Field Manual
No. 100-6

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

INFORMATION OPERATIONS

Contents

Page

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).

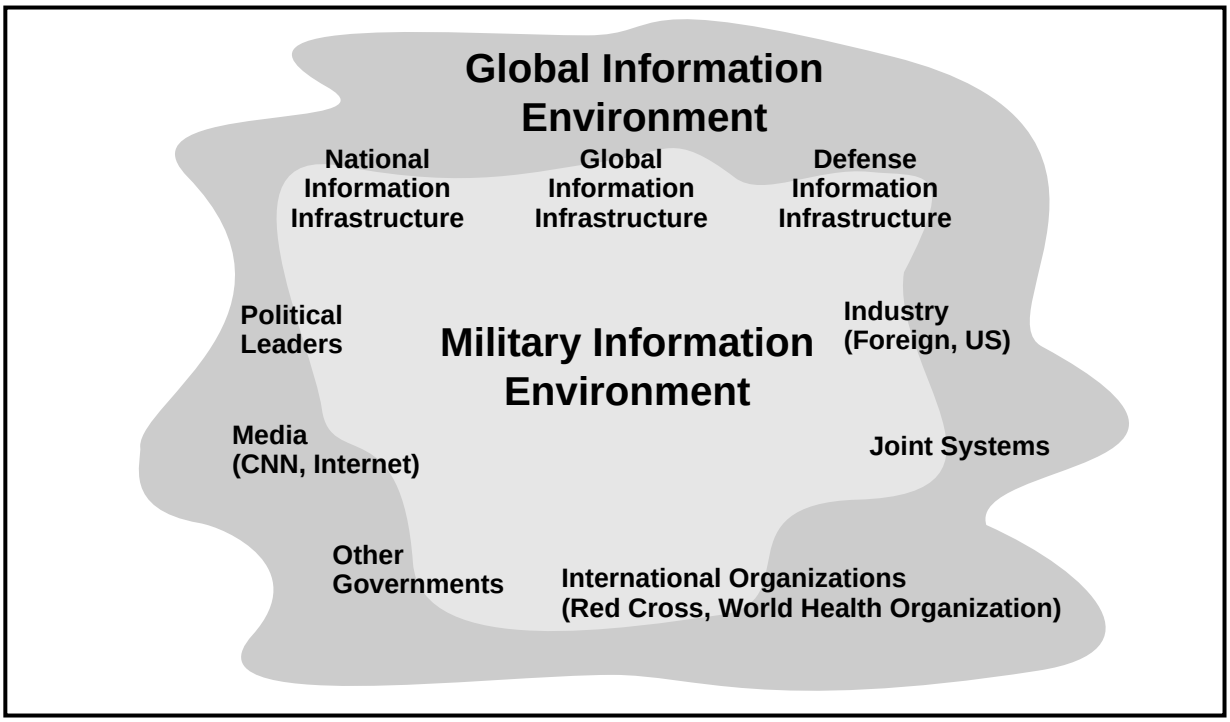

Figure 1-1. Information Environments (GIE and MIE)

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.

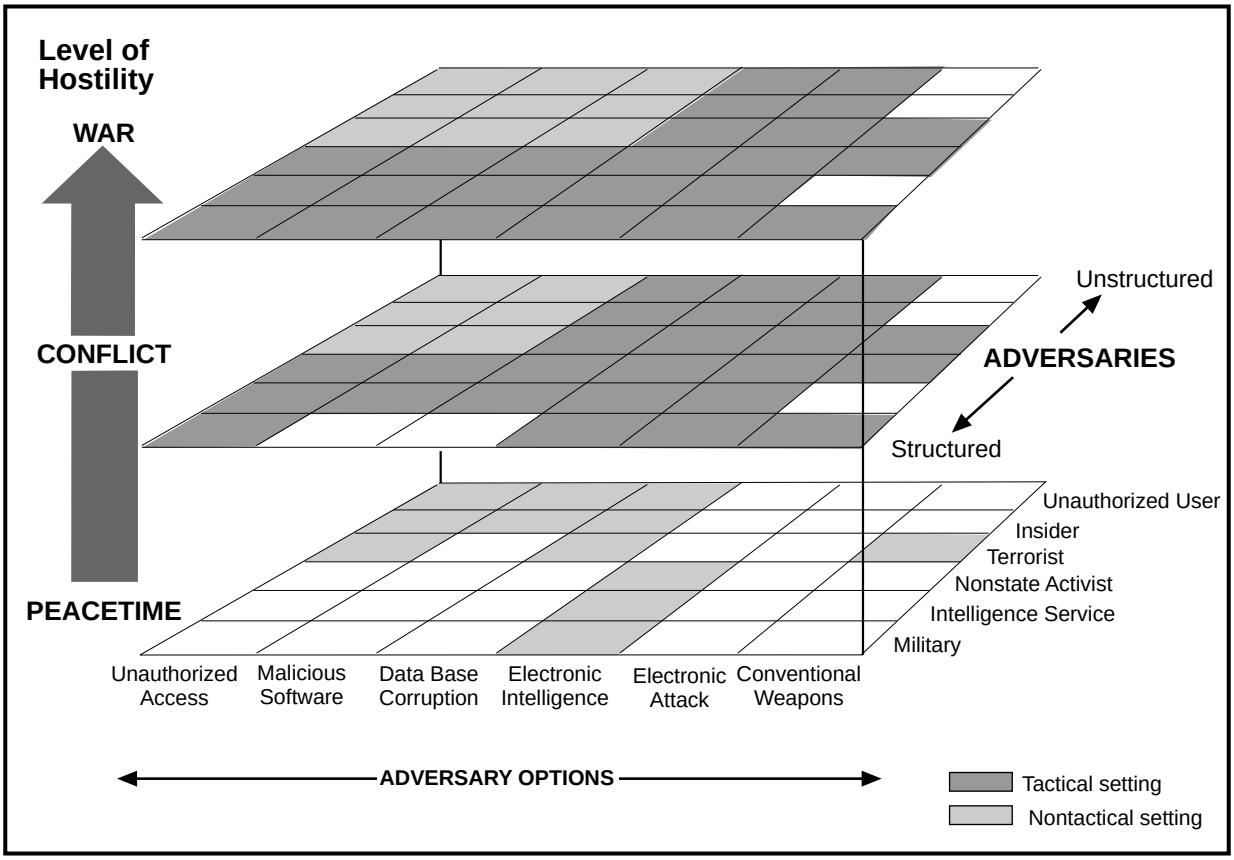

Figure 1-2. Threats to Information Systems

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.