Chapter 7: Information Warfare

This page is a section of TC 7-100.2 Opposing Force Tactics.

The OPFOR is constantly increasing the levels of technology used in its communications, automation, reconnaissance, and target acquisition systems. In order to ensure the successful use of information technologies and to deny the enemy the advantage afforded by such systems, the OPFOR has continued to refine its doctrine and capabilities for information warfare (INFOWAR). The OPFOR knows it cannot maintain continuous information dominance, particularly against peer or more powerful opponents. Therefore, it selects for disruption only those targets most critical to ensuring the successful achievement of its objectives. It attempts to gain an information advantage only at critical times and places on the battlefield. This chapter focuses on INFOWAR activities at the tactical level.

Tactical-Level INFOWAR

The OPFOR defines information warfare as specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The primary goals of INFOWAR are toâ

- Influence an enemyâ decisionmaking through his collected and available information, information systems, and information-based processes.
- Retain the ability to employ friendly information and information-based processes and systems.

Information and its management, dissemination, and control have always been critical to the successful conduct of tactical missions. Given todayâ advancements in information and information systems technology, this importance is growing in scope, impact, and sophistication. The OPFOR recognizes the unique opportunities that INFOWAR gives tactical commanders, and it continuously strives to incorporate INFOWAR activities in all tactical missions and battles.

INFOWAR may help degrade or deny effective enemy communications and blur or manipulate the battlefield picture. In addition, INFOWAR helps the OPFOR achieve the goal of dominating the tempo of combat. Using a combination of perception management activities, deception techniques, and electronic warfare (EW), the OPFOR can effectively slow or control the pace of battle. For example, the OPFOR may select to destroy lucrative enemy targets. It may also orchestrate and execute a perception management activity that weakens the enemyâ s international and domestic support, causing hesitation or actual failure of the operation. It executes deception plans to confuse the enemy and conceal true OPFOR intentions. More traditional EW activities also contribute to the successful application of INFOWAR at the tactical level by challenging the enemyâ quest for information dominance.

INFOWAR also supports the critical mission of counterreconnaissance at the tactical level. The OPFOR constantly seeks ways to attack, degrade, or manipulate the enemyâ reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capabilities. All enemy target acquisition systems and sensors are potential targets.

Associated Tactical Tasks

The effects of INFOWAR can be multidimensional and at times hard to pinpoint. However, the OPFOR highlights the following tasks and associated effects as critical to the application of INFOWAR at the tactical level:

- Destroy. Destruction tasks physically render an enemyâ information systems ineffective. Destruction is most effective when timed to occur before the enemy executes a command and control (C2) function or when focused on a resource-intensive target that is hard to

reconstitute. Neutralizing or destroying the opponentâ s information capability can be brought about by physical destruction of critical communications nodes and links.
- Degrade. Degradation attempts to reduce the effectiveness of the enemyâ s information infrastructure, information systems, and information collection means.
- Disrupt. Disruption activities focus on the disrupting enemy observation and sensor capabilities at critical times and locations. Disruption impedes the enemyâ s ability to observe and collect information and obtain or maintain Information dominance.
- Deny. Denial activities attempt to limit the enemyâ s ability to collect or disseminate information on the OPFOR or deny his collection efforts.
- Deceive. Deception activities strive to mislead the enemyâ s decisionmakers and manipulate his overall understanding of OPFOR activities. Deception manipulates perception and causes disorientation among decisionmakers within their decision cycle.
- Exploit. Exploitation activities attempt to use the enemyâ s C2 or RISTA capabilities to the advantage of the OPFOR. The OPFOR also uses its various INFOWAR capabilities to exploit any enemy vulnerability.
- Influence. Influencing information affects an enemyâ s beliefs, motives, perspectives, and reasoning capabilities, in order to support OPFOR objectives. This may be done through misinformation or by manipulating or â spinningâ information.

Systems Warfare

In the systems warfare approach to combat (see chapter 1), the OPFOR often focuses on attacking the C2, RISTA, and/or logistics elements that are critical components of the enemyâ s combat system. It is often more feasible to attack such targets, rather than directly engaging the enemyâ s combat or combat support forces. Tactical-level INFOWAR can be a primary means of attacking these assets, either on its own or in conjunction with other components of the OPFORâ s own combat system.

Windows of Opportunity

To conduct successful action against a more powerful force enjoying a technological overmatch, the OPFOR must exploit windows of opportunity. Sometimes these windows occur naturally, as a result of favorable conditions in the operational environment. Most often, however, the OPFOR will have to create its own opportunities. INFOWAR can help create the necessary windows of opportunity for any type of offensive or defensive action by executing effective deception techniques, EW, and physical destruction.

When the OPFOR must create a window of opportunity, INFOWAR activities can contribute to this byâ -

- Destroying or disrupting enemy C2 and RISTA assets.
- Deceiving enemy imagery and signals sensors.
- Selectively denying situational awareness.
- Slowing the tempo of enemy operations.
- Isolating key elements of the enemy force.

Elements of INFOWAR

Integrated within INFOWAR doctrine are the following seven elements:

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

The seven elements of INFOWAR do not exist in isolation from one another and are not mutually exclusive. The overlapping of functions, means, and targets requires that they all be integrated into a single, integrated INFOWAR plan. However, effective execution of INFOWAR does not necessary involve the use of all elements concurrently. In some cases, one element may be all that is required to successfully execute a tactical INFOWAR action. Nevertheless, using one element or subelement, such as camouflage, does not by itself necessarily constitute an application of INFOWAR.

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

Tools for waging INFOWAR can include, but are not limited toâ

- Conventional physical and electronic destruction means.
- Malicious software.
- Denial-of-service attacks.
- The Internet.
- The media.
- International public opinion.
- Communication networks.
- Various types of reconnaissance, espionage, and eavesdropping technologies.

The OPFOR can employ INFOWAR tools from both civilian and military sources and from assets of third- party actors.

The OPFOR sees the targets of INFOWAR as an opponentâ sâ

- Decisionmakers.
- Weapons and hardware.
- Critical information infrastructure.
- C2 system.
- Information and telecommunications systems.
- C2 centers and nodes.

Information links, such as transmitters, communication devices, and protocols, will be targeted. The OPFOR is extremely adaptive and will employ the best option available to degrade, manipulate, influence, use, or destroy an information link. See table 7-1 for typical examples of INFOWAR objectives and targets.

Table 7.1. INFOWAR elements, objectives, and targets

INFOWAR Element	Objectives	Targets
Electronic Warfare	Exploit, disrupt, deny, and degrade the enemyâ s use of the electromagnetic spectrum.	C2 and RISTA assets and networks.
Deception	Mislead enemy decisionmakers. Cause confusion and delays in the decisionmaking process. Persuade the local population and/or international community to support OPFOR objectives.	Key military decisionmakers. General population and international media sources and Internet sites.
Physical Destruction	Destroy the enemyâ sinformation infrastructures.	C2 nodes and links, RISTA assets, telecommunications, and power sources.
Protection and Security Measures	Protect critical assets.	Enemy RISTA assets.
Perception Management	Distort reality or manipulate information to support OPFOR goals.	Enemy RISTA assets. Local populace and leaders.

		Media sources (international and domestic).
Information Attack	Alter or deny key information.	Decisionmakers and other users of information. Systems reliant on accurate information.
Computer Warfare	Disrupt, deny, or degrade the enemyâ s computer networks and information flow.	C2 and RISTA assets and networks.

Electronic Warfare

Electronic warfare is activity conducted to control or deny the enemyâ s use of the electromagnetic spectrum, while ensuring its use by the OPFOR. EW capabilities allow an actor to exploit, deceive, degrade, disrupt, damage, or destroy sensors, processors, and C2 nodes. At a minimum, the goal of EW is to control the use of the electromagnetic spectrum at critical locations and times or to attack a specific system. The OPFOR realizes that it cannot completely deny the enemyâ s use of the spectrum. Thus, the goal of OPFOR EW is to control (limit or disrupt) his use or selectively deny it at specific locations and times, at the OPFORâ s choosing. In this way, the OPFOR intends to challenge the enemyâ s goal of information dominance.

The OPFOR employs both nonlethal and lethal means for EW. Nonlethal means range from signals reconnaissance and electronic jamming to the deployment of corner reflectors, protective countermeasures, and deception jammers. The OPFOR can employ low-cost GPS jammers to disrupt enemy precision munitions targeting, sensor-to-shooter links, and navigation. Lethal EW activities include the physical destruction of high-priority targets supporting the enemyâ s decisionmaking processâ ¯ such as reconnaissance sensors, command posts (CPs), 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.

EW activities often focus on the enemyâ s advanced C2 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 INFOWAR 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 INFOWAR purposes.

Signals Reconnaissance

Signals reconnaissance is action taken to detect, identify, locate, and track high-value targets (HVTs) through the use of the electromagnetic spectrum. It includes both intercept and direction finding, which may enable a near-real-time attack on the target. OPFOR commanders determine the priorities for signals reconnaissance by determining which HVTs must be found in order to have the best chance for success of their plan. If the collected intelligence value is of higher significance than the destruction of the target, the commander determines the best tactical course of action. He may decide either to destroy the target, to jam it, or to continue to exploit the collected information.

Signals reconnaissance targets must be detectable in some manner in the electromagnetic spectrum. The OPFOR must have some system(s) available that can perform this detection. HVTs that do not generate an electromagnetic signature of some sort must be detected by some

means other than signals reconnaissance.

HVTs sought by signals reconnaissance efforts are specific to the battle, the OPFOR plan and capabilities, and the enemyâ s plan and capabilities. However, there are some typical targets of signals reconnaissance efforts:

- Maneuver unit CPs.
- Forward air controllers (FACs).
- Logistic CPs.
- Fire support and tactical aviation networks.
- Target acquisition systems.
- Reconnaissance and sensors networks.
- Battlefield surveillance radars.

Signals reconnaissance information gained from electronic means is fused with information obtained from other sources. For example, the OPFOR can use trained reconnaissance teams or elements toâ

- Put eyes onâ targets and objectives.
- Collect required information.
- Provide early warning.
- Monitor lines of communication and movement corridors in a target area.

Such reconnaissance could possibly include a signals reconnaissance capability.

Note. Successful EW operations are not reliant on high-technology equipment and huge amounts of resourcing. While state actors tend to have higher EW capabilities, nonstate actors (or affiliated forces) can present a challenge to their opponents. For example, Hezbollah effectively used what the OPFOR would call signals reconnaissance and protection and security measures against Israeli forces in the summer of 2006. It successfully monitored Israeli cellular phone communications and was able to evade Israeli jamming devices by using fiber-optic lines instead of wireless signals. Commercial off-the shelf (COTS) equipment is commonly used to provide actors with the means to conduct EW. For example, the Viet Cong (Vietnamese National Liberation Front) used readily available COTS equipment to conduct extremely successful tactical signals reconnaissance operations against U.S. forces. Another nonstate actor, the Fuerzas Armadas Revolutionarias de Colombia (FARC), has utilized ground assets (man- portable radio equipment and other COTS technology) to conduct signals reconnaissance against Colombian and U.S. forces. As these examples prove, an effective EW threat can come from actors with high- and/or low-technology assets. Thus, a sophisticated military, in the Western sense, is not required for a successful signals reconnaissance exploitation and subsequent electronic attack.

Electronic Attack

Electronic attack (EA) supports the disaggregation of enemy forces. The primary form of EA is jammingâ interferencewith an enemy signals link in order to prevent its proper use. Jamming priorities are similar to those for signals reconnaissance. Maneuver units are jammed in order to disrupt coordination between and within units, especially when enemy units are achieving varying degrees of success. Reporting links between reconnaissance and engineer elements and the supported maneuver units are attacked, since they attempt to exploit OPFOR weaknesses the enemy may have found.

Targets

The OPFOR can and will conduct EA on virtually any system connected by signals transmitted in the electromagnetic spectrum. This includes communications and non-communications signals and data. As with signals reconnaissance, the choices of which links to disrupt varies with the scheme of maneuver, the impact of the disruption, the enemyâ sophistication, and the

availability of OPFOR EA assets. A limited but representative list of example targets includesâ

- C2 links between a key unit and its higher command.
- Link between a GPS satellite and a receiver.
- Link between a firing system and its fire direction center (FDC).
- Link between a missile and/or munition and its targeting system.
- Computer data links of all types.

Distributive Jamming

Instead of wideband barrage jamming using large semi-fixed jammers, the OPFOR often fields small distributive jammers. These may be either dispersed throughout the battle area or focused on one or more select targets. These jammers may be both fixed and mobile. Mobility may be by ground vehicle or unmanned aerial vehicle. They can be controlled though civilian cellular phone networks and/or controlled by local forces. Along with known military frequencies, the OPFOR can target civilian radios and/or cellular phonesâ

- Of a regional neighbor.
- Of nongovernmental organizations (NGOs).
- Of other civilians from outside the region).

Distributive jamming can causeâ

- Loss of GPS, communications, and non-communications data links (such as Blue Force and personal or unit communication).
- Degradation of situational awareness and common operational picture.
- Disruption of tempo.
- Reduction of intelligence feeds to and from CPs.
- Opportunities for ambush, with the resulting ambush videoed and used for perception management operations.
- Enemy units forced to use alternative, less secure communications.

Expendable Jammers

The OPFOR can take advantage of the time prior to an enemy attack to emplace expendable jammers (EXJAMs). These jammers can disrupt enemy communications nets. When used in conjunction with terrain (such as at natural choke points, mountain passes, or valleys), they can achieve significant results despite their short range and low power. The OPFOR can also use them to support a deception plan, without risking expensive vehicle-based systems. While limited in number, artillery-delivered EXJAMs may be employed. These jammers are especially useful in those areas where support is not available from more powerful vehicle-mounted jammers.

Proximity Fuze Jammers

Proximity fuzes used on some artillery projectiles rely on return of a radio signal reflected from the target to detonate the round within lethal range of the target. Proximity fuze jammers cause the round to explode at a safe distance. The OPFOR can deploy such jammers to protect high-value assets that are within indirect fire range from enemy artillery.

Deception

The OPFOR integrates deception into every tactical action. It does not plan deception measures and activities in an ad hoc manner. A deception plan is always a major portion of the overall INFOWAR plan. The extent and complexity of the deception depends on the amount of time available for planning and preparation. The OPFOR formulates its plan of action, overall INFOWAR plan, and deception plan concurrently.

The OPFOR attempts to deceive the enemy concerning the exact strength and composition of its forces, their deployment and orientation, and their intended manner of employment. When

successfully conducted, deception activities ensure that the OPFOR achieves tactical surprise, while enhancing force survivability. All deception measures and activities are continuously coordinated with deception plans and operations at higher levels. Affiliated forces may assist in executing deception activities.

The OPFOR employs all forms of deception, ranging from physical decoys and electronic devices to tactical activities and behaviors. The key to all types of deception activities is that they must be both realistic and fit the deception story. Due to the sophistication and variety of sensors available to the enemy, successfully deceiving him requires a multispectral effort. The OPFOR must provide false or misleading thermal, visual, acoustic, and electronic signatures.

While creating the picture of the battlefield the OPFOR wants the enemy to perceive, deception planners have two primary objectives. The first is to cause the enemy to commit his forces and act in a manner that favors the OPFORâ s plan. The second objective, and the focus of deception activities when time is limited, is to minimize friendly force signatures. This limits detection and destruction by enemy attack.

Integral to the planning of deception activities is the OPFORâ s identification of the deception target. This target is that individual, organization, or group that has the necessary decisionmaking authority to take action (or to neglect to do so) in line with the OPFORâ s deception objective. On the tactical battlefield, this target is typically the enemy commander, although the OPFOR recognizes the importance of focusing actions to affect specific staff elements.

Successful deception activities depend on the identification and exploitation of enemy information systems and networks, as well as other conduits for introducing deceptive information. Knowing how the conduits receive, process, analyze, and distribute information allows for the provision of specific signatures that meet the conduitsâ requirements. On the tactical battlefield, the enemy reconnaissance system is the primary information conduit and therefore receives the most attention from OPFOR deception planners. The international media and Internet sites may also be a target for deceptive information at the tactical level. The OPFOR can feed them false stories and video that portray tactical-level actions with the goal of influencing operational or even strategic decisions.

Deception Forces and Elements

The battle plan and/or INFOWAR plan may call for the creation of one or more deception forces or elements. This means that nonexistent or partially existing formations attempt to present the illusion of real or larger units. When the INFOWAR plan requires forces to take some action (such as a feint or demonstration), these forces are designated as deception forces or elements in close-hold executive summaries of the plan. Wide-distribution copies of the plan make reference to these forces or elements according to the functional designation given them in the deception story.

The deception force or element is typically given its own command structure. The purpose of this is both to replicate the organization(s) necessary to the deception story and to execute the multidiscipline deception required to replicate an actual or larger military organization. The headquarters of a unit that has lost all of its original subordinates to task organization is an excellent candidate for use as a deception force or element.

Deception Activities

Deception forces or elements may use a series of feints, demonstrations, ruses, or decoys. All activities must fit the overall deception story and provide a consistent, believable, and multidiscipline representation. Basic tactical camouflage, concealment, cover, and deception (C3D) techniques are used to support all types of deception.

The OPFOR conducts deception activities to confuse the enemy to the extent that he is unable to distinguish between legitimate and false targets, units, activities, and future intentions. Inserting false or misleading information at any point in the enemy decisionmaking process can lead to increased OPFOR survivability and the inability to respond appropriately to OPFOR tactical actions. Manipulation of the electromagnetic spectrum is often critical to successful deception activities, as the OPFOR responds to the challenge posed by advances in enemy C2 systems and sensors.

Some example deception activities may includeâ¯

- Executing feints and demonstrations to provide a false picture of where the main effort will be.
- Creating the false picture of a major offensive effort.
- Maximizing protection and security measures to conceal movement.
- Creating false high-value assets.

Feints

Feints are offensive in nature and require engagement with the enemy in order to show the appearance of an attack. The goal is to support the mission and ultimately mislead the enemy. Feints can be used to force the enemy toâ¯

- Employ his forces improperly. A feint may cause these forces to move away from the main attack toward the feint, or a feint may be used to fix the enemyâ s follow-on forces.
- Shift his supporting fires from the main effort.
- Reveal his defensive fires. A feint may cause premature firing, which reveals enemy locations.

Demonstrations

Demonstrations are a show of force on a portion of the battlefield where no decision is sought, for the purpose of deceiving the enemy. They are similar to feints, but contact with enemy is not required. Advantages of demonstrations includeâ¯

- Absence of contact with enemy.
- Possibility of using simulation devices in place of real items to deceive the enemyâ s reconnaissance capabilities.
- Use when a full force is not necessary because of lack of contact with the enemy.

Ruses

Ruses are tricks designed to deceive the enemy in order to obtain a tactical advantage. They are characterized by deliberately exposing false information to enemy collection means. Information attacks, perception management actions, and basic C3D measures all support this type of deception.

Decoys

Decoys represent physical imitations of OPFOR systems or deception positions to enemy RISTA assets in order to confuse the enemy. The goal is to divert enemy resources into reporting or engaging false targets. It is not necessary to have specially manufactured equipment for this type of visual deception. Decoys are used to attract an enemyâ s attention for a variety of tactical purposes. Their main use is to draw enemy fire away from high-value assets. Decoys are generally expendable, and they can beâ

- Elaborate or simple. Their design depends on several factors, such as the target to be decoyed, a unitâ s tactical situation, available resources, and the time available.
- Preconstructed or made from field-expedient materials. Except for selected types, preconstructed decoys are not widely available. A typical unit can construct effective, realistic decoys to replicate its key equipment and features through imaginative planning and a working knowledge of the electromagnetic signatures emitted by the unit.

The two most important factors regarding decoy employment are location and realism.

Logically placing decoys can greatly enhance their plausibility. Decoys are usually placed near enough to the real target to convince an enemy that he has found the target. However, a decoy must be far enough away to prevent collateral damage to the real target when the decoy draws enemy fire. Proper spacing between a decoy and a target depends on the size of the target, the expected enemy target acquisition sensors, and the type of munitions likely to be directed against the target.

Decoys must include target features that an enemy will recognize. The most effective decoys are those that closely resemble the real target in terms of electromagnetic signatures. Completely replicating the signatures of some targets, particularly large and complex targets, can be very difficult. Therefore, decoy construction should address the electromagnetic spectral region in which the real target is most vulnerable.

Smart Decoys. Smart decoys are designed to present a high-fidelity simulation of a real vehicle or other system. They may present heat, electromagnetic, electro-optical, audio, and/or visual signatures. They are distributed, controlled decoys. Computerized controls turn on decoy signatures to present a much more valid signature than previous-generation â rubberduckâ decoys. Smart decoys can be emplaced close to prohibited targets (such as churches, mosques, schools, or hospitals) and civilian populations. If the enemy engages these decoys, the OPFOR can exploit resulting civilian damage in follow-on perception management activities. Smart decoys causeâ

- Loss of situational awareness.
- Flood of fake targets, bogging down the enemyâ ts targeting process.
- Expenditure of limited munitions on non-targets.
- Negation of multispectral RISTA assets (such as night vision goggles, infrared scopes, and other electro-optical devices).
- Negation of critical targeting planning and allocation of assets.

Deception CPs. The INFOWAR plan may also call for employing deception CPs. These are complex, multi-sensor-affecting sites integrated into the overall deception plan. They can assist in achieving battlefield opportunity by forcing the enemy to expend his command and control warfare effort against meaningless positions.

False Deployment. The OPFOR attempts to deny the enemy the ability to accurately identify its force dispositions and intentions. Knowing it cannot totally hide its forces, it tries to blur the boundaries and compositions of forces, while providing indications of deception units and false targets.

Specific OPFOR actions taken to hide the exact composition and deployment of forces may includeâ

- Establishing deception assembly areas or defensive positions supported by decoy vehicles.
- Establishing disruption zones to conceal the actual battle line of friendly defensive positions.
- Concealing unit and personnel movement.
- Creating the perception of false units and their associated activity.
- Creating false high-value assets.

By providing the appearance of units in false locations, the OPFOR attempts to induce the enemy to attack into areas most advantageous to the OPFOR. When the deception is successful, the enemy attacks where the OPFOR can take maximum advantage of terrain. False thermal and acoustic signatures, decoy and actual vehicles, and corner reflectors, supported by false radio traffic, all contribute to the appearance of a force or element where in fact none exists.

Signature Reduction. The reduction of electromagnetic signatures of OPFOR units and personnel is critical to the success of any deception plan. Minimizing the thermal, radar, acoustic, and electronic signatures of people, vehicles, and supporting systems is critical to ensuring

deception of the enemy and enhancing survivability. The OPFOR extensively uses a variety of signature-reduction materials, procedures, and improvised methods that provide protection from sensors and target acquisition systems operating across the electromagnetic spectrum.

Electronic Deception

Electronic deception is used to manipulate, falsify, and distort signatures received by enemy sensors. It must be conducted in such a manner that realistic signatures are replicated. Electronic deception takes the forms of manipulative, simulative, imitative, and often non-communications deception. The OPFOR may use one or all of these types of electronic deception.

Manipulative Electronic Deception

Manipulative electronic deception (MED) seeks to counter enemy jamming, signals intelligence (SIGINT), and target acquisition efforts by altering the electromagnetic profile of friendly forces. Specialists modify the technical characteristics and profiles of emitters that could provide an accurate picture of OPFOR intentions. The objective is to have enemy analysts accept the profile or information as valid and therefore arrive at an erroneous conclusion concerning OPFOR activities and intentions.

MED uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, an OPFOR unit might transmit false fire support plans and requests for ammunition to indicate that the unit is going to attack when it is actually going to withdraw.

MED can cause the enemy to fragment his intelligence and EW efforts to the point that they lose effectiveness. It can cause the enemy to misdirect his assets and therefore cause fewer problems for OPFOR communications.

Simulative Electronic Deception

Simulative electronic deception (SED) seeks to mislead the enemy as to the actual composition, deployment, and capabilities of the friendly force. The OPFOR may use controlled breaches of security to add credence to its SED activities. There are a number of techniques the OPFOR uses:

- With unit simulation, the OPFOR establishes a network of radio and radar emitters to emulate those emitters and activities found in the specific type unit or activity. The OPFOR may reference the false unit designator in communications traffic and may use false unit call signs.
- With capability or system simulation, the OPFOR projects an electronic signature of new or differing equipment to mislead the enemy into believing that a new capability is in use on the battlefield. To add realism and improve the effectiveness of the deception, the OPFOR may make references to â new â equipment designators on related communications nets.
- To provide a false unit location, the OPFOR projects an electronic signature of a unit from a false location while suppressing the signature from the actual location. Radio operators may make references to false map locations near the false unit location, such as hill numbers, a road junction, or a river. This would be in accordance with a script as part of the deception plan.

Imitative Electronic Deception

Imitative electronic deception (IED) injects false or misleading information into enemy communications and radar networks. The communications imitator gains entry as a bona fide member of the enemy communications system and maintains that role until he passes the desired false information to the enemy.

In IED, the OPFOR imitates the enemyâ electromagnetic emissions in order to mislead the enemy. Examples include entering the enemy communication nets by using his call signs and

radio procedures, and then giving enemy commanders instructions to initiate actions. Targets for IED include any enemy receiver and can range from cryptographic systems to very simple, plain-language tactical nets. Among other things, IED can cause an enemy unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to the enemy to have come from his own side.

Non-Communications Deception

The OPFOR continues to develop and field dedicated tactical non-communications means of electronic deception. It can simulate troop movements by such means as use of civilian vehicles to portray to radar the movement of military vehicles, and marching refugees to portray movement of marching troops. Simple, inexpensive radar corner reflectors provide masking by approximating the radar cross sections of military targets such as bridges, tanks, aircraft, and even navigational reference points. Corner reflectors can be quite effective when used in conjunction with other EW systems, such as ground-based air defense jammers.

Physical Destruction

Another method for disrupting enemy control is physical destruction of the target. The OPFOR integrates all types of conventional and precision weapon systems to conduct the destructive fires, to includeâ

- Fixed- and rotary-wing aviation.
- Cannon artillery.
- Multiple rocket launchers.
- Surface-to-surface missiles.

In some cases, the destruction may be accomplished by ground attack. The OPFOR can also utilize other means of destruction, such as explosives delivered by special-purpose forces or affiliated irregular forces.

Physical destruction measures focus on destroying critical components of the enemy force. Enemy C2 nodes and target acquisition sensors are a major part of the OPFOR fire support plan during physical destruction actions. Priority targets typically includeâ

- Battalion, brigade, and division CPs.
- Area distribution system communications centers and nodes.
- Artillery FDCs.
- FACs.
- Weapon system-related target acquisition sensors.
- Jammers and SIGINT systems.

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

Special emphasis is given to destruction of RISTA capabilities prior to an attack on OPFOR defensive positions. Once the attack begins, the OPFOR heavily targets enemy C2 nodes responsible for the planning and conduct of the attack, along with supporting communications. Typically, destruction of C2 nodes prior to the attack may allow the enemy time to reconstitute his control. However, targeting them once forces are committed to the attack can cause a far greater disruptive effect.

The accuracy of modern precision weapons allows the OPFOR to strike at specific INFOWAR-related targets with deadly accuracy and timing. Due to the mobility and fleeting nature of many INFOWAR targets, precision weapons often deliver the munitions of choice against many high-

priority targets.

The OPFOR continues to research and develop directed energy weapons, to include radio frequency weapons and high-power lasers. While the OPFOR has fielded no dedicated weapon systems, it may employ low-power laser rangefinders and laser target designators in a sensor-blinding role.

Protection and Security Measures

Protection and security measures encompass a wide range of activities, incorporating the elements of deception and EW. Successfully conducted protection and security measures significantly enhance tactical survivability and preserve combat power. The OPFOR would attempt to exploit the large number, and apparently superior technology, of the enemyâ s sensors. For example, it employs software at the tactical level that allows it to analyze the enemyâ ssatellite intelligence collection capabilities and warn friendly forces of the risk of detection. The use of signature-reducing and -altering devices, along with diligent application of operations security measures, supports deception activities in addition to denying information.

At the tactical level, protection and security measures focus primarily onâ

- Counterreconnaissance.
- C3D.
- Information and operations security.

These and other protection and security measures may overlap into the realms of EW or deception.

Counterreconnaissance

Winning the counterreconnaissance battle is very important, since it can limit what information the enemy is able to collect and use in the planning and execution of his operations. Tactical commanders realize that enemy operations hinge on situational awareness. Therefore, counterreconnaissance efforts focus on destruction and deception of enemy sensors in order limit the ability of enemy forces to understand the OPFOR battle plan. A high priority for all defensive preparations is to deny the enemy the ability to maintain reconnaissance contact on the ground.

The OPFOR recognizes that, when conducting operations against a powerful opponent, it will often be impossible to destroy the ability of the enemyâ sstandoff RISTA means to observe its forces. However, the OPFOR also recognizes the reluctance of enemy military commanders to operate without human confirmation of intelligence, as well as the relative ease with which imagery and signals sensors may be deceived. OPFOR tactical commanders consider ground reconnaissance by enemy special operations forces as a significant threat in the enemy RISTA suite and focus significant effort to ensure its removal. While the OPFOR may execute missions to destroy standoff RISTA means, C3D is the method of choice for degrading the capability of such systems.

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 throughout the disruption, battle, and support zones. These range from the simplest and least expensive methods of hiding from observation to the most modern multispectral signature-reducing technology.

The OPFOR dedicates extensive effort to employing C3D to protect its defensive positions and high- value assets. All units are responsible for providing protective measures for themselves

with their own assets, with possible support from engineer units. The OPFOR employs a variety of signature-reducing or -altering materials and systems, to include infrared- and radar-absorbing camouflage nets and paints.

Information and Operations Security

Information and operations security can protect the physical and intellectual assets used to facilitate C2. Security must function continuously to be effective. It must conceal not only the commanderâ s intentions and current locations, configurations, and actions of tactical units but also the tactics, techniques, and procedures for employment and operation of information systems.

The OPFOR clearly understands the importance of information and operations security. Commanders understand their vulnerabilities to being attacked 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.

Perception Management

Perception management involves measures aimed at creating a perception of truth that best suits OPFOR objectives. It integrates a number of widely differing activities that use a combination of true, false, misleading, or manipulated information. Targeted audiences range from enemy forces, to the local populace, to world popular opinion. At the tactical level, the OPFOR seeks to undermine an enemyâ s ability to conduct combat operations through psychological warfare (PSYWAR) and other perception management activities aimed at deterring, inhibiting, and demoralizing the enemy and influencing civilian populations.

The various perception management activities include efforts conducted as part ofâ ¯

- PSYWAR.
- Direct action.
- Public affairs.
- Media manipulation and censorship.
- Statecraft.
- Public diplomacy.
- Regional or international recruitment and/or fundraising for affiliated irregular forces.

The last three components, while not conducted at the tactical level, can certainly have a great impact on how and where the OPFOR conducts tactical-level perception management activities. Perception management activities conducted at the tactical level must be consistent with, and contribute to, the Stateâ s operational and strategic goals.

Psychological Warfare

PSYWAR is a major contributor to perception management during combat. Targeting the military forces of the enemy, PSYWAR attempts to influence the attitudes, emotions, motivations, aggressiveness, tenacity, and reasoning of enemy personnel. Specialists plan PSYWAR activities at all levels of command.

In addition to the enemyâ s military forces, the specialists also concentrate on manipulating the local population and international media in favor of the OPFOR, turning opinion against the enemyâ s objectives. Planners focus special emphasis on highlighting enemy casualties and lack of success. They also highlight enemy mistakes, especially those that cause civilian casualties. The enemy nationâ s population is a major target of these activities, due to the criticality of public support for enemy military activities.

The OPFOR skillfully employs media and other neutral players, such as NGOs, to further influence

public and private perceptions. However, if the OPFOR perceives the presence of NGOs to be detrimental to its objectives, it can be extremely effective in hindering their efforts to provide humanitarian assistance to the populace, thus discrediting them.

Public Affairs

The OPFOR can conduct public affairs actions aimed at winning the favor and/or support of the local leadership and populaceâ either within the State or in territory it has invaded. This civil support from the OPFOR takes many forms, such as public information and community relations. It can involve providing money, schools, medical support or hospitals, religious facilities, security, other basic services, or just hope. The OPFOR accompanies these support activities with the message or impression that, if the OPFOR loses or leaves, the local population will lose these benefits.

Media Manipulation

Perception management targeting the media is aimed at influencing domestic and international public opinion. The purpose is to build public and international support for the OPFORs military actions and to dissuade an adversary from pursuing policies perceived to be adverse to the Stateâ interests. The OPFOR exploits the international mediaâ willingness to report information without independent and timely confirmation. While most aspects of media manipulation are applicable to levels well above the tactical, the trickle-down effect can have a major effect on the tactical fight.

The willingness of the local population to either support or to oppose the OPFOR effort can be critical to OPFOR success. If, for example, media reports convince the populace that the enemy is on a religious vendetta, the local population may decide to join the OPFOR in a fight to the death against the enemy. The OPFOR understands that perception management is not about right and wrong, it is about what people believe is right and wrong. For most people, their perception is their reality.

Note. The State employs media censorship to control its own populationâ access to information and perception of reality. Successful preparation of the population significantly enhances public support for the OPFORâ military actions. As part of this, the State prepares its forces and population for enemy INFOWAR.

Target Audiences

OPFOR perception management techniques seek to define events in the minds of decisionmakers and populations in terms of the OPFORâ choosing. Successful perception management consists of two key factors: speed and connection. Speed means reaching the target audience before enemy-provided information can alter the perception of events. Connection means having the right media to provide the story to the target audience in a way they will find credible and memorable. World opinion is a primary target of perception management, either to gain support for the OPFOR cause or to turn world opinion and support against the enemy. Reinforcement of its message (preferably by different sources) is also a powerful tool the OPFOR uses to convince the target audience of the OPFOR position.

Information Attack

Information attack (IA) focuses on the intentional disruption or distortion of information in a manner that supports accomplishment of the OPFOR mission. 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. The OPFOR

recognizes the increasing dependence of modern armies on tactical information systems. Therefore, the OPFOR attempts to preserve the advantages of such systems for its own use, while exploiting the enemyâ reliance on such systems.

IA is a critical element of INFOWAR, offering a powerful tool for the OPFOR. For example, an information attacker may target an information system for electronic sabotage 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 creating false information in a targeting or airspace control system.

Data manipulation is potentially one of the most dangerous techniques available to the OPFOR. Data manipulation involves covertly gaining access to an enemy information system and altering key data items without detection. The possibilities are endless with this technique. Some examples areâ

- Navigation. Altering position data for enemy units, soldiers, and systems, making them think they are in the right place when they are not.
- Blue Force Tracking. Altering position data of enemy units, soldiers, and systems to make other units, soldiers and systems believe them to be in one place where they are not or to lose track of them altogether. Alternatively, data manipulation can make OPFOR units appear as enemy or vice versa.
- Battlefield information systems. Enhancing OPFOR success by the ability to mitigate and/or influence enemy activities controlled via battlefield information systems.
- Survey and gun or mortar alignment. Causing enemy weapons to fire on the wrong target location.
- Targeting and sensors. Misdirecting sensors to have false reads, locate false targets, or identify the enemyâ own units as OPFOR targets.
- Weapon guidance. Sending weapons to the wrong location or wrong target.
- Timing. Changing internal clocks, thereby disrupting synchronization.
- Logistics tracking. Sending logistics packages to the wrong place or delaying their arrival. This can be done by altering bar codes on equipment or by hacking and altering logistics (delivery or request) data.
- Aviation operations. Changing altimeter readings, position location data, or identification, friend or foe codes.

The OPFOR attempts to inject disinformation through trusted networks. It tries to make the enemy distrust his RISTA and situational awareness assets by injecting incorrect information. Attacks could take the form of icon shifting (blue to red) or moving the iconâ location. Fire missions and unit control would require significant human interaction, thus slowing the enemyâ target engagement cycle time.

Likely targets for an IA are information residing in the critical tactical systems of the enemy. Such targets includeâ

- Telecommunications links and switches.
- Fire control.
- Logistics automation.
- RISTA downlinks.
- Situational awareness networks.
- C2 systems.

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, includingâ

- Unauthorized access (hacking) of information systems for intelligence-collection purposes.
- Insertion of malicious software (viruses, worms, logic bombs, or Trojan horses).

Such attacks concentrate on the denial of service and/or disruption or manipulation of the integrity of the information infrastructure. 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.

Distributed denial of service attacks use a network of slave computers to overwhelm target computers with packets of data and deny them outgoing access to networks. Such attacks could disrupt logistics, communications, intelligence, and other functions.

The OPFOR can employ various types of malicious software or â malwareâ on enemy computers to slow operations, extract data, or inject data. Poor operational procedures can enable this type of attack, with significant loss of capability and/or spillage of data to the OPFOR. These attacks also cause the enemy to waste data time and cycles in prevention and remediation. Malware could affect internal clocks (creating positional errors and communications difficulties) and slow the functional speed of computing. Any Internet-capable or networkable system is at potential risk.

OPFOR computer warfare activities may be conducted prior to or during a military action. For example, by damaging or destroying networks 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. It has 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.