived by different audiences are an increasingly prevalent and required calculation of battle command and a prerequisite for effectively visualizing battlespace. The requirement to identify the critical audiences, messages, and communications means is not new to leaders. However, it is gaining major significance for successful operations.

HISTORICAL PERSPECTIVE

During the course of the Gulf War, the combined operations of the allied coalition effectively isolated, both physically and psychologically, a large element of Iraqi forces on Faylaka Island. Rather then reduce the island by direct assault, a tactical PSYOP team from the 9th PSYOP Battalion, aboard a UH-1N helicopter, flew aerial loudspeaker missions around the island with cobra gunships providing escort. The message told the adversary below to surrender the next day in formation at the radio tower. The next day 1,405 Iraqis, including a general officer, waited in formation at the radio tower to surrender to the Marine forces without a single shot having been fired.

Open Media Coverage

Besides forcing a broader view of the environment, IO imply closer attention to the media and the global visibility of operations. DOD and Army policy for principles of combat coverage require Army commanders to provide open and independent coverage by the news media as the standard means of providing the American public information about the employment and capabilities of their armed forces. This policy gives commanders and leaders at all levels the clear mission of preparing their soldiers to effectively deal with the media before, during, and after all operations.

The commander's primary tool at division-level and above for dealing with the news media is PA. PA addresses issues that are integral to all levels of war. Below division level, however, the commander has no special staff to discharge this responsibility. Often, brigade and smaller units have to house, support, and escort reporters. Commanders must understand and train their soldiers, as well as themselves, to plan for the presence of media and provide effective interviews to communicate legitimate information to the public, strengthen soldier morale and unit cohesion, and enhance their ability to accomplish their mission.

While the clear intent of this doctrine is to require commanders to pay closer attention to the media and its potential impact upon military operations, it is also clear that doctrine does not sanction in any way actions intended to mislead or manipulate media coverage of military operations. To the contrary, the Army accepts and fully endorses the healthy tension that exists between the normal desire of the media to inform the public as much as possible about military operations and the normal desire of commanders to control the information environment about those same operations to the greatest possible degree.

Information Management

Information management takes on increasing importance in meeting the challenges of global visibility, rapidly changing information technology, and their impact on the GIE. Mountains of data must be acquired and quickly translated into knowledge and understanding. Accomplishing this challenge requires a continuous, cyclical process. Decision-making has become increasingly dynamic and multidimensional. Decisions about current operations must occur simultaneously with decisions and planning about future operations. Decision-making must match the pace with which situational awareness changes.

Information technology now permits the horizontal movement and integration of information and provides a framework for local decision-making, potentially allowing the commander's span of control to increase without losing effectiveness. The dynamics affecting a commander's span of control are critical because the modern battlefield sees forces increasingly separated, leaving large gaps between formations and requiring each cluster of forces to act with greater autonomy within an expanded AO. Dispersion creates more subordinate force clusters, decentralizes decision authority, and creates a major requirement for coordinated effort. The nominal span of control is increased and overall situational awareness is more complicated.

Harnessing the potential of information to transform how the Army operates is critical to its success in the future. However, technology alone cannot provide leaders with automatic battlefield visualization, flawless situational awareness, easily expanded vision, or highly effective information management. In the final analysis, the products of our initiative to harness the potential of information can only support the application of a leader's judgment, wisdom, experience, and intuition to enhance his battle command.

An increase in the amount of information available does not guarantee certainty; in fact, it potentially increases ambiguity. Current staff organizations, procedures, and analytical methods must adjust to master the richer flow, faster pace, and huge volume of information. The challenge is to find better, not just faster, analysis and decision-making procedures.

Chapter 2

Fundamentals

While reflecting the increased complexity and lethality of the modern battlefield, Army doctrine recognizes that advanced weapons and technologies are no better than the skill with which leaders and soldiers employ them against the enemy.

FM 100-5

This chapter outlines the nature of information and the fundamentals of IO by stating what they are, what they apply to, and how they relate to various activities of IO. The chapter discusses the components of IO—*operations, relevant information and intelligence (RII),* and *information systems (INFOSYS)*. It concludes with a discussion of the six critical activities essential to a sound IO program: *acquiring, using, protecting, exploiting, denying,* and *managing* information and INFOSYS.

COGNITIVE HIERARCHY

Information is defined as—

Data collected from the environment and processed into a usable form.

A given piece of data is largely meaningless by itself. Only when data is processed, that is, placed into a situational context, does it gain meaning and become, by definition, information. Knowledge is derived from information. Knowledge is information that has been tested and accepted as factual—

- Through cognition—the mental process that receives or develops unverified information (beliefs).
- Through assessment or testing to prove the information.
- By acceptance of the information as factual.

Commanders and their planners must always be sensitive to the difference between beliefs and knowledge. Untested beliefs, even when commonly held, differ from *facts* and are, in essence, opinions that can later prove to be wrong. Decisions based upon beliefs instead of facts are always at risk.

Understanding is achieved by using judgment to give knowledge relevance within a specific situational context. Ideally, understanding a situation supports a commander in battlefield visualization and creates the conditions from which plans can be formed and effective actions taken. See Figure 2-1.

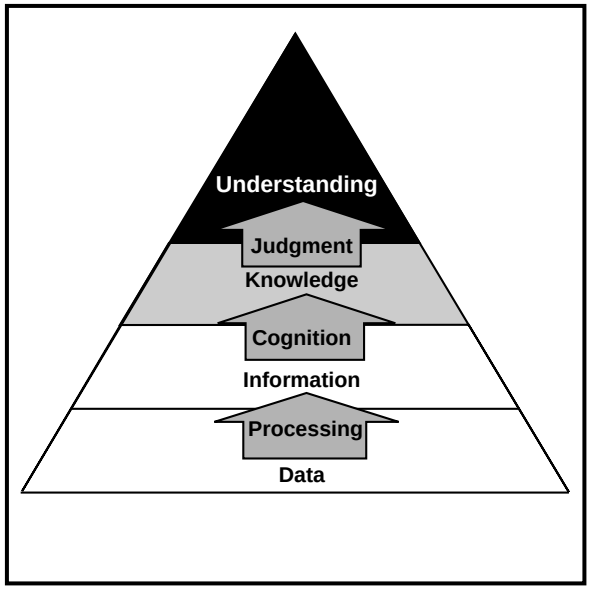

Figure 2-1. The Cognitive Hierarchy

While it is certainly desirable to achieve full understanding of a situation before making decisions, commanders must be fully prepared to make decisions in an operational environment of ambiguity, characterized by imperfect information and incomplete understanding. Command decision-making will remain an art, not a science, even in the Information Age. A goal of IO is to narrow the gap between the art and science of command decision making.

STRATEGY

The *National Military Strategy* recognizes that information warfare (IW) is one of many capabilities within the US military elements of national power. IW can support the overall US Government strategic engagement policy during peacetime, crisis, conflict, and postconflict. The ability of the US Government to influence the perceptions and decision making of others greatly impacts the effectiveness of deterrence, power projection, and other strategic concepts.

This paragraph introduces and defines *information warfare* and explains its relationship with the Army's interpretation—*information operations.* In times of crisis, information can deter adversaries from initiating actions detrimental to interests of the US Government or its allies or detrimental to the conduct of friendly military operations. If carefully conceived, coordinated, and executed, IW—

- Contributes to defusing crises.
- Reduces the period of confrontation and enhances the impact of informational, diplomatic, economic, and military efforts.
- Forestalls or eliminates the need to employ combat forces.

Information Warfare

Information warfare is the term adopted by the Department of Defense (DOD) and the joint staff to recognize a range of actions taken during conflict to achieve information superiority over an adversary. It is specifically defined in CJCSI 3210.01 as—

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

The objective of IW is to attain a significant information advantage that enables the total force to quickly dominate and control the adversary. The strategic goal of IW is to seize and maintain a decisive advantage by attacking an adversary's NII through exploitation, denial, and influence, while protecting friendly INFOSYS. IW offers either side the chance to strike at a distance with relative safety.

The Army, recognizing that IW as currently defined by DOD is more narrowly focused on the impact of information during actual conflict, has chosen to take a somewhat broader approach to the impact of information on ground operations and adopted the term information operations. The Army has adopted this broader approach to recognize that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace through global war. IO implement the IW policy for the land component commander.

Information Operations

Information operations integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources. IO are defined as—

> Continuous military operations within the MIE that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE and exploiting or denying an adversary's information and decision capabilities.

Units conduct IO across the full range of military operations, from operations in garrison, through deployment, to combat operations, and continuing through redeployment upon mission completion.

COMPONENTS OF INFORMATION OPERATIONS

Activities to support IO include *acquiring, using, protecting, managing, exploiting,* and *denying* information and INFOSYS. These activities take place within three interrelated components of IO: *operations*, *RII,* and *INFOSYS*. These components operate within a battlespace established by the MIE. (See Figure 2-2.) Army organizations conduct these IO activities as part of a dynamic, iterative process to support each component in an integrated full-dimensional operation.

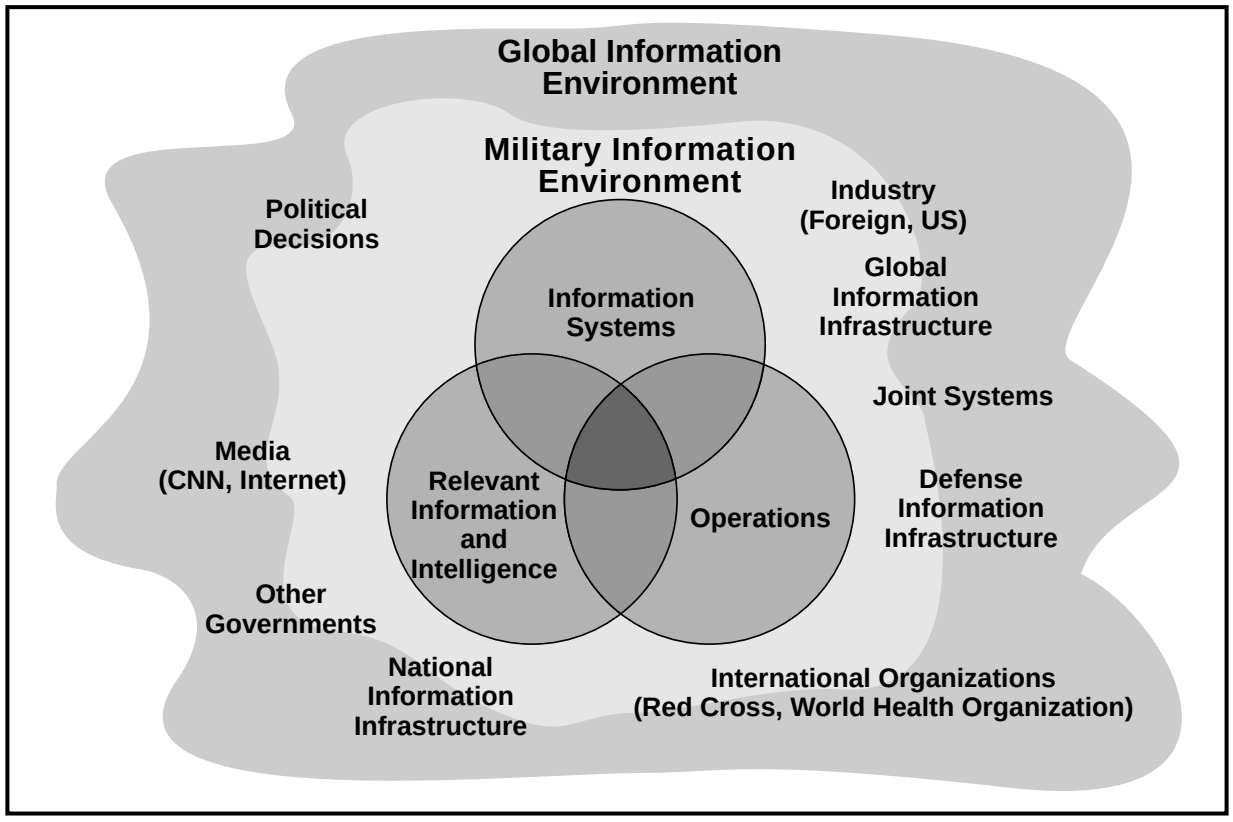

Figure 2-2. Information Operations

Operations

C^2W, CA, and PA are the three operations the Army currently uses to gain and maintain information dominance and effective C^2.

C^2W OPERATIONS

C^2W is the warfighting application of IW in military operations. The aim of C^2W is to influence, deny information to, degrade, or destroy adversary C^2 capabilities while protecting C^2 capabilities against such actions. C^2W is composed of two major branches:

- Command and control-attack (C^2-attack).
- Command and control-protect (C^2-protect).

C^2W planning is conducted throughout the military operational continuum, from peacetime through termination of hostilities. In the past, the primary warfighting objective was to concentrate physical and destructive combat power against the adversary's personnel and equipment, that is, tanks, airplanes, artillery, air defense. C^2W is discussed in detail in Chapter 3.

By 1986, AirLand Battle further evolved this thinking by linking ground and air operations to achieve depth and synchronization. A paramount consequence of AirLand Battle was the intention to strike at reserve, reinforcing, and second-echelon forces. This led in 1993 to an extended operational strategy of deep operations, with long-range weapons and Special Forces. Looking at high-value targets, deep operations strategy sought to destroy, degrade, deny, and disrupt critical C^2 nodes as one of its primary objectives.

Today, C^2W operations integrate and synchronize the capabilities of PSYOP, deception, OPSEC, and EW to facilitate the application of appropriate systems and forces to execute IO. While C^2W has had a primarily offensive focus in the past, it now includes both C^2-attack and C^2-protect. Although these two disciplines of C^2W have been practiced by successful armies since the beginning of recorded history, modern warfare with its emphasis on information and INFOSYS requires a new perspective. Three factors make C^2W considerations critical when operating in today's environment:

- Continuous, high-volume information flow dictated by the relationship of modern military technology and military operations.
- Vulnerabilities created by widespread incorporation of advanced technology for INFOSYS and intelligence.
- The radical improvement in INFOSYS and intelligence capabilities resulting from explosive advances in technology.

The complexity and range of today's MIE increases the difficulty of achieving a comprehensive disruption of an adversary's C^2 capabilities through any single attack or application of combat power. This places a premium upon the effective integration and synchronization of friendly physical destruction, EW, deception, and PSYOP to achieve maximum results when launching attacks. Likewise, careful integration and synchronization is also required to fully protect our critical INFOSYS/intelligence architecture from adversary attacks. Without the complete and thorough integration and synchronization of the five C^2W elements across both C^2-attack and C^2-protect, operational effectiveness will be reduced and potential vulnerabilities exposed.

C^2-Attack

The goal of offensive C^2W, specifically C^2-attack, is to gain control over our adversary's C^2 function, both in terms of flow of information and level of situational awareness. With effective C^2-attack, we can either prevent an adversary from exercising effective C^2 or leverage it to our advantage.

C^2-attack can strike at the adversary's capabilities at all echelons, targeting personnel, equipment, communications, and facilities in an effort to disrupt or shape adversary C^2. RII plays a key role in C^2-attack planning and operations, with the creation and maintenance of regional data bases on personal, historical, and cultural influences, intelligence-preparation-of-the battlefield (IPB), and battle damage assessments (BDA)—both soft and hard kill. The principal C^2-attack approach for influencing the adversary's C^2 is the synchronized application of the six information activities.

C^2-Protect

C^2-protect seeks to maintain effective C^2 of friendly forces by negating or turning to a friendly advantage the adversary's efforts to influence, degrade, or destroy friendly C^2 systems. C^2-protect is divided into active and passive measures and seeks to limit the vulnerability of forces (personnel, equipment, and information) to hostile action, even as deployed forces face ever-expanding threats and adversary capabilities. C^2-protect includes countering an adversary's propaganda to prevent it from affecting friendly operations, options, public opinion, and the morale of friendly troops.

CIVIL AFFAIRS OPERATIONS

CA support to IO provides an integral role of interfacing with critical actors and influences in the GIE. Whether in peace, conflict, or war, conducting military operations, consolidating combat power, and seeking information dominance are improved when leveraging CA support. Although conditions differ across the spectrum of conflict, CA activities establish, maintain, influence, or exploit relations among military forces, civil authorities, and the civilian populace in an AO to facilitate military operations. For example, during Operation Restore Democracy, CA activities informed the local populace through the news media, public discussion, and PSYOP informational products and programs about the reestablishment of the legitimate Haitian government. This created an information exchange that promoted understanding of, confidence in, and positive perception of measures supporting military operations.

The civil-military operations center (CMOC) can be established to interact with key actors and influences in the GIE, such as NGOs, PVOs, and local authorities. CA elements support military operations by applying their skills and experience in public administration, economics, public facilities, linguistics, cultural affairs, and civil information and by collecting information relevant to the commander's critical information requirements (CCIR). CA personnel have an intricate and important role in providing information during both the intelligence cycle and the operational planning cycle.

Commanders include CA operations in their planning guidance. CA planners must consider all available support and information to ensure successful completion of the CA mission. CA forces are well-suited to plan, coordinate, support, and, if directed, supervise various operations to support US objectives.

PUBLIC AFFAIRS OPERATIONS

Most military operations are conducted under the full glare of public scrutiny. National and international news media coverage plays a major role in quickly forming public debate and shaping public opinion. The news media serves as a public forum for the analysis and critique of goals, objectives, and actions. It can impact political, strategic, and operational planning, decisions, and mission success or failure. The reality of near real-time information, processed and transmitted at greater speeds and to wider audiences than in the past, has bridged the gap between what occurs on the ground and the goals and objectives of the *National Military Strategy.* Therefore, the public affairs officer (PAO) monitors public perceptions and develops and disseminates clear and objective messages about military operations. Moreover, commanders must involve themselves also in this dimension of IO. PA personnel—

- Assist the commander by working to establish the conditions that lead to confidence in and support of the Army.
- Support open, independent reporting and access to units and soldiers.
- Seek a balanced, fair, and credible presentation of information that communicates the Army story through an expedited flow of complete, accurate, and timely information.

The commander uses his internal information program (formerly command information) to inform soldiers about where they fit in, what is expected of them, and how they help accomplish the mission. This information also helps soldiers combat the effects of enemy propaganda or misinformation. Commanders, through their PAO, initiate, direct, and emphasize internal information topics and programs. Every soldier

must receive information specific to the operation through command channels and world, national, and local news. The media is an important information channel to the American public; however commanders, staff officers, and soldiers must balance OPSEC and other operational requirements when working with the media.

PA personnel support commanders by assessing the information environment and advising them on the PA implications of current and future operations. Leaders understand the importance of achieving a balanced, fair, and credible presentation of information to both internal and external audiences. Leaders integrate PA into their decision-making process by considering it in their assessment of the situation and development of courses of actions, plans, and orders. Commanders ensure that PA operations are synchronized with other combat functions and promote early coordination of PA, CA, and PSYOP functions during the planning process. A continual exchange of information must exist during execution as well. Although each function has a specific audience, information will overlap, making it crucial that messages are deconflicted and coordinated.

Relevant Information and Intelligence

Leaders have struggled with how to best capitalize on available information throughout the history of organized warfare. The drive to know as much as possible about their own forces—location, combat effectiveness, current activity—and the enemy's—location, disposition, combat effectiveness, intended actions—has been a durable characteristic of successful commanders, regardless of the time period or nationality. Today, commanders operate in an environment increasingly marked by the rapid flow of information and decisions among strategic, operational, and tactical levels. These factors are complicated by an explosive expansion in the opportunities for access and the manipulation of operationally relevant information by the wide array of individuals, organizations, and systems found in the GIE.

Ultimately, effective C^2 depends on ensuring that the right person has the right information at the right time. Intelligence, the commander's source of relevant information about the adversary, takes on increased, even crucial, importance in the Information Age. Because IO give battlespace global connectivity, intelligence on current or potential adversaries must be prepared on a global scale. Interaction with the MIE requires timely intelligence about many aspects of current or potential adversaries, to include cultural, political, and commercial aspects.

Commanders must have information to command. Information allows the commander's decision-execution cycle to function and gives direction to actions by the force to accomplish their operational missions.

The collection, processing, and dissemination of relevant information is the key to achieving situational awareness throughout the force, which creates the opportunity for unity of effort toward mission accomplishment. The commander operates within the GIE, adjusting his MIE to enhance his situational awareness as appropriate for the operation at hand.

The commander focuses on RII requirements. The commander's operational requirements dictate the critical information requirements, which in turn dictate the RII collection effort. To be effective, the unit's intelligence cycle must be managed to provide information based on the priorities in the concept of operations. A key to successful IO is an accurate IPB focused on the MIE. During combat operations intelligence analysts must continually perform an information-oriented BDA to ensure IO remain effective. RII support to IO begins in peacetime and must be continuous throughout all phases of an operation or campaign.

Advances in information technology are mandating changes in how RII support is provided. First, communications connectivity allows broadcast dissemination of information. This incorporates direct downlink of raw data from multiple sensors to multiple echelons simultaneously and the broadcast of finished

information products from theater, departmental, or national production agencies to deployed forces. Information can be provided on a push or pull mode to deployed units.

IO requires the fusion of information from a variety of sources. Advances in sensors, processors, and communicators are combining to provide detailed, timely reconnaissance and surveillance of almost any place on the globe. Both military and nonmilitary sources provide information that can be used to produce RII. Open-source intelligence or reporting will provide much order of battle (OB) and technical data. An OB focused on command, control, communications, computers, and intelligence (C^4I) includes data collection and information processing systems, command systems, and reconnaissance, intelligence, surveillance, and target acquisition (RISTA) systems.

Successful integration of IO requires an IPB grounded in a thorough understanding of an adversary's capabilities and decision-making style. An IPB based on C^4I focuses on an adversary's decision requirements. These are selected in relation to the friendly commander's priority intelligence requirements (PIR) and describe in detail the decisions the adversary must make to conduct his battle plan. From there, the focus shifts to the information sources that feed or influence the adversary's decisions such as sensors, the platforms on which they are deployed, and their supporting C^3 systems. The results should include data on current operations, capabilities, and vulnerabilities. RII as a component of IO is addressed in detail in Chapter 4.

Information Systems

INFOSYS collect, process, and disseminate information relating to current and future operations. Automation has made great advances in information processing, but human beings remain the most effective system for determining relevance and fusing information. INFOSYS are those means that enable commanders and their staffs to—

- Monitor the current situation.
- Synchronize operations.
- Integrate and synchronize operations across battlefield operating systems (BOSs).
- Coordinate joint air and naval support.
- Update weapon systems targeting parameters.
- Control close, deep and rear operations as one operation.

ARCHITECTURE

INFOSYS are essential to the effective application of military power. The Army's integrated architecture of advanced INFOSYS maximizes the C^2 capabilities of land forces in all operating environments. The road map for exploiting current and future information technologies to enhance Army operations is the Army Enterprise Strategy (AES). The AES and other initiatives like C^4I for the Warrior are reinforcing the important contributions INFOSYS make to information-based warfare. Of particular importance is the evolution of the Army's comprehensive information architecture with its three supporting initiatives focused on *operational, system,* and *technical architectures.* When completed, this initiative will create a common operating environment (COE) of standardized, interactive systems and templates for the collection, storage, and manipulation of all Army data bases.

Operational Architecture

The operational architecture will establish the required connectivity among processes, functions, information, and organizations. It will show what we do, what information we need to do it, and how often we need to exchange information within the force.

System Architecture

The system architecture seeks to identify relationships among C^4I components of systems and create physical connectivity within the information system. It uses an organizational

context to show system allocation and network structures and helps document engineering decisions, such as specific information protocols and bandwidth.

Technical Architecture

The technical architecture will establish a set of rules governing the arrangement, interaction, and interdependence of all the parts and elements that together constitute our INFOSYS. It specifies the permissible standards for designing C^4I capabilities and is critical to the creation and maintenance of interactive systems.

INTEGRATION

The integration of INFOSYS—both vertically and horizontally—facilitates tactical and operational agility, initiative, depth, synchronization, and versatility essential to Army success in joint and combined operations.

GLOBAL CONNECTIVITY

Global connectivity is essential for linking strategic, operational, and tactical aspects of IO and the ability to project forces worldwide. INFOSYS support operations globally with communications automation architectures, both space- and terrain-based. However configured, INFOSYS can provide such support with a minimum of physical repositioning to support C^2, whether in a strategic deployment phase or moving for a tactical attack. Both military and commercial INFOSYS play important roles in this architecture.

Today, the Army applies information technologies to digitize the battlefield by providing integrated C^2 that flows across each level of operation or war. The migration of the current Army Command and Control System (ACCS) to the Army Battle Command System (ABCS) incorporates a common C^2 operating environment at all echelons. This integration of modern INFOSYS with our tactical units continues to enhance their connectivity, decision-making, and, ultimately, lethality, survivability, and the ability to control the tempo of operations. Advanced weapons system and sensor technologies based on interoperability, digitization, and spectrum supremacy will contribute directly to improved effectiveness of the force. Chapter 5 discusses the Army INFOSYS architecture in detail.

Any military—like any company or corporation—has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries and or allies.

Alvin and Heidi Toffler

War and Anti-War: Survival at the Dawn of the 21st Century

INFORMATION ACTIVITIES

IO involves acquiring, using, protecting, exploiting, denying, and managing information and INFOSYS. When effectively executed, these critical activities supplement the human skills of battle command, speed decision making, minimize or eliminate uncertainty, focus combat power, help protect the force, harness organizational capabilities, link the MIE to the GIE, and enhance situational awareness for soldiers and leaders. These activities apply to both information and INFOSYS (hardware, people, organizations, and processes). Although listed sequentially, these activities are concurrent and seamless in their application (see Figure 2-3).

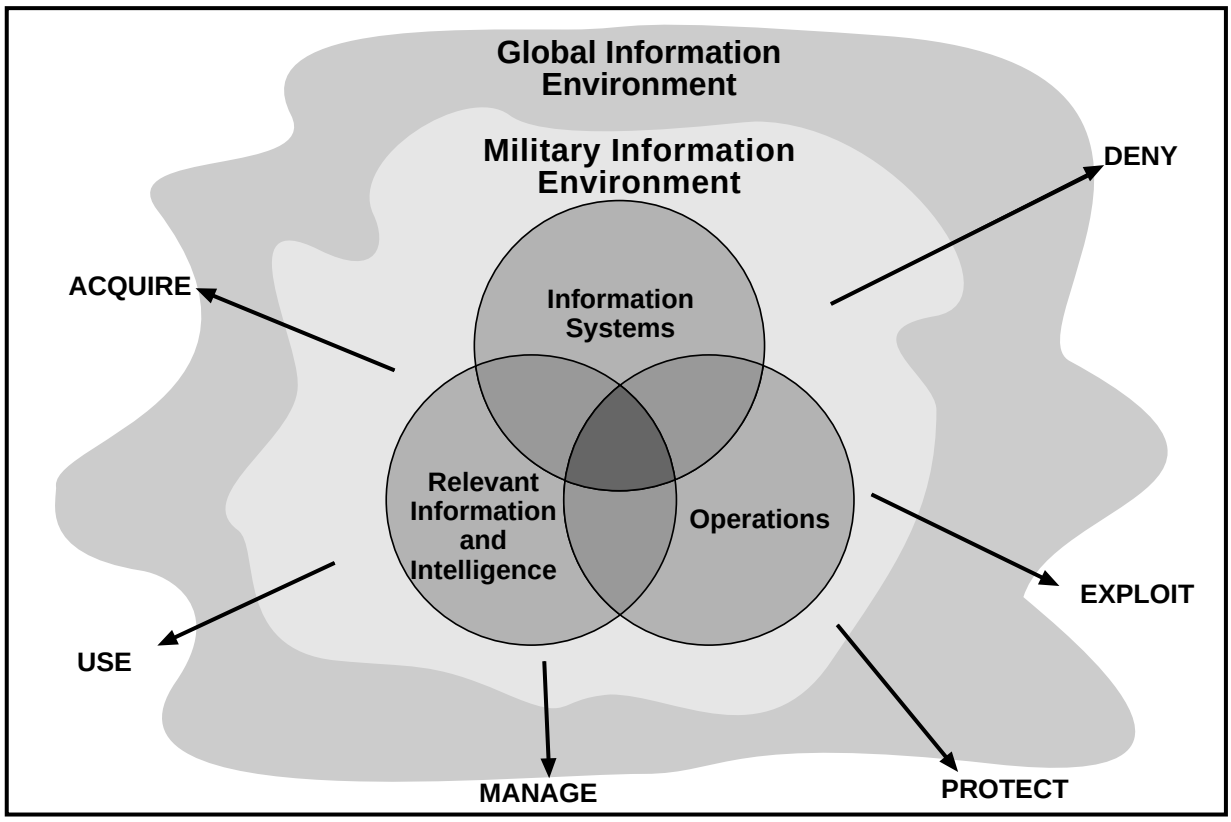

Figure 2-3. Information Operations Activities

Acquire

Commanders must consider the nature of the information required before allocating resources to acquire it. Initial questions include—

- What information is needed?
- What is the nature of that information?
- How can that information be acquired?

Necessary information includes mission, enemy, troops, terrain and weather, and time available (METT-T) and the basic who, what, when, where, why questions. The nature of that information includes its accuracy, timeliness, and its overall relevance to the situation in consonance with the CCIR. Considering the available information sources and the nature of that information, commanders develop technical and tactical plans to acquire critical information.

Information can be acquired through personnel, technical means, intelligence collection systems, tactical reporting, and intelligence or information disseminated from other DOD or non-DOD agencies at operational, strategic, or national levels. Collection of information about adversaries and the environment is managed through the RII collection cycle.

Commanders determine the critical information for each operation and publish those requirements through their CCIR. The commander alone decides what information is critical based on the mission, his experience, and the higher echelon commander's intent. The staff may recommend CCIR to the commander as—

- *Priority intelligence requirements* to determine what the commander wants or needs to know about the enemy, his purpose, and/or terrain *(how I see the enemy).*
- *Friendly forces information requirements (FFIR)* to allow the commander to determine the combat capabilities of his or adjacent friendly units *(how I see myself).*

- *Essential elements of friendly information (EEFI)* to allow the commander to determine how he must protect the force from the enemy's information-gathering systems *(how can I prevent the enemy force from seeing me).*

The CCIR is normally noted in paragraph 3d of the operations order/operations plan (OPORD/OPLAN). Information about friendly activities and status is coordinated through unit SOPs and OPLANs. Information is also acquired using a more general *information collection cycle* focusing on gathering relevant information from other sources and influences in the MIE. The information needs of the commander are not answered by a single source, but by—

- A combination of his own electronic systems.
- Operational activities such as reconnaissance and security.
- Human intelligence (HUMINT) activities.
- Strategic or national intelligence.
- Interface with local or international police and news media.

Information is perishable and has a temporal quality that is often controlled by a set of dynamic conditions or decisions. Events can make an item of information irrelevant or so unrepresentative as to portray a highly inaccurate picture of reality. Information beyond a certain age will detract from the commander's situational awareness. Standard operating procedures (SOPs), CCIRs, OPLANs, and collection plans must all be sensitive to perishability of information. Moreover, from a technical perspective, INFOSYS managers must respond by managing the systems and information to enable assured, timely communication and decision making.

Use

The commander is able to see his battlespace through the use of space, air, and ground systems to acquire relevant information and provide a current situation. The commander expands his thinking to include all INFOSYS and organizations accessible in the GIE. Once the data is acquired, analyzed, and collated, the information is used to update and validate a common situational awareness. This common situational awareness provides the basis to refine, continue, or adjust decisions, plans, and operations.

- Information is focused and used by issuing guidance, prioritizing assets, and establishing requirements.
- Staffs then refine the guidance into OPLANS or OPORDS. They seek to integrate information at all echelons and plan the use of all available information, regardless of the source.

The most timely, accurate, or relevant information, particularly in operations other than war (OOTW), may come from sources outside the unit or military channels. A unit must make use of both organic and nonorganic INFOSYS. Nonorganic systems are either DOD governmental or non-DOD (GIE). Use of other US Government systems, (DOD and non-DOD) is coordinated with higher commands. Using systems outside the government is more complex. Units can use some services openly and passively, such as listening to, or subscribing to, broadcast media. Units can also make overt use of services such as communications relays or weather forecasting. However, commanders must be aware of the legal and policy limits on their use of any non-DOD INFOSYS.

How the information nets within an organization are linked together can provide multiple conduits for information. Horizontal internetting of INFOSYS at the lowest possible levels provides a deeper, multidimensional picture than traditional, stovepipe reporting.

Protect

While the proliferation of information and information technology can be a great advantage, it is also a potentially significant risk that must be accounted for in every operation. Protection of soldiers and equipment, although not new, has increased in importance in today's information-rich environment. Friendly information and INFOSYS must be protected throughout the battlespace. Operationally, protecting information requires viewing friendly vulnerabilities from the enemy's C^2-attack perspective. Commanders must examine the vulnerability of their soldiers and systems to exploitation or attack by an enemy capable of attacking friendly C^2 on a wide front by employing EW, destruction, deception, and propaganda.

In order to stop or delay a weapon or system from functioning, an adversary might attack the information or INFOSYS that enable that system. For example, an adversary might introduce a malicious software code through a communications network directly into the Advanced Field Artillery Tactical Data System (AFATDS) to disrupt the sharing and distribution of combat information with other Army and joint C^2 systems. Actions taken to protect the capability to operate unconstrained in the MIE battlespace are considered part of C^2W (C^2-protect).

Information and INFOSYS must be protected at the electronic, physical, and human levels, as described in relationship to the potential threat—all without impeding the overall operation. Security programs that identify threats to C^4I systems also take on increased importance while in garrison because the porous and open nature of the GIE makes the C^4I information infrastructure vulnerable to attack or exploitation at any time. As part of planning for both battlespace and garrison operations, the signal officer analyzes the unit's information structure to prioritize critical paths, systems, and data for protection. Everything cannot be protected. Therefore, the operations officer must perform a risk management analysis to identify essential information and INFOSYS that must be kept free from disruption or corruption.

Elements of the infrastructure to be protected are data, computers, communications systems, and support facilities. Planners must integrate elements of the GIE into plans to ensure that commanders consider their impact, or potential impact in any operation. Assessment and vulnerability analysis systems must provide the timely and accurate data needed to identify and target threats and potential threats to friendly INFOSYS.

Protecting computer and communications systems from enemy intrusion, disruption, and destruction is an initial basic step in an overall protection approach. However, commanders must also be sensitive to enemy attempts at deception and propaganda. A resourceful enemy may employ propaganda to predispose a commander and his staff toward a specific course of action and then exploit that mindset with a deception operation. IO may often take place under degraded conditions. Besides adversary or accidental actions, natural phenomena may degrade or disrupt equipment or services. Because of the complexity and fragility of INFOSYS, a unit's plans should include procedures for operating without all the information infrastructure.

Exploit

Joint Pub 1-02 describes *exploitation* as "taking full advantage of any information that has come to hand for. . . military operational purposes." All information environments and systems surrounding an operation, friendly and adversarial, military and nonmilitary, offer chances for exploitation. Generally, exploiting an adversary's INFOSYS is making use of that adversary's INFOSYS data or communications without his knowledge. A flexible approach to exploitation is preferred. The level of exploitation, whether simply monitoring or corrupting data bases, depends on the situation and the desired objective. It may not always mean directly attacking or degrading an adversary's ability to C^2. Exploitation involves—

- Reading the adversary's signals.
- Intercepting communications.

- Analyzing signatures.
- Extracting from data bases.
- Establishing the order of battle.
- Taking action to deny, degrade, or manipulate those information capabilities.

Exploitation depends on a thorough understanding of the adversary and the GIE surrounding a potential AO.

Information-gathering and intelligence work must begin in peacetime to establish the analysis of the AO and how potential adversaries operate. Knowledge of the adversary's information infrastructure is as important as knowledge of a potential adversary's strategies, tactics, techniques, and procedures. Knowledge of the adversary's infrastructure will lead to an assessment of personnel, facilities, sensors, processors, and decision-making process. The assessment model asks the question: "How reliant is the adversary on the GIE for information?" This in turn affects how the unit (friendly) interacts with the GIE, to include the media, government agencies, NGOs, and foreign governments. Intelligence gained through exploitation supports C^2W planning and operations, especially deception, PSYOP, and physical destruction.

Deny

The offensive aspect of IO, *C^2-attack*, makes possible the goal of attacking an adversary simultaneously at all levels with overwhelming force. C^2-attack is intended to prevent an adversary from exercising effective C^2 of his forces by denying the adversary information or influencing, degrading, or destroying the adversary's information and INFOSYS.

IO gives the commander the means to attack an adversary throughout the depth of the battlespace, far beyond the range of direct or indirect fire systems. The goal is to degrade the adversary's confidence in either his data or his ability to command and control operations. By attacking or confusing his sense of the battlefield, friendly forces gain information dominance and a subsequent relative advantage in applying combat power or controlling a situation in OOTW.

Information denial operations generally require time and occur over relatively large areas. To blind or deafen an adversary requires that most of his major surveillance and reconnaissance systems be influenced or engaged. Therefore, attacks of adversary INFOSYS are normally planned as a series of engagements, contributing to a larger operation or higher objective. These engagements are normally conducted quickly and against a specific target, such as jamming a receiver or using the Army Tactical Missile System (ATACMS) to destroy an adversary's C^2 node.

Adversary space-based systems and UAVs pose significant problems. Because of difficulties in locating or engaging these platforms, commanders may be forced to use indirect means, such as camouflage or deception, to counter them. At echelons below corps level, the commander may lack the assets to perform all C^2-attack missions, particularly those involving battlefield deception and PSYOP. However, the value in denying an adversary effective command remains important and commanders at all levels need to be prepared to contribute to achieving that objective. Depending on METT-T, the commander might target an element of the adversary's information flow to blind him or prevent effective response. For example, by targeting RISTA, fire direction, or command nets, a commander can limit the effectiveness of an adversary's indirect fire systems.

Commanders must continually assess *exploit* and *deny* capabilities to strike an optimum balance that will achieve the greatest payoff in dominating enemy IO. Multiple attack options in IO will result from analysis and assessment of potential targets. Generally, the earlier an adversary's decision-making cycle is disrupted, the greater the effect it can have on his capabilities. It is often more effective to disrupt the adversary's early sensing or decision-making processes rather than trying to disrupt execution of a decision already made. Operational commanders must weigh the relative advantages to be gained by attacking adversary C^2 nodes

against the potential loss of intelligence from adversary signatures, radiation, or emissions and the need to protect intelligence methods and sources.

Manage

In order to conduct full-dimensional operations, information and INFOSYS require careful coordination and synchronization. With guidance issued, the staff coordinates and integrates information requirements and INFOSYS to synchronize the critical information flow with the operational concept. Management information and INFOSYS must focus on operational requirements that will derive information from reconnaissance, counterreconnaissance, communications, and security operations. Managing information includes managing the electromagnetic spectrum (EMS); deciding what sources and systems to use; ensuring a reliable flow of information between nodes and levels (horizontal and vertical integration); and resolving differences among information from multiple sources.

Operational requirements guide the management of the EMS. The principal functions using the EMS that require planning and control are—

- Communications.
- Intelligence collection.
- Jamming.
- Resolving electromagnetic interference.

This planning must be an integral part of operations planning—in many cases preceding a decision on a scheme of maneuver or fire support and definitely preceding mission execution.

Effective management of information and assets allows information to flow horizontally and vertically across BOSs to enable effective planning, preparation, decision making, and execution. Information should also flow vertically between echelons to enable concurrent planning. This serves to eliminate duplicate efforts and unnecessary redundancy, which allows systems to deal with time-sensitive, relevant information. It also reduces the signature and noise levels of units in the battlespace. The keys to this effective communications and information flow are connectivity, throughput, and resilience. Units can manage connectivity among their organic assets. The difficulty comes in maintaining horizontal and vertical connectivity outside the unit, particularly when dealing with forces using older or different communications and INFOSYS. Connectivity is accomplished through the maintenance of electronic and human links vertically and laterally outside the unit. When dealing with forces or units less technically capable, teams must be prepared to deploy with specialists or liaison personnel equipped with updated equipment.

Resilience is the ability of INFOSYS, from a technical and management perspective, to provide the necessary connectivity and continuity when INFOSYS are degraded. Additionally, Army leaders and planners must understand how military information and systems interconnect and interact with the GIE. Overreliance on commercial systems, particularly satellites and host nation telecommunications networks, may impose restrictions or limitations. Close management and consistent coordination will help assure the availability, reliability, and timeliness of C^4I assets.

Chapter 3

Operations

Commanders seek to apply overwhelming combat power to achieve victory at minimal cost. They integrate and coordinate a variety of functions with the elements of combat power to sustain it at the operational and tactical levels.

FM 100-5

C^2W, CA, and PA are interrelated operations[1] that are conducted to support the Army objective of achieving information dominance in any operational environment—combat or peace. This chapter discusses each element of C^2W and the functions of CA and PA and how they support achieving information dominance. CA and PA operations provide liaison and connectivity with essential actors and influences in the GIE and interact with specific elements of C^2W. Grouping C^2W, CA, and PA together as specific IO provides a framework to promote synergy and facilitate staff planning and execution. This idea is reinforced by including the CA and PA staff representatives in the IO cell or on the information operations battle staff (IOBS) in routine staff coordination (see Appendix D). This construct conceptually provides for greater integration and synchronization of CA and PA with the more traditional warfighting elements of C^2W.

Three specific operations contribute to gaining and maintaining information dominance:	
C^2W	Historically, the military has independently planned and executed all elements of C^2W. C^2W has a traditional warfighting orientation, both offensively and defensively, that focuses on ideas of threat, conflict, and the battlefield. An approved joint construct, C^2W employs various techniques and technologies to attack or protect a specific target set of C^2 that contributes to information dominance over any adversary or control of a situation during military OOTW.
CA	Active on the traditional battlefield but also pertinent to other operations such as peace operations or domestic support operations, CA elements perform an important connection and liaison with key actors and influences in the GIE. CA specialists help the commander shape his MIE and assist him in dealing effectively with NGOs, PVOs, and civil authorities. Through these sources, CA personnel provide valuable input that feeds the CCIR.
PA	PA help military leaders plan adequately for dealing with a very important member of the GIE—the media. The objective of PA is to ensure military operations are put in the proper context for an external audience, as well as to keep soldiers informed and protected from the effects of enemy propaganda and disinformation or sources of misinformation/rumor. The PA specialist can assist the commander in finding a good balance between OPSEC and the public's right to know about an operation.
Each of these operations can equally contribute to the success of any mission. One provides the commander a traditional warfighting capability, while the others support warfighting and provide essential links to the increasing influence of the GIE. Depending on the situation, C^2W, CA, and PA play an important role in both peace operations and combat operations. Each plays an important role in establishing and maintaining information dominance and collectively gives the commander the tools to define and control the information environment. In each situation the commander is required to balance these operations to achieve his objective.	

[1]. Joint Pub 3-13.1 states that beyond the five fundamental elements of C^2W "other capabilities in practice may be employed as part of C^2W to attack and protect." The Army recognizes that C^2W is the joint reference point for IO when working with the joint staff and other services in the realm of IW. However, the Army interprets this new paradigm more broadly and recognizes the more comprehensive integration of other information activities as fundamental to all IO; hence the term *operations*, which includes specifically C^2W, CA, and PA.

HISTORICAL PERSPECTIVE

Major emphasis was placed on C2W, CA, and PA activities during Operations Desert Shield and Desert Storm. Commanders integrated OPSEC, military deception, PSYOP, and EW efforts during Desert Shield to pave the way for successful combat operations. During planning for Desert Storm, the senior leadership recognized that Iraq's C2 was a critical vulnerability whose destruction could enable victory with minimal friendly loss. This is evident from the Secretary of Defense's guidance outlining the military objectives for Desert Storm:

- Neutralize the Iraqi national command authority's ability to direct military operations.
- Eject Iraqi armed forces from Kuwait.
- Destroy the Iraqi Republican Guard.
- Destroy Iraqi ballistic missile and nuclear, biological, and chemical warfare capabilities.
- Assist in the restoration of the legitimate government of Kuwait.

During Desert Storm's air operations, the enemy was selectively blinded by EW and physical destruction to mask friendly force movements and operations. Deception operations continued to enforce erroneous enemy perceptions of the CINC's intentions. EW and precision air strikes against C2 targets were used to disorganize and isolate Iraqi forces. When the ground attack commenced, Iraqi forces were close to disintegration, with numerous formations unable to coordinate their efforts. The need for synchronization was an early lesson learned and demonstrated immediate payoffs. Successfully denying Saddam Hussein the ability to command and control his forces substantially reduced casualties on all sides and significantly reduced the time required to achieve coalition objectives.

Fully aware that the enemy, as well as the public at home, was focused on PA coverage of the confrontation, the coalition used that coverage to confuse the enemy by encouraging speculation on the place, time, and size of the impending attack. At the same time, the coalition learned that immediacy of media attention could have unforeseen consequences for its own strategic, operational, and tactical planning. After the cessation of hostilities, CA elements enhanced the restoration of Kuwaiti governmental and social order and responded promptly and effectively to one of the central unanticipated consequences of the war as Iraqi forces created an enormous refugee crisis in the northern Kurdish provinces of Iraq and in southern Turkey.

COMMAND AND CONTROL WARFARE

To be effective, C^2W needs to be fully integrated into the commander's concept of the operation and synchronized with other operations. The synchronization of these actions will require rapid and reliable intelligence support and communications. JFCs [joint force commanders] should ensure that the C^2W objectives are part of the planning guidance and priorities.

Joint Pub 3-0

C^2W directly supports the Army goal of achieving information dominance and winning any conflict or succeeding in any OOTW quickly, decisively, and with minimum casualties. C^2W incorporates both the *sword* against an adversary's C^2 system and the *shield* against the C^2-attack actions of the adversary. This combination of both offensive and defensive aspects into an integrated capability provides expanded opportunities for synergy in warfare. C^2W allows the Army and individual commanders to accomplish missions with fewer risks, in shorter time frames, and with fewer resources.

Role of C^2W

C^2W applies to all phases of operations, including those before, during, and after actual hostilities. Even in OOTW, C^2W offers the military commander lethal and nonlethal means to achieve the assigned mission while deterring war and/or promoting peace. The offensive aspect of C^2W can slow the adversary's operational tempo, disrupt his plans and ability to focus combat power, and influence his estimate of the situation. The defensive aspects of C^2W minimize friendly C^2 system vulnerabilities and mutual interference. *C^2W* is defined as—

> The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C^2 capabilities, while protecting friendly C^2 capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.
>
> CJCSI 3210.03, 31 March 1996

C^2W Elements

The foundation for C^2W is robust and redundant command, control, communications, and computer (C^4) INFOSYS, coupled with seamless, national-to-tactical, relevant information and intelligence support. The building blocks, or elements, of C^2W include—

- OPSEC.
- Military deception.
- PSYOP.
- EW.
- Physical destruction.

These building blocks contribute to protection of the force and mission accomplishment in various ways, depending on the situation. This situation dependence leads to the building blocks that are shown in a constantly changing pattern in Figure 3-1. The integrated employment of these five elements leads to synergy on the battlefield and results in the most effective execution of C^2-attack and/or C^2-protect tasks. The commander drives this C^2W process to achieve agility by focusing attacks on the adversary's ability to command and control his forces while simultaneously protecting friendly C^2.

OPERATIONS SECURITY

Operations security is defined as—

> A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities; identifying those actions that can be observed by adversary intelligence systems; determining indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
>
> Joint Pub 3-54

OPSEC is the key to denial. It gives the commander the capability to identify those actions that can be observed by adversary intelligence systems. It can provide an awareness of the potentially friendly indicators that adversary intelligence systems might obtain. Such an awareness could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or courses of action that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate, or reduce to an acceptable level, indications and other sources of information that may be exploited by an adversary.

OPSEC planning is severely challenged by the new family of global commercial capabilities, to include imaging, positioning, and cellular systems that offer potential adversaries access to

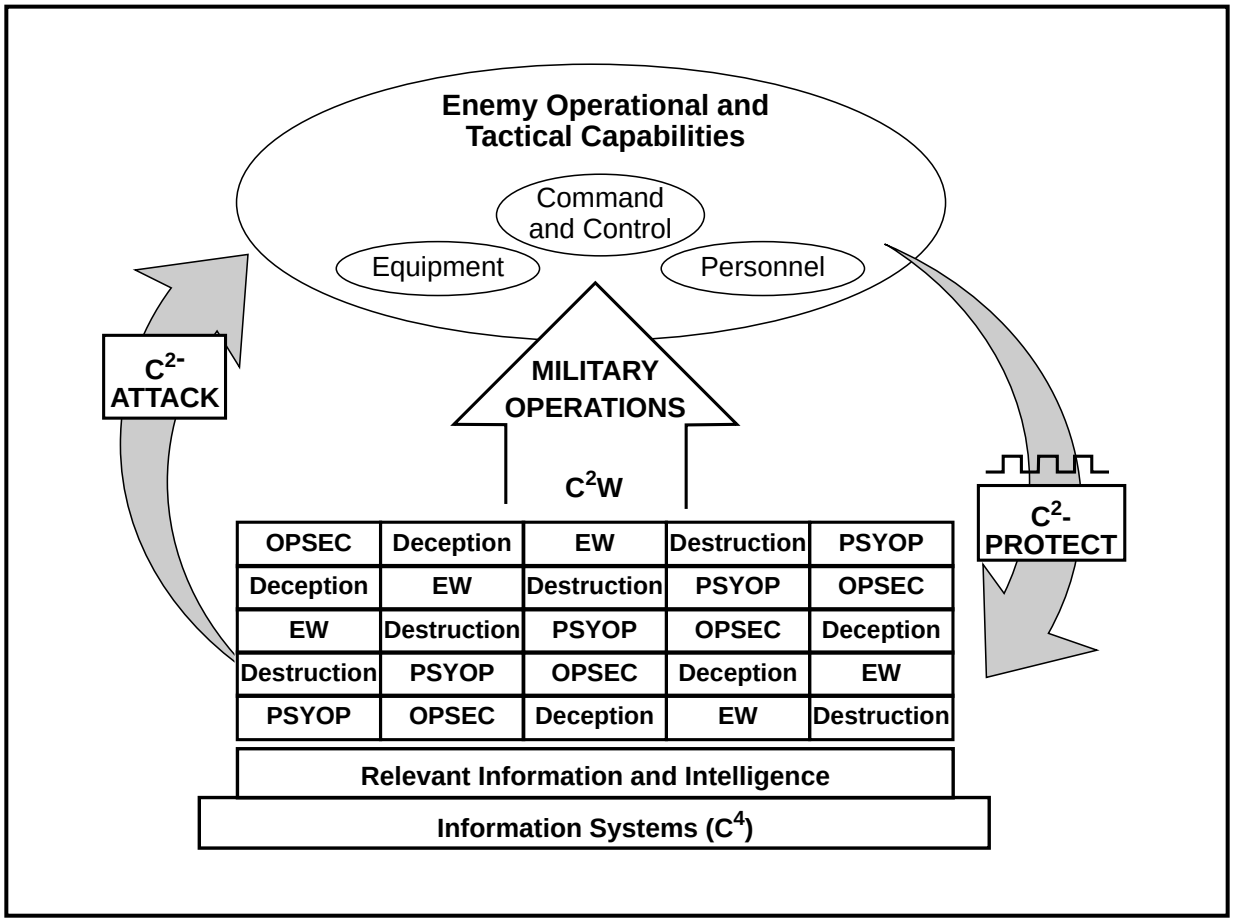

Figure 3-1. C^2W Construct

an unprecedented level of information against friendly forces. The inevitable presence of the news media during military operations complicates OPSEC. The capability of the media to transmit real-time information to a worldwide audience could be a lucrative source of information to an adversary. OPSEC planners, working closely with PA personnel, must develop the EEFI used to preclude inadvertent public disclosure of critical or sensitive information.

Many different measures impact OPSEC. These include counterintelligence, information security (INFOSEC), transmission security (TRANSEC), communications security (COMSEC), and signal security (SIGSEC). As more and more of the force is digitized, INFOSEC takes on an ever-growing importance.

MILITARY DECEPTION

Military deception is defined as—

> Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
>
> Joint Pub 3-58

Military deception is the primary means to influence the adversary commander's decisions through distortion, concealment, and/or falsification of friendly intentions, status, dispositions, capabilities, courses of action, and strengths. The goal of deception is to cause the opposing military commander to act in a manner that serves the friendly commander's objectives.

Historical Perspective

Tactical deception had significant positive impacts on the success of Operation Overlord, and, thus the retaking of the European continent in World War II. Deception worked hand in hand with OPSEC to keep the organization and location of the real Overlord cantonments, training sites, dumps, movements, and embarkations carefully hidden. Unbelievable effort was put into creating mock airfields and ports, phony ships, boats, planes, tanks, vehicles, and troop movements, both real and staged. A new era of deception was introduced—the electronic one. German coastal defense radars were destroyed in a calculated pattern. Deception planners purposely left some intact in the Calais region.

The night the invasion was launched, the Allies began massively jamming German radars with chaff. But they purposely did not completely cover their targets. German radar operators could "see" between Allied jamming curtains. And, what they saw was a ghost fleet of small ships towing barges and blimps headed for Calais at eight knots—or the speed of an amphibious fleet. Powerful electronic emitters received the pulse of the German radar and sent it strongly back to the German receivers. For each repetition of this deception it looked to the German operators like a 10,000-ton ship was out there. The small ships also had the recorded sounds of the amphibious assault at Salerno to play over speakers from 10 miles out. German troops ashore could hear the Allies "getting into their landing craft" for the run into the beach. This information threw German intelligence into chaos for several precious hours and played a major role in delaying German counteractions to the actual invasion taking place at Normandy.

PSYCHOLOGICAL OPERATIONS

Psychological operations are defined as—

> Operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.
>
> Joint Pub 3-53

PSYOP are based on projection of truth and credible message. PSYOP are an essential tool in both C^2-protect and C^2-attack operations. The Army has shown considerable strength in applying both PSYOP and deception to military operations. PSYOP can proliferate discrete messages to adversary C^4I collectors, enhance joint combat power demonstrations with surrender appeals, and magnify the image of US technological superiority. PSYOP elements must work closely with other C^2W elements and PA strategists to maximize the advantage of IO. As an example, the Army has shown considerable strength in applying both PSYOP and deception to military operations.

PSYOP's main objective in C^2-protect is to minimize the effects of an adversary's hostile propaganda and disinformation campaign against US forces. Discrediting adversary propaganda or misinformation against the operations of US/coalition forces is critical to maintaining favorable public opinion.

As an early commander of Combined Task Force Provide Comfort, it is my belief that much of the success achieved during Operation Provide Comfort can be attributed to the successful integration of PSYOP in support of the overall humanitarian assistance mission. Over five million PSYOP products were dispersed over northern Iraq and southeastern Turkey in support of the Operation's goals and objectives. PSYOP is a true force multiplier."

General John M. Shalikashvili

ELECTRONIC WARFARE

Electronic warfare is defined as—

> Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

Electronic Attack

EA is the use of jamming, electronic deception, or directed energy to degrade, exploit, or destroy the adversary's use of the EMS. EA can attack the adversary anywhere—from his tactical formations, back to his national infrastructure.

Electronic Protection

EP is the protection of the friendly use of the EMS. EP covers the gamut of personnel, equipment, and facilities. EP is part of survivability. As an example, self and area protection systems can interfere with the adversary's target acquisition and engagement systems to prevent destruction of friendly systems and forces.

Electronic Warfare Support

ES is conflict-related information that involves actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy to detect immediate threats. ES is the embodiment of combat information and capitalizes on the timeliness of sensor-to-shooter systems.

PHYSICAL DESTRUCTION

Physical destruction is defined as—

> The application of combat power to destroy or neutralize enemy forces and installations. It includes direct and indirect fires from ground, sea, and air forces. Also included are direct actions by special operations forces.

The destruction of a hostile C^2 target means that adversary C^2 capabilities are degraded for a period of time or, if necessary, permanently shut down. Physical destruction is used only after a full, comparative assessment—strategic-through-tactical perspectives—of the trade-offs between preserving the target versus its destruction.

Historical Perspective

On April 14, 1943, US intelligence experts intercepted and decoded a message revealing that Admiral Isoroku Yamamoto, Commander-in-Chief of Japan's Navy, would be flying to Bougainville in four days. When analysis determined that Bougainville lay just within the extended range of US P-38 fighters at Henderson Field on Guadalcanal, Allied planners recognized the opportunity to strike at the heart of Japanese command and control and strategic planning in the Pacific.

In less than 48 hours, Admiral Chester W. Nimitz's forces planned and coordinated an operation to shoot down Yamamoto's plane and obtained approval from Secretary of the Navy Frank Knox and President Roosevelt.

Yamamoto was known to be invariably punctual, and American planners were confident that his plane would appear over Bougainville on schedule—9:39 am, April 18. At that moment, 16 carefully positioned P-38s from Henderson Field spotted the two Japanese *Betty* bombers of Yamamoto's party and attacked.

Both aircraft were quickly sent plummeting to the ground, completing a classic information operation that took less than four days from start to finish and rendered irreparable damage to Japanese command and control. The Japanese would feel the impact of this single mission throughout the remainder of the war.

C^2W Disciplines

The two disciplines that comprise C^2W are *C^2-attack* and *C^2-protect.*

C^2-ATTACK

C^2-attack is defined as—

> The synchronized execution of actions taken to accomplish established objectives that prevent effective C^2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C^2 system.

C^2-Attack Principles

The three principles of C^2-attack are to—

- Plan based on the unit's mission, commander's intent, and concept of operations.
- Synchronize with and support the commander's plan.
- Take and hold the initiative by degrading the adversary's INFOSYS and forcing the adversary to be reactive. *Reactive* means that C^2-attack slows the adversary's tempo, disrupts the adversary's planning and decision cycles, disrupts the adversary commander's ability to generate combat power, and degrades the adversary commander's means for executing mission orders and controlling subordinate unit operations.

Figures 3-2 and 3-3 illustrate some of the potential relationships between the elements of C^2W.

C^2-Attack Effects

In general terms, C^2-attack has four effects that focus on the adversary's C^2 infrastructure and information flow to produce a lower quality and slower decision-making process.

- First, the adversary is denied information by disrupting his observation, degrading his orientation and decision formulation, and degrading information collection. Information collection can be degraded by destroying collection means, by influencing the information the adversary gets, or by causing the adversary not to collect at all.
- Second, the adversary commander is influenced by manipulating perception and causing disorientation of his decision cycle.
- Third, adversary IO are degraded by selectively disrupting C^4I systems.
- Fourth, adversary information capabilities can be neutralized or destroyed by physical destruction of nodes and links. Destruction operations are most effective when timed to occur just before the adversary needs a certain C^2 function or when focused on a target that is resource-intensive and hard to reconstitute.

Historical Perspective

Heraclitus of Ephesus in sixth century BC noted that "if you do not expect the unexpected, you will not find it." During the German invasion of the Soviet Union in June 1941, the Germans recognized, but the Russians did not, exploitable deficiencies in the existing Soviet C^2 system. Employing the tools of C^2W in an interrelated fashion, the Germans were able to effectively disrupt, exploit, and destroy the Soviet C^2 system. Using weapons specifically built for C^2W, the Germans attacked elements of the Soviet system by air, artillery, and sabotage. The results of these attacks were startling. Due to cross-border German sabotage efforts, many of the Soviet units "did not receive the war alert order when it was issued [from Moscow] on the night of 20-21 June 1941." By 24 June, large gaps had already been torn in the Soviet communications network, thus forcing commanders to rely on easily exploitable, unprotected, radio networks. This, in turn, led to the successful targeting of exposed command posts and associated units throughout the theater. These attacks, because of their effectiveness, led Soviet commanders to prohibit the use of radios because they might give positions away. Using C^2W, the Germans had effectively shut down the Soviet C^2 system, creating an operational environment that quickly led to a general collapse of the entire eastern front.

	OPSEC	MILITARY DECEPTION	PSYOP	PHYSICAL DESTRUCTION	EW
OPSEC can support by–		• Concealing competing observables • Degrading general situation information to enhance effect of observables	• Concealing competing information • Degrading general situation information to enhance effect of PSYOP	• Concealing dedicated systems for C^2-attack to deny information on extent of C^2-attack destruction capabilities	• Concealing EW units and systems to deny information on extent of EA/ES capabilities
Military Deception can support by–	• Influencing adversary not to collect against protected units/ activities • Influencing adversary to underestimate friendly OPSEC • Providing information to fill "gaps" created by friendly OPSEC		• Providing information compatible with PSYOP theme • Reinforcing PSYOP theme in content of deception information	Influencing adversary to– • Underestimate friendly C^2-attack destruction capabilities • Defend wrong C^2 elements/systems from friendly RISTA destruction	Influencing adversary to– • Underestimate friendly EA/ES capabilities • Defend wrong C^2 systems from friendly EA/ES
PSYOP can support by–	• Projecting information in OOTW • Creating perceptions that fit OPSEC activities	• Creating perceptions and attitudes that can be exploited by military deception • Integrating PSYOP actions with deception		• Causing populace to flee targeted areas • Reducing collateral damage limitations on destruction of adversary C^2 infrastructure	• Broadcasting PSYOP assets to disseminate products on adversary frequencies • Developing messages for broadcast on other service EW assets (AC-130)
Physical Destruction can support by–	• Preventing or degrading adversary reconnaissance and surveillance against protected units and activities	• Conducting physical attacks as deceptive executions • Degrading adversary capabilities to see, report, and process competing observables • Isolating decision maker from information at critical times to enhance effect of deception execution	• Degrading adversary capability to see, report, and process conflicting information • Degrading adversary capability to jam PSYOP broadcasts • Isolating target audience from conflicting information		• Reducing friendly EA target set for C^2-attack by selective and coordinated destruction of adversary C^2 infrastructure targets • Destroying selected electronic systems to force adversary use of systems susceptible to friendly EA/ES
EW can support by–	• Degrading adversary reconnaissance and surveillance in EMS against protected units and activities • Covering short-term "gaps" in OPSEC	• Conducting EA/ES as deceptive executions • Degrading adversary capability to see, report, and process competing observables • Isolating decision maker from information at critical times to enhance effect of deception executions	• Degrading adversary capability to see, report, and process conflicting information • Isolating target audience from conflicting information	• Providing C^2-attack target acquisition through ES • Destroying or upsetting susceptible assets using EMS with EA	

Figure 3-2. Mutual Support Within the Elements of C^2W

	OPSEC	MILITARY DECEPTION	PSYOP	PHYSICAL DESTRUCTION	EW
OPSEC Conflicts		• OPSEC requirements may limit information that can be revealed to enhance credibility of the deception story	• OPSEC requirements may limit information that can be revealed to develop PSYOP themes		
Military Deception Conflicts	• Deception story and associated executions may need to reveal information that OPSEC normally seeks to deny		• Deception story may limit selection of PSYOP themes • Deception story may limit information that can be revealed to develop PSYOP themes	• Deception executions may limit destructive targeting of the adversary C^2 infrastructure to allow survival and conduct of critical adversary C^2 functions	• Deception executions requiring EMS may limit EA targeting of the adversary C^2 infrastructure to allow survival and conduct of critical adversary C^2 functions
PSYOP Conflicts	• PSYOP may need to reveal information that OPSEC normally seeks to deny (especially in OOTW)	• PSYOP themes may limit selection of deception story • PSYOP may be limited by untruths in deception story	• Requires national policy	• PSYOP activities may limit destructive targeting of the adversary C^2 infrastructure to allow PSYOP themes to be conveyed	• PSYOP activities requiring EMS may limit EA against selected adversary communications frequencies to allow PSYOP themes to be conveyed
Physical Destruction Conflicts		• Physical destruction may limit the selection of deception execution by denying or degrading elements of the adversary C^2 infrastructure necessary to the deception	• Physical destruction may limit the selection of means to convey PSYOP themes by denying or degrading elements of the adversary C^2 infrastructure necessary to convey PSYOP messages		• Physical destruction may limit opportunities for communications intrusion by denying or degrading elements of the adversary C^2 infrastructure necessary to communications intrusion
EW Conflicts		• EA may limit the selection of deception executions by denying or degrading the use of certain electronic systems in the adversary C^2 system	• EA may limit the selection of means to convey PSYOP themes by denying or degrading the use of certain adversary or target audience communications frequencies	• EA activities may limit destructive targeting of the adversary C^2 infrastructure to allow PSYOP themes to be conveyed	

Figure 3-3. Potential Conflicts Within C^2-Attack

C^2-PROTECT

C^2-protect is defined as—

> The maintenance of effective C^2 of ones own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C^2 system.

C^2-protect can be offensive or defensive. Offensive C^2-protect uses the five elements of C^2W to reduce the adversary's ability to conduct C^2-attack. Defensive C^2-protect reduces friendly C^2 vulnerabilities to adversary C^2-attack by employing adequate physical, electronic, and intelligence protection.

C^2-Protect Principles

The C^2-protect process can best be understood by reverse engineering our C^2-attack process. Commanders ask how the adversary can employ destruction, EW, military deception, OPSEC, and PSYOP to disrupt our C^2 systems and decision-making process. Having wargamed the adversary's C^2-attack courses of action, the commander can develop a comprehensive protect operation, synchronized with the main effort and C^2-attack. The commander is guided by the five principles of C^2-protect.

- To gain C^2 superiority. This principle includes functions such as the unimpeded friendly processing of information, accurate development of courses of action, valid decision making, and efficient communications to and from subordinates.
- To stay inside the adversary's decision cycle. This is done by denying, influencing, degrading, and/or destroying the adversary's C^2 personnel, equipment, and systems.
- To reduce the adversary's ability to conduct C^2-attack.
- To reduce friendly C^2 vulnerabilities using C^2-protect measures. As an example, countering the effects of adversary propaganda or misinformation through PSYOP and PA.
- To reduce friendly interference in our C^2 systems throughout the EMS (deconfliction and coordination).

Historical Perspective

The history of the Information Age is being made now. In 1988 we saw the first well-publicized case of a computer virus. This insidious, self-replicating virus known as the *Internet Worm* penetrated the computer system at the University of California at Berkeley, corrupting thousands of computers on the internet. A computer emergency response team (CERT) had been created at Carnegie Mellon University. In 1993 they had their first large event as they put out a warning to network administrators that a band of intruders had stolen tens of thousands of internet passwords.

When CERT began in the late 1980s, they processed less than 50 events per year. Now they are in the thousands per year. The military is a target of this attack. Recent stories have told of a 16-year-old who compromised the security of more than 30 military systems and more than 100 other systems before he was caught after a 26-day international electronic manhunt. This experience hints at the impact a professional, well-financed effort could have against computer nets. The lesson this evolving history is showing us vividly today is that the information highway is creating a great vulnerability to US forces. We are all familiar with the security of transmitting information over a radio or telephone. But there is an even greater weak spot now in computers, data bases, software (such as decision-making aids and tools), servers, routers, and switches. This vulnerability exists today and is growing in geometric proportions.

C^2-Protect Effects

The effects of C^2-protect mirror those of C^2-attack. We can deny information the adversary needs to take effective action. We can influence the adversary not to take action, to take the wrong action, or to take action at the wrong time. We can degrade and destroy his capabilities to perform C^2-attack against friendly forces. PSYOP and PA supports C^2-protect. PSYOP can drive a wedge between the adversary leadership and its populace to undermine the adversary leadership's confidence and effectiveness. The Commander's Internal Information Program

(formerly the Command Information Program), publicized by the PAO, can be extremely beneficial in countering adversary propaganda in the US and among the deployed forces. PA specialists, working with PSYOP and intelligence personnel, can also develop information products that commanders can use to help protect soldiers against the effects of adversary disinformation or misinformation.

CIVIL AFFAIRS OPERATIONS

CA activities encompass the relationship between military forces, civil authorities, and people in a friendly or foreign country or area. CA activities support national policy and implement US national objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in operational areas. CA secures local acceptance of and support for US forces. CA is important to gain information dominance because of its ability to interface with key organizations and individuals in the GIE; for example, CA's traditional relationship with NGOs and PVOs such as the International Committee of the Red Cross.

Commanders fully integrate civil-military operations (CMO) into all operations and use CMO to influence, coordinate, control, or develop civilian activities and civil organizations. CA activities play a command support role in all operational environments and across the operational continuum. However, CA operations are most common when supporting the lower end of the operational spectrum.

Functional Specialties

Many CA activities require specific civilian skills. CA activities most relevant to the GIE and supporting IO are categorized into four major sections:

GOVERNMENT SECTION

Public administration provides liaison to the civilian government.

ECONOMIC SECTION

Economics and commerce monitors government economic and commercial agencies, normally only in a civil administration mission.

PUBLIC FACILITIES SECTION

Public communications allocates civilian communications resources for civilian and military use and directs civil communications agencies as required, normally only in a civil administration mission.

SPECIAL FUNCTIONS SECTION

Civil information advises, assists, supervises, controls, or operates civil information agencies and provides TV, radio, or newspaper services.

Collection Activities

The nature of CA activities and the need for CA personnel to develop and maintain a close relationship with the civilian populace puts them in a favorable position to collect information. CA information collection activities encompass the complete spectrum of cultural, social, political, and economic issues within the present or potential area of operations. In their daily operations, CA personnel deal with people, equipment, and documents that are prime sources of information. Information collected is often important to other units' staff sections or agencies and supports the CCIR.

Information Sources

CA units are included in the information collection plan of the supported unit. CA units report information that meets the criteria of the supported unit's collection plan. Prime sources of information available to CA units include, but are not limited to—

- Civilians who were housed with, catered to, or associated with enemy personnel.
- Dislocated civilians and other personnel participating in movement control, relief, or other assistance (normally referred to appropriate intelligence personnel).
- Government documents, libraries, or archives.
- Files of newspapers or periodicals.
- Industrial and commercial records.
- Technical equipment, blueprints, plans, or information of interest related to transportation, signal, engineer, and medical fields.

Relationships

The information collected can supplement the intelligence effort. US forces need timely and accurate information and intelligence to plan missions, secure the element of surprise, identify and develop targets, and protect US interests across the operational continuum. CA activities are closely tied to the intelligence functions and operations associated with the overall tactical mission.

CA personnel are not, and must not have the appearance of being, intelligence agents. The mission of the unit drives the intelligence cycle. As operational planning begins, so does intelligence planning. Requirements for operational planning are normally for finished intelligence studies, estimates, or briefings. CA planners prepare their estimates from basic intelligence documents that are not primarily written for CA use, such as an area study. Intelligence is the product resulting from the collection, evaluation, and processing of information.

Overall, CA elements collect information that the G2/J2 turns into intelligence. CA forces, if used correctly, can complement the intelligence collection process, especially HUMINT. In some cases, CA elements can also enhance the capabilities of technical intelligence (TECHINT) or intelligence concerning foreign technological development that may have eventual application for military use.

Coordination and Support

All CA activities require close coordination with military forces, US and foreign government agencies, and nonmilitary agencies with a vested interest in military operations. CA planners must consider all available support to ensure successful completion of the CA mission. In most cases, CA planners directly or indirectly support the agencies assigned by law to carry out national policy. CA planning is a command responsibility. It must be coordinated, at a minimum, with all other staff planners. To ensure success, coordination and cooperation with the following are vital to the conduct of all operations: other US staffs and units, host nation military, coalition military, US Government, foreign governments, international agencies, PVOs, and NGOs.

GOVERNMENT AGENCIES

Effective CA activities require close contact between the US military, the Department of State (DOS), and other US Government agencies. Because DOS formulates and implements foreign policy, it has a vested interest in CA activities. In the area of CA, DOS has primary or joint responsibility with DOD for policy. Some examples are matters involving PSYOP, PA, CA, civil information, or other measures to influence the attitude of the populace and plans for turning CA activities over to civilian control at the end of hostilities.

PVOs AND NGOs

The list of PVOs and NGOs that may be found in an AO could be very large. Approximately 350 agencies capable of conducting some form of humanitarian relief operation are registered with the USAID. Commanders must consider the presence and capabilities of PVOs and NGOs and, when appropriate, coordinate and cooperate with their efforts. Because many of these organizations may have been established in the AO in advance of the Army's presence, they may be a good source of information and knowledge.

CA, PSYOP, AND PA ELEMENTS

CA, PSYOP, and PA elements are able to use the same communications media with essentially the same messages but to different audiences. CA and PSYOP personnel address local populations and enemy forces, respectively, while PA personnel address US forces and national and international news media. Popular American public support contributes to the success of CA. CA and PSYOP personnel provide news and information to the local populace on the effects of combat operations.

CIVIL-MILITARY OPERATIONS CENTER

Commanders can establish a CMOC to perform liaison and coordination between the military PVOs and NGOs, as well as other agencies and local authorities. Figure 3-4 illustrates additional GIE players that may interact with the CMOC. Relationships with nonmilitary agencies are based on mutual respect, communication, and standardization of support. NGOs and PVOs have valid missions and concerns, which at times may complicate the mission of US forces. As an example, liaison with an organization that is caring for the sick and injured of the local populace may reveal that human rights abuses are occurring. This information could provoke a response by DOS officials to warn local authorities to stop such abuse from happening, as well as increasing the level of protection for the local population by US forces.

STAFF

CA operations must be integrated into the battle plan, to include providing for timely and accurate reporting of the operation and combating distorted or disinformation disseminated by the adversary. The CA representative to the IOBS—

- Represents CA concerns in IO.
- Coordinates with PA and PSYOP representatives to ensure consistency of messages and OPSEC without compromising CA credibility.
- Prepares CA estimates, assessments, and the annex to the OPLAN/OPORD to identify and integrate CA support.
- Coordinates the use of local resources, facilities, and support. Examples include civilian labor, transportation, communications, maintenance, or medical facilities, and miscellaneous services and supplies.
- Provides liaison to local agencies and civilian authorities.
- Advises on cultural and moral considerations.

In concert with the G2/J2 and chief of staff, the CA staff officer (G5/J5) controls, coordinates, and integrates the CA effort at each echelon. One essential function is to prepare and issue a CA annex as part of the unit's OPORDs or OPLANs. See Appendix A, Annex A.

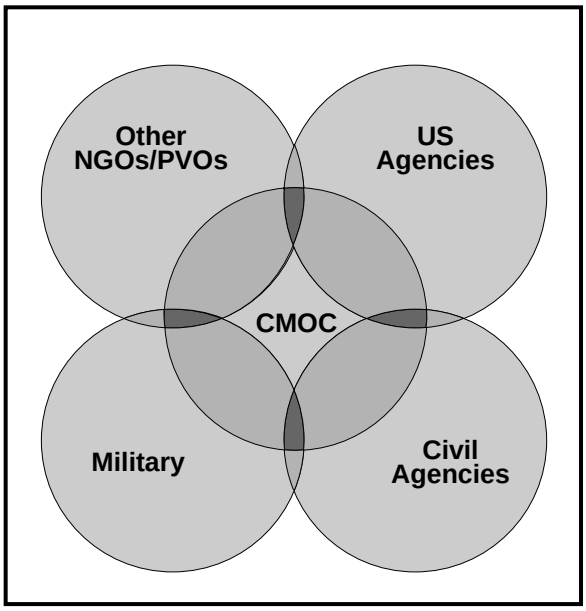

Figure 3-4. Additional GIE Players

Historical Perspective

In the early spring of 1991, in the aftermath of its humiliating defeat at the hands of US-led coalition forces, the Iraqi Army launched a violent attack against the Kurdish minority in northern Iraq. More than half a million refugees fled across the border into southeastern Turkey. Huddling on exposed mountainsides, they promptly began to become ill and die from starvation, exposure to the bitter cold, and various diseases. The world press reported that over a thousand Kurds, especially children and the elderly, were dying each day.

On April 5, President Bush directed US military forces to "stop the dying." Lieutenant General John M. Shalikashvili, then deputy commander of US Army Europe, was placed in command of the coalition task force Provide Comfort. Elements of several CA units, active and reserve, were redeployed from the Persian Gulf or deployed from Fort Bragg to Turkey under the 353d Civil Affairs Command (USAR), Bronx, New York.

In Turkey, the CA soldiers joined with 10th Special Forces Group to aid overwhelmed relief workers already on the scene. The latter included personnel from the United Nations High Commissioner for Refugees, the US Department of State Office of Foreign Disaster Relief, the Turkish Red Crescent, and more than 40 different civilian humanitarian relief organizations, all of which were attempting to care for the Kurds in 40 or more scattered locations. Shalikashvili's greatest problem became coordinating all the organizations' efforts with the US Air Force—the primary means for transporting emergency supplies into the region.

At US European Command Headquarters in Stuttgart, Germany, an Army Reserve CA captain with the 353d saw a possible solution. The captain, a software engineer in civilian life, joined with three other CA reservists in an intensive three-week effort, first in Stuttgart and later at Incirlik Air Base, Turkey, to design and implement a unique relief supply data base. Their program, later named the Disaster Assistance Logistics Information System (DALIS), combined key data from agencies on the type of aid arriving, storage locations, and intended destinations. DALIS allowed planners to coordinate efforts and deliver the right supplies to the right locations at the right time. These innovative soldiers used the power of the microprocessor to unscramble what threatened to be a logistical, diplomatic, and humanitarian nightmare. By combining data from multiple sources, they provided vital information that reduced redundancy and avoided maldistribution of resources at a critical moment, saving thousands of lives. Using IO, CA soldiers became masters of the situation and made a decisive contribution to the success of Provide Comfort.

PUBLIC AFFAIRS OPERATIONS

Public affairs must be integrated with other battlefield functions to achieve the desired effect of an accurate, balanced, credible presentation of information that leads to confidence in force and the operation

FM 46-1

PA fulfills the commander's obligation to keep the American people and the soldiers informed. PA operations help establish the conditions that lead to confidence in America's Army and its readiness to conduct operations. Army operations are of interest to the public and subject to being covered by the media. PA is therefore a function that supports both combat and noncombat operations and contributes to success in war and other military operations.

Missions

The inherent challenge is for commanders to understand the dynamics of media coverage. The media can potentially have a quick and pervasive impact on their plans and operations. Its coverage of the development of plans and the conduct of operations may impact and influence strategic decisions in a more profound and immediate way than in the past. PA operations enable commanders to effectively operate with the media. Commanders must also have a better appreciation for the immediacy of media coverage such as personal interviews, live versus taped reports, film versus written dispatches, methods of transmission, and so on.

The commander's information needs are not answered by a single source, but by a combination of many systems and functions, including the news media. The advances in information technology provide potential adversaries with the capability to exploit (deny, distort, degrade, or destroy) information. The PAO must have the capability to monitor the national and international media and identify and assess information relevant to the operation.

The missions of PA, PSYOP, and CA involve communicating information to critical audiences to influence their understanding and perception of the operation. Information communication must be fully coordinated to eliminate unnecessary duplication of effort and ensure unity of purpose. Planning for these operations must be synchronized, and the messages they communicate must be truthful and mutually supportive to ensure that credibility is not undermined and mission success is achieved

The PAO's support to the commander is multidimensional. The PAO advises the commander on media relations and the PA implications of current and future operations and events. He serves as the official command spokesperson and implements the Commander's Internal Information Program. PA focuses on achieving an accurate, balanced, and credible presentation of timely information that communicates the commanders perspective to enhance confidence in the force and the operation. It provides the critical battlefield function of media facilitation by serving as the interface between the media and the force.

With the broad scope and initiative given to soldiers and units today at every level, one of the primary tools the commander uses is the internal information program. Well-informed soldiers are likely to have higher morale and perform better. Soldiers need and want information from both external and internal sources and are interested in the public perception of an operation. Therefore, PA operations use various communication methods and channels to make this information available to soldiers, other Army audiences, and external audiences. The broad range of missions the Army executes today are done in an environment of global visibility. Media coverage can be pivotal to the success of the operation and achieving national strategic goals.

Impact of Change

Every aspect of every operation may be an issue of interest to the media and consequently to the public. Existing and emerging technology puts military operations onto the global stage, often in real time. Soldier actions can induce public reactions, which in turn causes NCA reactions that impact operations without ever engaging US forces. For example, real-time or near real-time reports of the actions of a soldier manning a roadblock, the results of a minor skirmish, or the effects of a major combat action become the subject of discussion. Media personalities, politicians, pundits, critics, academics, and the general public rapidly form positions and opinions, often in pursuit of agendas well beyond the scope and purpose of the operation being reported. They become active participants in the international public debate of events and issues.

Adversaries can also attack the *public opinion center of gravity* and affect operations without ever engaging US forces. All Army operations can be influenced through planned or inadvertent messages communicated via the GIE. PA and the associated GIE addresses simultaneous effects that are integral to all levels of war (Figure 3-5). In the Information Age, the

old separation of public information and internal information activities are compressed.

Providing accurate, timely news, information, and entertainment reduces distractions, rumors, fear, and confusion that could cause stress and undermine efficient operations. Such activities contribute to team building, morale, and unit cohesion. They enhance soldier confidence and understanding. They contribute to ethical behavior, respect for the law of war, private property, the rights of civilians and noncombatants, and human dignity.

Tactical	Operational	Strategic
Escort and support media	Reports from media on both sides of conflict	Public support
Live interviews	Instantaneous coverage and analysis	International opinion
Daily report from front line	Coalition support	Political support
Split-based internal information program	Operational security	Soldier and family morale

Figure 3-5. Multiple Levels of Public Affairs

Coordination and Support

PA is a battlefield function and has a direct impact on the conduct of operations. It must be fully integrated into the planning process at all levels and across the full continuum of operations. A member of the PA staff serves on the IOBS (see Appendix D). The PA representative assesses media presence, capabilities, information needs and interests, and content analysis of both traditional media and electronic forums such as those on the internet and electronic bulletin board.

Finally, PA operations must be integrated into the battle plan, to include providing for the timely and accurate reporting of the operation, combating distorted or disinformation disseminated by the adversary. The PA representative to the IOBS—

- Represents PA concerns in IO.
- Identifies, assesses, and advises the commander on information and issues with PA implications.
- Reviews strategic and operational information with PA implications such as events, missions, and propaganda.
- Coordinates with CA and PSYOP representatives to ensure consistency of messages and OPSEC without compromising PA credibility.
- Facilitates availability of battlefield information for PA purposes, for example, releasable visual imagery used to inform the public of Army capabilities and accomplishments.

PA is integrated into the OPLAN/OPORD through the PA Annex. Appendix A, Annex A provides the information to implement PA media facilitation, news, information provisions, and force training operations. This annex is coordinated with all staff agencies, especially those that significantly impact the information environment, that is, PSYOP, CA, signal, military intelligence, to ensure that PA activities are synchronized with other activities.

Historical Perspective

At 1800 hours local (Riyadh) on 27 February 1991, the Gulf War CINCCENT and ARCENT commanders agreed that in all likelihood no more than 24 hours of battle remained. At 2100 hours during a briefing for the press corps telecast live around the world, the CINCCENT reflected that opinion and indicated that coalition forces would be pleased to stop fighting when so ordered. The time of the briefing in CONUS (1300 hours EST) ensured a wide audience, including the President of the United States, for at least a portion. Reacting to the briefing, the President and the Chairman of the Joint Chiefs of Staff (CJCS) conferred, and the CJCS called Riyadh from the Oval Office, indicating the President's wish to stop the offensive as soon as practicable. The CINC called his component commanders, stating that the NCA was considering a cease-fire at 0500 (local) on 28 February.

Meanwhile, VII Corps had prepared a double envelopment movement, passing 1st Cavalry Division around to the north of 1st Armored Division, to crush what remained of the Iraqi Republican Guard. The corps intended to execute the double envelopment beginning at 0500 on the 28th. In accordance with an ARCENT warning order concerning the cease-fire, however, VII Corps units assumed a local security posture, focusing on force protection. An ARCENT frag order, published at 0200 and titled "Potential Temporary Cease-Fire," reiterated the 0500 implementation time.

At 0300, CENTCOM notified ARCENT that the President had set 1200 am eastern standard time on 28 February (0800 hours local) as the beginning of the cease-fire time and urged the Army component to inflict the greatest possible damage on the enemy before that hour. Accordingly, ARCENT published a new FRAG order at 0330, calling for the resumption of offensive operations. At 0406, the VII Corps commander ordered his division commanders to execute the double envelopment with a new departure time of 0600, being mindful of the 0800 cease-fire. Difficulties inherent in reordering battle and executing the mission for maximum gain over the next four hours led to confused communications, misunderstood commander's intent, and postwar questions over operational and tactical execution.

In the space of 11 hours, a press conference that included unguarded opinions about the past and future course of a war profoundly affected the strategic, operational, and tactical levels of that war. Commanders on the front lines were neither informed nor consulted on the intent of the public briefing, either before or after it had taken place. The ubiquitousness and immediacy of press reportage effectively erased boundaries between national and theater command authorities and dramatically compressed the time between strategic decision and operational consequences.

	C^2W	CIVIL AFFAIRS	PUBLIC AFFAIRS
C^2W can support by:		• Influencing/informing populace of CA activities and support. • Neutralizing disinformation and hostile propaganda directed against civil authorities. • Controlling EMS for legitimate communication purposes. • Providing myriad of information products to assist CA efforts.	• Conducting counterpropaganda and protection from misinformation/rumor. • Developing EEFI to preclude inadvertent public disclosure. • Synchronizing PSYOP and OPSEC with PA strategy.
Civil Affairs can support by:	• Providing information to support information infrastructure picture. • Synchronizing communications media and message with PSYOP. • Coordinating C^2 target sets with target cell. • Establishing and maintaining liaison or dialogue with indigenous personnel, NGOs, or PVOs.		• Providing information on CMOC activities to support PA strategy. • Synchronizing information communications media and message. • Identifying, coordinating, and integrating media and public information HNS.
Public Affairs can support by:	• Developing information products to protect soldiers against the effects of disinformation or misinformation. • Coordinating with PSYOP planners to ensure consistent message and maintain OPSEC.	• Producing accurate, timely, and balanced information for the public. • Coordinating with CA specialists to verify facts and validity of information	

Figure 3-6. Mutually Supported Roles of C^2W, Civil Affairs, and Public Affairs

Chapter 4

Relevant Information and Intelligence

In modern battle, the magnitude of available information challenges leaders at all levels. Ultimately, they must assimilate thousands of bits of information to visualize the battlefield, assess the situation, and direct the military action required to achieve victory.

FM 100-5

This chapter sets the doctrinal foundation for the role of relevant information and intelligence in IO. The chapter discusses the need for relevant information, the criteria to carefully assess such information, and the commander's decision and execution cycle. It also includes information on the role of intelligence in framing relevant information about the adversary.

RELEVANT INFORMATION

Relevant information is defined as—

> Information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand.

Relevant information has a direct relationship with the MIE in two important ways:

- One, the act of collecting, processing, or disseminating relevant information serves as the principal criteria a commander applies, to include an individual, organization, or system as part of the MIE.
- Two, it is the product or medium drawn from or used by those same players that serves as the basis or *currency* of IO. See Figure 4-1.

In the past the Army has tended to approach the collection and use of operational information from a *specialized* perspective. For example, different BOS elements have collected and used information necessary to support their particular functions, such as—

- Intelligence focused upon information about the adversary and foreign nations.
- Operators focused on situational information concerning friendly forces.
- Logisticians focused on friendly force sustainment conditions and requirements.
- PA and CA focused on the interface between military and nonmilitary sectors.

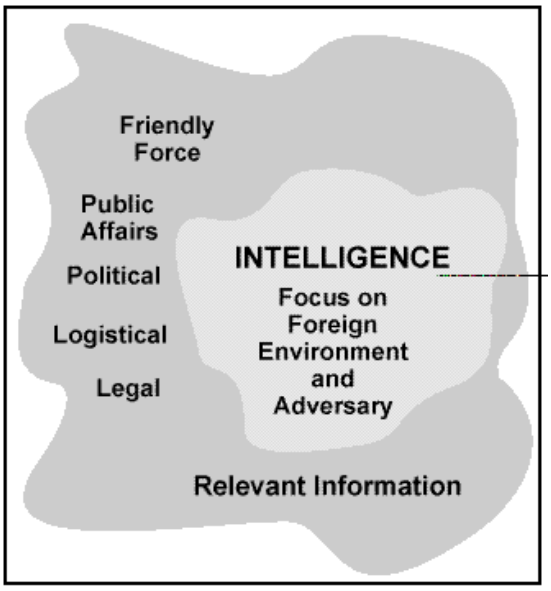

Figure 4-1. Relevant Information

Only a limited amount of such information was shared and that at relatively high levels within the military organizational hierarchy. Information flowed up and down *stovepipes* with routines that tended to slow the sharing of information across organizational boundaries. Relatively little effort was focused upon the systematic integration or synchronization of information. Normally, numerous specialized, noninteractive data bases were developed and maintained to meet the needs of particular elements on the battlefield.

Because of changes in the information and operational environments, we can now achieve new levels of efficiency and effectiveness in use of information by integrating and synchronizing the collection, processing, and dissemination efforts. Efforts must focus on leveraging the potential operational contribution of information by efficiently collecting and sharing information across all BOS elements.

Assessment Criteria

Because sources of information are imperfect and susceptible to distortion and deception, commanders and planners must carefully assess the quality of the information prior to its use. They can do so using the following six criteria:

- *Accuracy.* Information that conveys the true situation.
- *Relevance.* Information that applies to the mission, task, or situation at hand.
- *Timeliness.* Information that is available in time to make decisions.
- *Usability.* Information that is in common, easily understood formats and displays.
- *Completeness.* All necessary information required by the decision maker.
- *Precision.* Information that has the required level of detail.

As a first priority, information should be accurate and relevant. As a second priority, it should be both timely and in usable form. Finally, information should be as complete and precise as possible. The following rule of thumb supports these relationships: incomplete or imprecise information *is better than none at all*; untimely or unusable information *is the same as none at all;* inaccurate or irrelevant information *is worse than none at all.*

Decision and Execution Cycle

Commanders must have information to command. Information is the medium that allows the commander's decision and execution cycle to function. Information gives direction to actions by the force, provides courses of action for protecting the force, and helps the force accomplish its operational mission. Relevant information drawn from the MIE supports the creation of situational awareness that contributes directly to effective C^2 during all stages of the decision and execution cycle. C^2 in an environment of situational awareness helps the commander ensure unity of effort toward mission accomplishment. Ultimately, C^2 depends on the right person having the right information at the right time.

C^2 is a continuous, cyclical process by which a commander makes decisions and exercises authority over his forces to accomplish an assigned mission. A commander's decision and execution cycle has four sequential steps (see Figure 4-2).

- *Step 1.* First, the commander is the central element in the entire process of C^2. Accordingly, he strives to understand his current situation and environment by acquiring information about his battlespace and the status of relevant forces, both friendly and adversary, using all available sources, including personal observation, sensors, INFOSYS, and spot reports from subordinates.
- *Step 2.* Upon mission receipt, the commander combines his understanding of his current environment, visualizes the

desired future end state, and develops an initial concept of how to execute the mission.

- *Step 3.* Based on his understanding of the situation and his intent, the commander issues guidance and directs a planning process to develop and refine a viable course of action for mission accomplishment. Upon deciding on a course of action, he disseminates his orders to put the operation into motion. During this execution phase, the commander monitors the operation and gauges its results. This brings him full circle to acquire new or additional information from which he begins the cycle again. Throughout the entire cycle, the fog and friction of war continually affect the commander's ability to acquire information, visualize, plan, decide, and execute.
- *Step 4.* Since the decision and execution cycle is a continuous process, all parts of the cycle are active at each echelon of command. Commanders collect information, develop situational awareness, and plan for future operations at the same time they conduct current operations. Meanwhile, senior and subordinate commanders gather information and work through decision and execution cycles at their respective levels. Maintaining rapid decision and execution cycles—and thus a rapid tempo of operations—requires that seniors and subordinates alike have an accurate, common picture of the battlespace. From this common picture, a unit gains greater situational awareness with which to exercise initiative during combat or other situations.

The commander operates within the GIE, adjusting his MIE to enhance his situational awareness as necessary. Moreover, the commander uses his various means in the MIE to ensure that all elements of his force have a common, complete, and relevant situational awareness. This requires a sophisticated INFOSYS that enhances the commander's ability

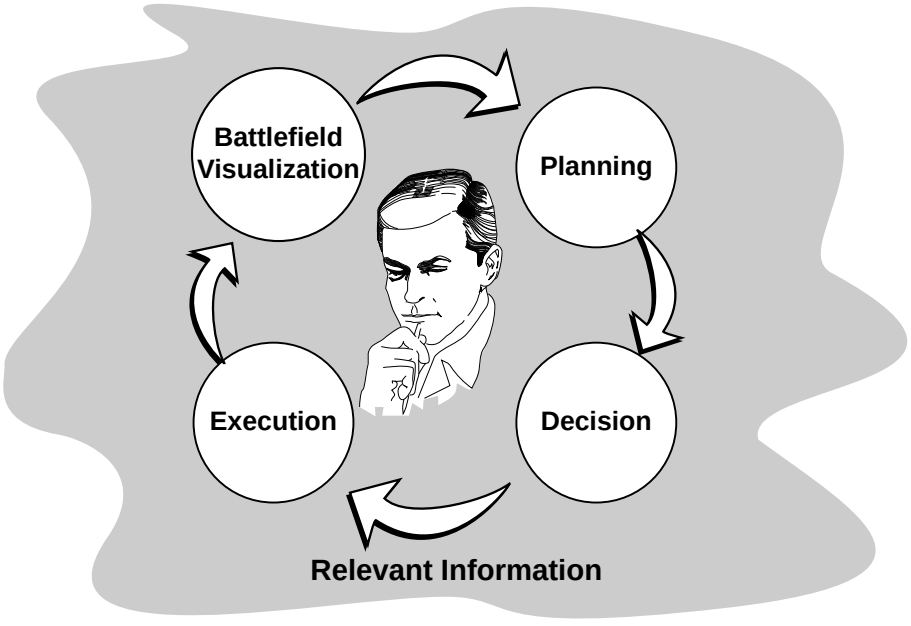

Figure 4-2. Decision and Execution Cycle

to share, manage, and move information among organizations. The commander also uses his information capabilities to support OOTW. The emphasis during such missions shifts away from the combat focus of C2W operations and starts to take in broader considerations contributing to efficient and effective operations. These operations often involve a variety of GIE players. For example, the G3/J3 works closely with PA and CA officers, among others, to determine critical information requirements pertaining to his AO.

INTELLIGENCE

Intelligence is—

> The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Also, information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
>
> Joint Pub 1-02

Intelligence is also the critical subelement of relevant information that focuses primarily upon foreign environments and the adversary. In support of friendly operations, intelligence helps produce a common, current, and relevant picture of the battlespace that reduces uncertainty and shortens the commander's decision-making process. Against an adversary, intelligence is vital for developing and executing effective C^2W operations that degrade and distort the enemy's decision-making process while protecting friendly C^2. Intelligence support to IW executed at the strategic and national levels must be leveraged to support C^2W and IO conducted at the operational and tactical levels. This effort requires a seamless intelligence-collection process and supporting architecture, providing real-time intelligence products focused on CCIR.

Role of Intelligence

Intelligence provides the commander with an accurate understanding of the threat situation as it relates to current and future operations. Intelligence personnel acquire, use, manage, and exploit information to produce such an understanding. For common situational awareness to be accurate and current, the intelligence effort is continuous. Intelligence collection includes all possible sources, from national-level covert operations through local open sources such as news media, commercial world contacts, academia, and local nationals.

In noncombat operations, HUMINT, open sources, and other government agencies provide timely information to augment the unit's more traditional battle-focused intelligence-collection effort. The intelligence effort provides current, accurate threat and targeting data to weapon systems and intelligence sensors. Their effectiveness is dependent upon the rapid movement of data between collector, processor, decision maker, and shooter. Intelligence supports C^2W, focusing on C^2-attack and C^2-protect.

Intelligence-Enabling Functions

The primary purpose of intelligence is to enable well-informed operational decisions based on an accurate understanding of the situation. The essence of intelligence is to collect, analyze, screen, and present information requested by the commander. Intelligence helps reduce uncertainty for the commander by screening out information that is not relevant to his decision-making process. Intelligence-enabling functions focus on assessing friendly vulnerabilities, understanding the adversary, employing IPB, and assessing battle damages.

ASSESSING FRIENDLY VULNERABILITIES

The first critical step in protecting IO capabilities is to identify specific and potential threats. Potential threats range from the adversary's direct overt and covert actions, to individuals and organizations seeking to exploit military INFOSYS, to natural phenomena. They include a new family of global commercial imaging, cellular telephone, and positioning systems that jointly or separately provide a potential adversary with near real-time information on forces and movements.

The fluid, porous nature of the MIE makes it difficult to protect INFOSYS from possible attacks. Therefore, intelligence provides the commander the necessary information to conduct risk assessments and develop risk management options to protect vital C^2 components and capabilities. The risk assessment is based on identification of such factors as specific threat capabilities, technical capabilities, doctrine, and past performance of the threat force. The risk assessment is not a finished document, but a continuous process that is constantly updated to reflect changes in the operating environment, technology, and threat acquisitions. Because C^2W offers potential adversaries the chance to strike at the supporting infrastructure of the US force—wherever it is located—the commander and his staff must be aware of threats to their INFOSYS at the home station.

UNDERSTANDING THE ADVERSARY

The effectiveness of C^2-attack is predicated on a thorough understanding of an adversary, his C^2 system, and his decision-making process. The deeper the understanding, coupled with the tools and techniques to take advantage of such knowledge, the more effective the exploitation of the potential adversary. At all levels of war, intelligence is an operational tool that identifies, assesses, and exploits the enemy's information and C^2 systems. Data is required on what information the adversary collects, by what means, what reliability he places on various sources, and how that data is evaluated.

Intelligence personnel must be able to describe the enemy's decision-making process and how direction is sent to subordinates. Detailed intelligence is required on the social and cultural environments and the psychological makeup of the adversary's key leaders and decision makers. How they interact and perceive one another are important aspects of the information necessary to develop effective PSYOP and deception operations. How subordinates execute decisions completes the picture. Having a detailed understanding of the adversary's use of information is necessary in order to determine where and how to effectively influence his actions (see Figure 4-3).

> *"Know the enemy and know yourself, and you will be victorious."*
>
> Sun Tzu (500 BC)

EMPLOYING INTELLIGENCE-PREPARATION-OF-THE-BATTLEFIELD

In this context, IPB is the continuous process used to develop a detailed knowledge of the adversary's INFOSYS. IPB is a continuous process of overlapping and simultaneous actions that produces situation updates on a continuous basis and providing options to the commander. This form of information IPB, as shown in Figure 4-4, is the basis for planning operations, developing C^2W courses of action, and targeting. The process builds upon the standard IPB but also requires—

- An understanding of the adversary's decision-making process and leadership style.
- Knowledge of the technical requirements on a wide array of INFOSYS.
- Knowledge of the political, social, and cultural influences at work in the MIE.
- The ability to conduct highly technical processes to produce C^2W course-of-action templates.
- Identification of and an in-depth understanding of the biographical background of the adversary's key leaders, decision makers, communicators, and advisors.

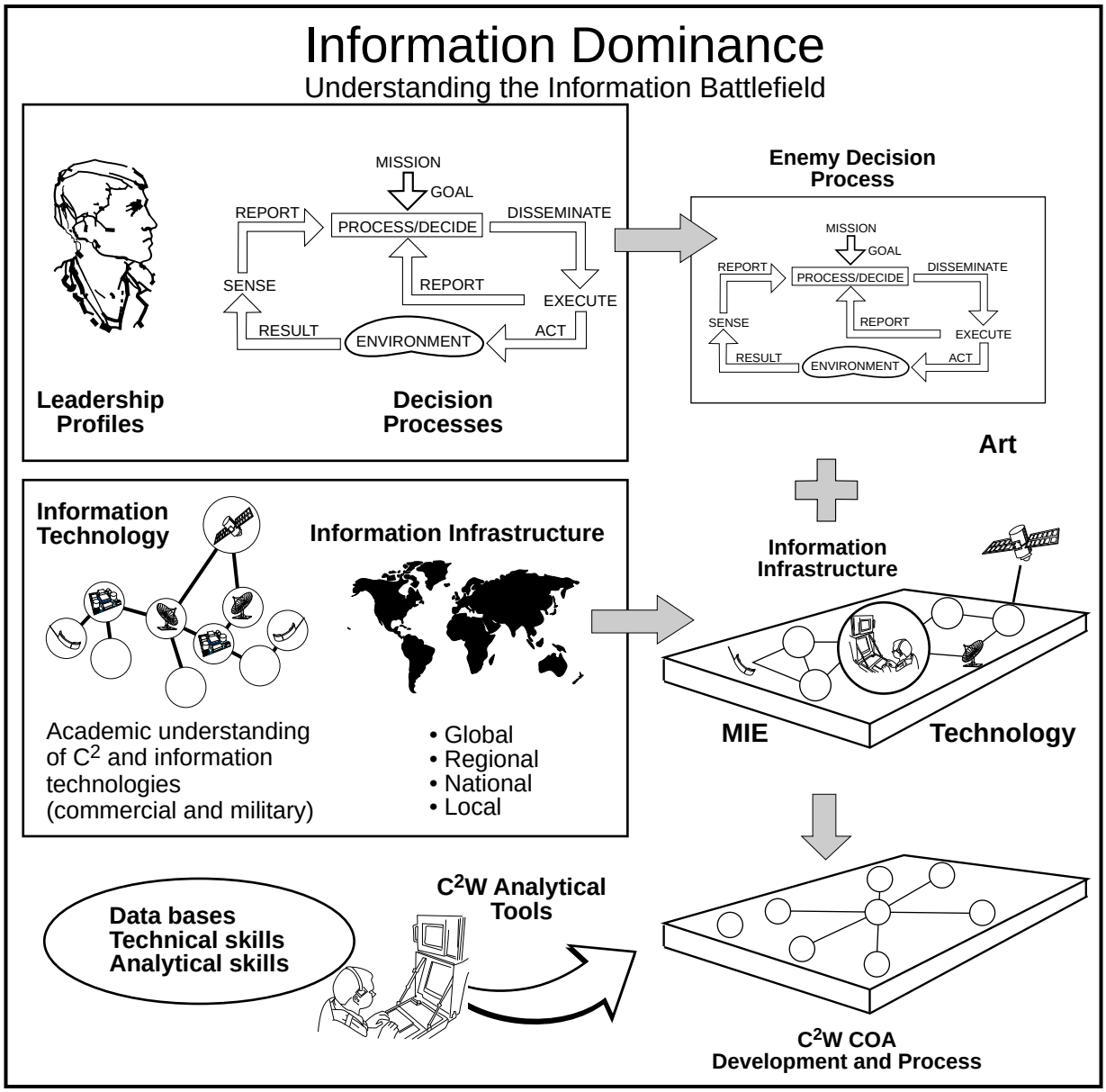

Figure 4-3. Understanding the Adversary

Much of this information should be routinely collected and maintained in national-level data bases and be readily available at the start of a mission.

The IPB actions the intelligence officer accomplishes to support IO include constructing a template of the adversary decision-making process, understanding the information infrastructure of the adversary, and analyzing the adversary's vulnerabilities.

Constructing a Decision-Making Template

The first step in the IPB process is to construct a template of the adversary's decision-making process. This aspect of information IPB focuses on developing an understanding of the

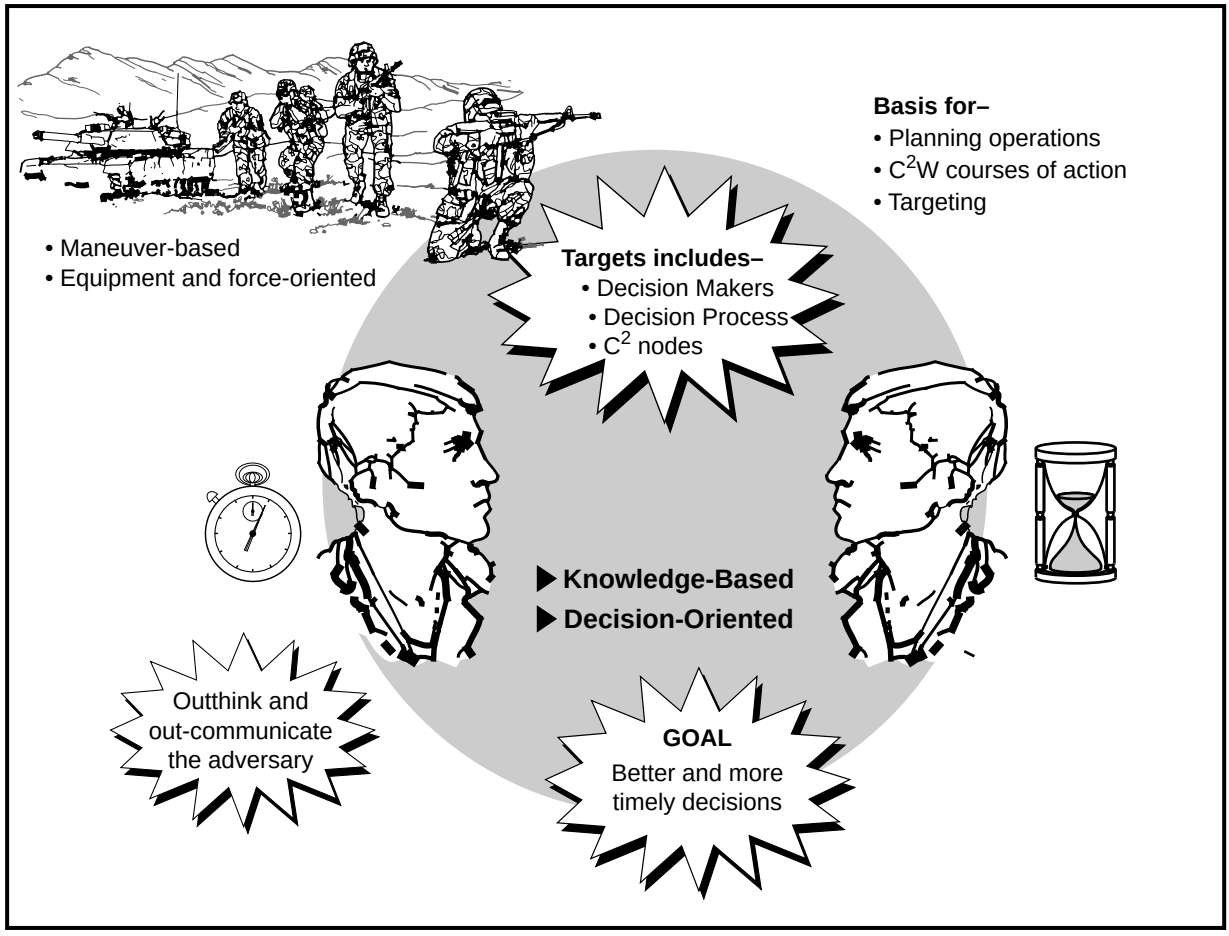

Figure 4-4. IPB Considerations in Information Operations

leadership/personality profiles of the critical adversary decision makers. It address how they use information to make decisions, how they interact as organizations to make decisions, and how they execute those decisions. This step is linked directly to the ultimate goal of IO, which is to find ways to create a desired response in the adversary decision-making process, to create a relative military advantage, or to achieve the desired end state of the military operation.

Understanding the Adversary's Information Infrastructure.

The second element of IPB is to understand the information infrastructure of the adversary. See Figure 4-3, which depicts how information flows within the unit, organization, and structure. This analysis includes the human interface as a valid form of information distribution and is not limited to only technology assessments. An understanding of how information from outside the adversary's unit, organization, or structure flows must also be developed for the commander's use. This includes understanding the local, regional, and global information environments. CA teams operating in-country can greatly assist in this process.

Analyzing the Adversary's Vulnerabilities.

Next, the intelligence officer analyzes the decision-making template and the infrastructure template to determine adversary vulnerabilities. Vulnerability analysis occurs on two levels.

- First, system vulnerabilities are identified which can be exploited to cause the desired effects on the decision process.
- Second, the appropriate attack mechanism and specific entry point (building, floor, air shaft) is determined.

Vulnerability analysis is then extended to include the collateral damage a C^2W action may cause on the operating environment. As an example, an option in attacking an adversary's C^2 might be to destroy his electrical power infrastructure. However, the strategic cost (political or logistical) of destroying this capability might outweigh the tactical gains. One implication of the GIE is that actions and their consequences are examined across the MIE, as opposed to the battlefield alone.

Developing Options

The decision-making template and the infrastructure template are combined to form a C^2-attack course-of-action template. Various courses of action can then be developed and analyzed to determine the best way to use IO to influence, support, or accomplish the overall mission.

ASSESSING BATTLE DAMAGES

BDA serves to confirm or deny previous intelligence estimates and update the IPB. The intelligence system continuously assesses the effectiveness of IO. This BDA allows commanders to adjust IO efforts to maximize effects. An important aspect of this *information BDA* is timely analysis to determine when exploitable vulnerability is created in the adversary C^2 structure. Compared to the way we look at conventional BDA reporting procedures, BDA in IO is not so apparent.

Information BDA is not always reported in terms of physical destruction of a target. The challenge of information BDA is to be able to assess the effects of our efforts without the benefit of physical confirmation. The effects may well be trends, activities, and patterns in future adversary actions. They could be as simple as an absence of activity on a C^2 net, combined with an increase of traffic elsewhere, that is, reduced very high frequency/ultrahigh frequency (VHF/UHF) transmissions coupled with observations of increased courier traffic or heavy land line activity. BDA also examines the collateral damage C^2W actions may cause to nonmilitary systems and capabilities within a commander's MIE.

Chapter 5

Information Systems

Microprocessing, miniaturization, communications, and space technologies have combined to permit almost real-time intelligence and information sharing, distributed decision making, and rapid execution of orders from a wide variety of forces and systems for concentrated effect.

FM 100-5

INFOSYS allow the commander to view and understand his battlespace, communicate his intent, lead his forces, and disseminate pertinent information throughout his chain of command and his AO. Effective military and nonmilitary INFOSYS help the staff get the right information to the right location in time to allow commanders to make quality decisions and take appropriate actions. This chapter describes how INFOSYS operate as part of IO. Specifically, the focus is on the functions, role, security, and management of INFOSYS. These INFOSYS consist of—

> The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.
>
> Joint Pub 6-0

FUNCTIONS

INFOSYS include personnel, machines, manual or automated procedures, and systems that allow collection, processing, dissemination, and display of information. These functions cover all aspects of the organization, providing commanders with an accurate, relevant, common picture and a common situational awareness. Accordingly, a commander should consider his staff as part of the INFOSYS because its chief function is to plan and integrate IO. INFOSYS collect, transport, process, disseminate, and protect information in support of the CCIR. In addition, INFOSYS enable the commander to use information effectively to maintain an accurate view of his battlespace, coordinate the activities of his tactical forces, and help shape his MIE.

INFOSYS directly support battle command; however, all aspects of land warfare—operations, logistics, planning, and intelligence—depend on a responsive information system infrastructure. INFOSYS are able to simultaneously support current operational deployments and future contingencies. Interoperability and flexibility are critical characteristics of any INFOSYS, especially given the requirement for Army forces to conduct force projection and split-based operations using strategic systems.

And to control many is the same as to control few. This is a matter of formations and signals.

Sun Tzu, *The Art of War*

ROLE

The role of INFOSYS is to provide the infrastructure that allows the Army to interface with the GII. INFOSYS enable the integration of all IO activities. INFOSYS form the architecture that—

- Supports the staff process.
- Supports the decision-making process.
- Provides the relevant common picture that helps synchronize force application.
- Links sensors, shooters, and commanders.
- Supports C^2-attack and C^2-protect capabilities.

The accelerated development of information technologies has created new techniques for managing, transporting, processing, and presenting data. These include imagery, video, color graphics and digital overlays, mapping, and data base technology.

With the revolution of information technology, developments in satellite communications, network and computer technology, and the infrastructure of military and nonmilitary INFOSYS combine to provide the commander with a global reach capability. See Figure 5-1. Communications and automation

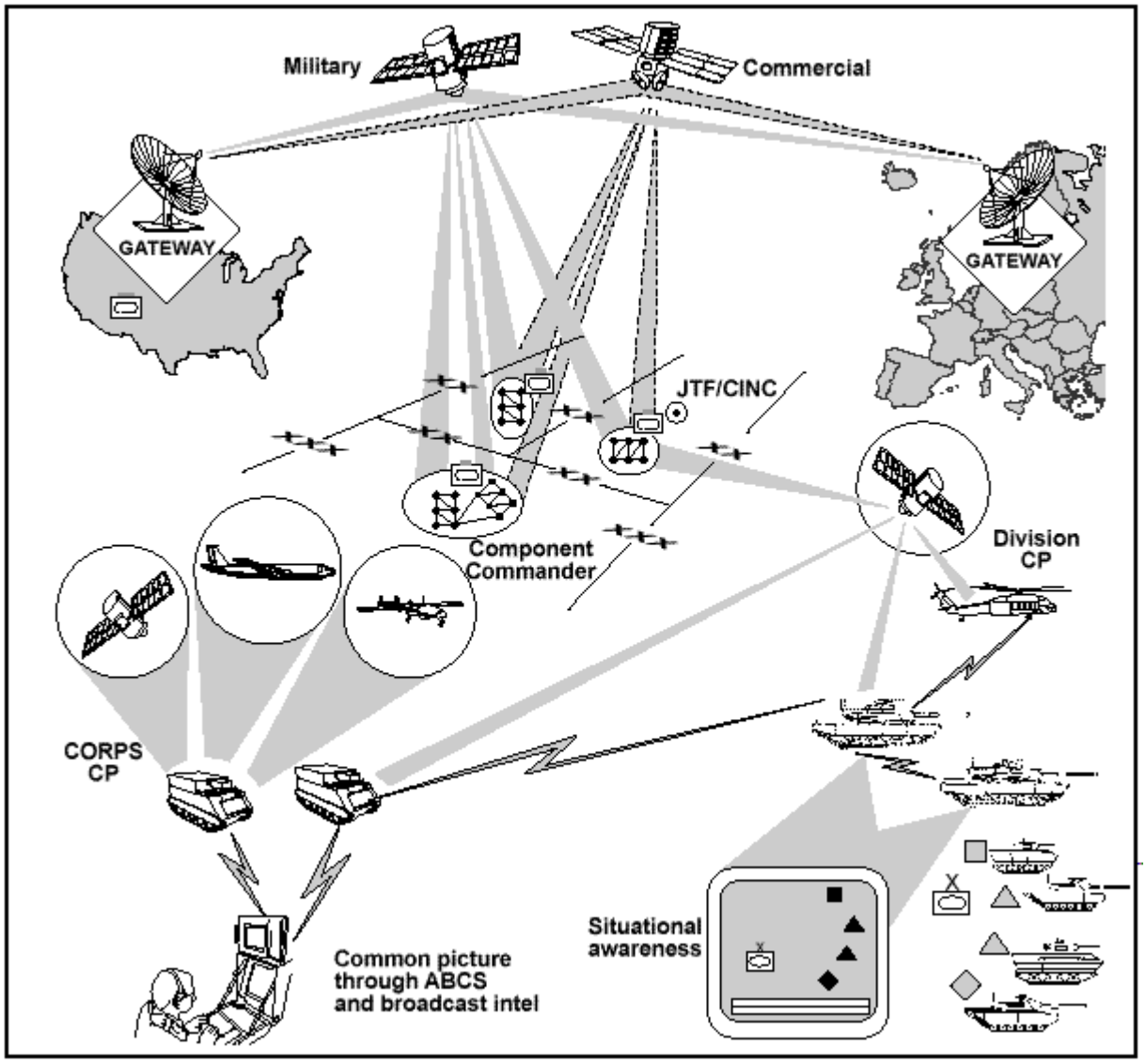

Figure 5-1. Global Communications Network

architecture allow for modular C^2 support for force tailoring during any phase of an operation. Operations take place in a global environment and demand information from a host of information sources. Military and nonmilitary INFOSYS provide that global capability to support commanders and units across the range of operations. Discussion includes the INFOSYS, the principles that form the foundation for their support, and the direction of future INFOSYS technology.

Military Information Systems

Military INFOSYS integrate fielded and developmental battlefield automation systems and communications to functionally link strategic, operational, and tactical headquarters. INFOSYS maximize available information networks through seamless connectivity as well as C^4 interoperability. Figure 5-2 depicts the relationships of strategic, operational, and tactical architectures that tie the many distributed elements into an integrated, interoperable, and cohesive network.

JOINT GLOBAL COMMAND AND CONTROL SYSTEM

The primary national warfighting C^2 information system is the joint Global Command and Control System (GCCS), which interfaces

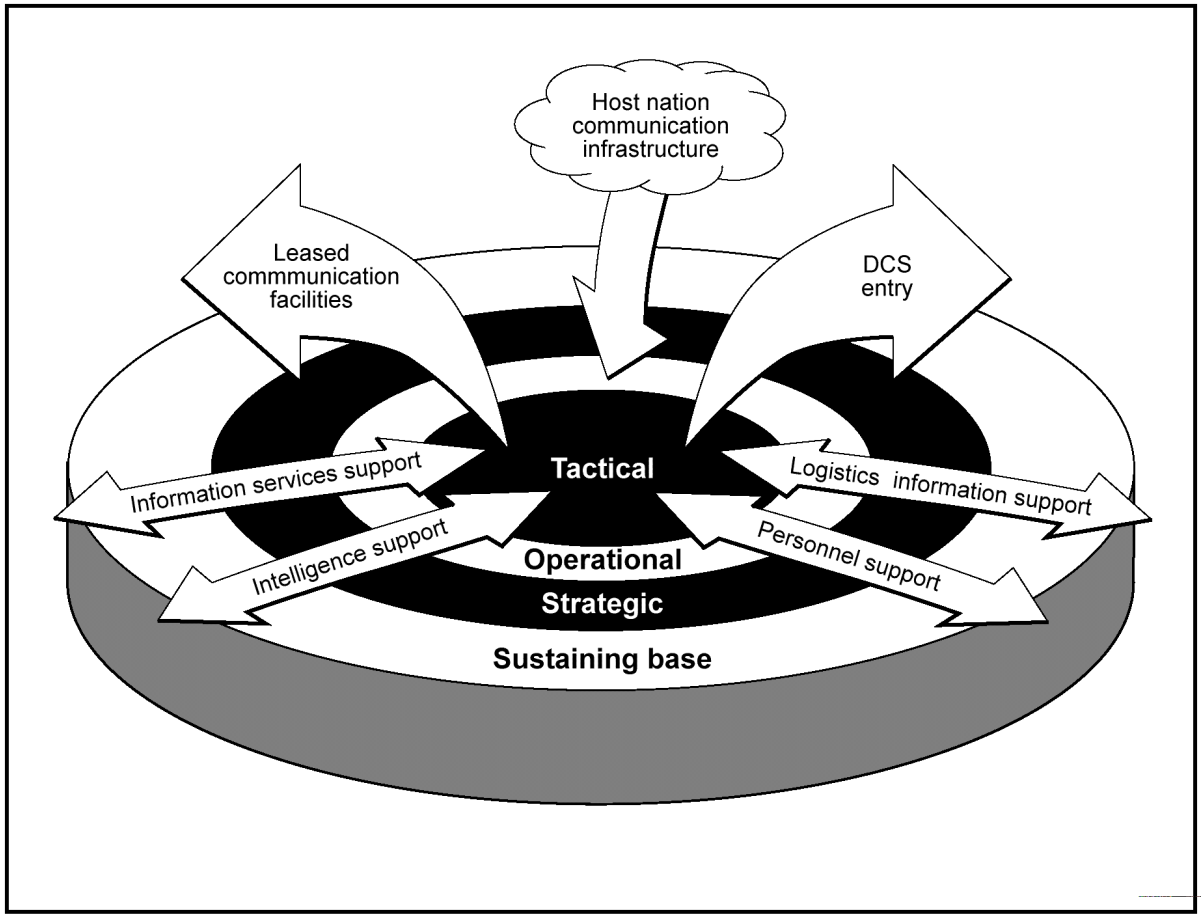

Figure 5-2. Seamless Architecture

with the Army Global Command and Control System (AGCCS).

ARMY GLOBAL COMMAND AND CONTROL SYSTEM

AGCCS is a seamless C^2 system operating at the upper echelons of the ABCS and supports C^2 for echelon-above-corps units.

ARMY BATTLE COMMAND SYSTEM

ABCS is the primary Army warfighting C^2 INFOSYS and employs a mix of fixed/semifixed installations and mobile networks, depending on the subsystem. ABCS is interoperable with theater, joint, and combined C^2 systems across the full range of BOS functions. It is vertically and horizontally integrated at the tactical and operational levels. ABCS provides connectivity to combat information data bases and processes information pertaining to each BOS. In addition to the theater-level AGCCS, the other components of the ABCS include the Army Tactical Command and Control System (ATCCS) and the Force XXI Battle Command Brigade and Below System ($FBCB^2$).

Army Tactical Command and Control System

ATCCS is linked directly to AGCCS, providing the framework of seamless connectivity from brigade to corps. Moreover, it integrates the traditional disparate stovepipe functions into a coherent, seamless infrastructure that binds the BOS together. Figure 5-3 depicts this INFOSYS architecture. Tactical internet capabilities to establish the use and allocation of new IO capabilities offered by digitization of tactical forces are in development. The tactical internet has both operational and systems information architectures. The operational architecture is for required connectivity of force elements and the type and volume of digital information-sharing by elements within the force. The system architecture is for specific hardware and software to provide connectivity and dissemination of battle command information.The two evolving architectures account for predetermined user information exchange requirements throughout the tactical force.

Each node of the tactical internet can provide information services while on the move. Network management is an important feature of the tactical internet and is highly critical to the successful delivery of information across the battlefield. It enables the tactical information manager to track tactical users on the battlefield. It provides a tool to assist in the dynamic configuration of battle command information networks needed to conduct tactical IO.

Force XXI Battle Command Brigade and Below System.

In the near term, the $FBCB^2$ system employs the GPS (POS/NAV) and communicates over the single-channel ground and airborne radio system/enhanced position location reporting system (SINCGARS/EPLRS) and the mobile subscriber equipment/tactical packet network (MSE/TPN). These systems form an integrated network to move information (data) between higher and lower echelons (vertically) and between adjacent organizations (horizontally) without routing through the brigade headquarters. Moreover, $FBCB^2$ provides digital connectivity from brigade to weapons systems or platform level. It transitions from a network of three separate systems to a homogeneous network and system of systems comprised of—

- *Appliqué*—a family of laptop-sized computers connected to navigation devices and radios to provide processing and display capabilities to platforms without an embedded processor.
- *Tactical Internet*—a battlefield communication systems networked together using commercially based internet protocols.

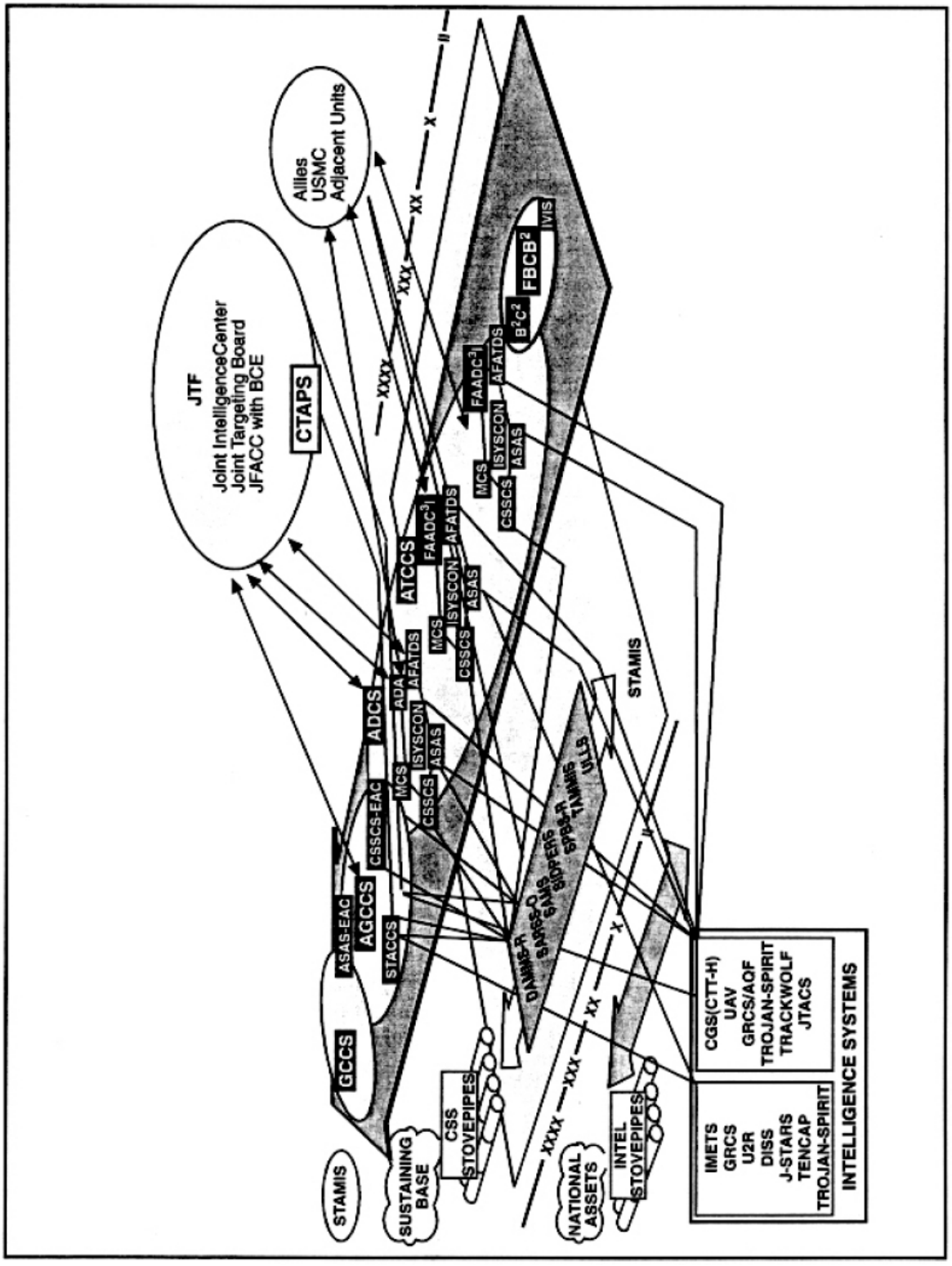

Figure 5-3. Army Information System Architecture

Nonmilitary Information Systems

Information technology is growing exponentially and transforming how the world conducts business, diplomacy, and war, requiring that commanders have a broader and externally oriented view of all sources of INFOSYS when executing IO. Moreover, DOD has limited authority for securing this civilian infrastructure or influencing the content of its products. Technological improvements in mobility, directed-energy weapons, digitization, and sensors continue to reduce factors of time and space and demand faster tempos of operation across vast areas.

Increasing global population, rapidly expanding world economic markets, and unprecedented advances in INFOSYS technology continue to perpetuate a global explosion of information networks of a nonmilitary or commercial nature. These ever-increasing networks are rapidly creating a global web or *infosphere* of information. Important changes are occurring in broadcast communications technology, computing, and space-based technology. The global nature and speed of news broadcasts can elevate apparently obscure events into international spectacles and has created a market for news known as *infotainment.* The number of players in the GIE are growing rapidly and sharing new information over computer networks at a steadily increasing rate.

Cellular communications and data compression advances increasingly provide greater communications freedom to individuals in ever wider regions of the globe. These advances enable individual soldiers as well as independent media or other actors to independently reach home using the internet or broadcast and publication sources. Potential sources of immediate information and the number and variety of MIE influences (both intentional and inadvertent) are rapidly multiplying. The cumulative effects of these changes permanently alter the shape of organizations and C^4I architectures in ways that are just becoming evident.

- Networks are, in many fields, supplanting traditional hierarchies as the major organizing concept.
- In the business world, greater connectivity and access to information at all levels is eliminating much of the status-monitoring functions performed by middle management.
- New ways of thinking and operating are necessary because elements that are relatively low in an organization now have the information to make and execute decisions.

Like the rest of the nation, the Army relies on elements of an information environment it does not control. These nonmilitary INFOSYS include—

- US and host nation PSNs and postal and telegraph systems.
- Commercial communications satellite systems such as intelligence satellites (INTELSAT) and international maritime satellites (INMARSAT).
- Commercial receivers that use precision, space-based navigation systems such as GPS.
- Electric power systems that support information networks.
- Commercially developed software applications.
- Commercial, international news media.
- Public-accessed data bases and bulletin boards.

Historical Perspective

In 1944, at the Battle of Arnhem, the British First Airborne Division landed with the wrong radio crystals. They couldn't communicate with the outside, not even to their relief column at Nijmegen, a few miles away. They were isolated, under attack by superior numbers, and surprised at being dropped where they weren't supposed to be. During the entire multiday battle, members of the Dutch resistance in Arnhem were routinely talking to the counterparts in Nijmegen by telephone, because the national telephone system had not been taken down. It never occurred to a single paratrooper to knock on the door of a house and call Nijmegen, because the battlefield had been defined outside the civilian infrastructure. The Dutch underground assumed the paratroopers were talking by radio, and the paratroopers had never thought about using the civilian

The availability of nonmilitary INFOSYS often offer the command an alternative means to satisfy its informational C^2 needs, but only after a careful assessment of security risks. As an additional benefit, use of available nonmilitary INFOSYS may reduce the requirement for deployed military information system packages. Operational use of a nonmilitary system allows planners to compensate for system shortages and to meet the surge of information requirements in the early stages of deployment.

The J6/G6 is responsible for standardization of nonmilitary equipment and software used throughout the AO. However, planners have to ensure the deployed modular INFOSYS packages implement open, nonproprietary, commonly accepted standards and protocols to interface with nonmilitary systems. Proper use of INFOSYS creates new challenges at individual user, organization, and system levels. Planners should consider these challenges in IO planning because they will affect the end user and the information management structure.

The user will be challenged by the digitization of the battlefield, by interface requirements between the operator and the system, and by the need to develop effective training strategies. The optimal use of INFOSYS ultimately depends on the availability of quality soldiers and leaders who are trained to employ advanced INFOSYS technology. Organizations will be challenged to develop flexible task-organization strategies that use the INFOSYS to adapt to the wide range of different conditions existing in the GIE. In addition, organizations will improve their battlefield functional capability in a digital environment by using advanced computer applications and tools. System challenges will emerge as a result of—

- Constantly advancing technology.
- Uneven distribution of early generation equipment mixed with new, improved digital INFOSYS.
- Limited EMS availability.
- The search for commercial-off-the-shelf products available for use within the INFOSYS architecture.

Meeting these challenges will enable and enhance the conduct of future operations.

Signal planning increases the commander's options by providing the requisite signal planning support systems to pass critical information at decisive times, thus leveraging and exploiting tactical success and facilitating future operations.

FM 100-5

SIGNAL SUPPORT

Throughout all force-projection stages, a paramount need exists for a *signal support means* to transport information from the sustaining base power-projection platform at CONUS installations, through strategic gateways, to the forward-most warfighters. Signal support requirements to fulfill this task are enormous and vary greatly, depending on the type of military operation.

Mission-Essential Tasks

Information battlespace requires an end-to-end, protected, seamless, multigigabyte information-transfer and processing capability for the warfighter to conduct IO virtually anywhere at any time. This capability must be a multimedia system of systems that transports video, imagery, data, and voice information to create an infosphere that the battle commander

can *plug-in* and *pull* what he needs to *visualize* the battle from the current state to a successful end state. The signal support mission-essential tasks to project and construct the infosphere are to—

- *Link* the force to the infosphere to achieve seamless global connectivity.
- *Transport* information with broadband, high-capacity systems optimizing satellites and terrestrial signal support to connect CONUS, installation sustaining bases (ISBs), and joint operational areas (JOAs).
- *Reach back* through strategic entry points to power-projection platforms and information fusion centers.
- *Extend* the communication range of battle command operations centers and fighting platforms by providing C^4 for mobile operations (C^4FMO).

Support Enablers

The enabling objective of signal support to IO is to provide the warfighter the capabilities he needs to obtain and share in near real-time. Signal support requires the total integration of all information management functions into a system of systems or ABCS. ABCS provides knowledge-based information that is adaptable and responsive to the commander's IO requirements. The ABCS has a suite of C^4 hardware and software capable of *collecting, processing, fusing, managing, transporting, disseminating, displaying,* and *protecting* force-level information (status) and force-level control information (intent, plans, orders). The signal support mission-essential tasks to enable IO are to—

- *Digitize, compress,* and *broadcast* multimedia battle command information in five categories, using increased bandwidth, high-efficiency transport systems. The multimedia categories *control, monitor, alert, inquire,* and *explore* critical information.
- *Encrypt* and *provide* multilevel information security.
- *Manage* information networks with smart software that dynamically allocates throughput capacity on demand and then routes and disseminates information.
- *Display* via ABCS, a three-dimensional interactive knowledge-based relevant common picture (RCP).

While the core of the twentieth century land warfare has been the tank, the core of the twenty-first century will be the computer.

General Gordon Sullivan, CSA (1993)

FUTURE TECHNOLOGY

As technology advances, the conduct of operations will continue to change. Each advance in information technology will—

- Help leaders form a more complete picture of the battlespace.
- Generate the potential for faster, higher quality decisions.
- Support more rapid maneuver in terms of both time and space.
- Increase a unit's flexibility and agility.

Nevertheless, technology is only an enabling tool. Quality soldiers and well-trained leaders remain the true centerpiece to successfully planning and operating this increasingly digitized and automated information system of systems. The following examples illustrate where information technology could enable military operations by the turn of this century.

- Today, tactical radio communications networks exist separately with no automatic routing or interconnection between nets. On the future digitized

battlefield, a tactical internet capability will enable direct communications among and between virtually all users. This could enable a whole new level of horizontal integration, coordination, and synchronization that will coexist with the current vertical system (Figure 5-4).

- Direct broadcast satellites enable wide access to information at various echelons in real time or near-real time. This in turn enables a new level of empowerment and self initiative for lower echelons.
- Image compression and transmission technologies will allow transfer of images and video from numerous sensors and platforms, enabling better understanding of battlespace for planning, rehearsal, and mission execution.
- Finally, multimedia technology will enable three-dimensional presentation of imagery and graphics to help commanders visualize their battlespace for more effective training, planning, rehearsal, and execution.

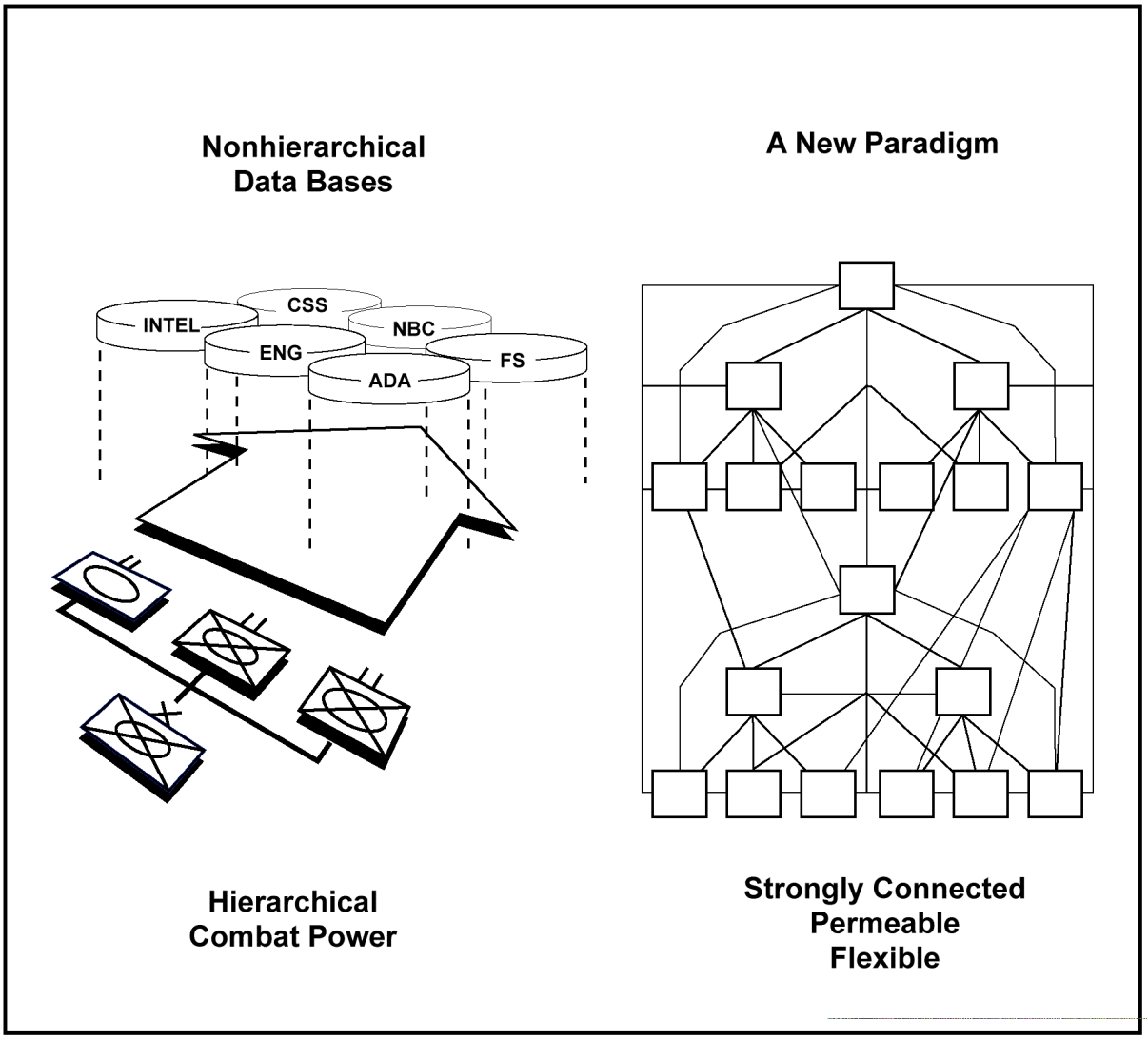

Figure 5-4. Horizontal and Vertical INFOSYS

SECURITY

Due to the present and ever-increasing dependence upon automated INFOSYS within the Army, INFOSEC and information systems security (ISS) has become critical. In both war and peace, computer systems and networks on which units rely for logistics, personnel, administration, maintenance, and financial data processing and transfer are vulnerable to attack. Often, the internet is a favorite communication platform for intruders. Gaining access to a unit's computer and communications network can be accomplished by a wide range of methods and techniques. Some of the more common methods include—

- Inserting malicious software through contractors.
- Tracking software maintenance changes and system operations activities.
- Alternating access paths or sniffer devices that trap information about traffic and passwords.

These intrusions may be initiated during peacetime or at any point in an operation. It is even possible that a military system could come from the factory with an embedded *logic bomb* or virus. In the past, new commercial floppy disks used by government agencies have been found to contain a virus upon delivery from the factory.

Accordingly, security measures and procedures must actively as well as passively preserve the confidentiality, integrity, and functionality of INFOSYS. Protection requirements include near-real-time measures that detect intrusions and alterations, then react and counteract by restoring the INFOSYS needed by commanders to support the military operation. A series of security measures that are facets of an overall C^2-protect effort ensure ISS. The three primary security measures are—

- Procedures for quality assurance.
- Denial of unauthorized intrusion.
- Hardening of programs.

Historical Perspective

In 1994 a computer hacker operating from the United Kingdom attacked the Rome Air Development Center at Griffiss Air Force Base, NY, where he compromised the security of 30 systems and penetrated more than 100 other systems before being caught in a 26-day international electronic manhunt. The victims included the South Korean Atomic Research Institute, NASA, the Goddard Space Flight Center in Greenbelt, and the Jet Propulsion Laboratory in California.

The Defense Information Systems Agency estimates that DOD experienced 231,000 incidents, or security intrusions, in 1994. These incidents included destruction of data, modification of data or software, stolen data or software, and shut-down of hosts or networks. Affected DOD functions include—

- Ballistic weapons research.
- Inventory and property accounting.
- Knowledge-based simulation.
- Payroll and business support.
- Mail hub for postwide electronic mail.

US Senate Permanent
Subcommittee on Investigations, June 1996

Procedures for Quality Assurance

Quality assurance procedures include configuration control and reduction of inadvertent corruption of both data and processes. In order to protect automated INFOSYS, the first step is to understand the threat against them. Security threats to INFOSYS fall into two categories:

- Compromise of data and information.
- Denial, corruption, or loss of service.

Protection Against Intrusion

Protection against intrusion into friendly computer networks is accomplished through denying unauthorized entry into these systems. The vast percentage of intrusion results from human error. Training and OPSEC compliance by system managers, operators, and users are the best measures to combat system compromises. In addition, systems administrators must be able to track down intruders.

Hardening of Programs

In addition to tracking down intruders, system programs should be hardened against intruders' attempts to gain vital information or damage information flow. No protection plan is perfect, and protection/restoration resources are finite. OPLANs and OPORDs specify the priorities of protection efforts.

MANAGEMENT

INFOSYS management consists of prioritizing information in a limited communications environment. The primary purpose of automated and manual INFOSYS is to achieve an information advantage by using and managing information for timely and accurate decision making in any type of operation. The focus of battle staffs is to leverage available technology by employing INFOSYS that give the commander the desired information at the right time and the right place. See Appendix C.

> *General consensus is that the desire for information by higher headquarters is quickly exceeding the subordinate commander's ability to provide it in a timely manner. Commanders at all levels must carefully define their critical requirements.*
>
> CALL Newsletter, July 1994

Management Process

All information that the staff provides is predicated upon the commander's intent, concept of operations, and supporting commander's CCIRs. The CCIRs govern the C^4I architecture and its use. The CCIRs define the commander's information needs, thus focusing the staff and INFOSYS support on the rapid acquisition, fusion, and analysis of information that yields knowledge-based operations. The INFOSYS augment routine or periodic reports (established by unit SOPs) with specific requests for information from BOSs or other data bases.

Technical Systems Management

The ABCS spans several systems and requires technical management with similar spans. INFOSYS provide an efficient and rapid means of retrieving information, enabling the battle staff to develop and maintain a single, virtual (or logical) data base that satisfies both current and anticipated CCIRs. This allows battle staffs to continue coordinating, integrating, and synchronizing current and future IO. The ABCS, which works primarily at the SECRET classification level, poses both a technical and tactical INFOSYS challenge.

Technically, the network of ABCS devices function as a seamless whole with redundant paths. Data flow among computers does not require intensive operator action. However, understanding and interacting with the information received is generally a user requirement. The INFOSYS architecture covers the entire battlefield, enabling the command and

control of forces. This architecture consists of integrated local area networks (LANs), wide area networks (WANs), and battlefield automated systems integrated into a single, seamless system subject only to the requirements of multilevel security (MLS) as depicted in Figure 5-5.

INFOSYS allow the commander and his staff to distribute critical information between higher,

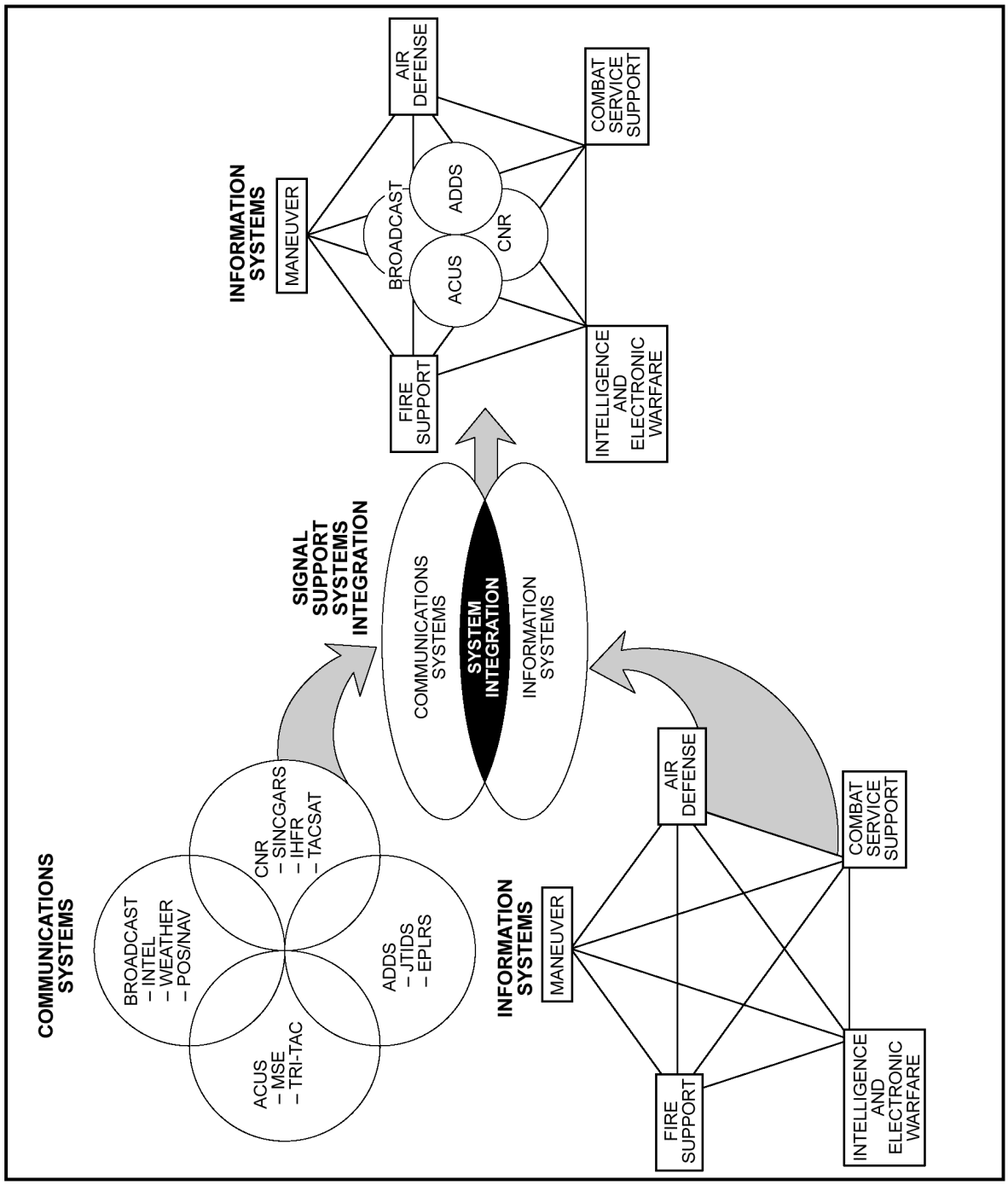

Figure 5-5. Battlefield Architecture Information Integration

lower, adjacent, joint, and multinational forces. Voice traffic and data distribution are the primary methods of passing this information. Voice traffic includes user-to-user, conference, and broadcast type of transmission. Data distribution includes formal record traffic (joint message text), informal record traffic (facsimile and electronic mail), system-to-system data, and POS/NAV data.

Technical systems management connects all INFOSYS devices into a multilevel secure network that supports the commander's concept of operation and maintains the correct security levels at each network node throughout the battle. Technical systems management requirements include—

- Planning the INFOSYS network.
- Planning communications connectivity.
- Planning network security.
- Allocating frequencies.
- Controlling and monitoring the connection of systems devices to one another and to supporting communications systems.
- Reconfiguring the network as required by the tactical situation or equipment failures.
- Maintaining the network.
- Maximizing network performance.

Tactically, the information flow must support the needs of commanders. Commanders and staffs must have the information they need to plan, direct, control, and coordinate an operation. The information must be secure and readily available. Tactical systems management ensures that information is exchanged inside and outside the unit and made available according to the needs of commanders and staffs to support the tactical plan.

Within each BOS, the information flow, processing, and storage are managed according to the needs of the BOS. Flow, processing, and storage of information among BOSs are collectively managed according to the needs of the overall force-level commander. Tactical systems management includes—

- Planning information exchanges.
- Planning data base locations and replications.
- Planning continuity of operations (including security).
- Controlling and monitoring information exchanges and data base transactions.
- Implementing continuity of operations plans as required.
- Planning for degradation of the network.

Appendix C contains detailed information on INFOSYS planning.

Electromagnetic Spectrum Management

In a dynamic battlespace, each echelon of command must effectively contribute to achieving a state of information dominance. To do so, it uses the EMS for its own purposes, while effectively preventing similar use by an adversary. The EMS is a valuable and finite resource. Controlling it is the linchpin for digitization. Commanders must have a battle staff with knowledge of the EMS.

The J6/G6 or signal officer has staff responsibility for battlefield spectrum management. The spectrum manager under his supervision manages all spectrum use. Major considerations in IO planning include deconfliction of frequencies, development of joint signal operating instructions (JSOI), and development of the joint restricted frequency list (JRFL), as well as all other bandwidth requirements levied by intelligence, C^2W, CA, PA, and signal elements. These elements must be balanced to ensure that users maximize the EMS effectively.

Uncontested ownership of the EMS is not guaranteed. However, to gain control of the flow and content of information, units must effectively manage the EMS to reduce the likelihood of electromagnetic interference (EMI). For unopposed entry operations, the status of forces agreement made with a host nation defines frequency provisions and procedures to be

followed in all frequency and radio regularity matters. Parts of the spectrum are reserved by nations and other international agencies and therefore are not available for use by the US military.

Where agreements do not exist, coordination of frequency use is made through DOS. The United Nations (UN) recognizes the International Telecommunications Union (ITU) as the specialized agency in the telecommunications field. The ITU allocates the international radio frequency spectrum, registers frequency assignments, and coordinates resolving interference. Forced entry operations create the greatest demands for flexible and adaptive spectrum management. An adversary will use the spectrum as he sees fit, creating potential interference with friendly usage. For example, a television station may interfere with combat net radios, yet the OPLAN may call for capturing the station intact for future friendly use, thereby hindering efforts to eliminate the interference. During initial spectrum planning, planners must consider adversary spectrum usage and management and adapt to events as they unfold.

Communications dominate war; they are the most important single element in strategy.

Chapter 6

Planning and Execution

JFCs employ air, land, sea, space, and special operations forces in a wide variety of operations...to not only attack the enemy's physical capabilities but also the enemy's morale and will.

Joint Pub 3-0

The challenge for commanders in the twenty-first century is to operate effectively in a dynamic joint and multinational environment against a wide array of threats. Maintaining the information high ground helps commanders meet that challenge. As full-dimensional operations evolve, information and IO become increasingly important to Army operations as the Army executes missions to deter conflict, to compel opponents, to reassure allies and friends, and to provide domestic support. This chapter discusses considerations for planning and executing IO.

PLANNING

IO planners must consider the conditions that affect the Army as it deploys. They must focus on the principal objective of achieving information dominance, and, in doing so, follow a planning process that applies the components of IO correctly in support of military operations.

Employment Considerations

The IO discussed herein depend on a series of considerations and conditions that affect the force-projection army as it deploys and operates to support joint, multinational, and interagency power-projection operations. Figure 6-1 depicts how IO apply across the spectrum of operations and how the use of the IO components, especially C^2W operations, increases in times of conflict and war

Information is the currency of victory on the battlefield.

GEN Gordon Sullivan, CSA (1993)

LEVELS OF WAR

The levels of war—strategic, operational, and tactical—provide a useful framework for ordering IO activities within a commander's battlespace. This framework helps clarify IO activities by echelons within the theater across the full range of military operations. In the theater, all land operations are conducted as part of a larger, integrated, joint, multinational, and/or interagency campaign. Under the direction of the NCA, a unified CINC sets the campaign in motion. The campaign is supported by all elements of national power: social, economic, political, and military. The interconnectivity and interoperability of INFOSYS are the critical elements that tie these disparate sources of power together. As described in Chapter 5, INFOSYS connectivity is a prerequisite to success in this multidimensional environment.

Strategic Level

At the national and theater levels, the employment of IO techniques offers a series of

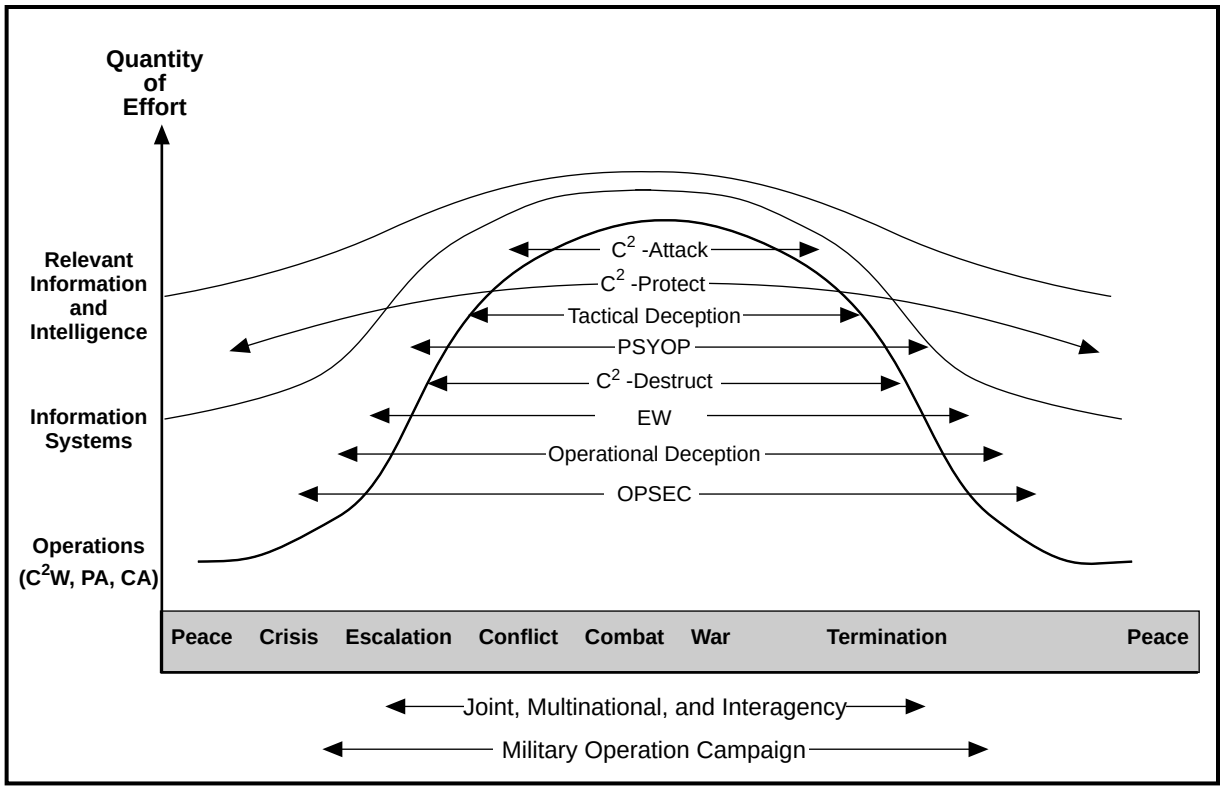

Figure 6-1. Employment of Information Operations

strategic options for consideration. The potential for nuclear exchange and major power conflicts in the post-Cold War world is diminishing. Therefore, military options to effectively attack a strategic target—while minimizing the potentially devastating social, economic, and political effects of conventional military use—increase in importance. Army IO offer both a potential deterrent capability and coercive capability at all levels of war.

As with nuclear warfare, nations can engage in IO at strategic, operational, and tactical levels. Similar to nuclear warfare, the effects can be widespread or targeted against a narrow range of hostile capabilities. As with nuclear warfare, nations may eventually develop IO capabilities that are perceived to be principally offensive or defensive. National strategies can be supported by building an IO capability based upon varying combinations of C^2-protect and C^2-attack and other capabilities. From purely a technical viewpoint, the spectrum of candidate information targets and the range of operational alternatives are virtually unlimited.

US Army force component commanders, in support of national and theater strategic objectives, are responsible for employing the full range of their information capabilities during war or OOTW. As part of a national IO strategy, the Army can be called upon to employ its capabilities to support both direct and indirect actions. Occasions have arisen and will continue to arise that dictate the use of Army capabilities outside a purely battlefield context. The Army component commander has capabilities ranging from PSYOP support to deep battle strikes to contribute to joint warfighting operations.

Information and INFOSYS capabilities inextricably link the traditional levels of war. These phenomena require commanders and staffs at each level to understand the information gathered, where the information is required, and

the means or connectivity necessary to deliver and/or receive that information. National-level systems (DOD and commercial) are increasingly capable of supporting and enhancing tactical operations (weather, communications, imagery, navigation). The challenge for leaders is to—

- First know the information is available.
- Include the requirements for the information in plans and exercises.
- Understand how to get the information into a system, unit, or headquarters that provides an enhanced operational capability.

In many cases the connectivity is found through other services or through civilian agencies. For example, the long-haul connectivity during Operation Desert Shield/Storm was augmented by commercial satellite terminals. Systems such as the Army High Frequency Electronic Warfare System (AHFEWS), employed at the strategic or operational level with other joint C^2W assets, could diminish an opponent's confidence and will to fight before operations begin. Army UAVs could contribute to the domination of OOTW situations as an initial show of strength before the possibility of hostilities occur. If necessary, they could provide the selected intelligence needed to dismantle an adversary's C^2 structure. Combined with deception and PSYOP, these contributors to C^2W could erode a potential opponent's confidence in his own forces and conceal the OB and intentions of the friendly forces.

Army component commanders strive to support the joint force attack strategy at all levels in order to commit and employ Army capabilities—including C^2W, CA, and PA—to the best possible advantage. As with other military activities, IO need to be coordinated and integrated with the OPLAN and JTF campaign plan and synchronized to achieve decisive results. IO offer the prospect of maintaining friendly C^2 and situational awareness at a highly dependable level, while simultaneously degrading an adversary's ability to effectively command and control his forces. Such a combination should create a state of information dominance.

Operational Level

At the operational level, IO occur across the full range of operations and are critical to the success of each stage of force projection. In peacetime, IO support—

- Deterrence and reassurance.
- General situational awareness.
- Operational assessments and estimates.
- Contingency planning.
- Training in support of the CINC's planning and preparation activities.

During conflict or hostilities, IO implement C^2W activities at each level of war. Continuous engagement in IO helps the commander seize and sustain the initiative and synchronize operational capabilities. This allows the commander to control the tempo of operations so that friendly forces can effectively transition from peacetime to wartime operational environments and situations. During Operation Desert Storm, for example, the coalition experienced information dominance in near real time because the enemy's INFOSYS were almost totally disabled.

The linchpin permitting the operational maneuver of coalition forces in Iraq was the enemy's inability to visualize the battlespace. This enabled an entire US corps to move in relatively open desert terrain for distances beyond 200 kilometers and still achieve total operational surprise. The enemy's information flow had been so disrupted and his surveillance capabilities so suppressed that he could not *see* the battlefield. The success of that operational campaign depended critically on information dominance. Space sensors, aircraft-borne sensors, ground sensors, helicopter-transported Special

Historical Perspective

If the Iraqi forces moved in daylight, they were subject to immediate attack by coalition air and surface-to-surface missiles. At night, their movements were detected by superior night-capable sensors. They were then attacked by the coalition's all-weather attack aircraft. Further, their use of broadcast media, coupled with a lack of understanding of the coalition's intent, caused them to base their decision cycle on externally filtered information.

Forces teams, and Marine drones combined to give the operational commander an accurate and timely picture of the battlespace.

Tactical Level

At the tactical level, commanders usually accomplish their missions through combined arms operations. At this level, IO are often limited in scope. While a tactical-level commander uses all aspects of IO, the focus is often on disruption or destruction of enemy INFOSYS or nodes, primarily through EW and physical destruction. The commander maintains access to his INFOSYS through OPSEC, ISS, and EP. Other applications include—

- Planning and executing C^2W.
- Projecting and constructing the infosphere.
- Protecting friendly information.
- Establishing and maintaining user access to battle command information via ABCS.
- Enabling IO and battlefield visualization.
- Collecting and producing RII.
- Attacking the enemy's C^2 system.

Information dominance is a temporary tactical condition achievable through a deliberate process. It entails the construction and protection of the information environment, collection of intelligence and relevant information, processing and dissemination of such information, and focused attack against both the enemy's C^2 and his eyes and ears. Information dominance facilitates superiority in battlefield visualization at a specific time and place, creating a window of opportunity that is fleeting at best. The commander must seize the opportunity to gain the advantage through effective battle command. Two features are essential to this process: CCIR and tempo.

- *Commander's Critical Information Requirement.* The commander must control information, or he runs the risk of being overwhelmed or disoriented by it. CCIR can control the glut of information and separate the true signals from the noise. CCIR cannot be a fixed concept. Like IPB, it must be precise to ensure responsiveness and dynamic to survive.
- *Tempo.* The tempo is the time devoted to the tactical decision-making process. Execution must be dramatically compressed. But, because the information dominance advantage is achievable through deliberate action within a specific battlespace, battle command can be better synchronized, resulting in the creation of opportunities that lead to success.

Tactical units, both maneuver and CSS, participate in IO directed by higher headquarters. In some operations, tactical units perform targeting—striking C^2 nodes, deception, reconnaissance and surveillance, and PSYOP activities focused on supporting an overall theater-level IO. They are also linked to the layered information environment via a CMOC or the PAO. For example, CMOC connectivity to local governmental, cultural, social, and economic institutions can provide a wealth of information supporting military operations. The PAO facilitates media relations and contact *to support friendly forces.*

Historical Perspective

One of the earlier applications of C^2W was demonstrated during the American Civil War. From the beginning, telegraph lines became an important target of cavalry raiding parties from both sides. Since the Union forces were more extensively equipped with telegraphic systems, they were more vulnerable. This vulnerability was exploited by Confederate troops.

Among the more innovative soldiers were the telegraphers attached to Confederate cavalry commands. Their specialists, who were also qualified as flagmen, rode in the lead as Confederate cavalry units raided Union territory. They switched military traffic to the wrong destinations, transmitted false orders to the headquarters of Union commanders, and cast suspicion upon all orders that came by wire. When they had finished the job, they cut all the wire in sight and took home with them as much as they could roll up in a hurry.

With an expanded vision, tactical field commanders anticipate potential threats of disinformation, enemy PSYOP, and rumors within their command, as well as the potential backwash of public information into their battlespace. Establishing an effective internal information program enhances the morale of soldiers, reinforces the stated unit mission, and supports accurate media reports for both soldiers and their families.

RESTRAINTS AND CONSTRAINTS

An increased awareness of how operations shape and are shaped by the MIE is necessary as commanders and staffs plan, prepare, and execute IO. Because information can and will be interpreted differently by any number of individuals or groups, military operations can affect the economic, political, and social fabric of individual lives, organizations, and nations far beyond the scope and intent of the military operation. This reality creates a dynamic set of restraints and constraints that impact military operations.

Asymmetrical or hybrid operations are the norm as tailored forces are assembled to meet a wide variety of needs. Accordingly, different levels of modernization are found within the army, among joint or interagency task force members, and between US and coalition forces. Disparities in information and communications technology threaten continuity and interoperability. Information capabilities can offset these variances, providing the force and the connectivity needed to operate effectively.

Statutory constraints, international law, federal regulations, and rules of engagement (ROE) may limit a commander's options regarding IO. Laws and regulations, such as those governing the use of the frequency spectrum, public information, PSYOP, and espionage, provide examples of free access to information and INFOSYS and are intended to prevent misuse or abuse of these activities. IO may be further constrained or further enabled as new laws, rules, agreements, and protocols are established and as the international community adjusts to the impact of the *information explosion*.

Simple interference, willful manipulation, and corruption or destruction of data bases or INFOSYS, to include space-based systems, have become increasingly active and sensitive activities. The information web and its continuity or disruption has implications far beyond the military environment, into economic, political, and social dimensions. Competition for the EMS, space-based data systems, communications networks, and webbed computer networks all set the stage for potential interference, both intentional and unintentional. Collateral damage gains new meaning in this environment. The potential for the civilian population to be directly or indirectly affected is present and growing.

The laws governing the information environment and the law of land warfare are the guidepost, and every soldier is responsible for preventing violations. Close coordination with the supporting judge advocate is critical to assuring compliance with applicable restraints and constraints. As the Army moves into the Information Age, the features of the battlespace continue to change, and the means and methods of conducting all types of operations also change. Success in any operational environment depends on leadership, discipline, morale, and professional training.

Today's operations increasingly depend on intelligence and INFOSYS from tactical through strategic levels to provide critical information on all aspects of the friendly and enemy situation. The seamless and horizontal flow and integration of information provides valuable operational data to support planning and battle command. While the fog of war has thinned, it will never completely disappear. The commander will always face some uncertainty on exact enemy force dispositions, OB, and operations in general, not to mention some degree of uncertainty about the enemy's intentions. That uncertainty will be compounded by artful opponents (military or otherwise) and exacerbated by the consequences of unintentional actions or influences from other sources within the commander's MIE.

Information Dominance

The principal objective of IO is to gain information dominance—a relative advantage between the friendly commander's decision process and that of the adversary—and to use that advantage to enhance and enable the elements of combat power. IO are an essential foundation of knowledge-based, combined arms warfare. Likewise, full-dimensional operations require integrated IO.

BATTLE COMMAND

Army operations are profoundly affected by information and IO in the critical function of battle command. Although battle command remains principally an art, it relies increasingly on the ability to process information and move it rapidly to critical points in the operational area. To achieve the required level of information dominance, the Information Age commander treats IO as he would any other critical element of combat power, by providing guidance and direction to his staff and his subordinate commanders.

The commander's personal involvement in the development of the CCIR makes it the principal vehicle for ensuring that his battle command information needs are met. Advances in information technology have made decision making and control of units more technical and quantifiable; yet much of those functions remain well within the realm of art, not science. The commander understands that he will never have all the critical information he wants, when he wants it, and that leading soldiers and units to success will remain largely in the realm of art. Accordingly, he employs IO to retain an information advantage over his opponent.

Digital technology enhances C^2. It allows the Army to have previously unimaginable amounts of accurate and reliable information. It allows higher commanders to have detailed knowledge about events several echelons below. At the same time, it gives subordinates more information about the bigger picture and about what is happening in other areas of the picture. Based on the RCP, commanders are better able to continuously, and in near-real time, integrate combat power.

Technology and time do not change some aspects of battle command. Commanders and staffs will continue to make judgments based on less than perfect information. Likewise, they will have to inspire soldiers to perform their duties in the face of fear and fatigue. Commanders will continue to mold units to levels of high performance through training, chain-of-command development, personnel management, morale, and a positive command climate.

Elements

The three basic elements of battle command—*leadership, decision making,* and *controlling*—are characterized by both continuity and change.

Leadership. The commander's *leadership* continues to provide purpose, direction, and motivation to soldiers and units. Leaders will be better equipped to make informed decisions but will operate within a philosophy that will not change.

Decision Making. *Decision making* is facilitated through much-improved information technologies, maintenance of a relevant, common picture upon which to base decisions, and improved decision-making skills of leaders.

Control. *Control* is facilitated by better communications, to include video broadcasting and private links, new position locating and reporting technologies, greater situational awareness, remotely shared electronic maps, automated decision support aids, and other information technologies and procedures.

Challenges

The challenges for leaders are to provide purpose, direction, and motivation to forces operating over greater spaces, under greater time pressures, and amid more complex situations. Specific implications of IO as they apply to the commander's art include the following:

- Identifying, conceiving, and communicating the unit's purpose remains a complex art. This is largely the commander's domain. Understanding the mission, the intent of the next two higher commanders, and the concept of operation of the parent organization may be easier with improved communications, but the restatement of the

mission, the formulation of the intent statement, and the issuance of planning guidance are still functions the commander must perform himself.

- The current doctrinal approach of *mission orders,* or decentralized decision-making, is not anticipated to change. The ability to communicate with remote commanders and staffs by video conference and by other electronic means does not eliminate the commander's need to provide implicit direction to subordinates. Information technology enhances the effort by providing a RCP across the BOSs and functions in near real time. During critical actions the commander focuses most of his attention and decision making on the main effort. Therefore, relying on his subordinates to act within his intent and concept is vitally important.
- Commanders need to motivate their soldiers, as well as their staffs and others, to accomplish difficult tasks under dangerous, trying circumstances. Commanders will continue to inspire and mentor subordinates through face-to-face communications and physical presence. Although it may be difficult, commanders still need to position themselves where they can *see the battlefield* and where soldiers can see them. Commanders establish interpersonal relationships with their staffs and subordinate commanders. Commanders also contribute to unity of effort by establishing personal relationships among and between commands to foster mutual trust, cooperation, open communications, and teamwork in both national and multinational operations. Commanders remain the leaders that all members of the organization look to for timely decisions and informal feedback.
- Uncertainty will always exist. The commander may know what the enemy is doing at the moment, but will rarely know why. Sound command judgment is required to determine what the enemy may be doing tomorrow. In addition, no matter how well the commander knows the status of his forces today, he needs to make judgments about what their condition may be tomorrow. Unquantifiable information and information gaps will remain. No matter how much information the commander gathers before making a decision, uncertainty will remain.
- The ability to process information through risk management enables commanders to avoid unnecessary risks. Identifying, analyzing, and selecting control measures to manage risks gives commanders maximum force protection.

STAFF RESPONSIBILITIES

To facilitate IO, the commander establishes staff responsibilities for planning and execution. OOTW present unique challenges due to the heavy involvement of the media and other players in the GIE. The staff must consider the actions and reactions of US and foreign governmental and nongovernmental agencies, PVOs, and the media when planning operations. Depending on the situation, IO planning can be a complex undertaking or a relatively routine staff function. The commander's IO cell, however organized, draws upon selected expertise throughout the primary and special staff, with liaison and possibly augmentation from subordinate commands. A number of techniques and a variety of arrangements are available to accomplish these responsibilities.

Staff Members

Current staff members can integrate IO actions into the operation. This approach uses current staff procedures, processes, and techniques to plan, coordinate, and synchronize IO with the operation. The likely choice for the nonmodernized or partially modernized force is to designate a staff representative to supervise these actions.

Process-Oriented Group

A process-oriented or *ad hoc* task group, led by the J3/G3, can integrate and synchronize IO actions. This approach is similar to that used for targeting and deep attack. This too is a viable approach for the partially modernized force or nonmodernized force entering a complex combat or noncombat environment where a number of

IO capabilities and or threats exist. Appendix D provides a notional IO structure at Figure D-1.

Information Operations Battle Staff

A dedicated IOBS can be formed to integrate IO actions. This approach would apply to partially and fully modernized forces. The battle staff would consist of all staff members with a functional responsibility within IO, such as signal, fire support, PA, CA, OPSEC, EW, PSYOP, and battlefield deception. Figure D-2 of Appendix D illustrates a notional IOBS.

J3/G3 Staff

Since IO are only one facet of the larger operation, albeit an important one, the J3/G3 is the primary manager of information. He outlines and monitors the performance and responsibilities of the staff in processing information to support IO and the knowledge flow. The J3/G3 ensures that the staff collects, analyzes, and presents information that fulfills the CCIR. Specific requests for information from BOSs or other information source data bases are generated to fill specific needs. Routine or standard reports to the staff (established by unit SOPs) are used when information requirements remain stable through operations.

The J3/G3, within his overall staff responsibility for integrating IO into the OPLAN, usually designates one individual accountable for all IO actions. Key staff members participating in IO coordination and integration include intelligence, signal, fire support, PA, CA, EW, deception, OPSEC, PSYOP, and logistics personnel. In peacetime operations, the G5, PAO, and specialized staff, such as the SJA or chaplain, participate in IO planning and operations. Even as the role of PA expands, a separation between PA and PSYOP functions must be preserved to maintain the credibility of PA spokespersons and products. While essential coordination between these staff functions may be accomplished through the IO cell, the IO cell PA representative should not also serve as the primary command spokesperson.

Army Land Information Warfare Activity

C^2W requires the commander to develop and sustain staff members who are technically and operationally proficient in C^2W. Maintaining C^2W staff proficiency is a complex undertaking, demanding extensive training, education, and experience with other services, agencies, and joint commands. To enhance the capability of the Army component to conduct IO, Department of the Army established the Land Information Warfare Activity (LIWA). LIWA acts as the operational focal point for land IW/C^2W by providing operational staff support to active and reserve component land component commanders (LCCs) and separate Army commands.

LIWA field support teams (FSTs) are tailored to fill the specific needs of a component commander and are specifically earmarked to that land component command. Team members consist of a need-driven mix of PSYOP, deception, OPSEC, EW, and intelligence specialties, along with members of other service components, if required. LIWA FST members support the LCC's staff as it plans, coordinates, and executes IW/C^2W in joint and multinational environments.

LIWA FST supports commands ranging in size and capability from a numbered Army headquarters to a corps or division when these tactical commands are designated the land component of a joint task force. Appendix B provides information on LIWA support and services.

What separates good units from not so good units is the way the unit processes information.

General Donn Starry, US Army (1978)

Planning Process

The IO planning process consists of five basic steps that apply across the three components of IO (operations, RII, and INFOSYS).

MISSION ANALYSIS

The first step of the process begins as the commander analyzes the mission, formulates his overall concept of operations, and considers how IO can contribute to achieving his mission. Under the direction of the J3/G3, the staff analyzes the command's mission and concept of operations to derive a concept of IO. Simply put, "How can IO support the mission?" The staff must consider both C^2-attack and C^2-protect. Flexibility is essential, as IO support may shift over the course of the overall operation.

During analysis, the staff examines enemy and friendly INFOSYS within the context of the commander's MIE. The staff determines the capabilities both sides require to operate effectively. It also sets out the requirements and conditions needed to establish information dominance. The staff considers nonmilitary INFOSYS influences or capabilities beyond traditional military control—such as local or regional communications networks, radio, television, computer networks (internet or worldwide web), and the news media—that may influence the operation. The examination produces a list of critical nodes and vulnerability analyses.

- The *C^2-attack* analysis identifies adversary C^2 systems of C^2W interest and determines the critical C^2 and C^2-attack nodes in those systems. The C^2-attack focus increases payoff by identifying key target vulnerabilities for offensive action.
- The *C^2-protect* analysis focuses on the adversary's capability to detect, locate, and attack critical friendly C^2 nodes to disrupt the friendly decision-making process. As with C^2-attack, intelligence plays a major role by providing information on adversary sensor capabilities, target selection, and attack means. The staff considers the physical destruction, jamming, and intrusion, as well as deception and PSYOP means available to the adversary. The product is a list of critical, vulnerable nodes and processes that must be addressed by C^2-protect.

PRIORITIZATION

The second step is to prioritize both friendly and enemy critical nodes and vulnerabilities. This part of the process develops potential targets for C^2-attack and C^2-protect and ensures deconfliction of their integrated effects.

For C^2-attack purposes, nodes critical to more than one adversary system may have a higher priority. Vulnerability may override criticality, with more critical nodes that are less vulnerable receiving a lower priority. Priorities should be balanced and shifted between C^2-attack and C^2-protect as required to support the unit mission. The C^2-attack product is a prioritization of the list of critical, vulnerable adversary targets from earlier work. Similarly, C^2-protect targets should be identified in terms of criticality and vulnerability, then prioritized.

CONCEPT OF OPERATIONS

The third step of the process is the formulation of an IO concept of operations to influence the adversary's C^2 while protecting friendly C^2. The G3/J3 reviews his sets of potential C^2-attack and C^2-protect targets. He assesses available IO capabilities to develop an IO concept of operation that best supports the overall operational mission and is synchronized with the overall concept of operation. Synchronization of IO, both internally (among the five C^2W elements and CA and PA) and externally (across the BOSs), is absolutely critical for achieving decisive C^2-attack and C^2-protect results. The impact of proper synchronization is to focus the effect of the entire range of friendly capabilities to achieve maximum effect at the decisive point in time and space.

Although the situation dictates the critical areas for the operation, the commander and staff consider these specific areas in planning:

- *Operations*—both C^2-attack and C^2-protect objectives from a friendly and enemy perspective. The basic OPLAN/OPORD and the C^2W annex synchronize physical destruction, EW, OPSEC, deception, and PSYOP to maximize C^2-attack and

C^2-protect. Many C^2W activities can have the effect of maximizing protection while degrading adversary C^2 capabilities. Other influences in the commander's information battlespace can directly impact mission success, for example, the media, governmental and nongovernmental organizations, local or regional social/cultural influences, perceptions, attitudes, and opinions.

- *RII* requirements.
- *INFOSYS* support requirements.

The battle staff considers all these factors to arrive at an IO concept of operations. The concept is oriented on establishing information dominance in order to give the force dominant battlespace awareness and control of the MIE. A critical tool in developing an effective concept of operation is the synchronization matrix. The synchronization matrix is designed to array time-phased objectives along a horizontal axis against performing units usually organized by BOS along a vertical axis. Within the framework of the matrix, critical tasks that must be performed to achieve the IO objectives are identified, aiding the planner in recognizing the interrelationship between specific tasks and actions and the need to orchestrate them in a manner that maximizes the impact of their execution. See Figure 6-2 for an example of an IO synchronization matrix.

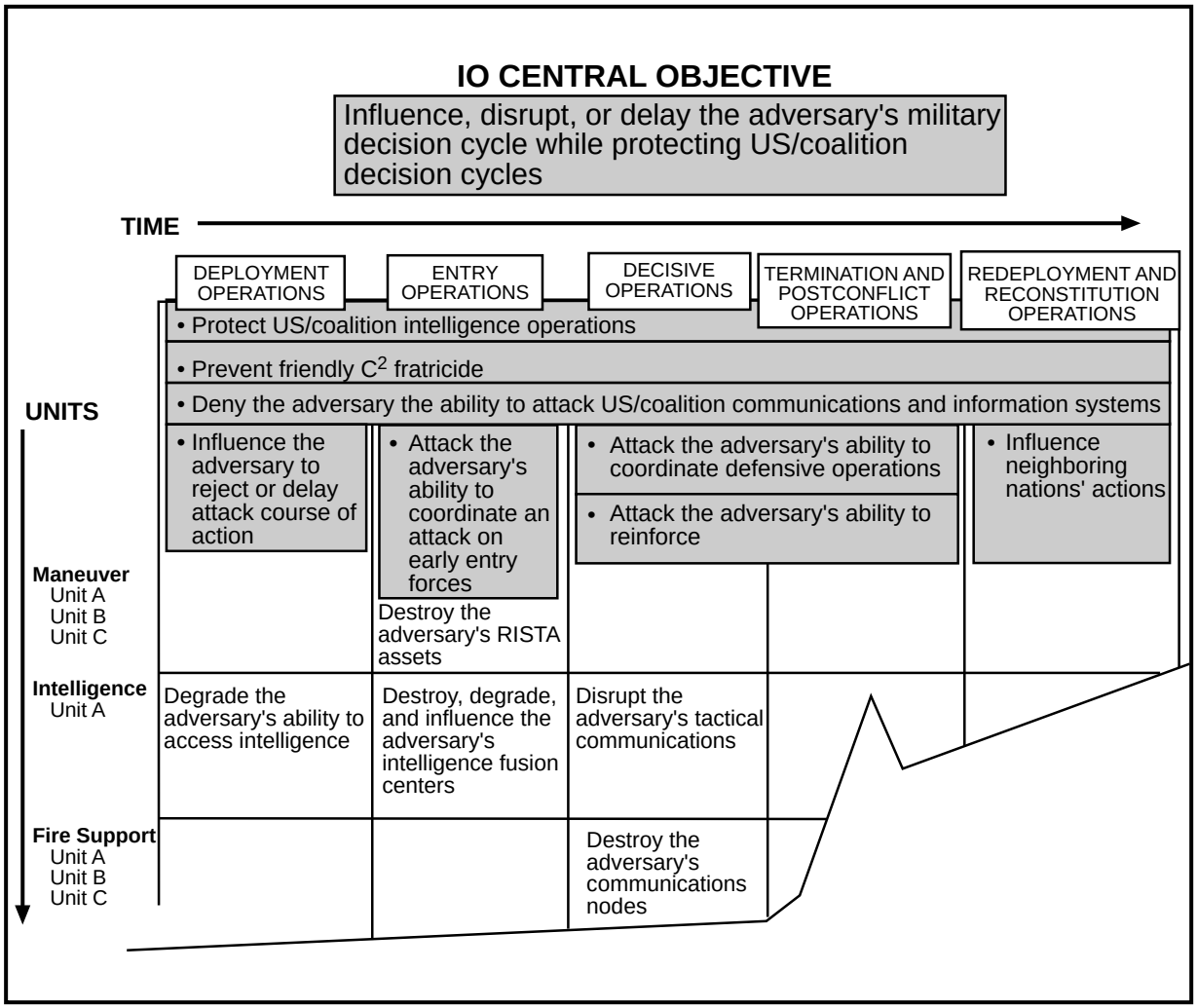

Figure 6-2. IO Synchronization Matrix

EXECUTION

Execution begins with tasking those elements that conduct IO missions. The G3/J3 controls and directs both the IO planning and execution phases of the process, with support from the G2 and IO element specialists on the staff. The keys here are—

- Selecting the best C^2-attack capability for the best effect (deny, influence, degrade, destroy).
- Synchronizing the application of effects to reinforce the five elements of C^2W, CA, and PA capabilities (not allow them to conflict). Similarly, protection of C^2 nodes needs to be tasked to available means and/or additional protective tactics, techniques, and procedures (TTP) adopted by the force.

IO taskings normally become part of the basic order paragraph 3 concept of operations and coordinating instructions. Additional IO details are covered in a separate annex that consolidates applicable IO/C^2W into one coherent operational discussion. When a separate IO/C^2W annex is written, it should include an IO/C^2W synchronization matrix that establishes time lines, responsibilities, sequence of actions, and desired effects.

As planning and execution take place, planners should consider a number of factors beyond strict combat capabilities. These include—

- The *opportunity cost of an action*—that is, what is the trade-off between attacking or destroying an adversary's capability now or exploiting that capability for future gain? As an example, destroying key C^2 facilities may give the operational commander freedom of action by denying the enemy effective C^2 of his forces. However, the opportunity cost of this action would be to deny national signal intelligence (SIGINT) systems a valuable link to the opponent's NCA. Therefore, the national command level would lose information about the adversary's national-level intent and resolve. Similarly, destroying an air defense network may give the tactical commander local air superiority, but it may also eliminate the only means the operational-level commander has to track or identify enemy formations.
- *Legal and policy restrictions and ROE*—in order to understand their impact on the linkage between the levels of war. Target planners are required to know the ROE as well as the laws and policy governing the attack of certain persons, places, or things. How does the commander deal with the commercial computer network, the local/regional phone network, or the cellular data net that not only supports the military effort but also the civilian population, commerce, and industry? Other considerations include when and what information to release to the media, NGOs, and PVOs.

Planners must be aware that the counter-IO the adversary launches will likely target US civilian infrastructures. The mere threat of such actions may also generate significant effects, both real and psychological. For example, an adversary's announcement claiming the insertion of a virus into a particular banking institution's computer operation could trigger a panic with major economic repercussions, regardless of the adversary's actual execution of such an attack.

FEEDBACK

The fifth step is to set up a monitoring and feedback mechanism. A continuous damage or effects assessment process is critical in order for the commander to revise his continuing estimate of the situation and adjust operations. See Appendix A to develop C^2W and IO-related planning products. The five-step planning process is illustrated in Figure 6-3.

EXECUTION

The force-projection cycle is an excellent framework to discuss how to execute IO. The packaging, timing, and employment of key IO activities is essential to attaining and maintaining information dominance in conducting operations across the full spectrum, to include OOTW.

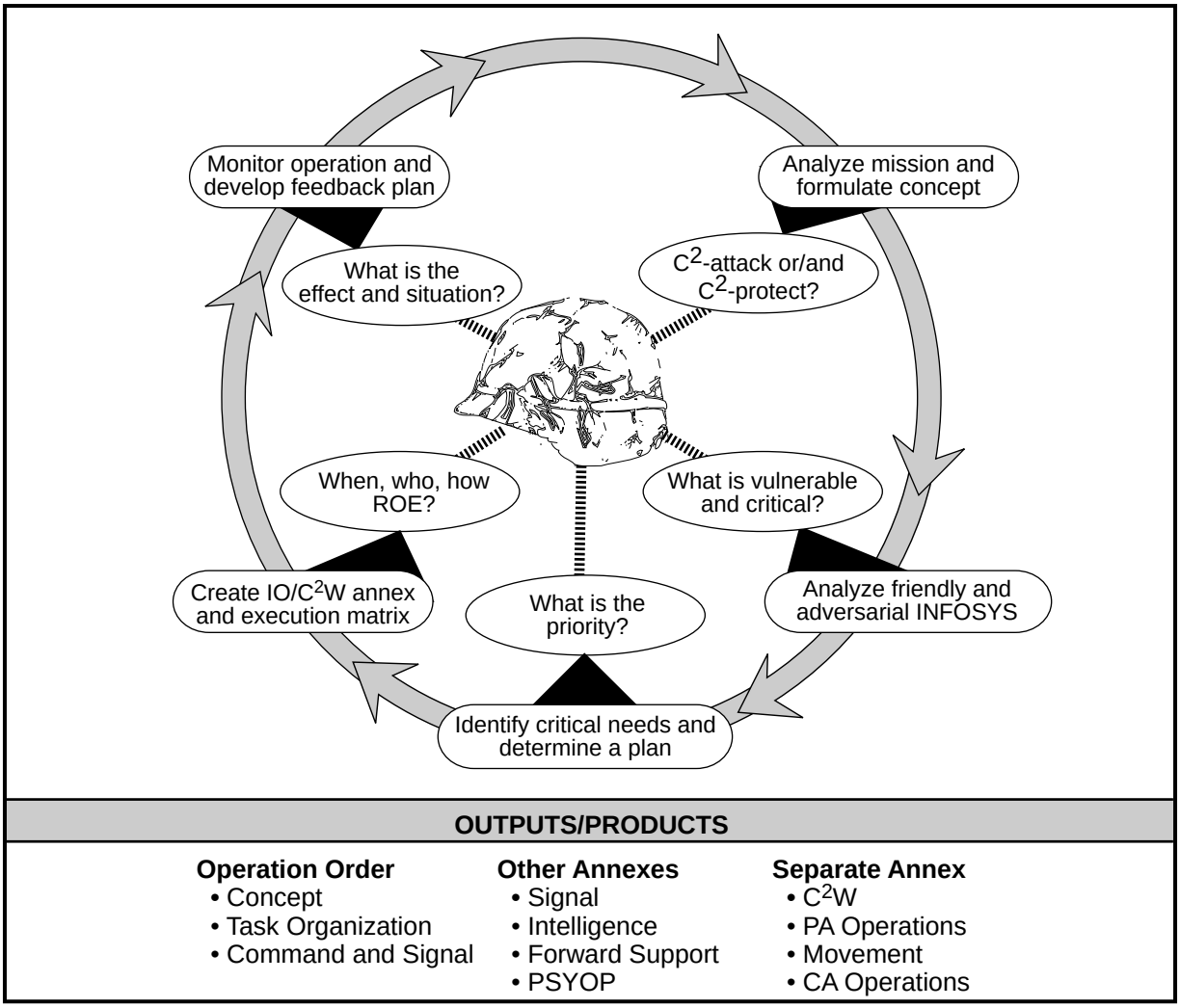

Figure 6-3. IO Planning Process

Force-Projection Operations

Our post-Cold War *National Military Strategy* calls for a primarily CONUS-based Army—one that is capable of rapid power projection on short notice to any region of the globe to decisively defeat a regional adversary. These force-projection operations follow a general sequence of stages that often overlap in space and time. IO considerations and actions apply to all force-projection stages. They focus on ensuring information support to battle command during all joint, multinational, and interagency operations and effective intervention against the adversary's C^2.

In many situations, GIE organizations will be present in the AOR before Army forces arrive. They will often be well-entrenched, with an established logistical framework and long-standing coordination and liaison arrangements. For example, initially the media may know the AOR better than the military. As it covers the buildup, the media gains a thorough understanding of and forms its own perspective about the situation, particularly in OOTW. The projection of Army forces into the situation is of national interest, with national and international media watching from the moment forces arrive. CA and PA personnel need to deploy early to

support the commander and the force in their interactions with these organizations. CA and PA operations not only reduce the potential distractions to a commander but also educate these organizations and facilitate their efforts to provide accurate, balanced, credible, and timely information to local officials and agencies, as well as external audiences. Some unique considerations apply for force-projection operations and OOTW.

The friendly communications infrastructure provides the means to integrate C^4I capabilities starting from the installation power-projection platform with reach-back capabilities while en route, during initial entry, during buildup, throughout the operation, and during redeployment. The variety of conditions under which the Army is employed in the Information Age requires close IO coordination, integration, and synchronization from the strategic to the tactical level. Figure 6-4 outlines this concept. Force projection, supported by IO, is continuous and seamless and compresses time and space.

MOBILIZATION OPERATIONS

Mobilization is an information-intensive operation. Once mobilization is declared, the unit's activities include assembling personnel, checking readiness factors, and time-phasing operations to meet force deployment schedules. IO assist in synchronizing arrival, processing, certifying, and moving to final points of departure. The Army depends on information management resources in its sustaining base to accomplish the mobilization process. These resources include—

- The Standard Army Management Information System (STAMIS).
- FORSCOM's Mobilization Level Application Software (MOBLAS).
- TRADOC's Reception Battalion Automated Support System (RECBASS).
- DOD INFOSYS such as the Defense Joint Military Pay System (DJMS) and the Defense Enrollment Eligibility Reporting System (DEERS).

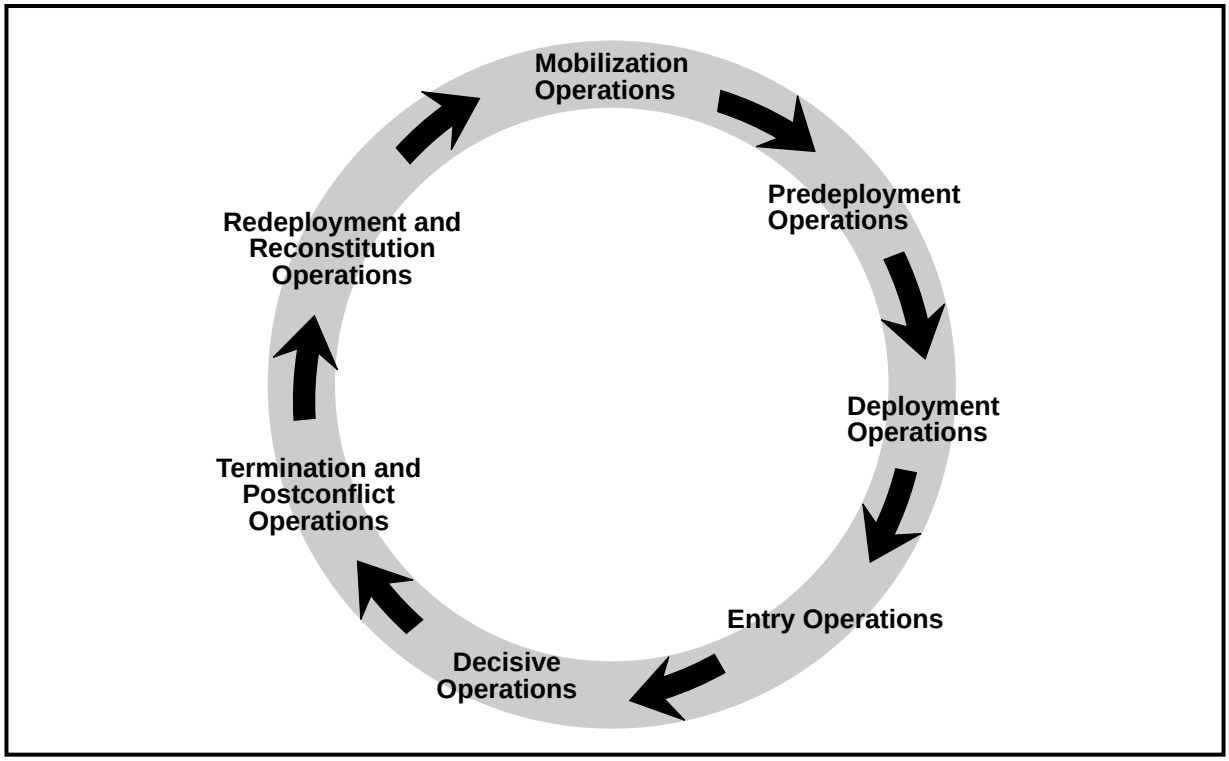

Figure 6-4. Army Force-Projection Cycle

Most of these systems depend upon the NII for their operation. Many run on standard commercial platforms such as personal computers (PCs), reduced instruction set computing (RISCs), or mainframes. The systems could be expanded or enhanced during a crisis. Their dependence also underscores the importance of engaging the interagency process to help secure the NII from possible attack or compromise.

Intelligence activities during the mobilization phase focus on collecting intelligence on probable operational environments and potential adversaries. The staff performs the initial information-based IPB during peacetime.

C^2W activities during mobilization are predominantly concerned with protecting information. Upon mobilization, protection of information is included in the commander's recall and assembly plans. C^2-protect measures protect the availability, integrity, and confidentiality of unclassified and classified information necessary to support mobilization operations. During this stage of force projection, bits of information conveyed in nonsecure public and military radio transmissions, news releases, friendly conversations, telephone calls, trash, and so forth, permit news media personnel or hostile intelligence analysts to piece together US intentions and capabilities. OPSEC and INFOSEC aid the commander in preventing adversaries from collecting information of intelligence value.

PREDEPLOYMENT OPERATIONS

Commanders establish objectives and unit requirements to set the stage for predeployment activities and seek to preserve friendly assessments and decision-making capabilities. IO integrate the elements of C^2W to mask deployment and enhance deception operations. Plans include—

- Engagement of the adversary's INFOSYS.
- Identification of tasks, C^2W target sets, specific procedures, and coordinating instructions—all displayed within a detailed IO synchronization matrix.

These steps ensure the implementation of IO and set the stage for ongoing military actions.

PA operations during predeployment contribute to establishing conditions that lead to confidence in the Army and its readiness to conduct operations while remaining attentive to OPSEC and INFOSEC. As units are identified for possible or actual mobilization, public and media attention increases dramatically. PA operations contribute to a reduction in rumors, misinformation, and uncertainty on the part of soldiers, family members, and the public.

During the predeployment phase, tactical INFOSYS continue to be used less than fixed military and civilian systems for routine actions during predeployment. Military systems that link operational and strategic echelons, such as the DISN and the Defense Switch Network (DSN), are the primary dedicated military systems used. Intelligence, logistics, and operational planning require extensive coordination with outside agencies, other services, and so forth, to provide the data required.

Intelligence activities continue to revolve around establishing an adversarial data base and an information-based IPB. Component commands require national intelligence and weather data to support detailed planning. Before deployment, the commander's staff should develop CCIR, PIR, CMO, and RISTA plans.

C^2W actions continue to focus on protecting information through exercising OPSEC procedures. With the support of the higher joint headquarters, as augmented by LIWA, C^2W planners consider offensive actions to establish information dominance once the force begins to deploy. Close coordination with PA personnel is required during deception and PSYOP planning to maintain OPSEC and ensure such efforts are not targeted against friendly audiences and, most importantly, US, allied, or coalition media.

PA develops assessments for current and future operations. Planning continues for appropriate media inclusion (journalists accompanying units). PA implications of all aspects of the operation are considered to include media attention and public response. Synchronized PA programs contribute to increased soldier understanding, confidence, dedication, discipline, will to win, and public

confidence in the Army. PA efforts focus on protecting and enhancing the *public support of gravity*.

DEPLOYMENT OPERATIONS

IO are necessary to establish the conditions for deploying forces into an AO. Deploying forces require near-real-time joint and/or interagency communications tailored for rapid deployment, en route operations, and links from strategic through tactical levels.

During the deployment stage, staff planning functions intensify. Contingency plans (CONPLANs) and PIR are updated, completed, or adjusted. Commanders and staff planners tap into joint and interagency planning systems and data bases, such as the Joint Operations Planning and Execution System (JOPES) and the Army Mobilization and Operations Planning and Execution System (AMOPES), to determine lift asset availability and sequencing. Intelligence requirements and assessments are continually monitored and adjusted. As forces begin deploying, commanders plan for the impact of force separation and reduced information support through low-capacity systems. They adjust their CCIR to those most critical to maintain situational awareness, training readiness, and mission accomplishment.

INFOSYS requirements for deploying forces demand home station, en route, and intertheater/intratheater communications that are secure, flexible, and deployable. These INFOSYS must be capable of interoperating with joint forces, civilian agencies, and multinational or coalition forces. INFOSYS support mission planning with multiple continuous intelligence and logistics links to the deploying/deployed force, home station, major commands, logistics agencies, and national and joint intelligence sources.

Deploying forces are highly dependent on CONUS-based intelligence, such as imagery and weather, derived from national or theater-based sensors. The forces require assured and survivable communications to numerous agencies. During deployment, echelons above division execute most of the C^2W actions such as deception, PSYOP, and continued OPSEC.

ENTRY OPERATIONS

IO are necessary to establish the conditions for successful early entry. IO capabilities are deployed into a contingency area with a focus on their ability to gather the information required by the commander while denying the enemy use of his information and IO capabilities. Early entry operations vary by region and mission. In both unopposed and opposed entry, counter-RISTA operations are essential. Air and missile defense is key to successful counter-RISTA operations during the early entry period when forces are most vulnerable. Air and missile defense systems negate enemy airborne RISTA, EW, and C^2 platforms while simultaneously protecting key geopolitical assets and the force's critical nodes from air and missile attack.

Unopposed Entry

Unopposed entry allows for greater use of IO capabilities. Early deploying assets focus IO on the adversary to support forward presence or host nation (HN) forces. Early entry forces rely on split-based communications with CONUS-based elements for most of their intelligence and communications support. Although HN or commercial systems may be available, planner awareness of statutory requirements regarding their use is essential.

Opposed Entry

When entry is opposed, commanders may have to rely on a limited number of INFOSYS to get the information they need to accomplish the mission. Because information requirements may well overwhelm the capability of available assets, commanders must clearly prioritize their information needs to best focus the use of these limited capabilities.

Working within the joint IW/C^2W plan, army commands employ their C^2W capabilities to satisfy assigned tasks. Successful opposed entry operations can be significantly enhanced by denying the adversary use of his INFOSYS through employment of C^2-attack assets. C^2-attack could include deceiving or overloading the adversary's INFOSYS and disrupting his use of the EMS.

DECISIVE OPERATIONS

Commanders visualize the battlespace and develop operational concepts that use common

situational awareness and the ability to rapidly and accurately move information about the battlefield. The IO capabilities available to the unit permit surprise and the decisive defeat of the adversary from dispersed positions. Defeat of the enemy is usually accomplished most effectively by countering enemy strengths with dissimilar (asymmetrical) systems and methods. Units begin to conduct offensive C^2W operations. This requires friendly commanders to exercise increased control over the tempo of battlefield activities. Tactical commanders leverage their information superiority to employ weapon systems, including joint assets, and to regulate the nature and tempo of enemy actions.

To optimize the flow of essential information, commanders prioritize their information requirements through CCIR and SOPs. The IOBS, however constituted, ensures that C^2W, PA, and CA are integrated into the commander's concept of operation. This is accomplished as the G3 integrates his IO assets into the operational scheme to get the best possible picture based on the commander's intent. Moreover, the G3 leverages organizations and assets from the GIE, that is, joint and national intelligence assets, to complete the IPB mosaic. Often, the assets available are less than those needed to perform the desired IO. The commander provides the focus to prioritize these IO assets. Constant monitoring of enemy and friendly IO status ensures this information is included in situation updates, IPB, and the commander's RCP of his battlespace.

Media and public attention is usually more intense during this phase. PA operations include media facilitation, advising the commander on PA implications of the operation, as well as providing for internal and external audience information needs. PA personnel review strategic and operational information with PA implications, coordinate with CA and PSYOP, and facilitate releasable information.

Unity of effort and massing of combat power effects are enabled by enhanced information flow, both vertically and horizontally, among commanders and staff members and supported by military INFOSYS. Tactical units employ military information to fully integrate the systems, capabilities, and functions of the combined arms team into the conduct of decisive operations. Control of decentralized maneuver and engagement is achieved by optimizing the enhanced situational awareness and communication provided by digital connectivity. This ability allows tactical units the opportunity to avoid adversary strengths and detection means while moving into the most advantageous positions to permit the destruction of the enemy force in both offensive and defensive operations. Units exercise the capability to focus and mass the effects of indirect fires against the adversary and to synchronize their effects with maneuver. By employing highly maneuverable artillery, aviation platforms, suites of digital sensors, and intelligent minefield systems, maneuver units establish *quick-fire* sensor-to-shooter links that acquire, strike, assess, and restrike enemy targets at a high rate and level of lethality.

Enhanced situational awareness and communications capabilities allow the maneuver commander to conduct decisive strikes within the enemy depth by employing both organic and supporting fire systems. Commanders use C^2-attack to destroy, disrupt, and exploit enemy INFOSYS. By providing the RCP at all echelons, IO facilitate the synchronization of all combat power across the BOSs. In conjunction with air and ground battle plans, commanders must select the proper vulnerable nodes and know whether to destroy or merely disrupt them and when to exploit through C^2W.

Available IO assets may dictate the arrangement of forces on the ground. Coalitions may be formed with armies that have varying IO technical capabilities. Intelligence can be used to ensure the validity of target nominations, while the C^2W planning process can ensure that the appropriate response is directed against that target.

Our present theory is to destroy personnel, our new theory should be to destroy commands. Not after the enemy's personnel has been disorganized, but before it has been attacked, so that it may be found in a state of disorganization when attacked.

Extracted from J.F.C. Fuller's memorandum
"Strategic Paralysis as the Object of the Decisive Attack," May 1918

TERMINATION AND POSTCONFLICT OPERATIONS

IO enter a new phase upon termination of hostilities. The aftermath of war could leave a significant dislocation of the infrastructure and population in the area of conflict. The potential for renewed conflict should not be discounted. In these circumstances the protection of information by OPSEC, the hand-off of military information to other nonmilitary organizations, and even the continued collection of new information may become necessary. Certain military information is protected, while other military information is required to be released publicly to prevent further bloodshed and permit resumption of normal life. Conscious decisions in the orchestration of these competing demands exist as IO continue. For example, the presence of minefields and their location should be released to all parties to prevent civilian causalities.

Dislocations and damage following combat generate requirements for new information. Monitoring, relocating, and providing humanitarian assistance for displaced persons is as much an information problem as it is a logistical one. Destruction of physical infrastructures may dictate that for humanitarian reasons the US leave particular items of equipment in place that would otherwise be redeployed. Such equipment may include temporary bridges that replace destroyed ones, radio broadcast band transmission equipment, and electrical generation or water purification equipment. Information is critical in making these decisions. Further uses of such information are required to adjust Army data bases and unit readiness affected by these actions.

When combat operations bring an end to the conflict, deployed forces transition to a period of postconflict operations. The transition to postconflict operations can occur even if residual combat operations are still underway in parts of the AO. Therefore, adjustments to IO must be anticipated and planned to ensure a smooth transition during the critical period after the fighting stops. IO adjustments during postconflict operations focus on providing support for restoring order, reestablishing the HN infrastructure, preparing forces for redeployment, and continuing a presence to allow other elements of national power to achieve strategic aims.

The transition plan for postconflict operations prioritizes and plans for information requirements and required connectivity to support civil administration mission activities; CMO such as civil defense, humanitarian assistance, and populace and resources control (PRC); and unified planning with DOS, NGOs, PVOs, and HN officials and agencies. CA personnel are uniquely qualified to advise the commander on these activities that reduce postconflict turmoil and stabilize the situation until international relief organizations or HN agencies assume control.

Postconflict operations require close coordination between PA elements and those conducting CMO to ensure consistent, accurate dissemination of information. Internal information programs aid the transition to redeployment and reconstitution by reducing rumors and uncertainty. IO transition planning addresses the smooth retrograde of assets from the theater of operations, while considering the possibility of renewed hostilities. Tactical and mobile information assets should be replaced as soon as possible by the fixed communications and information infrastructure of the HN. Part of this stage may include transition of INFOSYS and operations to DOS, PVOs, NGOs, the HN, or other agencies that represent nonmilitary options to support HN rebuilding. Planning begins at this point for support of the redeployment of friendly forces and continued reconstitution of assets destroyed in the conflict or retained by the HN.

REDEPLOYMENT AND RECONSTITUTION

Normally, reconstitution and redeployment actions occur in a benign regional environment; however this is not always the case. Sensitivity to the effect information has on the population remains a concern. PSYOP and CA may be used to gain and continue support of the population. Information about Army operations and CMO can be disseminated through local, national, and international media. PA operations do not focus on directing or manipulating public opinion, but on providing accurate, timely information about operations. PA personnel take action when necessary to counter misinformation communicated via the GIE.

Intelligence collection may focus on nonbattlefield aspects of the current environment and the potential for new threats or adversaries to emerge. Commanders must remain sensitive to the potential vulnerability of critical nodes or systems to renewed adversary operations and be prepared to shift to alternative means if necessary.

In this stage, IO support the redeployment of assets no longer needed or needed for another mission elsewhere. Commanders plan and prioritize their IO to allow a smooth transition for redeployment. Postconflict requirements have a direct impact on the redeployment flow. INFOSYS must integrate contractor and HN asset capabilities into the redeployment flow.

Units must be rapidly reconstituted to premobilization levels of readiness. To ensure rapid replacement and refitting for new missions, units must identify lost or incomplete equipment because of the high probability of some information assets being left in theater or not yet replaced by the logistics system. Commanders must continue to emphasize INFOSEC during redeployment operations, especially in the event of ongoing hostilities.

Operations Other Than War

Military operations other than war usually involve a combination of air, land, sea, space, and special operations forces as well as the efforts of governmental agencies and nongovernmental organizations in a complementary fashion.

Joint Pub 3-0

Army forces face complex and sensitive situations in a variety of OOTW. These range from supporting near hostilities in peace enforcement and peacekeeping operations; through drug interdiction, nation assistance, and humanitarian assistance; to support for US state and local authorities responding to natural disasters or civil unrest.

The primary tool for mission accomplishment in conventional military operations is the use of force directed against an adversary. In OOTW, however, such a threat may not be present or may not be clearly defined. The threat in these environments may be rogue elements, thugs, or even the adverse effects of the environment or a natural disaster. Hence, commanders employ a wider range of methods in less conventional ways that involve many more players to accomplish the mission. As such, IO capabilities to support the assigned missions may become essential for success. IO may be one of the most critical and acceptable means of achieving the assigned objectives because ROE may severely restrict the use of conventional military weapons.

In OOTW, as in other operations, military IO capabilities are not the only assets the commander may have available. Non-DOD, state, and local agencies; international organizations; military or paramilitary forces; and private organizations may also be available to contribute to IO. These players may offer a variety of services and resources, both military and nonmilitary, from within the GIE. This expanded field of individual and organizational senders and receivers of information, with varying methods of operation and focus, add a

Historical Perspective

Projection of information is essential to successful military operations. During Operation Restore Hope in Somalia in 1992-1993, a peace operation, the 10th Mountain Division (LI) adjusted its mission analysis and tracking by establishing information dissemination as a BOS. This BOS included PA, PSYOP, and information for soldiers. The division considered full integration of these activities into all aspects of the operation as critical to success.

variety of INFOSYS needs. Interoperability, cooperation, coordination, and liaison may significantly increase resource requirements.

COORDINATION AND LIAISON

IO can be extremely complex and demanding. The Army is often faced with formidable infrastructure and interoperability challenges, both at home for domestic support operations and abroad for multinational operations, often in austere environments.

To provide coherence to information efforts, IO planning must be in sufficient detail and coordinated with all participating agencies. This requires extensive coordination and liaison. As an example, CA, PSYOP, and PA elements are able to use the same communications media with essentially the same messages but to different audiences. CA and PSYOP personnel address local populations and enemy forces, respectively, while PA personnel address US forces and national and international news media. Employment of C^2W, intelligence, and INFOSYS capabilities requires coordination to ensure the synchronization of operations among participating organizations. Since military and civilian systems are often incompatible, military and supported agency communication planners must coordinate as early as possible in the operation. The Army may be required to coordinate IO with the following organizations:

United States Agencies

The Army may coordinate with non-DOD agencies in the broad spectrum of OOTW, especially when the Army is placed in a supporting role to US agencies during domestic support operations. FMs 100-19 and 100-23 and Joint Pub 3-08 list and describe various agencies requiring consideration. Among these is the United States Information Agency (USIA), which is especially pertinent for the conduct of public diplomacy information efforts conducted in foreign countries.

United Nations

The nations involved in specific UN operations rely on shared, relevant, and pertinent data concerning the situation and parties involved in the operation. IO help synthesize this data for a common understanding of threatened interests, to determine relevant and attainable objectives, and to achieve unified efforts. The methodology for exchanging intelligence information should be conceived and exercised well before operations begin. US intelligence personnel know and understand foreign disclosure policy and procedures. They generally obtain necessary foreign disclosure authorization from the Defense Intelligence Agency.

NGOs and PVOs

The number of NGOs and PVOs that may be found in a commander's AO could be extensive. NGOs and PVOs can be valuable sources of information that commanders involved in IO should consider. Commanders may also need to create centralized control and liaison structures, such as CMOCs or emergency operations centers (EOCs), to facilitate coordinated efforts with NGOs. See FM 100-23-1.

Local Assets

Local assets may provide the capability to support and secure the temporary setup of IO—telephone towers, satellites, ground cables, or other utilities that would allow commanders to achieve assigned objectives or tasks. Also, some localities may have the equivalent of non-DOD agencies. The US embassy or consulate can be contacted for assistance in establishing liaison with these agencies. These agencies may provide invaluable assistance in these environments.

SPECIAL CONSIDERATIONS

All operations require gathering and dissemination information, as well as some form of intelligence. Since intelligence is a restrictive term, the preferred terminology in UN operations is *information-gathering* and *dissemination.* Accurate information is essential for planning PSYOP, OPSEC, EW, destruction, and deception operations.

By gathering information from soldiers, NGOs, PVOs, and civilians personally involved in the day-to-day operation, a commander can gauge the mission's effectiveness and better plan current and future IO. Maximum use should be

made of open-source information. When practical, tactical information-gathering systems should be used so that information may be disseminated to UN/coalition forces, NGOs and PVOs, and other government agencies. However, parties to a conflict in peacekeeping operations or civilians in other operations may perceive information-gathering as intrusive or hostile. Therefore, intelligence activities must always be sensitive to legal constraints and/or maintaining the trust of the parties involved. The perception of impartiality is important for the protection of the peacekeeping force. Important intelligence considerations include the following:

- Every item of operational information becomes potentially important during OOTW.
- Personnel have to be information-conscious at all times.
- Participants must remain constantly alert to what takes place around them and to any change or inconsistency in the behavior, attitude, and activities of the military and civilian populace.

Information-gathering assets, sources, and agencies include those used in conventional operations as well as some that are not normally considered. Intelligence personnel will make traditional use of all organic or attached collection assets. However, they may also use other sources and agencies such as the local news media, NGOs, PVOs, international organizations, and exchanges with local police, governments, and militaries. Dissemination of intelligence is conducted using standard intelligence report formats. Intelligence personnel pass information to liaison officers (LOs) who pass intelligence products to parties requiring them in joint or multinational operations.

Although not peacetime operations, CA and PSYOP are critical operations that aid commanders in accomplishing their peacetime objectives. Commanders must understand CA and PSYOP abilities to support US and allied armed forces. PSYOP is a vital force employed to optimize the influence of US national policy on foreign target audiences, whether neutral, hostile, or friendly. In other operations, PSYOP provide the commander with the capability to project the purpose and mission of US forces and to influence target audience behavior to support the commander's mission. For PSYOP to achieve maximum effectiveness, planners must include them early in the planning process. In crisis situations, rapid production and dissemination of accurate information to the population are critical. PSYOP personnel can provide the commander with real-time analysis of the perceptions and attitudes of the civilian population and the effectiveness of the information being disseminated.

Signal support to OOTW missions requires the same detailed planning as any other operation. However, the scope and scale of planning may actually increase when the commander is considering or is confronted with—

- Nonmilitary INFOSYS such as commercial and local communications services. The operational principles of signal support apply.
- Interfaces among military and commercial communications, INFOSYS, and networks. Most civil and military communications systems are incompatible because of different equipment, frequency allocations, and usage parameters. For these reasons, military and civilian communications planners must exchange knowledgeable communications support personnel and compatible equipment to ensure connectivity is maintained between military and civilian operations centers. This exchange of personnel and equipment can occur at any level and should be implemented and modified as the situation dictates.

Appendix A

Plans and Orders

This appendix illustrates and explains how IO and C²W could be incorporated into a basic plan or order. The OPLAN format is used for this illustration. Annex A provides a sample campaign plan model and identifies the key annexes related to IO support. Annex B illustrates how a C²W annex is written.

PLANS

Commanders use operations, administrative, and logistics plans and orders to convey information and instructions to subordinate units. Plans and orders are similar in format and content. Although a plan may be effective immediately for planning purposes or for specified preparatory action, it is not executed until the commander so directs, usually when certain specified conditions, as set forth in the plan, are determined to exist. A plan specifies the time or conditions under which it is to be placed in effect.

ORDERS

A plan becomes an order when execution is directed. An order carries with it the obligation of immediate execution at a specified time or date. The major difference between a plan and an order is that a plan normally contains assumptions. See Chapter 6 for general information about planning and execution.

(SECURITY CLASSIFICATION)

Annex A

Major Operations Plan Model[1] Operational Level

(Sample Campaign OPLAN)

Copy No. ___
Issuing Headquarters
Place of Issue
Date/Time Group of Signature

MAJOR OPERATION PLAN: (Number or code name)

References: Maps, charts, and other documents

TASK ORGANIZATION/COMMAND RELATIONSHIPS.

1. **SITUATION.** Integrate tactical considerations important to IO in the early phases of an operation into the overall description of the operational situation. Refer to command and staff estimates, country studies, or OPLANs. Indicate trigger events that would signal execution of specific components to an IO within the OPORD.

a. **Intelligence.** Integrate adversary threats to friendly IO. A detailed discussion of the intelligence aspects of IO is found in the intelligence annex (Annex B) or the intelligence estimate.

b. **Friendly Forces.** Provide information on friendly forces that may affect the execution of the IO plan being put forth. These effects may impact directly on the command or on organizations subordinate to the command.

c. **Attachments and Detachments.** List attachments and detachments here.

d. **Assumptions.** Integrate a summary of the conditions and situations that must exist to enhance IO.

2. **MISSION.** Address IO to the degree necessary to fully state the overall operational mission.

3. **EXECUTION.**

a. **Commander's Intent.** Briefly include how IO will support the mission within the context of the commander's overall vision of the operation.

[1] This OPLAN format conforms to the format delineated in Joint Pub 5-00.2 and FM 101-5.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

b. **Concept of Operations.** Include a clear, concise statement of implied or specified IO tasks to be achieved in all phases of the major operation. One example is legitimizing an overall campaign through IO to prepare the people in the adversary country to accept results of the operation, particularly if it could be viewed with bitterness. Summarize IO tasks assigned by the CINC and other informational tasks derived from the commander's analysis of the environment and his understanding of his superiors' intent. At the operational level, the concept of operation is usually divided into phases.

(1) **Phase I.** The first operational phase of a contingency is usually the detailed preparation of the command to execute the operation. IO elements often addressed during this phase include the following:

(a) Establishing liaison with various entities, to include the unified command responsible for the target area; with other unified and subunified commands (especially those involved in deployment); with SOF already in the target area; and with appropriate US Government agencies. Each of these liaisons will form a portion of the overall IO support.

(b) Using diplomatic and interagency support to assist in transferring status of forces agreements, constraints (Annex E), and ROE (Annex F) for the proposed operation with participating nations (in coordination with DOS and appropriate embassies and country teams).

(c) Establishing INFOSYS forward to establish C^2 and to assist in establishing or preparing intermediate staging bases in the target region and directing the repositioning of supplies and equipment.

(d) Using CA, PSYOP, and PA to support political and diplomatic initiatives.

(e) Transmitting the commander's intent and scheme of operational maneuver, including close battle, deep battle, and rear security operations to ensure simultaneous understanding and execution of complex operations by all participants.

(f) Supporting operational fires with IO such as EW and appropriate C^4I architectures. This support assists complex arrangements for fire support (Annex G), including joint and multinational employment of fires and targeting.

(g) Determining IO support to civil affairs (Annex T), air defense (Annex H), EW and ES (Annex D, Appendix B), PSYOP (Annex D, Appendix D), and rear operations (Annex L), protection of forces and means (Annex M), provost marshal functions (Annex N), PA (Annex O), and space operations (Annex P).

(SECURITY CLASSIFICATION)

(h) Developing IO branches and sequels.

(i) Providing coordinating instructions applicable to two or more subordinate elements executing IO. Also include instructions for informational linkups with SOF or ground units involved in the deep battle.

(2) **Phase II.** The second operational phase is usually the execution of the operation itself. Address those aspects of IO that play a major role in supporting this phase.

(a) Include in the description of the concept of operations the role of IO elements in increasing the effectiveness of major units.

(b) Set forth the scheme of maneuver, as well as the deployment scheme, of IO units to attain initial objectives. The scheme should include, where appropriate, the forcible insertion of combat elements and necessary C^2 elements and their accompanying support. Address—

1. Sequencing of informational units as the operational situation becomes clearer. The deployment of contributing informational elements may be accelerated or delayed as appropriate.

2. Changes in the nature of the operation.

3. Major regrouping of informational forces.

4. Significant changes in enemy capabilities that would affect the informational units necessary in the operation.

(c) In the fire support subparagraph or its annex, address joint interfaces such as the joint targeting board (JTB) and the battlefield coordination element (BCE) and the IO considerations bearing on such interfaces.

(d) Include IO provisions for CA (Annex T), air defense (Annex H), EW and ES (Annex D, Appendix D), PSYOP (Annex D, Appendix D) and rear operations (Annex L), protection of forces and means (Annex M), provost marshal functions (Annex N), PA (Annex O), and space operations (Annex P).

(e) As necessary, state the location and tasks for IO elements held in reserve.

(f) Include coordinating instructions that apply to two or more subordinate elements executing IO. Also include link-up procedures through IO between the force and forces already in the operation, if appropriate.

(SECURITY CLASSIFICATION)

(3) **Phase III.** The third operational phase is usually the consolidation of the results of a successful end state for this phase. It does not contain the detail of the preceding phases. Address supporting IO as appropriate.

c. **Tasks for Major Subordinate Commands.** Ensure that IO are addressed as appropriate for each major subordinate command.

d. **Coordinating Instructions.** Integrate instructions on C ^{2}W whenever two or more phases of the operation are affected. Coordinating instructions may include the following:

(1) Times, events, or situations that may signal the transition of various IO between phases.

(2) Constraints (Annex E). IO in situations other than war are usually constrained significantly by factors other than strictly military ones. Describe such limitations on IO on military actions in the same annex detailing the provisions of treaties, agreements, and conventions governing the political, military, and informational limits on the military effort.

(3) Rules of engagement (Annex F). In addition to constraints imposed by international agreement, certain self-imposed ROE govern the use of military forces and certain weapons effects during the major operation. These rules may affect the use of EMS, computer networks, and interference with space-based communications and other signals.

(4) Resource management guidance that may limit IO (for example, limited communications circuits, limited equipment availability, or limited access to networks).

(5) Training guidance concerning IO procedures (for example, PSYOP, CA). Refer to a separate annex (Annex Q).

(6) Operational planning guidance involving IO.

(7) Space operations planning guidance (Annex P) providing enhancements to IO.

(8) Public affairs operations (Annex O).

4. **SUPPORT.** Insert specific information as to how IO support Army elements involved in an operation. In this paragraph or in a support annex (Annex R), the ARFOR commander includes IO among descriptions of those support matters necessary to accomplish the combat mission of his force. The IO support plan phases must coincide with OPLAN phases.

5. **COMMAND AND SIGNAL**.

a. **Command** . Enter liaison requirements and designate alternate command posts (CP) and succession of command if not adequately

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

covered in the SOP. This instruction includes CP locations and axis of CP displacement if not shown on an accompanying overlay.

b. **Signal.** As a minimum, list the current communications-electronics operations instructions (CEOI) index. These instructions can refer to an annex but should include rules concerning the use of communications and other electronic equipment (for example, radio silence).

ANNEXES: In recognition of the expanding contribution that IO can make to the accomplishment of the overall mission, OPLAN annexes have been reorganized by creating a new C ^{2}W Annex that consolidates the traditional annexes dealing with deception, EW, and PSYOP.

A Task Organization/Command Relationships . In a plan for a major operation composed of several phases, within this annex, identify and integrate the task organization required to conduct IO. Outline command relationships and their changes, if any, as the IO progresses from one phase to the next. Include information-specific task organizations for Army component support to contingencies in the annexes referring to the plans for those operations. Relate the informational structure against interfaces expected with the following activities involved in the operation:

a. **Civil-Political Relationships**. Embassies, country teams, non-DOD US Government agencies (Central Intelligence Agency [CIA], Drug Enforcement Agency [DEA], Agency for International Development [AID]).

b. **Multinational Force Relationships** . Host nations, allies, forces from regional/treaty organizations.

c. **Joint Relationships.** DOD agencies (DIA, NSA, DISA), unified and specified commands (subunified commands and joint task forces when appropriate), other services in uniservice roles.

d. **Other Army Forces.** The informational structure that enables connectivity from the highest level army component participating in operations down to the lowest level, including:

(1) Army components of subunified commands and joint task forces.

(2) Functional commands.

(3) Area commands.

(4) Major combat and combat support organizations directly under full theater army command in peacetime.

(5) Army organizations providing EAC support to the BCE and air combat elements.

(6) ARSOF, especially deployable informational structures, to include PSYOP, SF, and supporting communications units.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

B **Intelligence**. This annex should incorporate critical information needed to support IO and integrate those elements into the larger overview of the enemy situation. Detailed information needed to conduct C^2W operations should be further developed in the C^2W Annex.

C **Operations Overlay** . This annex is a graphic representation of the concept of operations.

D **C^2W Annex.** The C^2W annex focuses on providing the necessary information to conduct C^2W operations and consolidates all information previously found in the annexes dealing with deception (formerly Annex D), EW (formerly Annex I), and PSYOP (formerly Annex K). The intent is to integrate all aspects of C^2W to best identify and synchronize the application of available capabilities to achieve the overall mission. A sample C^2W Annex is provided in Annex B of this appendix.

E **Constraints**. This annex contains those political, humanitarian, economic, and social/cultural limitations on applying military power during the operation.

F **Rules of Engagement**. This annex contains guidelines to subordinate and supporting organizations regarding the rules for the control of forces and their weapons systems, to include guidance on the conduct of IO.

G **Fire Support.** This annex contains a statement of the fire support operations to be carried out, to include major groupings of fire support means and priorities and the integration of nuclear, chemical, and conventional fires, as appropriate.

H **Air Defense** . This annex should state the air defense operation to be carried out, to include air defense priorities and reference to the deployment overlays appendix. It should contain the allocation of counterair units, tasks, and coordinating instructions.

I **Not Used.**

J **Engineer**. This annex should include a statement of how the engineering support is to be carried out, to include priorities of mobility, countermobility, and survivability tasks within sectors and priority of uncommitted engineering resources to subordinate units or sectors.

K **Not Used.**

L **Rear Operations**. This annex contains guidance and priorities for securing the rear areas and facilities to prevent or minimize enemy interference, disruption of combat support and service support, or movement of friendly troops. It designates a unit to find, fix, and destroy enemy incursions into the rear area and provides area damage control after an attack or incident.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

M Protection. This annex contains instructions for the protection of bases, installations, military personnel, family members, and other US nationals in the theater from terrorism, natural disasters, and other dangers. It also contains information on protection of C^4I architecture.

N Provost Marshal. This annex prioritizes the four MP battlefield missions: area security, battlefield circulation control, enemy prisoner-of-war operations, and law enforcement. It should specify any tasks and/or coordinating instructions not covered in the OPORD.

O Public Affairs. This annex contains guidance for facilitating the media effort to cover the operation and for supporting the information needs of soldiers and their families. While PA is clearly a part of IO, it is addressed in its own annex since it falls outside C^2W as defined by joint doctrine.

P Space Operations . This annex describes planned and available space support to the OPLAN. It explains how to obtain and coordinate space support and lists operational constraints and shortfalls. This annex is linked to space-based systems such as communications and, as such, is closely related to IO.

Q Training . This annex contains guidance for multinational, joint, and service training of individuals and units assigned or attached to the theater army, which includes liaison teams and other forms of connectivity that enable coalition C^4I.

R Support . This annex spells out in detail the necessary support for subordinate formations to accomplish their missions. It may include special instructions for INFOSYS support of software support, configuration support, evacuating criteria, repair criteria, and so forth.

S Communications-Electronics. This annex describes the link provided by the force headquarters between the ATCCS, which exists among its subordinate units and joint and multinational C^2 systems, as well as those of the sustaining base. It addresses INFOSYS and must be carefully coordinated with C^2W operations.

T Civil Affairs. This annex describes civil affairs operations and organizations that affect the overall operation. It specifies how CA activities can provide relevant information supporting the CCIR from nontraditional sources in the GIE. While CA is clearly a part of IO, it is addressed in its own annex since it falls outside C^2W as defined by joint doctrine.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

Annex B

Sample C^2W Annex

Copy No____
Issuing Headquarters
Place of Issue
Date/Time Group of Signature

Annex D to ( ) Corps OPORD Exercise Xxxx Xxxx
Command and Control Warfare (U)

(U) **REFERENCES:** List appropriate joint and Army publications or documents on IO such as the following:

a. CJCSI 3210.03, *Joint Command and Control Warfare Policy*, 8 March 1993.

b. CJCS MOP 6, *Electronic Warfare*, 3 March 1993.

c. Joint Pub 3-13, *Joint Doctrine for Command and Control Warfare Operations*, 7 February 1996.

d. Joint Pub 3-51, *Electronic Warfare in Joint Military Operations*, 30 June 1991.

e. Joint Pub 3-53, *Joint Psychological Operations Doctrine*, 30 July 1993.

f. Joint Pub 3-54, *Joint Doctrine for Operations Security*, 27 August 1991 (Change 1, 14 April 1994).

g. Joint Pub 3-58, *Joint Doctrine for Military Deception*, 6 June 1994.

h. FM 34-1, *Intelligence and Electronic Warfare*, 27 September 1994.

1. (U) **SITUATION.** Thoroughly describe the operational environment as it applies to IO, as well as appropriate aspects of the strategic environment that may impact IO. Include tactical considerations important to IO in the early phases of an operation and establish the adversary's most probable C^2-attack course of action. Indicate trigger events that would signal execution of specific components of an IO within the OPORD.

a. **Enemy.** Expand discussion of the enemy situation in terms of C^2W, to include both strengths and weaknesses. Information components should include the following:

(1) A summary of information concerning the AO, which consists of—

(a) A strategic overview of the area that includes how the climate, politics, geography, topography, demography, economics, and social and cultural factors, as well as those of adjacent nation neighbors, may affect IO.

(SECURITY CLASSIFICATION)

(b) Specific, localized information, particularly about conditions affecting the early phases of the operation. Include availability of advanced technologies within the area such as national, multinational, or commercial information networks (telephone, telegraph, television, satellite linkages, and frequency spectrum), and the value of protecting or disrupting key capabilities of the country.

(2) A description of the adversary, which consists of—

(a) Strategic and operational factors such as the level of sophistication of the adversary's use of information technology to disseminate information to counter US efforts against its people. Ability of the adversary to restore key disrupted information facilities and maintain the initiative in the informational arena. The adversary's past experience in dealing with disruption over long periods of time (natural disasters, internal dissent, or subsystem failures such as loss of electric power, wear-out of components), stockpiling of key components, and vulnerability to disruptions in supply of key information equipment from outside the country.

(b) Factors of immediate concern during the early phases of the operation are dispersal of information equipment within the country and locations of qualified repair, broadcast, and production technicians and operators. Additional factors are the adversary's use of space-based communications, navigation, imagery, and weather systems, as well as C^2 W capabilities. Understanding the origin of the technology base enables easier disruption of the adversary's systems.

(c) Information about affiliations of the adversary that could counter US efforts against the adversary. Include order-of-battle information, numbers of INFOSYS, personalities of leaders, and levels of training or combat experience.

b. **Friendly.** State the mission and applicable parts of the concept of operation as it applies to IO/IW of the joint or multinational command to which the ARFOR is subordinate. These are normally as written in the theater campaign plan. Provide sufficient detail so that key individuals know and understand the higher joint or multinational commander's intent, the end state desired at the conclusion of the campaign, and how their actions mesh with the attainment of joint or multinational goals.

(1) **Higher headquarters.** Include the mission, concept, and intent of the unified/joint theater CINC. His concept determines the contributions of various informational elements and from which services or nations they are likely to be provided. His charter is to

(SECURITY CLASSIFICATION)

achieve US interests in the theater and should be stated so that the ASCC/ARFOR, his staff, and subordinates know and understand the part they play in achieving the CINC's strategic aim.

(2) **Other service components.** Highlight the roles of the Navy, Air Force, and Marine Corps components of the unified command in IO/IW.

(3) **Joint, unified, and subunified commands and DOD agencies.** Highlight the roles of these other commands and agencies that affect IO.

(4) **Multinational forces.** Highlight the organization, capabilities, and activities of friendly nations in the operation as they affect IO. Emphasize the capabilities of their military forces and other assets that their participation may bring. State their roles and missions that support the CINC's objectives to further US policies.

(5) **Special operations forces.** Describe the activities of SOF in the region that affect the operation, to include expected information activities of these forces.

(6) **Department of State.** Highlight the contributions of US embassies and country teams as they support IO of the force.

(7) **Other Non-DOD US Agencies**. Describe the activities of US Government agencies not included in country teams, such as DEA and USAID, as they affect IO.

c. **Attachments and Detachments.** Highlight critical elements of the *Task Organization/Command Relationship* section (Annex A) that may provide additional capabilities as the IO unfolds.

d. **Assumptions.** Include predictions and presumptions concerning the following:

(1) Information conditions within host countries and other nations in the region.

(2) Previous US policies in the region that affect speed or ability to change informational themes.

(3) Involvement by other powers, both outside and within the region, in the internal affairs of nations in the theater, which could result in changes to IO.

(4) Effects of US actions in IO on relations with nations adjacent to the adversary nation.

(5) Adequacy of interagency support, to include methods of increasing the role of other information agencies to reduce, where possible, sole military contributions.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

(6) Bilateral and multilateral consensus on the degree or extent of IO conducted within the overall operation.

(7) Availability of informational resources.

(8) Times and locations of anticipated hostile actions as they affect IO.

(9) The timing of political decisions in friendly nations that could change the IO scheme.

(10) The timing of the use of special events in the IO.

2. (U) MISSION. Include an explicit statement of the C^2W mission to support the operation, such as the following: On order, ( ) Corps conducts C^2W operations to deter (country name) attack on (country name). If deterrence fails, D-Day, H-Hour ( ) Corps conducts C^2W operations to support combat operations to disrupt (country name) C^2 of operational forces and degrade situational awareness of ( ) Corps operations, while protecting coalition C^2 capabilities from enemy disruption and destruction.

3. (U) EXECUTION.

a. **Concept of Operations**. Provide a detailed discussion of the overall C^2W operation, with the specific details developed in appendixes organized around the five elements of C^2W.

(1) **Military Deception**. This appendix includes a description of the deception objective, the deception story, available resources, excerpts of higher headquarters deception plans, and the active and passive deception measures to be taken by subordinate organizations. See Appendix A to this annex.

(2) **Electronic Warfare**. This appendix includes the EW mission, enemy EW capabilities, defensive and offensive EW measures, and coordination with other parts of the OPLAN (deception, communications, PSYOP, operational fires). See Appendix B to this annex.

(3) **Operations Security**. Deny the enemy information concerning the speed and size of the US buildup, as well as the specific course of action the US will execute in the decisive combat phase. Emphasis in initial stages is on denying the enemy access to his own or foreign intelligence capabilities. Deception, PSYOP, EW, and physical destruction all support these objectives. See Appendix C to this annex.

(4) **Psychological Operations**. This annex refers to the intelligence annex, designates PSYOP targets, and describes the PSYOP plan, to include its integration into higher headquarters plans and any deception plan operations or related tasks for subordinate units. See Appendix D to this annex.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

(5) **Physical Destruction**. When employed in a C^2W role, physical destruction is used to destroy the enemy's communications, integrated air defense system (IADS), and intelligence collection and fusion capabilities and to destroy the enemy's ability to strike at friendly C^2 and C^2W capabilities.

b. **C^2W Tasks**. Review specified and unspecified tasks by command.

(1) **Higher Headquarters.**

(a) Exercise centralized coordinating authority of all theater C^2W operations.

(b) Ensure that C^2W cell responsibilities are accomplished as described in CJCSI 3210.03.

(c) Advise component and supporting commanders of (_) Corps C^2W objectives and provide guidelines for their accomplishment.

(d) Develop the joint restricted frequency list (JRFL) to support operations.

(e) Provide oversight and ensure coordination of any reprogramming actions.

(2) **Component and Supporting Commands.**

(a) Provide for a single C^2W point of contact.

(b) Plan for and be prepared to conduct C^2W operations.

(c) Identify any operations that may impact or degrade effective C^2 of coalition forces.

(d) Recommend to (_) Corps the intelligence collection requirements necessary to support C^2W operations.

(e) Direct reprogramming actions as required.

c. **Coordinating Instructions.**

(1) The (_) Corps IO cell will coordinate, as appropriate, actions associated with operations against (country name) C^2. These actions include physical destruction, EW, PSYOP, military deception, and OPSEC.

(2) Planning and support of C^2W operations for (_) Corps should, as appropriate, be coordinated and draw support from the following:

(a) Army forces.

(b) US Special Operations Command.

(c) National Security Agency.

(d) Central Intelligence Agency.

(e) Defense Intelligence Agency

(f) Land Information Warfare Activity.

(SECURITY CLASSIFICATION)

(SECURITY CLASSIFICATION)

4. (U) **ADMINISTRATION AND LOGISTICS.**

a. **Administration**.

(1) C^2W significant activity reports will be submitted to (__) Corps/ G3.

(2) See Annex _.

b. **Logistics**. Increasingly, all operations entail another service, such as the Navy or Air Force, providing some common support. During these operations, the lack of specific standard support structures may be overcome through enhanced information connectivity available through common data bases and common hardware or software available across the services or through liaison teams.

(1) Features of such mechanisms could reduce the number of soldiers or units exposed to an operational environment, with a higher ratio of combat troops to support troops in the operational location. Consider some of the following areas for this type of idea:

(a) Personnel strength reports sent to Army component commands electronically.

(b) Telemedicine support reducing the number of specialized staff deployed to an operational area.

(c) State of the art radio and television studios located out of the immediate operational area that could be used in PSYOP.

(d) Local production of newspapers that could facilitate PSYOP while reducing support infrastructures within an AO.

(2) Identify information network support facilities from friendly third countries. Set forth in detail the procedures for making use of these resources.

(3) Include procedures for IO support of contingency forces from CONUS or other theaters.

(4) Highlight IO that routinely support force sustainment, to include the operation of temporary installations.

5. (U) **COMMAND AND CONTROL.**

a. (_) Corps will centrally coordinate assets to be used in a C^2W role. G3 heads the command IO cell.

b. See Annex S.

APPENDIXES:

A Military Deception

B Electronic Warfare

C Operations Security

D Psychological Operations

(SECURITY CLASSIFICATION)

Appendix B

Responsibilities of Supporting Agencies

This appendix discusses the functions and responsibilities of Army and joint agencies supporting IO and C^2W across the operational spectrum. It discusses the missions and functions of the Joint Command and Control Warfare Center (JC^2WC) and LIWA. It delineates the responsibilities to the commander-in-chief (CINC) and Army component commander, respectively. IO/C^2W planners should use this appendix to gain a better understanding of the support available from these agencies.

JOINT COMMAND AND CONTROL WARFARE CENTER

CJCS Instruction 5118.01 is the charter for the JC^2WC. This paragraph provides key excerpts from that document to provide combatant commanders, JFCs, and other units requiring assistance in C^2W with a ready reference of the support provided by the JC^2WC.

Mission

The mission of the JC^2WC, formerly the Joint Electronic Warfare Center (JEWC), is to provide direct C^2W support to operational commanders. The JC^2WC supports the integration of the constituent elements of C^2W—OPSEC, PSYOP, military deception, EW, and destruction. It also supports the noncombat military applications of IW throughout the planning and execution phases of operations. The JC^2WC provides this direct support in the following priority order:

- Joint force commanders (combatant commanders, subordinated unified commanders, and joint task force commanders).
- Service component commanders.
- Functional component commanders.

The JC^2WC also provides support to the Office of the Secretary of Defense, the joint staff, the services, and other US Government agencies. The JC^2WC maintains specialized expertise in C^2W-related—

- Systems engineering.
- Operational applications.
- Capabilities.
- Vulnerabilities.

Functions

The JC^2WC, through the joint staff director for operations (J3) serves as the principal field agency within DOD for C^2W support.

J3

As stated in CJCSI 5118.01 the JC^2WC, acting through the joint staff J3—

- Interfaces with the joint staff, services, DOD, and non-DOD agencies to integrate IW (see DOD Directive TS3600.1) with DOD C^2W efforts.
- Participates in the Joint Special Technical Operations System by analyzing capabilities (in coordination with the intelligence community), as tasked by the director of the joint staff, to optimize special technical operations support to combatant commanders.

- Serves as the joint staff central point of contact for reviewing joint C^2W mission needs statements (MNS).
- Coordinates with the joint staff director for C^4 systems (J6) for C^2-protection issues.
- Assists the CJCS, through the joint staff J3/STOD (special technical operations division that serves as the doctrine sponsor for C^2W and EW) in the development of joint doctrine and joint tactics, techniques, and procedures.
- Evaluates C^2W effectiveness in combat.
- Serves as the DOD focal point for defining, coordinating, and overseeing the integration of those data bases/data systems necessary to establish a common joint *information base* for conducting C^2W. This information base comprises intelligence and *operational* data bases/data systems, that is, data on US equipment, systems, and forces. It also includes other types of data bases (the remainder of the world's systems—geophysical, topographical, psychological, and doctrinal) necessary to conduct C^2W in the combatant commander's battlespace. It includes US and, as available, allied WARM (weapons assignment research model) descriptions and descriptions of US-manufactured systems sold to other nations. For the most part, this information base:
  - Is releasable to allied nations annually in coordination with the services, intelligence agencies, and other cognizant agencies and commands.
  - Provides a report to the joint staff J3 on the currency and shortfalls in the C^2W information base.
  - Participates in the development of decision aids used to manipulate the C^2W information base.
  - Orchestrates efforts for interoperability and connectivity of data and systems to support C^2W with the GCCS in cooperation with the DOD intelligence community and the joint staff J6.
- Organizes, manages, and exercises the joint aspects of EW reprogramming. Develops procedures to assist commanders with the identification, validation, and dissemination of electronic threat changes. Coordinates compatibility and facilitates exchange of data used in joint EW reprogramming among the intelligence community, services, and combatant commands.
- Organizes and facilitates development of joint C^2W simulations supporting wargaming among the joint staff, services, combatant commands, and combat support agencies, in conjunction with the Joint Warfighting Center.
- Serves as the joint staff's point of contact through the J3 for C^2W joint universal lessons learned (JULLS) reported under the Joint After-Action Reporting System (JAARS) and referred for action as remedial action projects (RAPs).
- Participates in C^2W research or studies of an operational nature for DOD organizations and agencies.
- Maintains knowledge and coordinates with the services on C^2W systems engineering initiatives, laboratory programs, and industrial developments.
- Performs vulnerability and effectiveness analyses of US equipment used in C^2W. Coordinates C^2 vulnerability analyses with the joint staff J6.
- Supports allied nations or international organizations on a case-by-case basis. Support includes representing the US in appropriate international forums.
- Produces the annual DOD EW Plan in conjunction with the Services and combat support agencies.
- Develops and produces an annual DOD C^2W plan in conjunction with the services and combat support agencies.

COMBATANT COMMANDER

For direct combatant commander C^2W support, the JC^2WC maintains deployable C^2W augmentation teams to support the combatant commander as requested. To provide timely

analysis and advice for planning and coordination of C^2W, these teams maintain an awareness of the threat and the OPLANs in the respective combatant commanders' AORs. In addition, the teams—

- Train with and develop routine working relationships with other organizations having specialized expertise in the constituent elements of C^2W.
- Provide C^2W technical assistance.
- Function as the central coordinating element for organizations that support the CINC's C^2W effort.
- Maintain the capability to assist in planning and coordinating the employment of joint and combined EW assets as part of the JCEWS.
- Provide in-theater guidance and assistance for the joint coordination of EW reprogramming.
- Provide timely advice and comprehensive EW analysis support, such as radar terrain masking overlays, and predictive analyses (for example, Proud Flame).

As required, the JC^2WC requests augmentation from specialized organizations, through the joint staff J3, for a deploying JC^2WC team to provide a more comprehensive C^2W capability to the supported commander. The JC^2WC also—

- Maintains a dedicated action officer at the JC^2WC for each combatant command to interface with each CINC's staff and integrates C^2W into appropriate OPLANs. These action officers are responsible for all JC^2WC actions regarding C^2W support of their respective CINCs.
- Provides tactical and technical analyses of C^2W in military operations.
- Supports C^2W training by assisting combatant commanders in planning, conducting, and evaluating the C^2W aspects of joint exercises, including field training exercises, command post exercises, and computer simulations for wargaming in collaboration with the Joint Warfighting Center.
- Coordinates and conducts field demonstrations of emerging technologies responsive to CINC C^2W needs.

For additional information, contact the JC^2WC by writing to– Joint Command and Control Warfare Center
2 Hall Blvd, Suite 217
San Antonio TX 78243-7008

by sending a message to– **JC^2WC SAN ANTONIO TX/DR/DV/DT/OE/OW/XR/OT/SI//**

or by telephoning–
Gray: 973-6152
DSN: 969-XXXX (STU III-equipped)
Unclassified Fax: 969-4166
Classified Fax: 969-4451/4682
Commercial: (210) 977-XXXX

KEY PERSONNEL

DR: Director 969-2071
DV: Vice Director 969-2071
DT: Technical Director 969-2071
XR: Plans and Resources 969-4681

DIRECTORATES

SI: Systems Integration 969-2579
OW: Operations West 969-2911
OE: Operations East 969-2174
OT: Operations Support and Technical Integration 969-2482

LAND INFORMATION WARFARE ACTIVITY

AR 520-20 established the Land Information Warfare Activity to integrate OPSEC, military deception, PSYOP, EW, and physical destruction to support IO and C^2W. A memorandum of understanding (MOU) delineates the command, control, and functional relationships of HQDA and the US Army Information Systems Command (USAINSCOM) with LIWA. It further delineates HQDA command and staff responsibilities for IO/C^2W. LIWA is under the command of USAINSCOM. The director of operations, readiness, and mobilization exercises operational tasking authority of LIWA, including IO/C^2W operational support policy and program planning guidance.

This provides a quick reference of the support that LIWA provides. CJCS has directed Army commanders to integrate IW/C^2W into exercises, OPLANs, and OPORDs. Emerging Army doctrine calls for the formation of an IO activity to help land operational and tactical commanders integrate C^2W with other information domains such as the GIE, collector-to-shooter linkages, INFOSEC, counterintelligence (CI), HUMINT, and survivability. Given the technical complexity of this doctrinal requirement and the need to operate in a resource-constrained environment, LIWA fields tailored support teams such as FSTs to help operational and tactical battle staffs integrate IO/C^2W with plans, operations, and exercises.

Mission

LIWA coordinates multidisciplined intelligence and other support for operations planning and execution, to include C^2W data base support, HUMINT, CI, and TECHINT. LIWA is electronically connected with other national, DOD, joint, and service IW facilities or centers. Integral to LIWA is the Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA) collocated with the US Air Force at the Air Warfare Center. ARAT-TA provides the technical expertise to ensure target-sensing weapons systems are correctly programmed to meet the specific conditions of a designated AO.

LIWA has been specifically designed to provide tailored support to the land component commands. LIWA's purpose is to provide commanders with technical expertise that is not resident on the command's general and special staff and to provide responsive technical interfaces with other commands, service components, and national, DOD, and joint information centers. When deployed, the LIWA FSTs become an integral part of the command's IO staff. To facilitate planning and execution of IO, LIWA provides IO/C^2W operational support to land component and separate Army commands and active and reserve components (AC/RC).

Functions

LIWA acts as the operational focal point for land IO/C^2W by providing operational staff support to AC/RC land component commands and separate Army commands. It coordinates, arranges for, and synchronizes IO/C^2W intelligence and CI support to land component commands. LIWA coordinates and deploys FSTs to assist and support LCCs in C^2-protect, including—

- C^4 security support.
- Analyses, investigations, and surveys to assess the vulnerability of the LCCs' C^2 facilities to IO/C^2W sabotage, deception, and attack and to assess their ability to maintain personnel and security programs and protect such facilities.
- C^4 threat advisories with recommendations for counter-countermeasures.

LIWA coordinates and deploys FSTs to advise LCCs on C^2-attack, including—

- Preparing deliberate and contingency plans and orders.

- Preparing target lists, estimates, and assessments.
- Analyzing the threat and interpreting the situation, critical nodes, enemy vulnerability, defeat criteria, and BDA.
- Maintaining selected, tailored IO/C^2W data bases and monitoring the accuracy of supporting data bases.

LIWA coordinates and deploys FSTs to provide battlefield deception planning support to LCCs. Through participation in the Battle Command Training Program (BCTP), combat training center (CTC) rotations, battle labs, and Force XXI studies, LIWA coordinates with and provides assistance to TRADOC in the development and integration of doctrine, training, leader development, organization, materiel, and soldier requirements (DTLOMS) for IO/C^2W. In addition, LIWA—

- Acts as the functional proponent for battlefield deception.
- Coordinates the establishment of requirements for unprogrammed IO/C^2W studies to support operational contingencies.
- Provides operational insight and recommendations to TRADOC and HQDA on Army IO/C^2W requirements and input into Army modernization strategy, policy, scenarios, modeling, and simulations.
- Assists TRADOC in the development and evaluation of IO/C^2W systems' performance and operational employment TTP in combat operations, operational tests, and training exercises.
- Establishes, develops, and promotes IO/C^2W interoperability with other services and allies and recommends improvements.
- Coordinates and facilitates operational IO/C^2W matters with other military services and allies as appropriate.
- Assesses and reports to the director of operations, readiness, and mobilization IO/C^2W force readiness and IO/C^2W operational capabilities of land component forces to accomplish assigned missions under real or assumed conditions.

Responsibilities

LIWA, as the designated Army operational focal point and Army executive agent for IO/C^2W operational support matters, is responsible for—

- Supporting HQDA ODCSOPS with subject-matter technical expertise regarding IO/C^2W matters and land force deployments.
- Advising major Army and component commands on available and emerging IO/C^2W capabilities within the Army and other services and agencies.
- Publishing threat impacts requiring software or hardware adjustments of IO/C^2W knowledge-based weapons systems.

FSTs deploy on exercises with designated commands to support training and to develop an in-depth understanding of the support command's organization and procedures. FSTs, adhering to the component commander's intent and guidance, provide a wide range of support, by—

- Assisting in the preparation of war plans, contingency plans, and orders.
- Helping develop target lists, estimates, and assessments.
- Supporting the analyses of threat critical nodes, enemy vulnerabilities, defeat criteria, and BDA.
- Providing C^2-protect technical support, to include operating a help line to immediately deal with communications and computer disruptions.
- Recommending how and when to employ IO/C^2W capabilities, including those of other services and agencies.

For additional information, contact LIWA writing to–	Commander US Army Information Systems Command ATTN: LIWA 8825 Beulah Street Fort Belvoir, VA 22060-5246
by sending a message to–	DIRLIWA FT BELVOIR VA //XX/XX// MIL NET Address: (user id) liwa@vulcan.belvoir.army.mil
or by telephoning–	Commercial: (703) 706-XXXX DSN voice: 235-XXXX (STU III-equipped) Commercial Fax 703-806-XXXX DSN Fax: 656-XXXX Unclassified Fax: 656-1003 Classified Fax: 656-1004 Gray: 964-7861

KEY PERSONNEL

Commander:	235-1069/2263	SA: Studies and Analysis	235-2269
Operations:	235-1791/2259	DO: Director of Operations	235-1069
DR: Director	235-1791	RT: Red Team	235-2262
XO: Executive Officer	235-2266	IM: Information Support	235-1420
DD: Deputy Director	235-2263	PR: Plans and Resources	235-2987

Appendix C

Planning Considerations

Effective battle staff planning requires a framework that focuses on the commander's concept of operation. Planners integrate all available information and resources that facilitate mission accomplishment at the strategic, operational, and tactical levels. This appendix discusses the INFOSYS support planning principles, signal support requirements, and C^2W planning process the commander uses to plan and conduct military operations. The principles serve as a starting point from which to create solutions to mission requirements that focus on resolving all INFOSYS and C^2W issues and problems before the start of operations.

SUPPORT PLANNING PRINCIPLES

The INFOSYS planning principles are derived from Joint Publications 6-0 and 6-02. These principles focus the planners' attention on what is important to the commander. The principles outlined here help accomplish this effort.

Modularity

Modular INFOSYS packages consist of sets of equipment, people, and software tailorable for a wide range of missions. Planners must understand the mission, the commander's intent and operational plan, availability of assets, and the information structure required to meet the needs of each mission. These packages must satisfy the commander's informational requirements during the execution phases of the mission. Modular INFOSYS packages must be flexible, easily scaled, and tailored with respect to capacity and functional capability.

Interoperability

Interoperability is the capability of INFOSYS working together as a system of systems. Interoperability implies compatibility of combined, joint, and service common information or data elements procedures. Interoperability is the foundation on which INFOSYS capabilities depend. An interoperable INFOSYS is visible at all functional levels—a secure, seamless, cohesive, infrastructure that satisfies C^2 and information requirements from the NCA to the lowest information request. INFOSYS should comply with the Army's technical architecture. Adherence to these standards and protocols helps ensure interoperability and a seamless exchange of information among the battlefield functional areas and joint services. Older INFOSYS that do not comply with the common operating environment and technical architecture require special planning and may not be interoperable.

Liaison Officers

LOs provide a means for the commander and planners to increase interoperability during different phases of an operation and between commanders and staffs that have not previously

worked together. LOs are especially important for interpreting intent and relevance to the parties they serve and in overcoming the natural friction that develops between disparate organizations. LOs ease technical coordination and enable planners to manage information more efficiently and effectively. LOs are especially important when working with government agencies and allies.

Flexibility

Planners must be flexible when supporting INFOSYS requirements in changing situations. They must anticipate the possibility of changes in the mission or tactical situation and build a plan to accommodate them.

Economy

Scalable system packages ease the application of economy. Space, weight, or time constraints limit the quantity or capability of systems that can be deployed. Information requirements must be satisfied by consolidating similar functional facilities integrating commercial systems

Survivability

INFOSYS must be reliable, robust, resilient, and at least as survivable as the supported force. Distributed systems and alternate means of communications provide a measure of resilience. Systems must be organized and deployed to ensure that performance under stress degrades gradually and not catastrophically. Command procedures must be capable of adaptation to cope with degradation or failure.

Redundancy

From an INFOSYS network perspective, planners provide diverse paths over multiple means to ensure timely, reliable information flow. From an equipment perspective, planners ensure that sufficient backup systems and repair parts are available to maintain the system's or network's capabilities.

Standardization

The commander's information requirements must not be compromised by the use of nonstandard equipment. Planners must ensure that the equipment, its configuration, and the installed operating systems included in a modular package are standardized throughout the joint force. Standardization also includes INFOSYS training, symbology, switch network diagrams, packet network diagrams, and terminology.

Commercial Capabilities

The availability of commercial INFOSYS often offers the commander a guide, as well as an alternative means, to satisfy his informational C^2 needs. Further, it may reduce the number and size of deployed modular packages; however, security must be considered. Operational use of a commercial system allows planners to compensate for system shortages and to meet the surge of information requirements in the early stages of deployment. The G6 has staff responsibility for the standardization of commercial equipment and software used

throughout the AO. However, planners have to ensure the deployed modular INFOSYS packages implement open, nonproprietary, commonly accepted standards and protocols to interface with commercial systems.

Security

The level of security depends on the nature of the information to be protected and the threat of interception or exploitation. Electronic on-line encryption devices usually provide communications security. Controlling physical access to terminals, software, and disks helps to ensure security of INFOSYS. Security must be balanced by the need to disseminate critical information quickly.

SIGNAL SUPPORT REQUIREMENTS

Throughout all force-projection stages, signal support must provide the means to transport information from CONUS sustaining-base installations, through strategic gateways, to the forward-most deployed units. The signal support requirements to fulfill this mission are critical to the successful execution of IO and are METT-T-dependent. Building on the essential tasks for INFOSYS described in Chapter 5, the INFOSYS planning process consists of five phases. These phases take the planner from construction through reconstitution of the INFOSYS.

Phase I: Construct and Project the INFOSYS

The security aspects of occupying a dispersal area are pretty standard. What is new is the notion of establishing a sanctuary operations center—a place from which to anchor the unit's INFOSYS. It may actually be in CONUS or aboard ship. From this sanctuary, supporting data bases and staffs provide additional support such as logistics, medicine, and wargaming. US forces dig in and physically protect their components and establish strict emission control. Even in the setup process, forces posture information capabilities to support the division's forward movement.

Phase II: Extend the INFOSYS

The division moves forward via multiple routes during this period of extreme vulnerability. Redundant C^2 headquarters are pushed forward. The *A* and *B* forward CPs have identical capabilities for communications and intelligence. Intelligence and RISTA capabilities are pushed forward early, both for security and to provide overwatch of routes. Key signal nodes are positioned forward to kick in when the unit begins to maneuver, but the division is silent. Strict control on emissions is observed. The Joint Surveillance Target Attack Radar System (J-STARS) provides situational awareness and force tracking. UAVs and satellites extend communications and networks. Units receive updates on the move via satellite broadcasts. Concurrently, the unit begins to shape the battlespace.

Phase III: Shape the INFOSYS

When thinking about shaping the battlespace, one must understand the enemy's organizational whole. The targets, tempo, echelon, networks, and groupings are not physical things on the ground; they are entirely C^2 concepts. For example, if our intent is to talk about *stripping* the enemy's artillery, then it is his grouping capacity—his capability to generate his fire plan and maneuver with fires—that we want to attack.

Phase IV: Maneuver the INFOSYS

Without a pause in the tempo of the attack, units shift to close combat with maneuver forces. Shaping activities are already isolating the current battle zone and closing off the enemy's capacity for reconnaissance. Decisive combat is possible without defeating the enemy force in detail. This is accomplished by focusing combat power at precise locations that destroy the organizational integrity of the force. Force tracking and predicative tools allow maneuvering *where the enemy is not* and *orchestrate effects* not where he is, but *where he is going to be.*

The intelligence processes reach the crossover point, and organic collections kick in. The commander looks at how the enemy will react to his plan. Complete situational awareness is critical. The communications network and/or tactical internet must be maneuvered to maintain information flow and needed communications capacities to weigh the bandwidth to the main effort. During decisive operations, the information flow reaches a crescendo and so does the potential for information overload. This is where a well-thought-out CCIR comes into play—a schedule that lays out the frequency and character of certain reports. CCIRs need to focus on visualizing the sequence of events that moves the commander from his current situation to an end state.

Phase V: Reconstitute the INFOSYS

INFOSYS are consolidated and reconstituted to police up the digits on the battlefield. This is accomplished by repairs on the internet, cleanup, and purging of data bases. Addressees and protocols match actual reorganization, reflecting losses. Forces communicate through the INFOSYS for telemaintenance and telemedicine and call forward combat service support. Repositioning of the INFOSYS for branches and sequels begins.

C^2W PLANNING PROCESS

In almost every case, Army commanders employing C^2W can expect to do so in a joint context. But regardless of whether the operation is joint or purely Army, *the commander drives C^2W in his organization.* The operations staff (G3/J3) plans for and executes the C^2W plan. The command and staff process for C^2W operations is no different than any other, except in the parameter of focus. Joint and multinational C^2W planning and the process that follows apply to all levels of war and all echelons.

Joint and Multinational Planning

C^2W is inherently joint and multinational. The development of C^2W capabilities, plans, programs, tactics, employment concepts, intelligence, and communications support, as a part of military strategy, requires coordination with responsible DOD components and allied and coalition nations. In coalition operations the key to C^2W is the need to plan in a multinational manner and achieve a workable multilevel security program. An exchange of LNOs may be the most effective way to secure these objectives.

The joint force conducts C^2W efforts around a joint force C^2W organization. This may be a C^2W cell in a JTF or a C^2W battle staff for a CINC. The key to joint employment of C^2W is to leverage the needed capabilities from the service or component that has them available and employ them to support the JTF/CINC mission. Just as there is a synergy by employing the five elements of C^2W in a synchronized manner, there is a synergy in blending the capabilities of the services to focus on mission accomplishment. CJCSI 3210.03 and Joint Pub 3-13.1 provide joint policy and doctrine on C^2W. The ability of service staffs to integrate effectively to support joint operations is critical. Two existing staff elements

that may be used to facilitate joint IO activities are the BCE found within corps headquarters and the air/naval gunfire liaison company (ANGLICO) found within most fleet Marine forces. Both already serve as information nodes to coordinate activities across service lines.

Battle Staff Planning

Effective C^2W planning requires a framework that focuses the battle staff, thereby ensuring a plan that supports the commander's concept of operation by integrating the elements of C^2W into a coherent, synchronized plan.

C^2-ATTACK PLANNING STEPS

This seven-step process provides a structure and facilitates the planning process for C^2-attack.

- *Step 1.* Identify how C^2-attack could support the overall mission and concept of operations. Product: C^2W mission.
- *Step 2.* Identify enemy C^2 systems whose degradation will have a significant effect on enemy C^2. Product: Enemy potential C^2-target list.
- *Step 3.* Analyze enemy C^2 systems for critical and vulnerable nodes. Product: high-value target (HVT) list.
- *Step 4.* Prioritize the nodes for degradation. Product: Prioritized high-payoff target list.
- *Step 5.* Determine the desired effect and how the C^2W elements will contribute to the overall objective. Product: C^2W concept of operation. When developing the concept of operation, it is important to recognize the potential for both mutual reinforcement and mutual conflict among the five elements of C^2W.
- *Step 6.* Assign assets to each targeted enemy C^2 node. Product: Subordinate unit taskings.
- *Step 7.* Determine the effectiveness of the operation. Product: BDA.

C^2-PROTECT PLANNING STEPS

This seven-step process provides a structure and facilitates the planning process for C^2-protect.

- *Step 1.* Identify how C^2-protect could support the overall mission and the concept of operations. Product: C^2W mission.
- *Step 2.* By phase, identify critical friendly C^2 systems that support the mission and concept of operations. Product: Friendly C^2 list.
- *Step 3.* Determine the enemy's capability to conduct C^2-attack and the effects of friendly C^2-attack on our C^2 systems (mutual interference). Product: Threat assessment.
- *Step 4.* Analyze friendly C^2 systems for critical and vulnerable nodes. Product: Identification of friendly critical and vulnerable nodes.
- *Step 5.* Prioritize friendly nodes for protection. Product: C^2-protect concept of operation.
- *Step 6.* Recommend protection measures for nodes. Product: Subordinate unit taskings.
- *Step 7.* Monitor effectiveness of C^2-protect plan. Product: BDA.

Preparation of C^2W Annex

C^2W-related information is in the operations, intelligence, and communications-electronics (C^3) annexes. For most operations, a C^2W annex consolidates and integrates deception, EW, PSYOP, and OPSEC activities into a coherent and cohesive operation. On occasion, based upon METT-T, the commander may elect to produce EW, PSYOP, military deception, and OPSEC

annexes as stand-alone parts of the plan or order. The C^2W annex includes—

- The specific C^2W objectives the commander is seeking for the operations covered by the plan.
- The concept for C^2W that ensures the commander can attain his objectives.
- A lay-down of the commander's assets and capabilities that can be used to achieve the objectives.
- An identification of shortfalls or problems that may hamper the achievement of the commander's objectives.

A sample format of the C^2W annex to the OPLAN/OPORD is found in Appendix A, Annex B. Coordination of the C^2W plan, action, direction, and objectives is illustrated in Figure C-1

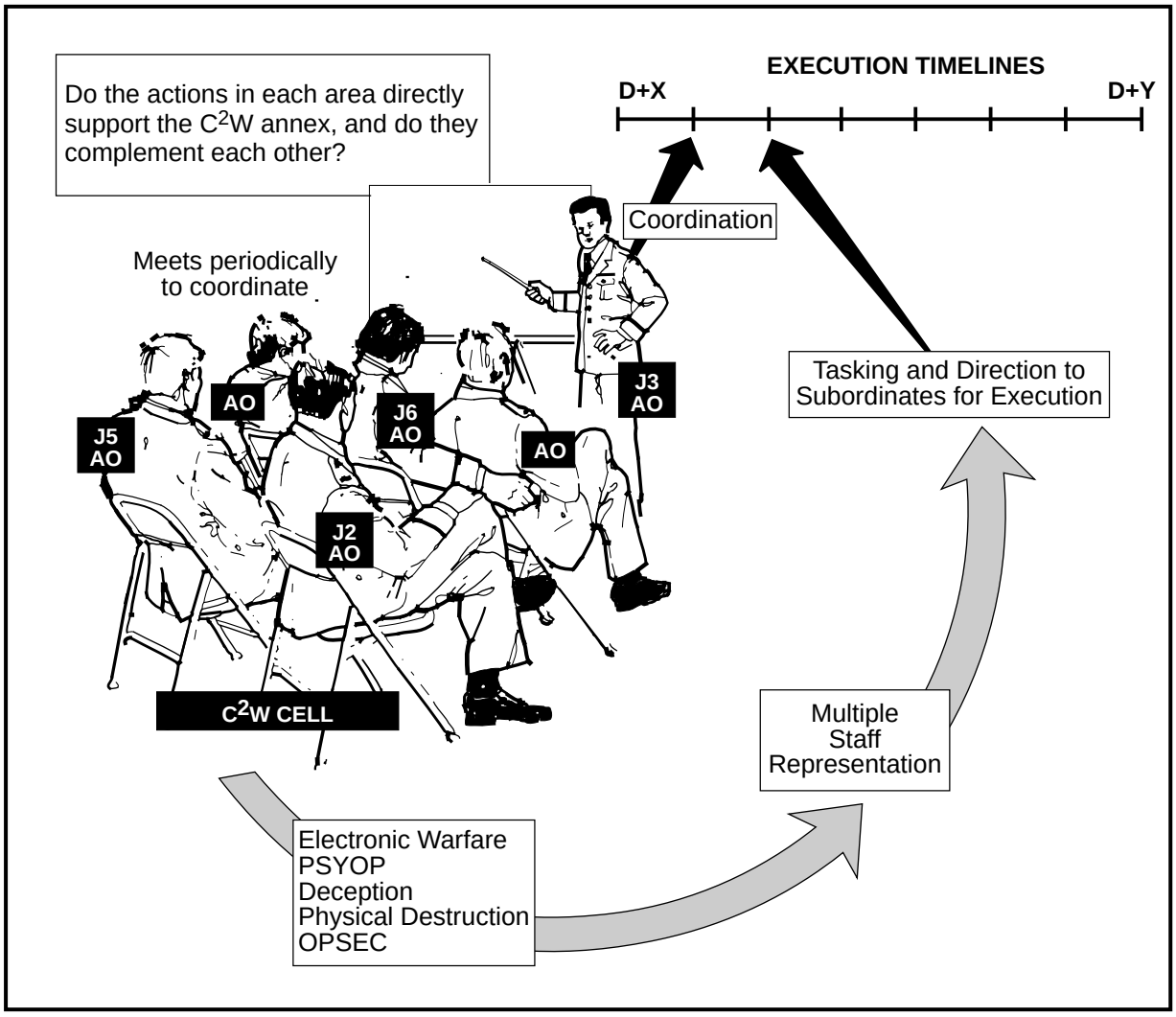

Figure C-1. C^2W Execution

Appendix D

Staff Organization and Training

Based on the considerations of METT-T, the commander may designate an IO cell on his staff. The structure of the cell is the prerogative of the commander. It may be something as simple as periodic use of an expanded targeting cell or a more formal approach establishing a standing cell with a specifically designated membership. The IO cell is normally found at the task-force level, independently operating brigade level, or above. A notional view of the IO cell is shown in Figure D-1.

ORGANIZATION

The IO cell should have representatives from the targeting cell, targeting board, joint operations and targeting coordination board, or whatever integrating process the commander uses to integrate and synchronize his resources. Each element of C2W should be represented where possible. In OOTW situations the CA representative and/or PA representative may take on more importance. In conflict and war the targeting representative may become the focus of activity. Functions of the IO cell include—

- Planning the overall IO effort for the commander.
- Developing IO concepts to support the scheme of maneuver.
- Establishing IO priorities to accomplish planned objectives.
- Determining the availability of IO resources to carry out plans.

Consolidated tasking will assist in the integration and synchronization required for effective IO, including coordination with the joint IW community.

As the spectrum of engagement moves from peace to war, it may be more appropriate to stand

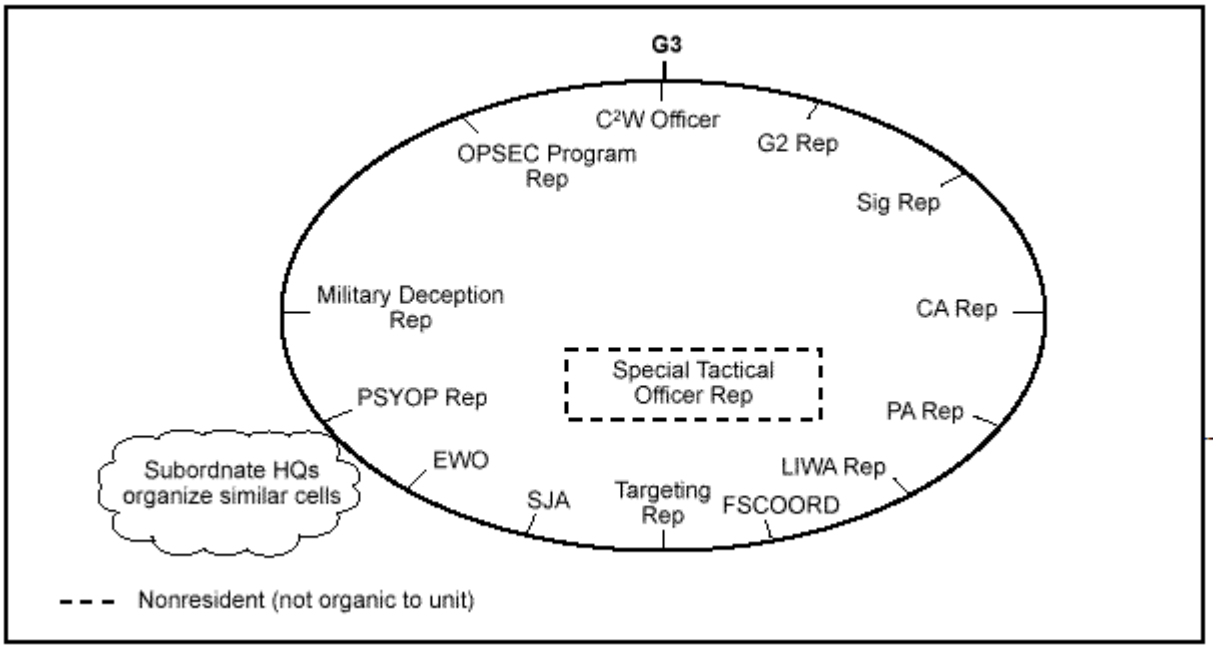

Figure D-1. Notional IO Cell

up an IOBS. An IOBS would be appropriate at division and above and most appropriate at corps. Although the functions would be relatively the same as the IO cell, they would be much broader in scope. This type of staff organization would be best suited for deployment in the context of a campaign, as discussed in Appendix A (see Figure D-2).

TRAINING

As in all areas, effective IO requires soldiers to train the way they are going to fight or operate. The basic task is to train the force on IO, with an initial focus on those personnel responsible for planning and coordinating the individual elements. When our leaders and units are exposed to realistic IO elements in training, such as information distribution in OOTW, their readiness and confidence increases.

When employing IO in exercises, the following considerations are important:

- Developing concrete, attainable IO objectives.
- Providing for sufficient IO elements to support the objectives of the exercise.
- Creating as realistic an IO exercise environment as possible.

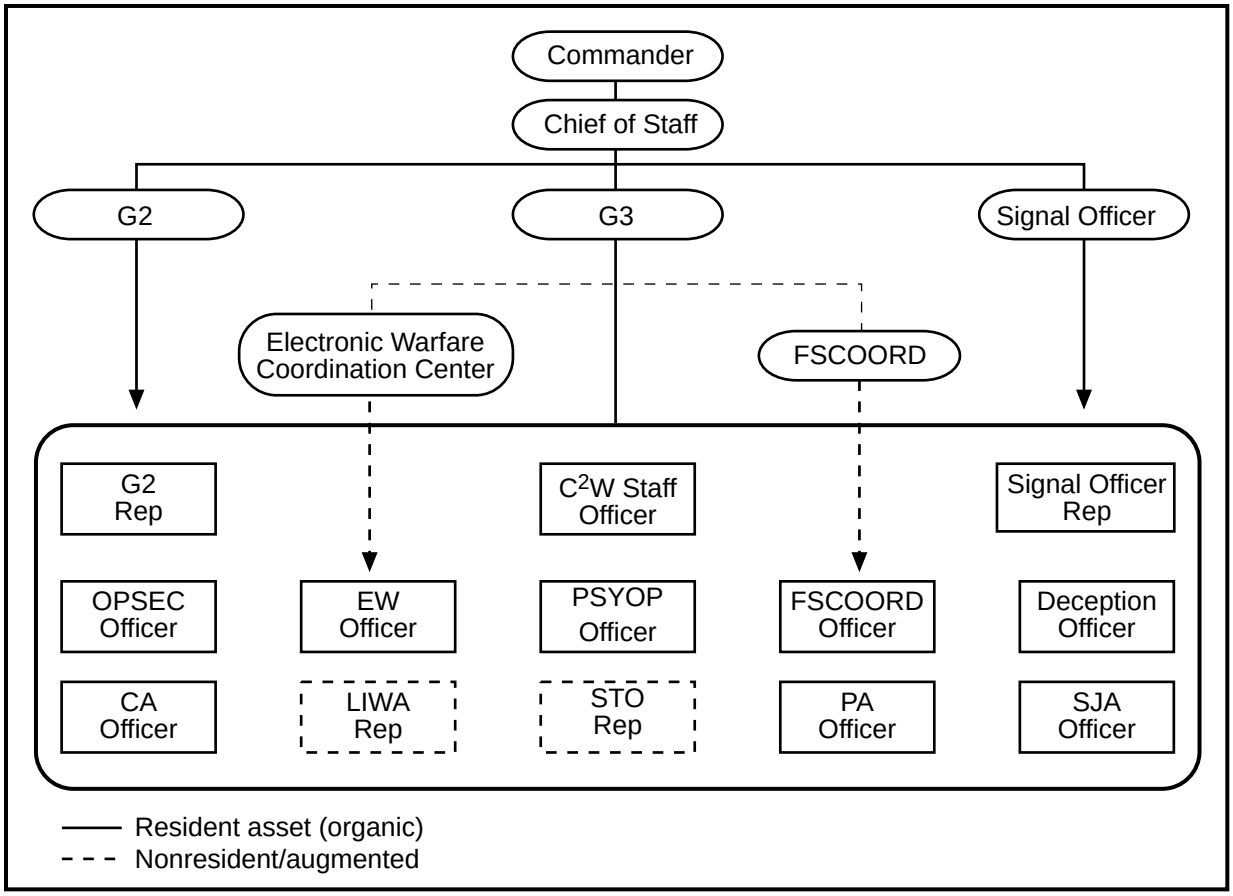

Figure D-2. Notional IO Battle Staff

- Assessing and evaluating the employment of IO activities.
- Exercising all six IO activities in the context of the exercise.
- Using appropriate security measures to protect the IO elements.
- Evaluating the use of computer support products to execute IO (synchronization tools).
- Using simulations to augment IO where and when applicable.
- Exercising all five C^2W elements in the context of the exercise.

Effective IO *first* requires specific information products on the adversary's military (C^2, intelligence, and capabilities), social, religious, and economic background that may have to be provided by exercise planners. The data needed to create, update, and use these products needs to be built into the exercise scenario and master scenario events list.

Secondly, the opposition force should have an IO capability consistent with the OPLAN/CONPLAN scenario that is the basis for the exercise. Realistic IO are essential to evaluating friendly IO.

Finally, consistent with the tenets of the exercise, free play of IO should be allowed by both sides. Prestructured, mechanical IO will degrade the participant's ability to gain valuable experience from the demands of mental agility and creativity that unstructured IO can provide. Senior exercise participants should allow, even welcome, the C^2 chaos that effective IO can cause to the exercise participants and work through such problems.

A basic IO mission-essential task list (METL) includes tasks and subtasks. Tasks involve each IO component—*operations*, *relevant information and intelligence,* and *INFOSYS.* The METL enhances the objective of *achieving information dominance* at selected places and times during an operation. Tasks include—

- Determining required IO information and how to get answers.
  - Identify the commander's IO CCIR, PIR, and high-priority targets and synchronize intelligence and information plans and military plans on a near-real-time basis.
  - Establish information-linked strategic, operational, and tactical collection, fusion, and report processes (incorporating RISTA/sensor and CI/HUMINT data) to develop continuous, timely IO IPB.
- Knowing your IO capabilities and vulnerabilities to the enemy, the natural environment, the political setting, international law, and so forth.
  - Provide IO modeling and simulation for training and evaluating performance, mission rehearsal, and decision making.
  - Identify and prioritize IO EEFI.
- Knowing enemy IO capabilities and vulnerabilities.
  - Maintain a continuous IO estimate of potential adversaries and/or other operational situations in support of IO situational awareness and battlefield visualization.
  - Assess adversary C^4I/C^2W operations, strengths, and vulnerabilities continuously.
- Knowing how the enemy sees your capabilities and vulnerabilities in terms of IO, the battlefield, and PIR.
  - Understand the enemy's decision-making process.
  - Identify the enemy's critical IO nodes.
  - Develop enemy leader personality profiles.
  - Understand the enemy's decision-making doctrine, tactics, and standard operating procedures.

- Protecting critical and vulnerable friendly IO.
  - Establish open-source processes to obtain, process, provide, secure, and release critical IO information, including PA, CA, governmental, and nongovernmental information within legal and policy constraints.
  - Establish and maintain critical, secure, intertheater/intratheater, military communications and computer networks that support IO; for example, digitization, RCP, situational awareness, battlefield visualization, distribution, and C^2 across the battle space.
  - Assess friendly C^2 vulnerabilities and C^2-protect operations continuously and adjust to maintain C^2 effectiveness.
  - Achieve C^2 protection in support of data integrity and infrastructure protection, IO/C^2 node protection, spectrum superiority/control, and graceful degradation.
  - Establish procedures to regain information dominance when it is discovered that the enemy has achieved information dominance.
- Attacking critical enemy IO vulnerabilities.
  - Establish C^2-attack targeting and BDA and establish links to expedite dissemination of adversary information, to include timely sensor-to-shooter links.
  - Attack, deny, degrade, exploit, and/or influence adversary C^4I/C^2W capabilities or other operations using lethal and nonlethal means.

Glossary

ABCS	Army Battle Command System
ACCS	Army Command and Control System
adversary	often used in this manual in lieu of enemy; the term *enemy* is reserved to indicate adversaries engaged in lethal operations against US forces
AEA	army executive agent
AES	Army Enterprise Strategy
ACE	air combat element
AC	active component
ACU	area common user
ACUS	Army common user system
ADP	automatic data processing
ADSO	assistant division signal officer
AFATDS	advanced field artillery tactical data system
AFGWC	Air Force Global Weather Central
AGCCS	Army Global Command and Control System
AHFEWS	Army High Frequency Electronic Warfare System
AID	United States Agency for International Development
AMOPES	Army Mobilization and Operations Planning and Execution System
ANGLICO	air/naval gunfire liaison company
AO	area of operation
AOR	area of responsibility
appliqué	a family of laptop-sized computers connected to navigation devices and radios to provide processing and display capabilities to platforms without an embedded processor
appreciation	personal conclusions, official estimates, and assumptions about another party's intentions, capabilities, and activities used in planning and decision making
ARAT-TA	Army Reprogramming Analysis Team-Threat Analysis
ARCENT	Army component to Central Command
ARFOR	Army force headquarters
ARSOF	Army special operations forces

ASAS all-source analysis system

ASCC Army service component command

assured communications certain electronic transmission capabilities needed throughout the strategic, operational, and tactical areas of operations

ATACMS Army Tactical Missile System

ATCCS Army Tactical Command and Control System

ATSS Army Target Sensing System

B^2C^2 Brigade and Below Command and Control System

battle command the art of battle decision making, leading, and motivating soldiers in their organizations into action to accomplish missions; includes visualizing current state and future state, then formulating concepts of operations to get from one to the other at least cost; also includes assigning missions, prioritizing and allocating resources, selecting the critical time and place to act, and knowing how and when to make adjustments during the fight (FM 100-5)

battle dynamics five major interrelated dynamics that define significant areas of change from current operations to Force XXI Operations; dynamics are *battle command, battlespace, depth and simultaneous attack, early entry,* and *combat service suppor*t

battlefield visualization the process whereby the commander develops a clear understanding of the current state with relation to the enemy and environment, envisions a desired end state that represents mission accomplishment, and then subsequently visualizes the sequence of activity that moves the commander's force from its current state to the end state

battlespace components determined by the maximum capabilities of friendly and enemy forces to acquire and dominate each other by fires and maneuver and in the electromagnetic spectrum

BCE battlefield coordination element

BCTP Battle Command Training Program

BDA battle damage assessment

BOS battlefield operating system

C^2 command and control

C^2-attack command and control-attack

C^2-protect command and control-protect

C^2W command and control warfare

C^2W-I	command and control warfare-intelligence
C^3I	command, control, communications, and intelligence
C^4	command, control, communications, and computers
C^4FMO	command, control, communications, and computers for mobile operations
C^4I	command, control, communications, computers, and intelligence
CA	civil affairs
CCIR	commander's critical information requirements
CEOI	communications-electronics operation instructions
CERT	computer emergency response team
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	commander-in-chief
CIOS	commander's information operations staff
CIOSO	commander's information operations staff officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCS MOP	Chairman of the Joint Chiefs of Staff Memorandum of Policy
CMO	civil-military operations
CMOC	civil-military operations center
CNR	combat net radio
COA	course of action
COE	common operating environment
command and control	the exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; C^2 functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (Joint Pub 1-02)
command and control-attack	the synchronized execution of actions taken to accomplish established objectives that prevent effective C^2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C^2 system
command and control-protect	the maintenance of effective C^2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C^2 system; C^2-protect can be offensive or defensive in

	nature; offensive C^2-protect uses the five elements of C^2W to reduce the adversary's ability to conduct C^2-attack; defensive C^2-protect reduces friendly C^2 vulnerabilities to adversary C^2-attack by employment of adequate physical, electronic, and intelligence protection (adapted from CJCSI 3210.03)
command and control system	the combination of personnel, equipment, communications, computers, facilities, and procedures employed by the commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission; the basic functions of a command and control system are sensing valid information about events and the environment, reporting information, assessing the situation and associated alternatives for action, deciding on an appropriate course of action, and ordering actions in correspondence with the decision (Joint Pub 1-02)
command and control warfare	the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C^2 capabilities, while protecting friendly C^2 capabilities against such actions; command and control warfare applies across the operational continuum and all levels of conflict (Joint Pub 1-02)
common operating environment	an environment that provides a familiar look, touch, sound, and feel to the commander, no matter where the commander is deployed; information presentation and command, control, communication, computers, and intelligence system interfaces are maintained consistently from platform to platform, enabling the commander to focus attention on the crisis at hand; also called COE
communications	a method or means of conveying information of any kind from one person or place to another (Joint Pub 1-02)
communications security	the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications or to mislead unauthorized persons in their interpretation of the results of such possession and study; also called *COMSEC*; includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information
computer security	involves the measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer; these include policies, procedures, and the hardware and software tools necessary to protect the computer systems and the information processed, stored, and transmitted by the systems
COMPUSEC	computer security

COMSEC communications security

CONPLAN contingency plan

CONUS continental United States

counterintelligence those activities which are concerned with identifying and counteracting the threat to security posed by hostile services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism (Joint Pub 1-02)

COUNTERRECON counterreconnaissance

CP command post

critical information specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (Joint Pub 1-02)

CSS combat service support

CTC combat training center

DALIS Disaster Assistance Logistics Information System

DAMMS-R Department of the Army Movements Management System-Redesign

DDN Defense Data Network

DDS data distribution system

DEA Drug Enforcement Agency

defense information the shared or interconnected system of computers,

infrastructure communications, data, applications, security, people, training, and other support structures serving DOD's location and worldwide information needs; the DII connects DOD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services and provides information processing and value-added services to subscribers of the DISN

DEERS Defense Enrollment Eligibility Reporting System

DEW directed-energy weapon

DII defense information infrastructure

DISA Defense Information Systems Agency

DISE deployable intelligence support element

DISN Defense Information Systems Network

DJMS Defense Joint Military Pay System

DOD Department of Defense

DOS Department of State

DSN Defense Switch Network

DTLOMS doctrine, training, leader development, organizations, materiel, and soldiers

e-mail electronic mail

EA electronic attack

EAC echelons above corps

ECM electronic countermeasures

ECCM electronic counter countermeasures

EEFI essential elements of friendly Information

electromagnetic spectrum the range of frequencies of electromagnetic radiation from zero to infinity; it is divided into 26 alphabetically designated bands (Joint Pub 1-02)

electronics security the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiation, e.g., radar (Joint Pub 1-02)

electronic warfare any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES)

EM electromagnetic

EMI electromagnetic interference

EMP electromagnetic pulse

EMS electromagnetic spectrum

EOB electronic order of battle

EOC emergency operations center

EP electronic protection

EPLRS enhanced position location reporting system

ES electronic warfare support

essential elements of friendly information key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness (Joint Pub 1-02)

EW electronic warfare

EWIR electronic warfare integrated reprogramming

FAADC^{3}I forward air defense command, control, communications, and intelligence

FBCB^2 Force XXI Battle Command Brigade and Below System

FEMA Federal Emergency Management Agency

FFIR friendly forces information requirements

FM frequency modulation; field manual

force protection any collection or combination of measures to prevent or mitigate damage or disruption to an aggregation of military personnel, weapon systems, vehicles, installations, or support

FORSCOM United States Forces Command

FST field support team

full-dimensional operations the application of all capabilities available to an Army commander to accomplish his mission decisively and at the least cost across the full range of possible operations

G2 division intelligence

G3 division operations

G5 division civil affairs

G6 division communications

GCCS Global Command and Control System

GIE global information environment

GII global information infrastructure

global information environment all Individuals, organizations, or systems, most of which are outside the control of the military or National Command Authorities, that collect, process, and disseminate information to national and international audiences

GPS global positioning system

GR/CS Guardrail/Common Sensor

HCA	host civil affairs
HF	high frequency
HN	host nation
HNS	host nation support
HQDA	Headquarters, Department of Army
HUMINT	human intelligence
HVT	high-value target
I&W	indications and warnings
IADS	Integrated Air Defense System
IBDA	information battlefield damage assessment
ICP	intertheater communications security package
IEW	intelligence and electronic warfare
IMETS	Integrated Meteorological System
information	data collected from the environment and processed into a usable form
Information Age	the future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems
information data bases	visualization of a future system where commanders and units can continually access and update a common data base of relevant information (for example, logistics, intelligence, movement)
information dominance	the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary
information operations	continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities
information security	the protection of unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats

information systems	the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (Joint Pub 6-0)
information systems security	a composite means to protect telecommunications systems and automated information systems and the information they transmit and/or process
information warfare	actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (CJCSI 3210.01)
INFOSEC	information security
infosphere	the rapidly growing global network of military and commercial command, control, communications, and computer systems and networks linking information data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission; provides the worldwide automated information-of-exchange backbone support to joint forces; and provides seamless operations from anywhere to anywhere that is secure and transparent to the warrior; this emerging capability is highly flexible to support the adaptive command and control infrastructures of the twenty-first century
INFOSYS	information systems
infrastructure	the basic facilities, equipment, and installations needed for the function of a system, network, or integrated network
INMARSAT	international maritime satellite
intelligence	the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; also, information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (Joint Pub 1-02)
INTELSAT	intelligence satellite
internet	interoperable network
IO	information operations
IOBS	information operations battle staff
IOC	information operations center
IPB	intelligence-preparation-of-the-battlefield
ISB	installation sustaining bases

ISS information systems security

ISYSCON integrated systems control

ITU International Telecommunications Union

IW information warfare

J2 joint staff intelligence

J3 joint staff operations

J5 joint staff plans and policy

J6 joint staff communications-electronics

JAARS Joint After-Action Reporting System

JCS Joint Chiefs of Staff

JC^{2}WC Joint Command and Control Warfare Center

JCEWS joint commander's electronic warfare staff

JDISS Joint Deployable Intelligence Support System

JEWC Joint Electronic Warfare Center

JFC joint force commander

JOA joint operational area

JOPES Joint Operations Planning and Execution System

JRFL joint restricted frequency list

JSOI joint signal operating instructions

J-STARS Joint Surveillance Target Attack Radar System

JTACS Joint Theater Air Control System

JTB joint targeting board

JTF joint task force

JTTP joint tactics, techniques, and procedures

JULLS Joint Universal Lessons Learned System

JWICS Joint Worldwide Intelligence Communication System

LAM Louisiana Maneuvers

LAN local area network

LCC land component commander

LIWA Land Information Warfare Activity

LO liaison officer

MACOM	major Army command
MASINT	measurement signature
MCS	maneuver control system
METL	mission-essential task list
METT-T	mission, enemy, terrain, troops, and time available
MIE	military information environment
MI	military intelligence
MIID/IDB	Military Integrated Intelligence Data Base System/ Integrated Data Base
military deception	actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission
military information environment	the environment contained within the global information environment, consisting of information systems and organizations—friendly and adversary, military and nonmilitary—that support, enable, or significantly influence a specific military operation
mls	multilevel security
MNS	mission needs statement
MOBLAS	Mobilization-Level Application Software
MP	military police
MOP	memorandum of policy
MSC	major subordinate command
MSE	mobile subscriber equipment
MTP	mission training plan
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NEO	noncombatant evacuation operations
NII	national information infrastructure
NGO	nongovernment organization
NMS	National Military Strategy
NTSDS	National Target/Threat Signature Data System

OA operational architecture

OB order of battle

ODCSOPS Office of the Deputy Chief of Staff for Operations

OOTW operations other than war

OPFOR opposing force

OPCON operational control

operations security a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities; identifying those actions that can be observed by adversary intelligence systems; determining indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation; also called *OPSEC*

OPLAN operations plan

OPORD operations order

OPSEC operations security

OPTEMPO operation tempo

PA public affairs

PAO public affairs officer

PC personal computer

PEO program executive office

PIR priority intelligence requirements

physical destruction the application of combat power to destroy or neutralize enemy forces and installations; includes direct and indirect fires from ground, sea, and air forces; also includes direct actions by special operations forces

physical security that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft (Joint Pub 1-02)

PM project manager

POS/NAV position/navigation

PRC populace and resource control

priority intelligence requirements	those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making (Joint Pub 1-02)
PSN	public switch network
psychological operations	operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals; the purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives
PSYOP	psychological operations
PVO	private voluntary organization
RAP	remedial action project
RC	reserve components
RCAS	Reserve Component Automation System
RCP	relevant common picture
RDT&E	research, development, test, and evaluation
RECBASS	Reception Battalion Automated Support System
RECON	reconnaissance
relevant common picture of the battlefield	the aggregate of data that is shared among all friendly forces on the disposition of friendly and enemy force; this data is used to build a tailored relevant graphic display for the warfighter that increases in detail shown as the echelon served is closer to the soldier; commonly called situational awareness
relevant information	information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand
RII	relevant information and intelligence
RISC	reduced instruction set computing
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
ROE	rules of engagement
SAMS-I/TDA	Standard Army Maintenance System-Installation/ Table of Distribution and Allowances
SARSS-O	Standard Army Retail Supply System-Objective

SF Special Forces

SIDPERS Standard Installation/Division Personnel System

SIGINT signals intelligence

signal security a generic term that includes both communications security and electronic security (Joint Pub 1-02)

SIGSEC signal security

SINCGARS single-channel ground and airborne radio system

SJA staff judge advocate

SOF special operations forces

SOP standard operating procedure

SPBS-R Standard Property Book System-Redesign

spectrum management planning, coordinating, and managing operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference (Joint Pub 1-02)

STAMIS Standard Army Management Information Systems

STO special technical operations

STOD special technical operations division

TAA total Army analysis

tactical internet a battlefield communication system networked together using commercially based internet protocols

TAMMIS The Army Munitions Management Information System

TAFIM technical architectural framework for information management

TEARS Telecommunications Equipment Automated Retrieval System

TECHINT technical intelligence

TF task force

TPN tactical packet network

TRADOC United States Army Training and Doctrine Command

TRANSEC transmission security

transmission security *see* communications security

TRI-TAC triservice tactical

TROJAN-SPIRIT	TROJAN-special purpose integrated remote intelligence terminal
TSP	training support package
TSS	target-sensing system
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UHF	ultrahigh frequency
ULLS	unit-level logistics system
UN	United Nations
US	United States
USAF	United States Air Force
USAID	United States Agency for International Development
USAINSCOM	United States Army Information Systems Command
USIA	United States Information Agency
USN	United States Navy
USSOCOM	United States Special Operations Command
VHF	very high frequency
WAN	wide area network

References

SOURCES USED

Strategic Publications

ASD (C^3I) Memorandum, *Information Management Definitions.* 25 February 1994.

CJCSI 3210.01. *Joint Information Warfare Policy.* 2 January 1996.

CJCSI 3210.03.Joint Command and Control Warfare Policy (U). 31 March 1996.

CJCSI 3211.01. *Joint Military Deception*. 1 June 1993.

CJCSI 6212.01. *Compatibility, Interoperability and Integration of Command, Control, Communications, Computers, and Intelligence Systems*. 30 July 1993.

CJCS MOP-6. *Electronic Warfare*. 3 March 1993 (S).

DOD Directive S-3600.1. *Information Warfare*.

DOD Directive 5122.5. *Public Affairs Program*. 12 February 1993.

DOD Directive 5205.2. *Operations Security Program*. 7 July 1983.

Memorandum of Understanding Among Deputy Chief of Staff for Operations and Plans; Deputy Chief of Staff for Intelligence; Director of Information Systems for Command, Control, Communications, and Computers; and Commander, US Army Intelligence and Security Command, *The US Army Intelligence and Security Command's Land Information Warfare Activity.* February-March 1995.

National Military Strategy. February 1995.

National Security Strategy. January 1995.

Joint and Multiservice Publications

Joint Command and Control Warfare Staff Officers' Course Student Text. Armed Forces Staff College. January 1995.

Joint Pub 1. *Joint Warfare for the US Armed Forces*. 10 January 1995.

Joint Pub 1-02. *DOD Dictionary of Military and Associated Terms*. 24 March 1994.

Joint Pub 3-0. *Doctrine for Joint Operations.* 1 February 1995.

Joint Pub 3-13. 1. *Joint Command and Control Warfare (C^2W) Operations*. 7 February 1996.

Joint Pub 3-51. *Electronic Warfare in Joint Military Operations*. 30 June 1991.

Joint Pub 3-53. *Doctrine for Joint Psychological Operations*. 30 July 1993.

Joint Pub 3-54. *Joint Doctrine for Operations Security*. 15 April 1994.

Joint Pub 3-56. *Command and Control Doctrine for Joint Operations*. 3 May 1995.

Joint Pub 3-57. *Doctrine for Joint Civil Affairs.* February 1995.

Joint Pub 3-58. *Joint Doctrine for Operational Deception*. 6 June 1994.

Joint Pub 6-0. *Doctrine for Command, Control, Communications, and Computer (C^4) Systems Support to Joint Operations*. 3 June 1992.

Army Publications

AR 360-5. *Public Information.* 31 May 1989.

AR 360-81. *Command Information Program*. 2 October 1989.

AR 380-5. *Army Information Security Program.* 1 March 1988.

AR 380-19. *Information System Security.* 1 August 1990.

AR 381-11 (C). *Threat Support to US Army Force, Combat and Material Development.* 1 March 1993.

AR 525-21. *Battlefield Deception Policy.* 30 October 1989.

AR 525-22. *Intelligence and Electronic Warfare*. 1 October 1982.

AR 525-20. *Information Warfare/Command and Control Warfare (IW/C^2W) Policy.* (draft). No date.

AR 530-1. *Operations Security.* 3 March 1995.

FM 11-45. *Signal Support: Echelons Above Corps (EAC).* April 1993.

FM 11-75. *Battlefield Information Services (BIS).* 20 September 1994.

FM 24-1. *Signal Support and the Information Mission Area*. May 1993.

FM 24-7. *Army Tactical Command and Control System (ATCCS) System Management Techniques.* August 1993.

FM 27-100. *Legal Operations*. 30 September 1991.

FM 33-1. *Psychological Operations*. 18 February 1993.

FM 34-1. *Intelligence and Electronic Warfare Operations*. 27 September 1994.

FM 34-37. *Echelon Above Corps Intelligence and Electronic Warfare Operations*. 15 January 1991.

FM 34-130. *Intelligence-Preparation-of -the-Battlefield*. 8 July 1994.

FM 41-10. *Civil Affairs Operations.* 11 January 1993.

FM 46-1. *Public Affairs Operations*. 23 July 1992.

FM 71-100. *Division Operations*. July 1994.

FM 90-24. *Multiservice Procedures for Command, Control, and Communications Countermeasures.* 17 May 1991.

FM 100-1. *The Army.* 14 June 1994.

FM 100-5. *Operations*. 14 June 1993.

FM 100-7. *Decisive Force: The Army in Theater Operations*. 31 May 1995.

FM 100-15. *Corps Operations.* 13 September 1989.

FM 100-17. *Mobilization, Deployment, Redeployment, Demobilization*. 28 October 1992.

FM 100-18. *Space Support to Army Operations*. 20 July 1994.

FM 100-19. *Domestic Support Operations.* 1 July 1993.

FM 100-23. *Peace Operations*. 30 December 1994.

FM 100-23-1. *Multiservice Procedures for Humanitarian Operations.* October 1994.

FM 101-5. *Command and Control for Commanders and Staffs*. August 1993

FM 101-5-1. *Operational Terms and Symbols*. 21 October 1985.

TRADOC Pam 525-5. *Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century.* 1 August 1994.

TRADOC Pam 525-69. *Concept for Information Operations*. 1 August 1995.

TRADOC Pam 525-70. *Battlefield Visualization Concept*. 1 October 1995.

Center for Army Lessons Learned (CALL) Newsletter. *Logistical Reporting.* July 1994.

Center for Army Lessons Learned (CALL) Newsletter. *Dealing with the Media.* September-October 1995.

Other Publications

Army Battle Command Master Plan (ABCMP). HQDA, Office of the Deputy Chief of Staff for Operations and Plans. 19 September 1994.

Army Digitization Master Plan. HQDA, Army Digitization Office. 30 January 1995.

Army Enterprise Strategy Implementation Plan. Office of the Secretary of the Army. 8 August 1994.

Baig, Ed C. and John Cary. “Shielding the Net against Cyber-Scoundrels.” *Business Week*. 14 November 1994.

Bentley, Mark and Paul Evancon. “CVW - Computer Virus as a Weapon.” *Military Technology*. May 1994.

“C^4I for the Warrior.” The Joint Staff Pamphlet. J6. 12 June 1993.

CJCS Pamphlet. *Psychological Operations Support for Operation Provide Comfort*. March 1994.

de Borchgrave, Arnado. “Airbase No Match for Boy with a Modem.” *Washington Times*. 3 November 1994.

FMFM 3. *Command and Control*. 16 June 1993.

Fuller, J.F.C. Memorandum on *Strategic Paralysis as the Object of the Decisive Attack.* May 1918.

Gingrich, Newt, Rep. “Information Warfare: Definition, Doctrine and Direction.” Speech at the Information Research Management College, National Defense University. 3 May 1995.

Griffin, Gary B. MAJ (USA). *The Directed Telescope: A Traditional Element of Effective Command.* Combat Studies Institute, US Army Command and General Staff College. 20 May 1985.

Leaflets of the Persian Gulf War. 4th Psychological Operations Group (Airborne) Pamphlet. Undated.

Naval Doctrine Publication 6. *Naval Command and Control*. 19 May 1995.

Otis, Glenn General (USA, Ret) and W. Peter Cherry, Dr. "Concept Paper: Information Campaigns." *VRI Study*. 19 November 1991.

Price, Alfred. *The History of US Electronic Warfare.* Arlington, VA: Association of Old Crows. 1984.

Spiller, R.J. *Combined Arms in Battle Since 1939.* Fort Leavenworth, KS: US Army CGSC Press. 1992.

Steele, Robert D. *US Newswire*. 24 August 1993.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little, Brown and Co. 1993.

US Army Modernization Plan Update (FY 95-99). HQDA, Office of the Deputy Chief of Staff for Operations and Plans. May 1994.

Case Study: Rome Laboratory, Griffiss Air Force Base, NY, Intrusion. US Senate Permanent Subcommittee on Investigations. 5 June 1996.

DOCUMENTS NEEDED

DA Form 2028. *Recommended Changes to Publications and Blank Forms*. February 1974.

FM 11-45. *Signal Support: Echelons Above Corps (EAC).* April 1993.

FM 11-75. *Battlefield Information Services (BIS).* 20 September 1994.

FM 24-1. *Signal Support and the Information Mission Area*. May 1993.

FM 24-7. *Army Tactical Command and Control System (ATCCS) System Management Techniques.* August 1993.

FM 27-100. *Legal Operations*. 30 September 1991.

FM 33-1. *Psychological Operations*. 18 February 1993.

FM 34-1. *Intelligence and Electronic Warfare Operations*. 27 September 1994.

FM 34-37. *Echelon Above Corps Intelligence and Electronic Warfare Operations*. 15 January 1991.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 41-10. *Civil Affairs Operations*. 11 January 1993.

FM 46-1. *Public Affairs Operations*. 23 July 1992.

FM 71-100. *Division Operations*. (Coordinating Draft). July 1994

FM 90-24. *Multiservice Procedures for Command, Control and Communications Countermeasures.* 17 May 1991.

FM 100-1. *The Army.* 14 June 1994.

FM 100-5. *Operations*. 14 June 1993.

FM 100-15. *Corps Operations*. 13 September 1989.

FM 100-7. *Decisive Force: The Army in Theater Operations*. 31 May 1995.

FM 100-17. *Mobilization, Deployment, Redeployment, Demobilization*. 28 October 1992.

FM 100-18. *Space Support to Army Operations*. 20 July 1994.

FM 100-23. *Peace Operations*. 30 December 1994.

FM 101-5. *Command and Control for Commanders and Staffs*. (final draft). August 1993

FM 101-5-1. *Operational Terms and Symbols*. 21 October 1985.

DOD DIR 3600.1. *Information Warfare*. 21 December 1992 (TS).

Joint Pub 3-13. *Joint Command and Control Warfare (C^2W) Operations*. (final draft). September 1995.

READINGS RECOMMENDED

TRADOC Pam 525-5. *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century.* 1 August 1994.

TRADOC Pam 525-69. *Concept for Information Operations*. 1 August 1995.

Index

B

C

D

E

F

G

N

O

P

Q

R

S

T

U

V

W

FM 100-6
27 AUGUST 1996

By order of the Secretary of the Army:

DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

DISTRIBUTION:
Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11E, requirements for FM 100-6 (Qty rqr block no 5425).