Chapter 5: Information Warfare

This page is a section of FM 7-100.1 Opposing Forces Operations.

Modern information technologies (ITs) have created conditions for the confrontation of states, combatants, and non-state actors in a fundamentally new arenaâ the information sphere. Information, information processing, and communications networks are at the core of every military activity. The concepts of time, space, force, navigation, speed, precision, and lethality have changed because of the capabilities of information-age technology and the availability of information. These changes have a tremendous effect on how military forces conduct activities. The OPFOR addresses this issue through continued refinement of its information warfare (IW) doctrine.

The OPFOR defines information warfare as the specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The ultimate goal of IW is to influence decision makers. The OPFOR conducts IW at all levels of warfareâ strategic, operational, and tacticalâ but without regard to strict definitional boundaries among these levels. Opponents of the State are subject to IW regardless of the level and degree of engagement in other types of operations. The Stateâ s leadership integrates all instruments of powerâ diplomatic-political, economic, military, and informationalâ to implement an information strategy. One element of power may have primacy over the others at a given time, but all work together.

In the OPFORâ s view, skillful application of IW can facilitate the defeat of a technologically superior enemy. It can challenge or counter an enemyâ s goal of information dominance. The OPFOR can target key components (such as technology providing situational awareness, and advanced computing and communications technologies) that provide such dominance, thus shaking the opponentâ s confidence.

New Concepts of Information in Warfare

The State envisions an operational environment (OE) in which the battlespace stretches from the depths of an opponentâ s territory to the center of the Stateâ s political, economic, and military organizations. This OE is conducive to the practice of IW. Combat cannot be confined to a single battlespace, but instead will often expand globally to encompass attacks on an adversaryâ s information and space systems or his entire information environment.

Information is a powerful strategic, operational, and tactical multiplier. It enhances leadership and magnifies the effects of maneuver, firepower, and protection at decisive points. The OPFOR can use information as a component of combat power to shape the OE and create the conditions for employing the other components of its combat power. Information has become a vital strategic and operational resource. The OPFOR clearly understands the power of information and the revolution in IT and is actively developing doctrine and tactics to supplement more traditional types of warfighting. The OPFOR can use IW activities to create and/or exploit windows of opportunity for itself.

The importance of information, and its flow and control, to the conduct of military operations is not a new concept. The OPFOR has for years employed an integrated approach to attacking, disrupting, or manipulating information inside the enemyâ s decision-making cycle. Objectives have included not only the systems and information its enemies collect, process, and analyze, but also the leaders and the decisions they make. What is new, however, is the speed and volume of information available; networking, routing, and switching technologies; and the global connectivity of information systems and infrastructures. This information explosion, coupled with an integrated IW doctrine, provides the OPFOR a greater opportunity to inflict damage, trigger chaos, weaken national will, or permanently cripple an opponent. In effect, IW challenges traditional approaches to warfare. The following are ways in which IW redefines operations.

Information Infrastructure

Most of todayâs information environment is outside of military control, making it harder to regulate, dominate, or protect. While neither the State nor its opponents can control the global information environment or global information infrastructure (GII), they must prepare to operate within it. The GII is defined as the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. Within the GII, various countries have their own national information infrastructures (NIIs) and defense information infrastructures (DIIs).

The NII is the physical and virtual backbone of a nation. It is composed of multiple critical infrastructures. Critical infrastructures are those information and communication assets, systems, and functions so vital to a nation that their disruption or destruction would have a debilitating effect on national security, economy, governance, public health and safety, and morale.

The DII is defined as the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving an actorâs defense needs. The DII connects computers used for mission support, command and control (C2), and intelligence through voice, telecommunications, imagery, video, and multimedia services.

The interaction of the GII, NIIs, and DIIs introduces multiple actors into the information environment. This increases vulnerabilities and dependencies, and creates many legal issues.

Blurred Boundaries

The OPFOR understands that there is no clear-cut line of demarcation between the military, economic, and diplomatic-political aspects of an operation or strategic campaign and that the informational element cuts across the other three. Therefore, it uses all types of IW across all these dimensions.

In an information-based world, the boundaries between nations, individuals, and private-sector organizations can be undefined and nebulous. The traditional distinction between enemy and friendly forces becomes harder to observe, define, and ultimately defend against. The OPFOR is keenly aware of this development and can use it to its advantage when conducting IW actions. For example, the OPFOR could employ third-party individuals or organizations (either domestic or international) to conduct IW activities, making traceability difficult.

There may also be an inherent difficulty in isolating a specific OPFOR IW activity. For example, the distinction between OPFOR-sponsored IW attacks and other types of activities and events (such as espionage, accidents, system failures, disgruntled employee actions, and hacker pranks) are hard to distinguish. This period of confusion, and time spent trying to identify the attacker, can benefit and be manipulated by the OPFOR.

The interaction of the GII, NIIs, and DIIs compresses and blurs the distinction among tactics, operations, and strategy. For example, images of tactical military actions, disseminated by the media, are likely to influence strategic decision makers or the populace.

Expanded Role for Perception Management

Thus, perception management is a critical piece of IW. The OPFOR constantly attempts to â spinâ any conflict or situation to its advantage. IW planning and implementation emphasizes increased use of psychological warfare (PSYWAR) and deception designed to manipulate public opinion, coupled with attacks against an opponentâs centers of gravity.

New information-based techniques and tools can dramatically increase the ability to conduct perception management and supporting deception operations. Modern technologies allow the OPFOR to target a global audience for support and sympathy. The OPFOR stresses the importance of perception management from the strategic to the tactical level. (SeeÂ theÂ Perception Management section of this chapter for further detail.)

Role of Technology

Rapid advances in technology have produced an incredibly complex global information environment. Information and communications technologies have grown exponentially in recent years. Satellite and cellular communications, direct-broadcast television (expanding the awareness of events, issues, and military activities), personal computers, global positioning system (GPS) technologies, wireless communication capabilities, and the Internet are a few examples of the capabilities widely available to nations, as well as independent organizations and individuals. Given such advances, the capabilities of both the OPFOR and its potential adversaries are increasing in both sophistication and lethality. The OPFOR tries to exploit such technologies to gain the operational advantage.

Investment in Technology

The State is committed to creating an IT research and development base. However, until such a capability is developed, the State actively seeks international sources (overt and covert) and commercial off-the-shelf (COTS) products to satisfy its civilian and military requirements.

The OPFOR focuses its investment strategy on the following areas:

- ComputersÂ (including Â increasingly Â complexÂ distributed Â information systems).
- Telecommunications (traditional and wireless communications).
- Electronics (to included microelectronics).
- Computer integrated manufacturing.
- Nanotechnology.
- Robotics.
- Biotechnology.
- Space-based communications.
- Sophisticated sensing capabilities.

Vulnerability of Technology

The OPFOR can manipulate an enemyâ s unresolved problems of interoperability and dependence on COTS systems to its advantage. COTS materials are usually not hardened against electronic spikes, remote collection capabilities, or extreme weather conditions. The OPFOR understands that security cannot be constructed or guaranteed when depending on COTS. For example, if hackers (working independently or for a government or criminal organization) disrupted Internet communications or links while a military operation was in progress, information exchange between combat units could be severely disrupted.

Neutralizing Technological and Information Superiority

The OPFOR recognizes the increasing dependence of modern extraregional forces on information systems and their desire to obtain information superiority. However, the OPFOR also understands that information superiority does not equate to perfect information, nor does it eliminate the â fog of war.â Information systems, processors, and links add their own source of friction and vulnerability to the operational environment. Systems and sensors can be tricked, destroyed, or overwhelmed with data, thus causing an enemy to question the value and validity of his gathered intelligence. The OPFOR seeks to exploit this uncertainty and friction at all times.

The OPFOR recognizes that it cannot stand toe-to-toe with most extraregional enemies in a conventional war, and therefore seeks to target enemy weaknesses. IW will be the tool of choice to counter a technologically superior opponent and to challenge his relative information dominance. In addition, IW actions designed to break the will of a conventionally more powerful adversary will be common.

New Targets

Societies rely increasingly on a high-performance, networked information infrastructure for everything from air travel to electric-power generation and telecommunications to financial transactions. This means that a new set of lucrative strategic and operational targets is now open to attack. The OPFOR will focus all elements of its power, as well as the Stateâ s, on the destruction of the adversaryâ s critical information infrastructures.

Easy of Operation and Low Cost

In contrast to other forms of warfare, IW actions might occur without access to large financial resources or backing or without state sponsorship. Information weapons could be software logic bombs or computer worms and viruses. IW could be conducted with such easily accessible means such as cellular telephones and the Internet.

Elements of IW

OPFOR IW occurs through the combinations of seven elements:

- Electronic warfare (EW).
- Computer warfare.
- Deception.
- Physical destruction.
- Protection and security measures.
- Perception management.
- Information attack (IA).

The seven elements of IW do not exist in isolation from one another and are not mutually exclusive. Often they are mutually supporting. The overlapping of functions, means, and targets makes it necessary that they all be integrated into a single, integrated IW plan. However, effective execution of IW does not necessary involve the use of all elements concurrently. Although one element might be all that is required to successfully execute a tactical IW action, that would seldom be the case at the operational level. Likewise, using one element or subelement, such as camouflage, does not by itself necessarily constitute an operational application of IW.

The use of each element or a combination of elements is determined by the operational situation and support to the overall strategic objective. The size and sophistication of an enemy force also determines the extent to which the OPFOR employs the various elements of IW. The commander has the freedom to mix and match elements to best suit his operational needs, within the bounds of guidance from higher headquarters.

Electronic Warfare

EW consists of measures conducted to control or deny the enemyâ s use of the electromagnetic spectrum, while ensuring its use by the State and the OPFOR. EW capabilities allow the OPFOR to exploit, deceive, degrade, disrupt, damage, or destroy sensors, processors, and C2Â nodes. Spectrum supremacy and delay, denial, or distortions of information in the adversaryâ s information infrastructure are the objectives. At a minimum, the goal of OPFOR EW is to control the use of the electromagnetic spectrum at critical locations and times in the battlespace or to attack the enemy.

To accomplish these EW goals and objectives, the OPFOR employs both lethal and nonlethal measures. Lethal EW activities include the physical destruction of high-priority targets supporting the enemyâ s decision-making processâ such as reconnaissance sensors, command posts, and communications systems. They also include activities such as lethal air defense suppression measures. If available, precision munitions can degrade or eliminate high-technology C2 assets and associated links. Nonlethal means range from signals reconnaissance and electronic jamming to the deployment of corner reflectors, protective countermeasures, and deception jammers. Sophisticated camouflage, deception, decoy, or mockup systems can degrade the effects of enemy reconnaissance, intelligence, surveillance, and target acquisition (RISTA) systems. Also, the OPFOR can employ low-cost GPS jammers to disrupt enemy precision munitions targeting, sensor-to-shooter links, and navigation.

EW activities especially focus on the enemyâ s advanced C2Â systems developed to provide real-time force synchronization and shared situational awareness. The enemy relies on the availability of friendly and enemy force composition and locations, digital mapping displays, and automated targeting data. By targeting vulnerable communications links, the OPFOR can disrupt the enemyâ s ability to digitally transfer and share such information. The OPFOR enhances its own survivability through disrupting the enemyâ s ability to mass fires with dispersed forces, while increasing enemy crew and staff workloads and disrupting his fratricide-prevention measures.

EW is a perfect example of the integrated nature of OPFOR IW elements. It overlaps significantly with protection and security measures, deception, and physical destruction. Reconnaissance, aviation, air defense, artillery, and engineer support may all contribute to successful EW for IW purposes.

Computer Warfare

Computer warfare consists of attacks that focus specifically on the computer systems, networks, and/or nodes. This includes a wide variety of activities, ranging from unauthorized access (hacking) of information systems for intelligence-collection purposes, to the insertion of malicious software (viruses, worms, logic bombs, or Trojan horses) and deceptive information entry into enemy computer systems. Such attacks concentrate on the denial, disruption, or manipulation of the infrastructureâ s integrity. The OPFOR may attempt to accomplish these activities through the use of agents or third- party individuals with direct access to enemy information systems. It can also continually access and attack systems at great distances via communications links such as the Internet.

OPFOR computer warfare activities may be conducted prior to or during a military action. For example, by accessing databases related to an enemyâ s projected force deployments and troop movements, the OPFOR can effectively disrupt planning and misdirect movement, producing substantial confusion and delays. As modern armies increasingly rely on â just-in-timeâ logistics support, targeting logistics-related computers and databases can produce delays in the arrival of critical materiel such as ammunition, fuel, and spare parts during critical phases of a conflict.

The OPFOR can successfully conduct invasive computer warfare activities from the safety of its own territory, given the distributed ability to reach targeted computers anywhere in the world (as long as they are connected to the Internet). The OPFOR can continuously exploit the highly integrated information systems of an adversary.

Deception

OPFOR deception activities include measures designed to mislead adversaries by manipulation, distortion, or falsification of information. The aim of deception is to influence opponentsâ situational understanding and lead them to act in a manner that favors the OPFOR or is prejudicial to their own interests. Deception measures are a part of every military operation, and are also used to achieve political and economic goals. The international media may be a target for deceptive information at the operational level, being fed false stories and video that portray tactical-level actions with the goal of influencing operational or even strategic decisions.

The OPFOR applies all forms of deception in support of IW. These range from physical decoys and electronic devices to operational activities. The OPFOR can even use its own information systems to pass misleading or false information in support of deception activities. Such information may cause the adversary to analyze incorrectly OPFOR capabilities and intentions.

Because of the number and sophistication of sensors available to an extraregional adversary, the OPFOR recognizes that a multispectral effort is required to deceive him. This includes providing false or misleading thermal, visual, and electronic signatures.

Successful deception activities depend on the identification and exploitation of enemy information systems and networks, as well as other â conduitsâ for introducing deceptive information. Knowing how the conduits receive, process, analyze, and distribute information are priority intelligence requirements for the OPFOR.

Physical Destruction

Physical destruction, as an element of IW, involves measures to destroy critical components of the enemyâs information infrastructure. The OPFOR integrates all types of conventional and precision weapon systems to conduct the destructive fires, to include fixed- and rotary-wing aviation, cannon artillery, multiple rocket launchers, and surface-to-surface missiles. It can also utilize other means of destruction, such explosives delivered by special-purpose forces (SPF), insurgents, terrorists, or even co-opted civilians.

The OPFOR may integrate all forms of destructive fires, especially artillery and aviation, with other IW activities. Physical destruction activities are integrated with jamming to maximize their effects. Specific missions are carefully timed and coordinated with the IW plan and the actions of the supported units.

Due to the mobility and fleeting nature of many IW targets, precision weapons deliver the munitions of choice against many high-value targets. The increased accuracy provided by such weapons allows the OPFOR to attack specific IW-related targets rapidly and accurately. The OPFOR continues to research and develop directed energy weapons, to include radio frequency weapons and high-power lasers.

Protection and Security Measures

The purpose of protection and security measures in IW is to protect the OPFORâs information infrastructure, maintain OPFOR capabilities for effective C2, and deny protected information to other actors. The OPFOR continues to develop capabilities to effectively preserve OPFOR C2Â at all levels of command.

Protection and security measures conducted as part of IW includeâ

- Information collection, processing, and utilization.
- Reconnaissance and counterreconnaissance.
- Information and operations security.
- Camouflage, concealment, cover, and deception (C3D).
- Force protection.
- Secure use of information-collection and -processing systems.

Information and Operations Security

Information and operations security is used to protect the physical and intellectual assets used to facilitate command and control. It must function continuously to be effective. It must conceal not only operational intentions, current locations and configurations, and actions but also the tactics, techniques, and procedures of information systems employment and operation.

The OPFOR clearly understands the importance of information security. Commanders understand their vulnerabilities to being attacked Â through their own information systems and develop means to protect these systems. In addition, the OPFOR must be capable of isolating attacks on its information systems while maintaining the ability to execute. In order to reduce the vulnerability, the OPFOR emphasizes strong communications, computer, and transmission security. It uses all State assets to support this process and supply the necessary resources and intelligence.

Camouflage, Concealment, Cover, and Deception

The OPFOR gives particular attention to protective measures aimed at reducing the enemyâ s ability to target and engage OPFOR systems with precision munitions. Knowing that the enemy cannot attack what his RISTA systems do not find, the OPFOR employs a variety of C3D techniques. These range from the most simple and inexpensive methods to hide from observation to the most modern multispectral signature-reducing technology.

All OPFOR units can use one or more forms of technical camouflage. The purpose of these techniques is to alter the appearance of personnel and

equipment and to blend them with the surrounding terrain. Capabilities available includeâ

- Natural concealment.
- Camouflage paint.
- Artificial camouflage (nets and screens).
- Antiradar camouflage (radar-absorbing nets and paints).
- Decoy equipment (mockups) and deception positions.
- Light and thermal camouflage.
- Smoke camouflage.

Perception Management

Perception management involves measures aimed at creating a perception of truth that furthers the OPFORâ s objectives. It integrates Â several widely differing activities that use a combination of true, false, misleading, or manipulated information. Enemy or foreign audiences, as well as the Stateâ s own public, may be targets. Perception management can include misinformation, media manipulation, and PSYWAR. Perception management is critically important to all types of OPFOR operations.

PSYWAR is the capability and activities designed to influence selected friendly, neutral, and/or hostile target audiencesâ attitudes and behaviors in support of the OPFOR. PSYWAR can target either specific decision-making systems or the entire information system of the target audience, while influencing key communicators and decision makers. The OPFOR attacks an enemyâ s perceived centers of gravity. For example, prolonging an operation and using all forms of media to show the devastation of conflict can sway public opinion against the effort.

Statecraft (the art of conducting state affairs) and diplomacy (the art and practice of conducting negotiations with other states) are aspects of perception management conducted with foreign governments, and include those countriesâ populations as a target. The OPFOR skillfully employs media and other neutral players, such as nongovernmental and private volunteer organizations, to influence further public and private perceptions. It exploits the international mediaâ s willingness to report information without independent and timely confirmation. Individuals such as agents of influence, sympathizers, and antiwar protesters are also employed advantageously by the State or OPFOR to influence the enemyâ s media, politicians, and citizenry.

The Stateâ s Ministry of Public Information controls its own populationâ s access to information and perceptions of reality. Successful preparation of the population significantly enhances public support for the OPFORâs military actions.

Information Attack

An information attack (sometimes called cyber attack) focuses on the intentional disruption or distortion of information in a manner that supports a comprehensive IW campaign. Unlike, computer warfare attacks that target the information systems, IAs target the information itself. Attacks on the commercial Internet by civilian hackers have demonstrated the vulnerability of cyber and information systems to innovative and flexible penetration, disruption, or distortion techniques. OPFOR information attackers (cyber attackers) learn from and expand upon these methods.

IA offers a powerful tool for the OPFOR. For example, an information attacker may target an information system for sabotage (electronically or physically) or manipulate and exploit information. This may involve altering data, stealing data, or forcing a system to perform a function for which it was not intended, such as spoofing the air traffic control grid.

Likely targets for an IA are information residing in the critical infrastructures of an opponent: telecommunications links and switches, commercial infrastructures, and economic infrastructures. The OPFOR will attempt to manipulate, control, or monitor data and information that are critical for the infrastructures.

Tools and Targets

Tools for waging IW can include conventional physical and electronic destruction means, malicious software, denial-of-service attacks, news agencies, television, radio, the Internet, traditional print media, communication networks, and diplomatic activities and well as various types of reconnaissance, espionage, and eavesdropping technologies. The OPFOR can employ IW tools from both civilian and military sources and assets of third-party sources.

The OPFOR sees the targets of IW as decision makers, weapons and hardware, an opponentâ s critical information infrastructure, C2 system, information and telecommunications systems, and C2 centers and nodes. An adversaryâs national communications media are also among the important targets in an OPFOR IA. Information links, such as transmitters, communication devices, and protocols, will be targeted. These targets may be more susceptible to precision fires and more traditional forms of attack based on EW. However, the OPFOR is extremely adaptive and will employ the best option available to degrade or destroy an information link.

Strategic IW

Strategic information warfare (SIW) is the synergistic effort Â of Â the State to control or manipulate information events in the strategic environment, be they political, economic, military, or diplomatic in nature. Specifically, the State defines SIW as any attack (digital, physical, or cognitive) against the information base of an adversarial nationâs critical infrastructures. The ultimate goal of SIW is strategic disruption and damage to the overall strength of the opponent. This disruption also focuses on the shaping of foreign decision makersâ actions to support the Stateâs strategic objectives and goals.

The National Command Authority (NCA) is responsible for determining and articulating the Stateâs strategic goals. The Strategic Integration Department (SID) then develops a strategic information warfare plan (SIWP) to support the national security strategy. The SID has a special Strategic Information Warfare Planning Office (SIWPO) dedicated to reviewing and integrating information-related plans of all State ministries, both military and civilian. The SIWPO can directly task information- or IW-related elements of any ministry to support the SIWP. In time of war, the SIWPO continues to coordinate with all government ministries for further development and modification of the SIWP. However, it works most closely with the Ministry of Defense, specifically the General Staff, to ensure the development of the SIWP in concert with the military IW plan.

In the General Staff, the Chief of IW handles IW functions that transcend service component boundaries. He reviews and approves the IW plans of all operational-level commands as well as any separate theater headquarters that might be established. He drafts the overall military IW plan that, upon approval by the Intelligence Officer, is forwarded to the Operations Directorate of the General Staff for inclusion in the military strategic campaign plan (SCP). Once approved by the Chief of the General Staff, the military IW plan and the rest of the military SCP are forwarded to the SID for incorporation into the national-level SIWP and the national SCP, respectively. During peacetime and preparation for war, the Chief of IW continues to review and refine the military IW plan.

Operational-Level IW

The OPFOR conducts IW actions at the operational level to support strategic campaigns or operational objectives. The focus at this level is on affecting an adversaryâ s lines of communication (LOCs), logistics, C2, and critical decision-making processes. The OPFOR targets information or information systems in order to affect the information-based process, be it human or automated.

Systems Warfare

In the systems warfare approach to combat (see Chapter 1), the OPFOR often focuses on attacking the C2Â and/or RISTA elements that are critical components of the enemyâ s combat system. It is often more feasible to attack these types of targets, rather than directly engaging the combat power of the enemyâ s combat or combat support forces or even his logistics forces. Operational-level IW can be a primary means of attacking C2Â and RISTA assets, either on its own or in conjunction with other elements of the OPFORâ s own combat system.

Offensive IW

Offensive IW involves the integrated use of subordinate and supporting capabilities and activities, mutually supported by intelligence, to affect an adversaryâ s decision makers or to influence others in order to achieve or promote specific OPFOR objectives. Using the elements of IW offensively, the OPFOR can either prevent an adversary from exercising effective C2, challenge his quest for information dominance, or leverage enemy information systems to its own advantage.

Purpose of Offensive IW

Simply put, offensive IW seeks to deny, degrade, destroy, disrupt, deceive, and exploit an adversaryâ s information systems and capabilities. Offensive IW helps the OPFOR seize and retain the initiative by degrading the enemyâ s information systems and forcing the enemy commander to be reactive. This can result in slowing the enemyâ s tempo, disrupting his decision cycle, and impacting his overall ability to generate combat forces and execute and sustain operations.

Possible Actions

Possible OPFOR offensive IW activities and actions can includeâ

- Denying the enemy the information necessary to conduct operations (destroy, degrade, or distort).
- Influencing the information (misinformation, manipulation, or â spinningâ).

- Disrupting the enemyâs ability to observe and collect information and obtain or maintain information dominance.
- Degrading enemy information collection or destroying his collection means.
- Deceiving the decision makers by manipulating perception and causing disorientation within the decision cycle.
- Neutralizing or destroying the opponentsâ information capability by physical destruction of critical communications nodes and links.

Defensive IW

Defensive IW is the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive IW also seeks to conceal the physical locations of critical information systems. IW activities, particularly defensive measures, play a significant role in ensuring the viability and survivability of the OPFOR C2Â process. IW defensive actions are planned at the strategic, operational, and tactical levels. IW measures, combined with the mobility and redundancy of C2 systems, can provide a high degree of survivability, even if the enemy is successful in disrupting or destroying some elements of the process.

Purpose of Defensive IW

The objectives of OPFOR defensive IW activities and actions areâ

- Protecting the information environment.
- Detecting attack.
- Restoring capabilities.
- Responding to attack.

Specific objectives of defensive IW include misleading the enemy concerning the OPFORâ s force structure, location, and intent; protecting all critical information and communication links; and ensuring maximum survivability of friendly high-value assets and combat power.

Possible Actions

To achieve these objectives, the OPFOR conducts a variety of activities and actions that canâ

- Provide for uninterrupted control of friendly forces.
- EnsureÂ survivability Â through Â extensiveÂ useÂ of Â signature-reducing measures.
- Conceal the identities and locations of critical elements.
- Portray false force dispositions and OPFOR unit strengths.
- Portray false levels of preparation, readiness, and morale.
- Portray false impressions of OPFOR operational intent.

Figure 5-1. IW Elements, Planning Objectives, and Targets

IW Element	Objectives	Targets
Electronic Warfare	Exploit, disrupt, deny, and degrade the enemyâs use of the electromagnetic spectrum.	C2Â and RISTA assets and networks.
Computer Warfare	Disrupt, deny, or degrade the enemyâs computer networks and information flow.	C2Â and RISTA assets and networks (both civilian and military).
Deception	Mislead enemy decision makers. Cause confusion and delays in decision-making process. Persuade adversaryâs population and international community to support OPFOR objectives.	Key decision makers from political, military, economic, and diplomatic elite. General population and international media sources and Internet sites.
Physical	Destroy enemyâs information	C2Â nodes and links, RISTA assets, telecommunications, and

Destruction	infrastructures (both civilian and military).	power sources.
Protection and Security Measures	Protect critical assets.	Enemy RISTA assets.
Perception Management	Distort reality or manipulate information to support OPFOR goals.	RISTA assets, media sources (international and domestic).
Information Attack	Objectives vary based on situational needs and objectives of the attack.	Information residing in networks, software, data repositories, databases, and any other electronic source or conduit of communication or information.

IW Planning and Execution

An effective IW action demands the coordination of activities and capabilities into a single, focused plan. Any or all elements of IW may be effectively used in any given plan. Figure 5-1 provides examples of objectives and targets.

OPFOR IW planning occurs at all levels of conflict and before and after conflict. At the strategic level, the initial focus is achieving State objectives and supporting the strategic campaign plan. Perception management, protection and security measures, and computer warfare activities are critical at this level.

As tensions escalate, IW at the operational level can be employed to disrupt the enemyâ⊠ ⊠ s information systems, further demonstrating national resolve and military capability. The chief of IW formulates the IW plan as an integral part of all ground, air, sea, and space operations.

Staff Responsibilities

Just as there is a Chief of IW in the General Staff, there is a chief of IW under the intelligence officer in all military staffs down to brigade level. Within those operational- and tactical-level staffs, the intelligence officer and chief of IW are responsible for ensuring that all IW actions undertaken at their levels are in concert with the overall military IW plan and the SIWP. As necessary, the Chief of IW in the General Staff can directly task each operational- or tactical-level chief of IW to support the SIW campaign. (See the Strategic IW section of this chapter.)

The intelligence officer heads the intelligence and information section of the primary staff of an operational-strategic command (OSC). He ensures that all intelligence requirements are met and coordinates all necessary national- or theater-level assets for the IW plan. He must effectively task organize his staff resources to plan, conduct, and execute IW. Traditional staff functions and relationships may be expanded or even redefined. (See Chapter 2 for a more detailed discussion of staff responsibilities and organization.)

The chief of IW belongs to the secondary staff, heading a subsection under the intelligence officer. The chief of IW supervises the execution of the OSCâ⊠ ⊠ IsW plan. He is responsible forâ⊠ ⊠

- Coordinating the employment of IW assets, including those subordinate to the OSC or affiliated forces and any supporting assets available at the national or theater level.
- Planning for and supervising all information protection and security measures.
- Supervising the implementation of the deception plan and perception management objectives.
- Working with the operations section of the staff to ensure that targets scheduled for destruction support the IW plan, and if not, resolving conflicts between IW needs and operational needs.
- Recommending to the intelligence officer any necessary actions required to implement the IW plan.

The chief of IW at each level of command submits his IW plan to the chief of IW at the next-higher level. The senior chief of IW issues directives to subordinate unitsâ⊠ ⊠chiefs of IW. These directives are part of the operation plan or operational directive, and can be part of the SCP. What the subordinates plan and execute must be in concert with the higher plan, and the higher headquarters also needs to ensure that the IW plan of one subordinate does not conflict with that of its adjacent units.

The chief of IW also plays a key role in coordinating IW activities with other staff sections and subsections, particularly with members of the functional staff. For instance, he coordinates with the chief of integrated fires to ensure that deception and protection and security measures contribute to the success of fire support to offensive and defensive operations. He will also work directly with the chief of the RISTA and IW section of the OSCâ–IFC headquarters to coordinate all necessary IW support to the IFC. IW activities can support the overall fire support plan or provide a feasible nonlethal alternative to destroying key enemy formations or systems. The chief of IW also coordinates with the chief of force protection to prevent or mitigate the effects of hostile actions on critical information and information systems. He works closely with the chief of population management and representatives from the Ministry of Public Information regarding coordination of PSYWAR and other perception management activities.

Planning

The components of an IW plan include, at a minimum, the following:

- Statement of overall State and military objectives and goals.
- Definition of the missions of IW (public, private, military, and nonmilitary).
- IW objectives of the next-higher command.
- Use of affiliated forces.
- Use of civilians (individuals or organizations) on the battlefield.
- Identification of all applicable State elements of power to assist in the execution of the IW plan.
- Potential targets and tools for destruction, degradation, or exploitation.
- Specific unit responsibilities.

Specific plan elements include a review of the enemyâs IW capabilities, an operational analysis of all relevant information infrastructures (location, ownership and vulnerabilities), requirements of IW capabilities, an organizational plan and staff responsibilities, a deception plan, and perception management objectives.

Execution

Throughout the implementation of the IW plan, activities and success are monitored, and may result in a revision of the plan. The intelligence officer and the chief of IW are providing feedback to the planning process.

Strategic Context

The OPFOR uses IW activities during all four strategic-level courses of action: strategic, regional, transition, and adaptive operations (see Chapter 1 or FM 7-100). While certain elements of IW may be highlighted for a particular strategic course of action, all elements can be applied as necessary. IW can support the OPFOR against a regional peer or a technologically superior enemy. IW can also be used to create and/or exploit windows of opportunity across all types of operations.

Strategic Operations

Strategic operations can occur before and after armed conflict and in conjunction with any of the other three strategic courses of action during war. The State recognizes the value of IW in peacetime actions as well as during actual conflict. At this level, the State employs all the elements of IW to support its strategic objectives.

Perception management, deception, and protection and security measures are especially critical during strategic operations. The State attempts to use all forms of international media to support State actions and objectives. It uses all types of information dissemination to project its desired â spinâ of events, to gather international support, to weaken its enemyâ s resolve, and to force key decision makers to rethink any potentially damaging action against the State. In addition, the State develops a strategic deception plan to conceal its intentions from both the international audience and its own population. Once extraregional intervention begins, the military aspects of strategic operations become more aggressive, including use of physical destruction accompanied by other IW efforts to exploit its effects on enemy confidence and resolve.

Strategic operations involve the application of any or all of the four instruments of power (including the informational) to target enemy strategic centers of gravity. Thus, IW targets during strategic operations might includeâ

- Key leaders and decision makers (military and civilian).
- All relevant media outlets.
- Diplomatic entities.
- Relevant private institutions or influential organizations.
- Public opinion (international and domestic).
- National will (enemy and friendly).
- Commitment of alliance and coalition members.

The Ministry of Public Information is responsible for the control and appropriate dissemination of all political, diplomatic, economic, and military information to the public and the international audience. That ministry is a key player in the development and execution of all strategic IW campaigns. At the operational level, the intelligence officer and chief of IW are responsible for ensuring that all IW actions are in concert with the national-level SIWP.

Regional Operations

IW activities during regional operations focus on controlling foreign perceptions of such operations and preventing the development of any international consensus to intervene. The State tries to keep foreign perceptions of its actions below the threshold that could invite intervention by extraregional forces. To this end, perception management and deception campaigns are critical, for both domestic and international consumption.

During regional operations, the State also conducts an internal information campaign to help maintain and strengthen the national will. The overall goal is to give the entire country a common focus and guarantee internal support. All elements of IW are important in regional operations. Depending on the specific conditions, EW, IAs, protectionÂ and security measures, or perception management may dominate.

Transition Operations

During transition operations, the OPFOR focuses IW activities on access-control operations, perception management and deception campaigns, and protection and security of its IW assets. Deception activities focus on concealing the intentions of the OPFOR as well as the likely course of the transitionâ either into adaptive operations or back to regional operations.

Denying an adversary information dominance is critical during transition operations. The OPFOR attempts to take advantage of the enemyâ s reliance on advanced C2 and RISTA technology. Such technology and related communications and data links are critical to the enemyâ s maintaining enhanced situational awareness and thus become the key targets of all IW actions.

The protection and security of OPFOR IW assets and related communications is always a critical element. However, its importance increases during transition operations, since the OPFORâ s paramount goal is to preserve all instruments of power and prepare for a possible move to more adaptive operations.

The Stateâs internal IW goal might be to convince its citizens that transition operations are necessary in order to exploit the many gains it has already made and to prevent the intervention of an extraregional force. The State also conducts a ubiquitous information campaign to strengthen its national will by portraying the State as a victim of impending antagonistic actions, thus rallying support for State actions.

In perception management campaigns targeting the international community, the State increases its emphasis on popularizing the State and its actions. If it is obvious that the OPFOR will be overmatched by the extraregional force that is about to intervene, the State may depict the intervening force as an unwanted aggressor involving itself in regional affairs in order to support its own selfish interests. This may lead to intense international media pressure. During transition operations, the State may implement a cleverly developed plan to fracture alliance or coalition support to extraregional intervention.

Adaptive Operations

Against extraregional threats, the OPFOR begins to use more offensive and adaptive forms of IW. These include not only more aggressive information campaigns, but also IA, EW, and increased emphasis on physical destruction. As extraregional forces continue to deploy into the region, the OPFOR can use IAs on enemy C2Â systems and to strip away the enemyâs RISTA capabilities.

The OPFOR uses perception management and other tools to attack the enemyâs will to fight or otherwise continue its intervention, and to manipulate international opinion. If it still occupies territory of a neighboring country, it also tries to turn the populace there against the intervening extraregional force.

The State continues to leverage international media to influence world perception and public opinion within the extraregional powerâs own populace. It also continues to censor and manipulate the media.

The specific focus of IW in adaptive operations may includeâ

- Control access. Use all means necessary, including IW, to delay or disrupt entry into the region and ultimately defeat the intervening force.
- Control tempo. Use IW to attack critical C2 and logistics links.
- Exploit atrocities of conflict. Use IW to weaken the enemyâs resolve to remain committed while promoting the OPFORâs position as a victim.
- Neutralize technological overmatch. Use IW to attack critical C2Â and RISTA nodes and destroy supporting infrastructures.
- Attack reach-back links. Use IW to detect, jam, disable, or degrade critical nodes of communication.
- Counter information dominance. (See the following paragraph.)

The very systems and links upon which technologically advanced enemies rely for information dominance are also high-payoff targets for IAs or physical destruction. Denial of these resources at critical times can deny forces complete situational awareness. The OPFOR can also use the enemyâs robust array of RISTA systems against him. His large numbers of sensors can overwhelm his unitsâ ability to receive, process, and analyze raw intelligence data and to provide timely and accurate intelligence analysis. The OPFOR can add to this saturation problem by using deception to flood enemy sensors with masses of conflicting information. Conflicting data from different sensors at different levels (such as satellite imagery conflicting with data from unmanned aerial vehicles) can confuse the enemy and degrade his situational awareness.