Chapter 2
Threat

The enemy employs a variety of sensors to detect and identify US soldiers, equipment, and supporting installations. These sensors may be visual, near infrared (NIR), IR, ultraviolet (UV), acoustic, or multispectral/hyperspectral. They may be employed by dismounted soldiers or ground-, air-, or space-mounted platforms. Such platforms are often capable of supporting multiple sensors. Friendly troops rarely know the specific sensor systems or combination of systems that an enemy employs. When possible, friendly troops should protect against all known threat surveillance systems.

DOCTRINE

2-1. Many threat forces were trained and equipped by the former Soviet Union. Its long-standing battlefield doctrine of *maskirovka* is a living legacy in many former Soviet-client states. Maskirovka incorporates all elements of CCD and tactical battlefield deception into a cohesive and effective philosophy. During the Gulf War, Iraq used maskirovka to effectively maintain its capability of surface-to-surface missiles (Scuds) in the face of persistent coalition-force attacks. Enemy forces that are trained in maskirovka possess a strong fundamental knowledge of CCD principles and techniques. Friendly forces must be very careful to conduct CCD operations so that a well-trained enemy will not easily recognize them.

2-2. Typical threat doctrine states that each battalion will continuously maintain two observation posts when in close contact with its enemy. An additional observation post is established when the battalion is in the defense or is preparing for an offense.

2-3. Patrolling is used extensively, but particularly during offensive operations. Patrols are used to detect the location of enemy indirect- and direct-fire weapons, gaps in formations, obstacles, and bypasses.

2-4. Enemy forces use raids to capture prisoners, documents, weapons, and equipment. A recon-in-force (usually by a reinforced company or battalion) is the most likely tactic when other methods of tactical recon have failed. A recon-in-force is often a deceptive tactic designed to simulate an offensive and cause friendly forces to reveal defensive positions.

ORGANIZATION

2-5. A typical enemy force conducts recon activities at all echelons. A troop recon is usually conducted by specially trained units. The following types of enemy units might have specific intelligence-collection missions:

- **Troops.** An enemy uses ordinary combat troops to perform recon. One company per battalion trains to conduct recon operations behind enemy lines.
- **Motorized rifle and tank regiments.** Each regiment has a recon company and a chemical recon platoon.
- **Maneuver divisions.** Divisions have a recon battalion, an engineer recon platoon, a chemical recon platoon, and a target-acquisition battery.

DATA COLLECTION

2-6. An enemy collects information about United States (US) forces for two basic reasons—target acquisition and intelligence production. Enemy weapons systems often have sensors that locate and identify targets at long ranges in precise detail. Soldiers and units should take actions to hinder the enemy's target-acquisition process. These actions include all practical CCD operations expected to reduce the identification of soldiers, units, and facilities.

2-7. An enemy uses sensor systems to locate and identify large Army formations and headquarters (HQ) and to predict their future activities. Enemy detection of rear-area activities, such as logistics centers and communications nodes, may also reveal friendly intentions.

2-8. An enemy uses tactical recon to provide additional information on US forces' dispositions and the terrain in which they are going to operate. The enemy's tactical recon also attempts to identify targets for later attack by long-range artillery, rockets, aircraft, and ground forces.

SENSOR SYSTEMS

2-9. An enemy uses many different types of electronic surveillance equipment. Sensor systems are classified according to the part of the EM spectrum in which they operate. *Figure 2-1* shows the EM spectrum and some typical enemy sensors operating within specific regions of the spectrum. An enemy uses detection sensors that operate in the active or passive mode:

- **Active.** Active sensors emit energy that reflects from targets and is recaptured by the emitting or other nearby sensor, indicating the presence of a target. Examples of active sensors are searchlights and radar.
- **Passive.** Passive sensors do not emit energy; they collect energy, which may indicate the presence of a target. Examples of passive sensors are the human eye, night-vision devices (NVDs), IR imaging devices, acoustic sensors, and photographic devices.

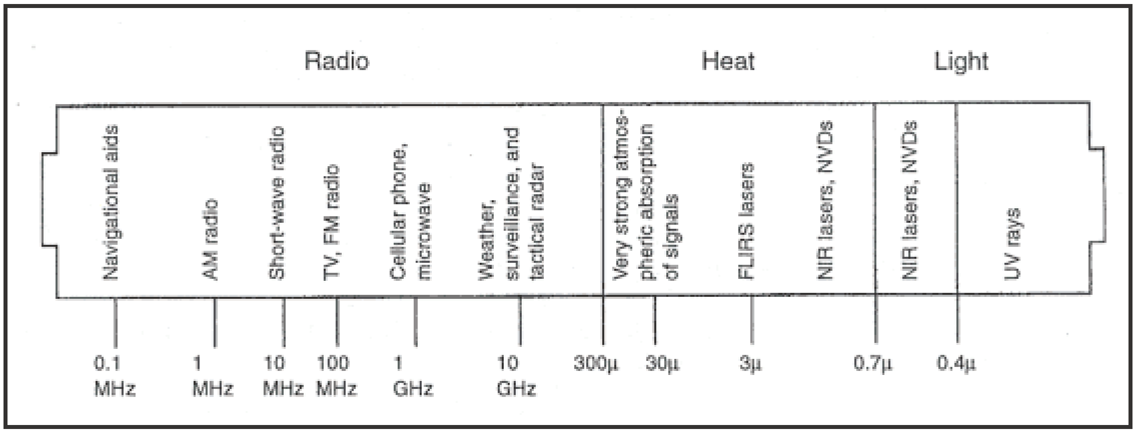


Figure 2-1. EM spectrum

VISUAL

2-10. Visual sensors work in the parts of the EM spectrum that are visible to the human eye. Enemy soldiers' eyes are the principle sensors on a battlefield. They may be aided by binoculars, telescopic sights, and image intensifiers. Civilian populations, enemy agents, recon teams, and patrols are visual-sensor systems from the enemy's intelligence viewpoint. Three types of enemy visual sensors are—

- **Image intensifiers.** Image intensifiers are passive night-observation devices. They amplify the low-level light that is present on even the darkest nights. These devices are used for surveillance and as weapon sights on small arms and vehicles. Airborne platforms are also capable of supporting image intensifiers.
- **Low-light television (LLTV).** LLTV combines image intensification with television technology, and it is usually mounted on airborne platforms.
- **Aerial recon, remote sensing, and imagery.** Aerial photography, satellite imagery, and video imagery allow image analysts to record and study visual information. These analysts then produce target nomination lists that are, in effect, priority lists of targets in a given target scene. Since analysts often have to make subjective determinations of the identity and/or importance of a given target, the ranking of targets provides the defender with an opportunity to use CCD to impact an enemy's target-prioritization process. Video systems allow transmission of visual images to the ground while the manned aircraft, satellite, or unmanned aerial vehicle (UAV) is still in flight.

NEAR INFRARED

2-11. NIR sensors operate at a wavelength immediately above the visible light wavelength of the EM spectrum (*Figure 2-1*). NIR energy reflects well from live vegetation but reflects better from dead vegetation and most man-made materials. NIR sensors, such as sights and periscopes, allow the human eye to detect targets based on differences in their reflection of NIR energy. NIR sensors are partially blocked by fog, mist, and smoke operations, although not as completely as visual sensors. An enemy's combat vehicles use active NIR sensors that employ searchlights, scopes, and sights; but these sensors are rapidly being replaced with image intensifiers and thermal gun sights.

INFRARED

2-12. IR sensors detect the contrasts in heat energy that targets radiate on the battlefield and display the contrasts as different colors or shades. Because longer wavelength IR radiation is more susceptible to atmospheric absorption than NIR radiation, IR sensors are less affected by typical concentrations of fog or conventional smoke.

2-13. Differences in thermal mass and surface properties (reflectivity) of man-made and natural materials result in target-to-background contrasts. These contrast levels change dramatically over a daily cycle. For example, operating vehicles and generators, heated buildings and tents, and soldiers are usually hotter than their background. Also, equipment exposed to direct sunlight appears hotter than most natural backgrounds. At night, however, equipment might appear cooler than its background if it is treated with special emissivity coatings. In other words, military equipment, particularly metallic equipment, generally heats up and cools off more quickly than its background.

2-14. Sophisticated, passive IR sensors (such as the Forward-Looking Infrared System [FLIRS]) can be mounted on aircraft. FLIRS sensors provide aircrews and enemy ground forces with real-time IR imagery that is displayed on video monitors.

2-15. Recon aircraft often employ special IR films to record temperature differences. Due to film processing, however, these systems are subject to time delays in obtaining the data. Newer versions of this sensor produce non-film-based images.

ULTRAVIOLET

2-16. The UV area is the part of the EM spectrum immediately below visible light. UV sensors are more important in snow-covered areas, because snow reflects UV energy well and most white paints and man-made objects do not reflect UV energy very well. Photographic intelligence systems with simple UV filters highlight military targets as dark areas against snow-covered backgrounds. These backgrounds require specially designed camouflage that provides a high UV reflectance.

RADAR

2-17. Radar uses high-frequency radio waves to penetrate atmospheric impediments such as fog, mist, and smoke. Radar works by transmitting a very strong burst of radio waves and then receiving and processing the reflected waves. In general, metal objects reflect radar waves well, while radar waves are either weakly reflected by or pass through most other objects. The shape and size of a metal object determine the strength of the reflected signal. A large, metal object generally reflects more signal than a small object. Therefore, large, metal objects can be detected from greater distances. The method by which the received radio wave is processed determines the type of radar. Radar systems commonly used against ground forces on the battlefield include—

- **Moving-target indicators (MTIs).** When an EM wave hits a moving target, the wave is reflected and changes frequency. The faster the target moves, the larger the changes in frequency. The simplest and most common battlefield radar detects this frequency change. Threat forces use MTIs for target acquisition. More sophisticated developmental radar systems, such as the Joint Surveillance Target Attack Radar System (JSTARS), use airborne surveillance platforms that downlink captured data to ground-station modules in near real time. Ground-based operators are then able to manipulate the data and gain heightened situational information, which is forwarded to command-and-control (C^2) nodes to enhance tactical decision-making.
- **Imaging radar.** An imaging radar's receiver and processor are so sensitive that an image of the detected target is displayed on a scope. Imaging radar, such as side-looking airborne radar (SLAR), is generally used on airborne or space-borne platforms. Imaging radar typically does not provide the same resolution as the FLIRS and is less likely to be used for terminal target acquisition.
- **Countermortar (CM) and counterbattery (CB) radar.** CM and CB radar usually transmit two beams of energy that sweep above the horizon. An artillery or mortar round or a rocket passing through the beams reflects two signals that are received and plotted to determine the origin of the round.

ACOUSTIC

2-18. The three predominant types of acoustical detection systems are—

- **Human ear.** Every soldier, whether engaged in normal operations or at a listening post, is an acoustic sensor. However, visual confirmation is usually preferred.
- **Flash-sound ranging.** Flash-sound ranging is used against artillery. Light travels faster than sound, so enemy sound-ranging teams can determine the distance to a gun tube by accurately measuring the time between seeing a muzzle flash and hearing the sound. If the sound is detected by two or more teams, analysts plot the ranges using automated data-processing computers. The target is located where the plots intersect.
- **Ground-based microphone array.** Ground-based microphone-array systems allow listeners to record acoustic signatures and accurately triangulate their positions.

RADIO

2-19. Threat forces make a great effort to search for, detect, and locate the sources of US radio communications. They use various direction-finding techniques to locate opposing emitters. Once an emitter is detected, an enemy can take a number of actions, ranging from simply intercepting the transmissions to jamming or targeting the emitter for destruction. (See FM 34-1 for more information on radio sensors.)

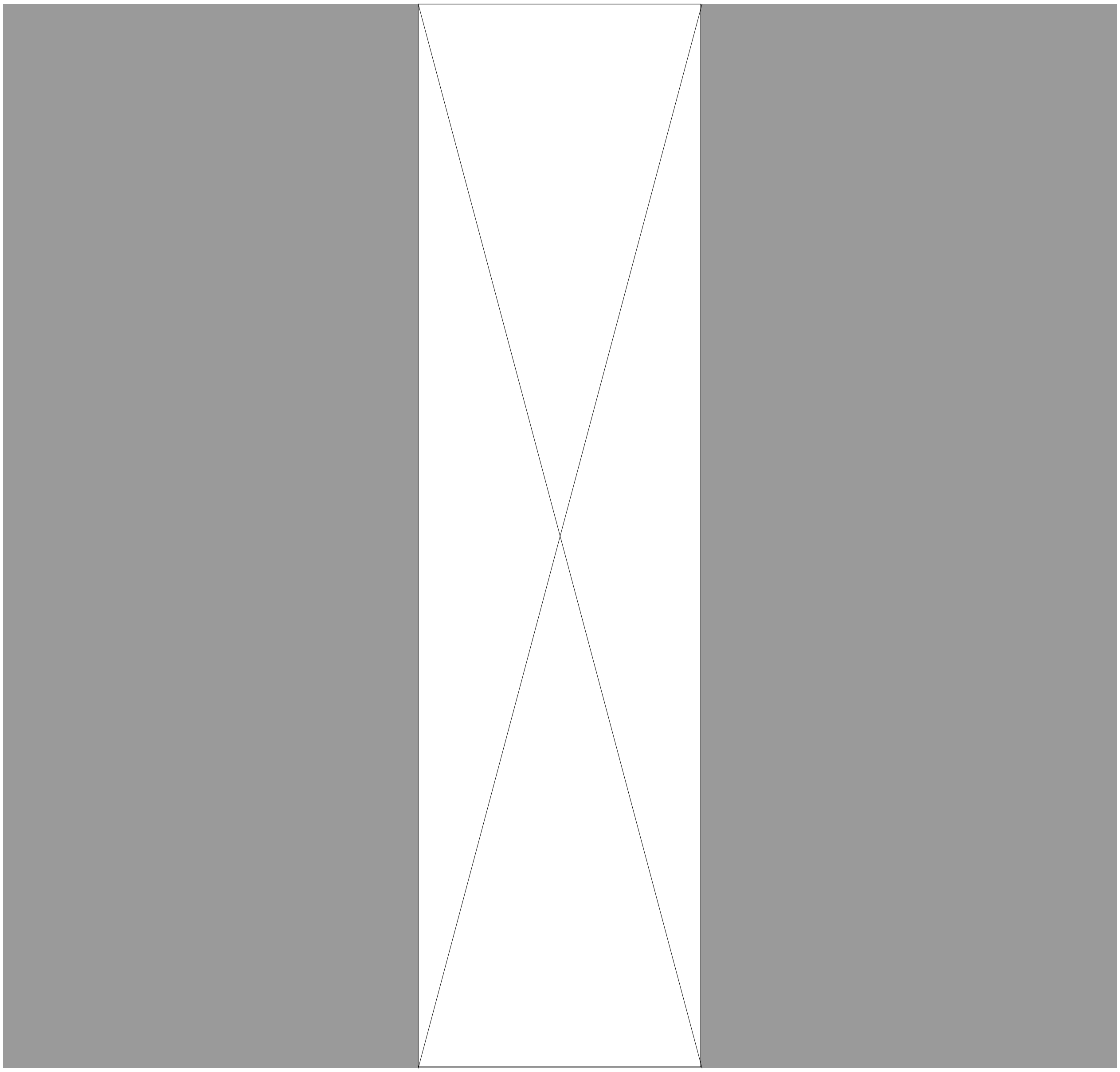
MULTISPECTRAL AND HYPERSPECTRAL

2-20. Recent advancements in sensor acquisition and information-processing technologies have fostered the advent of multispectral and hyperspectral sensors:

- **Multispectral.** Multispectral sensors typically scan a few broad-band channels within the EM spectrum. An example of a multispectral sensor might be one which coincidentally scans the visual and thermal IR portions of the EM spectrum. Such sensors allow an enemy to assess a cross section of EM wavelengths and acquire a target in one wavelength even though it might be effectively concealed in another.
- **Hyperspectral.** Hyperspectral sensors collect data across a continuous portion of the EM spectrum. These sensors scan many channels across a relatively narrow bandwidth and provide detailed information about target spatial and spectral patterns. Absorption and emission bands of given substances often occur within very narrow bandwidths. They allow high-resolution, hyperspectral sensors to distinguish the properties of the substances to a finer degree than an ordinary broadband sensor.

CCD VERSUS THREAT SENSORS

2-21. Target acquisition can be accomplished by a variety of sensors that operate throughout the EM spectrum. This poses a challenge in CCD planning and employment—determining which enemy sensor(s) that CCD operations should be designed to defeat. Unfortunately, no single answer is correct for all situations. Unit commanders without specific guidance from higher echelons assess their tactical situation and plan CCD operations accordingly. If intelligence data indicate that an enemy will use visual sensors for recon and target acquisition, then visual countermeasures must be employed. For IR or radar sensors, countermeasures that are effective in those spectra must be employed. If a multispectral or hyperspectral threat is anticipated, CCD operations are conducted to protect a unit in its most vulnerable EM bandwidths. Very few available camouflage materials or techniques provide complete broadband protection.



INTELLIGENCE

Further Reading

- Close Range - Tactical Unmanned Aerial Vehicle (CR-TUAV)

- CR-TUAV Specifications
- CR-TUAV Pictures
- CR-TUAV References

Tactical Unmanned Aerial Vehicle (TUAV)
Close Range - Tactical Unmanned Aerial Vehicle (CR-TUAV)

Evidence of the military utility of a land-based UAV was provided by the Outrider advanced concept technology demonstration (ACTD); nevertheless, a fully joint program could not be accomplished. Consequently, joint requirements were modified to permit use of more than one type of air vehicle. The Army and Navy initiated programs for land-based and sea-based UAV systems, respectively. The Navy seeks to develop a vertical takeoff and landing UAV for use on ships with small landing areas and in urban areas ashore. To ensure joint interoperability, both the Army and Navy UAVs will incorporate the Tactical Control System (TCS), which is designed to permit flexible control of all tactical unmanned air vehicles. TCS also will be used to control Predator endurance UAVs operated by the Air Force. The TCS program itself, originally scheduled to enter low-rate production in FY 1999, was restructured to accommodate changes in tactical UAV fielding schedules.

The termination of the Hunter acquisition created a gap in UAV coverage between the TUAV and Predator. In March 1998 a decision was made to transfer PM JTUAV to the Army. PEO-IEW&S was designated the centralized manager for the development, acquisition, testing, fielding, support and product improvement for the sensor payloads for the TUAV program. PEO-IEW&S was directed to define an end-to-end sensor/payload architecture concept for the TUAV. This architecture should consider the entire system level capabilities/limitations of the suite of payloads and also the processing, data link, and ground station capabilities necessary to define an effective TUAV system. A November 1998 JROC e endorsed the UAV Special Study Group (SSG) recommendation to allow the Services to pursue separate air vehicle solutions to meet their requirements

In August 1999 the Army selected four contractors to move forward to the Phase II portion of the Tactical Unmanned Aerial Vehicles (TUAV) source selection. Based on the results of the Phase I evolution the following contractors were in the competitive range and moved forward to the Phase II portion of the source selection. The four companies are: General Atomics-Aeronautical Systems Inc., TRW Systems and Information Technology Group, Alliant TechSystems, and AAI Corporation. The Phase II portion of the source selection included a Systems Capability Demonstration (SCD) at Ft. Huachuca, Arizona along with continued evaluation of the contractor's overall proposal. The SCD was scheduled for early October though November. The Army was scheduled to make a final decision by the end of 1999. AAI Corporations was the winner of the Tactical Unmanned Aerial Vehicle competition.

The Close Range - Tactical Unmanned Aerial Vehicle (CR-TUAV) is a ground maneuver brigade commander's UAV. It allows him to "see and understand" his battlespace and gain dominant situational awareness on the Army XXI battlefield. The CR-TUAV is the critical component of the Army XXI Brigade's collection package. It gives maneuver commanders the ability to look into the battlespace where ground recon assets can not penetrate or cover in a timely manner. It can also observe heavily protected areas where commanders are hesitant to commit manned aerial platforms. Lastly, it gives commanders a dedicated, rapidly-taskable asset with the capability to look wide as well as deep into their battlespace. It allows them to "see critical elements of the battlespace" and support the increased demand for immediate situational awareness on the Army XXI battlefield. The CR-TUAV is a critical tool to obtain the hard to get information needed to satisfy the commander's Priority Intelligence Requirements (PIR) and Commanders Critical Information Requirements (CCIR). It's a command and control enabler for tactical decision making.

A CR-TUAV system consists of four basic components: the Ground Control Stations (GCS) and related equipment; Air Vehicles (AV); Modular Mission Payloads (MMP); and communications.

The CR-TUAV system will have an endurance of four hours on station at 50 kms (3-4 hrs at 200km objective).

The CR-TUAV baseline is capable of 12 hours of continuous operations within a 24-hour period. The system has the capability of surge operations for 18 hours within a 24-hour period for no more than three consecutive days, with the following day being limited to eight hours of operations. Although the system has the capability to surge for 18 hours of 24 hours for 72 hours, the CR-TUAV baseline and its' parent brigade may be reconstituted after 36 hours. The objective system will be capable of 18 hours of continuous operations within a 24-hour period with a surge capability of 24 hours of 24 hours for a period of 3 days.

It can operate during less than ideal weather conditions (operates in environments similar to a small light aircraft) with a range of 50 kms from the launch and recovery site, flying at altitudes of 14,000 feet Mean Sea Level (MSL) or greater. Nominal operating altitudes/survivable altitudes are from 8,000 to 10,000 feet Above Ground Level (AGL) for day operations and between 6,000 to 8,000 feet AGL for night operations.

The system will have a minimum of two GCSs, two Ground Data Terminals (GDTs), one Portable Ground Control Station (PGCS) and one Portable Ground Data Terminal (PGDT) with line of sight (LOS) command and control links to, and receipt for telemetry and imagery from, the Air Vehicle (AV). Additionally, it will have four Remote Video Terminals (RVT) to provide payload information in the area of operations. The system's four RVTs that receive NRT video/telemetry from the AV can be used by: the brigade in the Tactical Operations Center (TOC) (if a GCS is not collocated), the brigade's subordinate maneuver battalions, or by direct support artillery or supporting aviation assets. RVT's will be allocated by the commander, based on METT-T, to support his scheme of maneuver.

The system will have sufficient AVs to support a wartime surge OPTEMPO, as well as a means of launch and recovery, and the necessary transportation and ground support equipment for the operations and maintenance of the system. The system is designed to be easy to launch, operate, recover, and maintain with a minimum of training, logistics, and personnel. It must present a small profile in order to reduce its signature) rapidly tear down, deploy and set up; and minimize any impact on brigade CSS resources. A crew of approximately 14 will operate and maintain a full baseline (AVs and two GCSs) at the OPTEMPO indicated below augmented with the divisional Mobile Maintenance Facility (MMF) for sustainment beyond the initial 72 hours of operations.

The system will be capable of near real time (NRT) transmission of Electro Optic/Infrared (EO/IR) imagery. Initially, the system will have a basic BO/IR mission payload, but will have a capability for growth to accommodate additional MMPs.

The CR-TUAV provides unclassified products via an unsecured datalink. The GCS gives ready interface to the existing Command, Control, Communications, Computers, and Intelligence (C4I) architecture, to include CGS, AFATDS, ASAS, FAADS, and A2C2. Intelligence reports from the GCSs include voice, electronic dissemination and/or video via the various communication systems in the GCS. Communications for the system are integrated into the air vehicles and ground control components and allow for transmission and receipt of command and control data, telemetry and imagery. Additional communications and intelligence dissemination are provided via the standard DoD tactical (VHF and UHF) radios, Mobile Subscriber Equipment (MSE), and the Tactical Local Area Network (TACLAN).

The complete CR-TUAV system will fit in no more than two High Mobility Multipurpose Wheeled Vehicles (HMMWVs) with shelters, two Cargo/Troop carrying HMMWVs, and two trailers with enough room for all personnel, crew members' combat equipment (rifles, helmets, camouflage netting, individual protective equipment, etc.) and enough Class I (subsistence) and Class III (Petroleum, Oils, and Lubricants) and Class IX (repair parts) supplies for initial operations (threshold)/seven-day period (objective). A threshold requirement is for a system configurable to deliver 72 hours of operational capability at a minimum of 12 flight hours on station in a 24 hour period deployable in a single C-130 sortie (using the HMMWV as the prime mover and including transportation for the entire "reduced" crew). Sustainment beyond the initial 72 hours is supported with a divisional mobile maintenance facility (MMF) consisting of a HMMWV and trailer.

The complete baseline CR-TUAV system with personnel and equipment, must be transportable in no more than two C-130 sorties. The addition of a mobile maintenance facility (HMMWV with shelter and trailer) will require an additional C-130.

The CR-TUAV equipment will be supported in accordance with the IEW Sustainment Streamlining (IEWSS) System, to include Contractor Logistics Support (CLS). The CR-TUAV maintenance concept may be Life Cycle Contractor Logistics Support. The system will be maintained IAW Aviation Unit Maintenance (AVUM) "on system repair" and Aviation Intermediate Maintenance (AVIM) "off system repair" Concept. Routine maintenance will be provided by system operators and the assigned maintenance personnel augmented (as required) by the divisional MMF. Higher level maintenance will be accomplished at the Forward Repair Activity (FRA) and/or the Electronic Service Support Center (ESSC) within theater to allow for quick turn around of critical system components.

The CR-TUAV system software will be maintained through standard Army life cycle software support concepts, to include CLS. The CR-TUAV system software will be updated, as required, to ensure compatibility with Military Intelligence, Aviation, and targeting systems. CR-TUAV system software will retain compatibility with older fielded systems and provide improved performance through Pre-planned Product Improvements (P3I).

The CR-TUAV system will provide flexible, responsive RSTA, Battle Damage Assessment (BDA), and battle management support to ground maneuver commanders at brigades, armored cavalry regiments (ACR) and light divisions. The CR-TUAV is dynamically retaskable in flight to ensure it is responsive to the commander's immediate needs/changing CCIR. To optimize its capabilities, CR-TUAV is fully integrated with and cued by sound IPB and other collection systems such as JSTARS, Guardrail Common Sensor (GRCS), Artillery Counter Mortar/Battery Radars and FAADC2, in a synchronized effort to support the Warfighter. As demonstrated during the Force XXI AWEs, the information is fed directly to the brigade commander (as well as the S3 and FSCOORD); but in the meantime, the information is fused to answer CCIRs. Regardless of the UAV's role, the operations officer must ensure the UAV is synchronized with all of the other assets within the battlespace.

The maneuver brigade is the premier combined arms formation for dominant maneuver on the Army XXI battlefield. The Army XXI brigade will operate on a non-linear battlefield moving at high speeds and controlling a greatly enlarged battlespace. Armed with superior situational awareness and continuous real-time Intelligence Preparation of the Battlefield (IPB), the brigade maneuvers with speed and precision to gain positional advantage on the enemy. When in position, the brigade executes decisive operations by massing the effects of direct and indirect fires at a tempo the enemy cannot match to seize and retain terrain and defeat or destroy enemy forces.

This is a ground maneuver brigade commander's tactical UAV. The UAV priority is to support the maneuvering of the brigade and battalions, including fire support of maneuver. The brigade commander's UAV must be simple (threshold capability-no bells and whistles), inexpensive, easy to maintain; profiled to meet the brigade commander's needs. It needs to keep pace on the Army XXI battlefield. Launch and recovery must be from an area easily accessible to a brigade commander. Rapid set up and tear down times will ensure it keeps pace with the brigade's movement. To facilitate rapid movement, the control of the UAV may be passed to other control stations or launch/recovery stations to allow continuous flight operations to meet the commander's requirements. Due to the signature associated with the launch and recovery (L/R) of the UAV, the L/R area will normally not be collocated with the brigade TOC. However, the mission planning, tasking, and dissemination will occur through the TOC via a collocated ground control station (GCS) or, at a minimum a remote video terminal (RVT) with compatible communications for tasking and dissemination. Additionally, the brigade commander can locate up to four remote video terminals (RVT) throughout the brigade. As an example, he may choose to keep one with him, locate one each with a forward battalion, scouts, and the direct support artillery battalion. Additionally, future operations demand "information on the move". As such, the UAV is a key brigade collection asset that supports the near real time visualization of the battlespace and is focused on the brigade's decisive operations.

The brigade commander requires sufficient coverage to fight on his and the battalion commanders' piece of ground. Specifically, the UAV is used to cover the dead space in front of the ground reconnaissance -- it extends the ground reconnaissance capability. It complements the Brigade Recon Troop's (BRT) ability to collect ground-level recon targets with a wider-area overhead look. As such, it helps eliminate the unknown and allows the commander to anticipate and respond - to pre-empt. In terms of IPB, the UAV helps the commander during the planning, preparation, and execution phases.

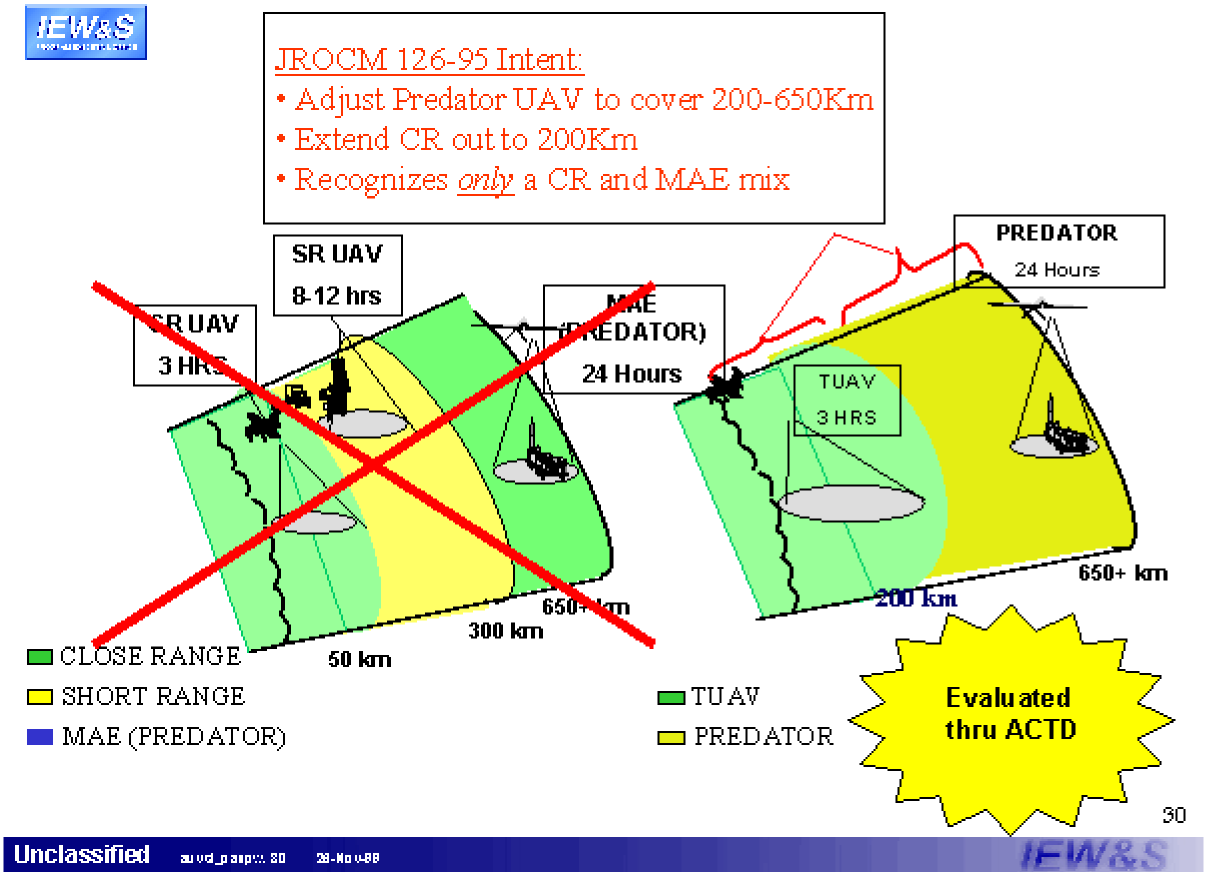
During the planning phase the commander needs to understand the ground, and answer the following questions: Where can I move? What are the avenues? Where are the obstacles? The UAV allows the commander to see and assess environmental benefits and limitations and answer those questions. In turn, those factors will support the development of friendly considerations, and formulation of enemy COAs for the planning staff. The UAV allows the commander to quickly assess critical components of his battlespace, such as trafficability, suitability for logistical and fire support assets, and activities of civilians on the battlefield during the planning process. Without this asset, the Commander will have to commit slower moving, precious ground maneuver assets to answer these planning questions.

During preparation, the commander validates his templates by BOS - he recons, in accordance with the plan, verifies the templates, and determines where the enemy is and is not. Additionally, the commander can redirect/frag his air recon (UAV) to a different mission and area. He cannot always do this with ground recon - once in, if they are fixed and attempt to move, they may die. Additionally, the commander needs to determine where he can take risk; where he can economize on forces. Instead of using troops on the flanks, the UAV can assist by providing surveillance in those areas. The UAV greatly enhances the effectiveness of the commander's counter-recon effort during the preparation phase. The UAV's mobility and range allow him to economize limited ground recon assets for the execution phase, without sacrificing his ability to detect indications of unexpected enemy spoiling actions such as Raids, Reconnaissance in Force, Fire Support Raids, etc.

During execution, the UAV helps determine maneuver options/friendly courses of action. As an example, it helps answer the question, "Is that truly an assailable (or unassailable) flank?" Another example: As the brigade penetrates the enemy defense, the commander may want the UAV over the enemy reserves, to determine when and where they are moving. The brigade commander may use a UAV capability to simultaneously look deep into his battlespace while his ground recon assets and maneuver units observe closer NAIs. With this confidence that he can receive critical information during the fight-" just-in-time intelligence"-the commander can take prudent risk without fear that he will outrun his collection assets.

The brigade commander's UAV needs to be dedicated for the close battle. It needs to be responsive to the current situation. The commander needs the information when it happens - not maybe; not later; not reprioritized by a higher command. The brigade commander's UAV needs to be focused for decisive operations in the brigade battlespace.

In summary, the CR-TUAV is the brigade commander's most versatile confirming sensor -- his "dominant eye" -- and responds directly to his requirements. To optimize its capabilities and responsiveness to the commander, it is linked to/cued by sound IPB and wide area sensors, such as the direct feed to the JSTARS CGS when collocated with the GCS, and as an objective, direct live feed from the UAV to the CGS. Additionally, it must be interoperable with C4ISR systems and linked into the Army's Battle Command System, in particular ASAS, AFATDS, and FAADS for distribution via intelligence channels, targeting, and to meet air defense identification requirements. Due to the complexities of airspace management (ASM), even at the brigade, it needs to feed into the A2C2 system.



JROCM 126-95 Intent:

- Adjust Predator UAV to cover 200-650Km
- Extend CR out to 200Km
- Recognizes *only* a CR and MAE mix

🟩 CLOSE RANGE
🟨 SHORT RANGE
🟦 MAE (PREDATOR)

🟩 TUAV
🟨 PREDATOR

■

Chapter 13
Electronic Combat

CONTENTS

The OPFOR is keenly aware of the dependence of modern military forces on communications that support command and control (C^2) and intelligence. Effective communications contribute to sound C^2; the loss of communications is the loss of C^2. The loss of C^2 in combat ultimately ends in defeat. The OPFOR therefore seeks to control the electromagnetic spectrum and deny its use to its enemy during combat actions, while retaining its own capabilities.

To support this the OPFOR has actively developed systems and techniques to degrade the C^2 assets of enemy forces. It has also taken measures to provide secure, dependable communications, information collection, and information processing for its own forces. The OPFOR has combined these capabilities with detailed, integrated planning to form the integrated doctrine of electronic combat (EC).

CONCEPT

EC consists of the use of all means of manipulation of electronic emissions throughout the electromagnetic spectrum. These means constitute the five components of EC: signals reconnaissance, electronic jamming, electronic protection measures (EPM), destruction, and electronic counterreconnaissance. (See the Components section in this chapter for further detail.) The purpose of EC is to--

- Disorganize enemy C^2.
- Suppress, capture, or destroy enemy C^2 systems.
- Detect enemy electronic systems.
- Degrade enemy intelligence and equipment.
- Protect OPFOR electronic assets.

EC is the primary contributor to the conduct of information warfare (IW) during combat operations, supporting to various degrees all six elements of IW.

Integration and Planning

Integration and planning are critical to the overall success of EC. The OPFOR planning process stresses close coordination among the reconnaissance, EC, and combat planners. This is to ensure the supported combat units receive massed jamming and other resources at the critical times and places. It also ensures that a more complete interruption of enemy electronic control occurs through the combination of jamming with physical destruction.

The OPFOR accepts that it is not possible to completely deprive enemy forces of their means of control for extended periods of time. It also recognizes the value in exploiting enemy communications for their intelligence value until a time when their disruption can most influence the course of action. If destruction is not feasible at that critical time, the net is jammed. Even a few minutes of disruption, if properly timed, are immensely valuable.

Therefore, OPFOR EC planners have established models to estimate critical times in the enemy C^2 process. These critical times are the total time needed to complete the following C^2 steps:

- Collection and reporting of data.
- Evaluation and decision.
- Issuance of orders and preparation.
- Completion of action.

Target Priorities

The OPFOR assigns enemy C^2, communications, computer, and intelligence nets a priority based on the expected impact on the battle at the time the OPFOR targets them. It selects targets with the intention of disrupting them either by physical destruction or by jamming. Although EC target priorities depend on the command level and can change as the combat situation develops, they generally are as follows:

- Precision weapons systems and NBC delivery means.
- C^2 systems.
- Conventional artillery, tactical aviation, and air defense systems.
- Intelligence collection systems (including radar stations).
- Engaged maneuver units.
- Reserves.
- Logistics centers.
- Point targets that jeopardize advancing forces.

ASSETS

The OPFOR has developed state-of-the-art EC systems specifically for military use. However, it can also take advantage of a wide variety of extremely capable off-the-shelf systems commercially available at relatively low cost. Together, these systems are capable of providing the level of electronic intercept, direction-finding (DF), or jamming sophistication required on the modern battlefield.

The OPFOR also has modernized those systems that can disrupt enemy communications and electronics through deception. Where practical, the OPFOR mounts EC systems it uses at the tactical and lower operational level on tracked vehicles to match the mobility of the maneuver units they support. It integrates this equipment into signals reconnaissance and jamming units that support combined arms combat.[1]

Ground Forces

The EC assets of the OPFOR's ground forces are found primarily within a number of signals reconnaissance and jamming units. While some of these EC assets exist at the tactical level, the following paragraphs focus on the assets available at the operational level.

Army Group

An army group can have one or two signals reconnaissance brigades, and may have a jamming regiment or battalion. A signals reconnaissance brigade consists of a radio intercept battalion, a radio DF battalion, and a radar intercept and DF battalion. In lieu of a second signals reconnaissance brigade, an army group may have a signals reconnaissance regiment or separate battalion of the types found at army level. Assets from these units typically deploy where they can best support the operations of a subordinate army or corps conducting the main effort in the offense or defense, as well as supporting army group-level taskings.

The jamming regiment has three battalions of like composition. Each battalion has a mix of VHF and HF jammers, along with the intercept and DF assets that provide targeting support. The battalion also includes fuze jammers that deploy to protect high-value assets from artillery proximity-fuzed munitions. Some army groups might have only a single jamming battalion instead of an entire regiment.

An army group typically includes an unmanned aerial vehicle (UAV) regiment with three UAV squadrons. The multimission UAVs are capable of carrying signals reconnaissance or jamming payloads, as well as other sensors that provide targeting for artillery, surface-to-surface missiles (SSMs), or army group aviation.

The army group may allocate all or part of the three UAV squadrons to support operations of an army or corps in the army group's main effort. The remaining UAV assets support army group-level targeting.

Compared to other airborne EC systems, UAV-borne systems have the main advantage of being able to get in close to the intended target with a relatively low-cost platform and minimal risk to the operator. Thus, UAVs provide high levels of payoff in terms of intelligence and targeting.

An entire small UAV system (including aircraft, ground control station, launcher, and payloads) costs a fraction of what a large airborne standoff jamming (SOJ) platform can cost. Nevertheless, due to the proximity of the UAV-borne jammer to its intended target, it could in some instances deliver a higher level of jamming energy on the target than a high-power SOJ system. One drawback is that the small payload capacity of most UAVs precludes mounting jammers capable of covering the entire radio frequency range of interest. This means that a particular UAV-borne jammer usually can attack only one type of target. The limited jamming range of the UAV-borne system generally requires a high level of reconnaissance support to ensure that the UAV flight path takes it close enough to the target.

An army group also can have an air defense jamming regiment, with two to four battalions. Normal practice is to allocate an air defense jamming battalion to each army or corps in the main effort. The remaining battalion(s) protect high-priority army group assets. The battalions employ a variety of radar and communications jamming and target acquisition systems that target the onboard emitters of enemy aircraft. Electronic intercept systems provide targeting information to the radar jammers. This jamming capability supports the OPFOR's own air operations as well as improving the air defense of high-value assets. (For more detail on EC support to air defense, see Chapter 11.)

Army

As with the army group, subordinate levels of command have a mix of signals reconnaissance and jamming systems. An army can have one to two signals reconnaissance battalions. In lieu of these separate battalions, a high priority army may have a signals reconnaissance regiment, composed of three such battalions. These units differ from the battalions of the signals reconnaissance brigade in that they each include a mix of intercept and DF systems. The army can also have a jamming regiment or battalion of the same type found in the army group.

Corps

A corps can have a signals reconnaissance battalion and/or a jamming battalion. These battalions, if present, have the same structure as those found at the army level.

The signals reconnaissance battalions at corps and army normally have a higher proportion of VHF intercept and DF systems in relation to HF, whereas HF composes a greater proportion of systems at army group level.

Air Force

The Air Force has airborne assets that support the EC mission. It can employ airborne platforms in either an escort or a stand-off jamming role. The escort jammers provide protection to aircraft conducting a strike on targets in enemy territory. The SOJ platforms remain well behind the OPFOR's forward edge to avoid loss of these high-value assets and crews.

The use of an airborne platform can greatly enhance the effectiveness of both intercept and jamming, particularly of radio relay. These systems offer the advantages of greatly increased range, mission flexibility, mobility, and brute jamming power.

The reconnaissance aviation regiment of the army group's air army provides a wide variety of sensor packages on its fixed-wing aircraft. This regiment has up to three squadrons of high-performance reconnaissance aircraft, some of which are available in EC configurations.

An air army may also have substantial jamming capabilities in an airborne jamming aviation regiment and a heliborne jamming squadron. The regiment has two squadrons equipped with high-performance fixed-wing jamming platforms. The heliborne squadron has two to three flights, with a mix of heliborne jamming platforms.

A separate helicopter squadron with one heliborne jamming flight may also be organic to the air army, as well as to an army or corps. This flight consists of four to six heliborne platforms.

Space-Related Assets

Space-based warning, surveillance, navigation, and meteorological systems provide substantial benefits to the military commander. Aside from its own satellites, the OPFOR has access to many of these capabilities from other countries through ground stations or commercial firms. Radar reconnaissance satellites can lock onto intercepted signals to provide target location information. The OPFOR also has large-area radar surveillance satellites in its inventory.

EC activities targeting space-based systems involve a much greater degree of technical difficulty. The accuracy to which the OPFOR can determine the precise location of a space object plays a vital role in the employment of antisatellite jamming. Communications jammers designed to jam satellite uplinks or intersatellite links require accurate satellite location information.

The OPFOR could employ several methods to obtain satellite tracking information. Of these, some require little or no technical expertise. A large amount of satellite tracking data is available through computer bulletin board services or directly from several publications. The OPFOR and a second party could transfer satellite tracking information as part of an intelligence-sharing agreement. Finally, active and passive sensors are available, such as radars, optics, and passive detection equipment.

The OPFOR is continuing to expand its use of satellite communications in support of military operations. Space-based communications provide a more secure means of C^2 than ground-based systems, significantly contributing to protecting the OPFOR's use of the electromagnetic spectrum.

COMPONENTS

Essential to the success of OPFOR EC is the collection of accurate and timely information. OPFOR reconnaissance attempts to develop an accurate picture of the enemy's electronic order of battle, together with equipment types, emission characteristics, operating procedures, and operator characteristics. In addition to EC-dedicated systems, all reconnaissance, surveillance, and target acquisition assets at the various command levels feed the information-gathering and analysis process that supports EC. Signals reconnaissance provides the primary means of locating targets of specific interest to the EC effort. One of the most valuable assets for confirming EC targets remains ground reconnaissance forces. The OPFOR obtains some technical information concerning enemy electronic equipment from open-source material, such as technical manuals and field manuals.

Signals Reconnaissance

Identification and location of enemy electronic emissions and understanding their nature and use are key to countering and exploiting them. Signals reconnaissance is the sum of all means used in this collection and analysis. In the OPFOR, signals reconnaissance is the mission of--

- Airborne signals reconnaissance assets of the Air Force.
- Signals reconnaissance units at army group, army, corps, and division levels.
- Signals reconnaissance assets of the ground forces' jamming units.

The OPFOR expects to identify targets not only by DF, but also through signals analysis. For the latter, it plans to exploit lax enemy communications security and poor electronic counter-countermeasures. Specialists perform technical analysis to identify high-priority targets. In accordance with the EC plan, specialists target emitters for destruction, jamming, signals exploitation, or deception. Because signals reconnaissance systems only locate electronic emitters, not necessarily units, the OPFOR attempts to avoid enemy deception efforts by using other reconnaissance means for confirmation.

When signals reconnaissance units support a specific brigade or higher organization, an EC liaison representative augments the organization's main command post. He passes targeting information required for physical destruction through the supported unit's chief of reconnaissance.

The OPFOR has the ground-based capability to intercept and DF enemy emitters within the following distances from the forward edge of friendly troops:

- Artillery ground radar--about 25 km.
- VHF communications--about 40 km.
- HF groundwave--about 80 km.

- HF skywave--unlimited.

Greatly extended ranges are possible when mounting intercept and DF systems on airborne platforms, as well as when ground-based systems are targeting airborne emitters.

The fielding of radio communications systems employing spread-spectrum modulation techniques greatly complicates OPFOR signals reconnaissance efforts. Even when not coupled with encryption systems, these systems provide a significant electronic counter-countermeasures (ECCM) capability, with the potential for truly low probability of intercept and increased resistance to jamming. However, the OPFOR has developed a few high-technology EC systems designed to perform DF on these radios.

Direction Finding

The purpose of DF is to locate transmitting enemy radio and radar emitters. The OPFOR DF ranges are equivalent to that for intercept. The OPFOR uses DF to--

- Provide approximate locations of enemy electronic emitters.
- Provide locations that, when applied with intercept, terrain analysis, or other means, have sufficient accuracy to target with artillery fires.
- Develop a "picture" of the battlefield to reveal enemy unit locations and intentions.
- Provide adequate locations for firing on most radars and jammers.

Because of the length of transmission, the peculiarity of their signal characteristics, and power output, it is easy to locate jammers and identify them as targets for attack by suppressive fires. Due to a radar's unique signal parameters, DF can locate radars with greater precision than it can for radio emitters, often within 50 to 200 m.

It is possible to evaluate information from DF resources quickly, but this usually requires further confirmation by other sources. DF targets within conventional artillery range receive priority. Among these, targets that are time-sensitive and considered a serious threat receive priority and are candidates for immediate engagement.

With the OPFOR's older systems, if an enemy emitter remains active for at least 25 seconds, the targeting sequence can continue even after emissions cease. Newer systems are shortening the timelines considerably.

Priorities

The signals reconnaissance priorities correspond to the maneuver commander's EC information requirements. Priorities for intercept and DF are similar in both the offense and the defense, though they vary by phase.

Communications intercept and DF priorities include--

- Reconnaissance C^2 nets.
- Fire support nets.
- Air defense nets.
- Maneuver force C^2 nets.
- Electronic warfare nets.
- NBC-related communications.
- Engineer nets.

Radar intercept and DF priorities include--

- Radar jammers.
- Ground and battlefield surveillance radars.
- Target acquisition radars.
- Countermortar and counterbattery radars.
- Air defense radars.

Deployment

In the ***offense***, signals reconnaissance assets normally locate with the organization conducting the main attack, as far forward as possible. The unit commander coordinates with the chief of reconnaissance to ensure continuous coverage of the most critical sections of the battlefield. The signals reconnaissance unit commander and his staff select alternate positions for the signals reconnaissance assets that have line-of-sight (LOS) along the avenue of approach. This enables the assets to leapfrog forward in support of the battle.

In the ***defense***, the unit commander coordinates positioning of his signals reconnaissance assets with the chief of reconnaissance. Initially, many of the assets supporting tactical and operational missions may locate within the security zone, behind the security-zone forces in their initial positions. The depth to which the OPFOR deploys these assets depends on the terrain and disposition of forces in the security zone. As security-zone forces fall back to their successive positions, signals reconnaissance assets fall back to previously reconnoitered positions offering good LOS. If deployed within the main defensive zone, assets take up position behinds the first-echelon battalions of the first-echelon brigades. They choose terrain offering good LOS and reposition frequently to avoid enemy EC activities and subsequent destructive fires.

Electronic Jamming

A major part of EC is the requirement to jam, at critical times, enemy C^2 and weapon system voice and data communications that the OPFOR cannot destroy by firepower. All types of emitters are vulnerable to both jamming and deception. The jamming mission belongs to the airborne jamming assets of the Air Force, ground-based radar jammers, and ground forces' jamming units.

Jamming secure voice and data communications may force the enemy to transmit in the clear, which allows exploitation of combat information. Jamming can also aid in DF by forcing the enemy to transmit longer, allowing time for tip-off and multiple fixes. When not dedicated to a jamming mission, jammers may assist in signals reconnaissance. Jammers may also support EPM by providing a jamming shield to protect OPFOR communications from enemy electronic warfare efforts. To accomplish this, jammers emit jamming signals on those frequencies the OPFOR wishes to use. Due to considerations of signal geometry and strength, the jammers do not affect OPFOR communications, but do affect the enemy's signals reconnaissance receivers.

The primary OPFOR methods of jamming are--

- Radar jamming by using barrage, sweep, and spot noise, pulse, chaff, and decoys.
- Pulse and simulation jamming of command guidance systems.
- Radio jamming of AM and FM signals using barrage, sweep, or spot noise.

The OPFOR can supplement the radio jamming capability of its operational-level ground forces with assets allocated down from national level. These may include a considerable number of airborne radio-jamming and ground-based and airborne radar-jamming sets. Aircraft and air defense units have jammers that attempt to disrupt enemy target acquisition radars, weapon guidance systems, or aircraft navigation aids. Aircraft also may have some deceptive transmitters, mainly to project false locations to enemy air defense systems. The OPFOR continues to modernize its radar jamming assets in response to enemy advances in radar technology. This effort emphasizes the OPFOR intentions to disrupt enemy ground and airborne radars and support its own air activities and air defense of high-value rear area targets.

Effectiveness

A number of technical factors govern jamming effectiveness. These factors include--

- Target link distance (distance between the enemy transmitter and receiver).
- The distance between the jammer and the enemy receiver.
- Radio LOS between the jammer and the targeted receiver.
- Antenna polarization.
- Effective radiated power of the jammer and the enemy transmitter.
- Weather, terrain, and vegetation.

The most important of these are the distances of the target receiver from the jammer and from the transmitter.

Radios utilizing spread-spectrum modulations reduce the impact of conventional jammers. The effectiveness of jamming against these radios varies, depending upon the type of jamming employed. Options include narrow-band, partial-, or full-band jamming.

Priorities

Priorities for jamming vary with the operational or tactical situation. The following are general guidelines for initial priorities:

- Attack enemy communications and command guidance systems for artillery, rocket, and SSM forces.
- Disrupt enemy communications, target acquisition, and guidance systems for air defense forces.
- Jam enemy critical C^2 links.
- Protect friendly C^2 systems.

The OPFOR carefully coordinates its jamming activities with the signal officers at each level of command. The primary intent is to minimize, or preferably, avoid the accidental disruption of friendly systems.

Deployment

The enemy also considers jammers priority targets for destruction. Because of their high power and unique electronic signature, they are relatively easy to detect and locate. The majority of ground-based jammers must deploy within the range of indirect fire weapons, and are highly susceptible to damage. Taken together, these factors dictate the OPFOR must thoroughly plan and execute jammer deployment for their survival.

Jammers must be mobile to both survive and maintain favorable transmission paths against enemy emitters that are moving as the operation progresses. A fluid, high-tempo operation requires the jammers to displace frequently. The OPFOR preselects primary and alternate sites for each phase of the operation. These sites must--

- Be accessible and concealed from enemy direct fire weapons.
- Provide for continuity of mission.
- Facilitate electronic massing of several jammers against priority targets.
- Facilitate communications.

In the ***offense***, jamming assets normally deploy slightly behind the forward maneuver units. Jammers positioned near the forward edge selectively jam critical communications links, normally using barrage and spot noise or pulse signals. The priority of support is to support the units conducting the main effort.

In the ***defense***, jamming assets normally locate in the security zone and in the main defensive zone behind the first-echelon battalions of the first-echelon brigades. They select terrain offering good LOS and reposition frequently. In the security zone, priority is to disrupt enemy reconnaissance nets. As the enemy approaches the main defensive zone, priorities shift to divisional and brigade-level fire support and maneuver nets, in that order. Deployment of jamming assets would orient on those areas projected to be the enemy's main effort.

Electronic Protection Measures

Electronic protection measures (EPM) are any active or passive procedures to protect the friendly use of electronic systems. OPFOR commanders try to enforce a high level of EPM consciousness in their subordinates and equipment operators.

The OPFOR objective for EPM is the satisfactory operation of its electronic equipment in the face of enemy disruption efforts. EPM are the responsibility of every soldier who uses or supervises the use of radios, radars, or other electronic emitters.

The OPFOR achieves its EPM objectives through strict enforcement of signals security, equipment redundancy, system design, operator skill, and alternate methods of communication. It places emphasis on individual and organizational field-expedient techniques. Operator EPM training occurs at all organizational levels. The OPFOR practices major moves while in conditions of radio silence or even total electronic silence. Its use of battle drills lessens its dependence on extensive radio orders in the attack.

The OPFOR employs alternate passive EPM, such as wire, visual methods (such as flags or flares), messengers, and manual encryption. The OPFOR is also expanding its employment of secure communications devices. It practices false positioning of different types of emitters and establishes dummy nets for deception purposes. The OPFOR may protect its communications from enemy electronic warfare by using a jamming screen.

Destruction

Physical destruction is integral to OPFOR electronic combat doctrine. It is the preferred method of disrupting enemy communications and radars. Even a small raid or harassing fires on a headquarters can interrupt the enemy planning cycle.

Critical C^2 nodes, air defense radars, satellite terminals, and enemy electronic warfare assets are priority targets. The OPFOR can physically attack in three ways:

- **Indirect fire**. This includes artillery, mortars, rockets, and SSMs.
- **Ground attack**. While fighting in the enemy's rear, the OPFOR may attempt to destroy C^2 and communications elements by using tank or mechanized infantry, special-purpose, airborne or heliborne forces as raiding or enveloping detachments.
- **Air attack**. The OPFOR may attack with high-performance aircraft or helicopters. Ground forces may plant a transmitter within the enemy perimeter for beacon bombing.

Compared with other methods of disruption, physical destruction provides the longest-lasting effects, as the enemy must reconstitute its control. The effects of jamming last only as long as the jamming does, or until the enemy employs some form of ECCM, such as changing frequency or increasing signal power levels. The effects of deception, while potentially the greatest, are the most difficult to successfully achieve. Often, only well after the outcome of an operation are their effects known.

Electronic Counterreconnaissance

The OPFOR attempts to limit the enemy's use of the electromagnetic spectrum to gather critical intelligence information required to accurately estimate OPFOR unit strengths, composition, and activities. The goal is to disrupt the enemy's control process by either denying critical information, or by feeding false information into the enemy's information systems.

All enemy sensor types are potential targets for deception operations supporting the counterreconnaissance effort. False radio nets, dummy command posts, deception jammers, and even radar corner reflectors all contribute to providing a false or misleading picture of OPFOR capabilities and intentions. Targets include ground-based and airborne signals reconnaissance platforms, and radar surveillance systems.

DECEPTION SUPPORT

Deception in EC is part of the OPFOR's overall deception efforts. The OPFOR is responding to the challenge posed by advances in enemy sensors and weapons by emphasizing the use of camouflage, concealment, and deception.

Regulations require planning for deception activities in all combat actions. The OPFOR seeks to confuse the enemy to the extent where the enemy is unable to distinguish between real and decoy targets, units, and activities. It believes that this can cause the enemy to come to false conclusions about OPFOR intent, deployments, and troop movements.

The OPFOR employs several components of deception simultaneously for maximum effectiveness. In this multidisciplined approach, no aspect lends itself more to use of deception than interference with enemy communications. The purpose of electronic deception is to cause misinterpretations of intent, disruptions, and delays. Electronic deception is normally part of an overall deception plan. This ensures that what the enemy collects electronically agrees with, or at least does not refute, the indicators presented by other deception means.

The OPFOR seldom, if ever, uses electronic deception alone. Electronic deception normally consists of manipulative, simulative, and imitative deception. The OPFOR may use one or all of these types of electronic deception in its deception activities.

The OPFOR is continuing the development and fielding of dedicated tactical non-communications means of deception. It practices extensive use of dummy positions, using field-expedient materials. It simulates troop movements by such means as use of civilian vehicles to portray movement to radar, and marching refugees to portray movement of troops in the rear. 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 EC systems, such as ground-based air defense jammers.

Manipulative Electronic Deception

The OPFOR uses manipulative electronic deception to counter enemy electronic warfare and collection 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 friendly intentions. The objective is to have enemy analysts accept the profile or information as valid and therefore arrive at an erroneous conclusion concerning friendly activities and intentions.

Simulative Electronic Deception

Simulative electronic deception 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 simulative electronic deception 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 callsigns.

With ***capability 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 "new" equipment designators on other or 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.

Imitative Electronic Deception

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

The OPFOR exercises extreme care in entering the enemy communications system because each emitter produces its own signature. Most techniques require extensive technical support and specially trained operators.

The modern battlefield contains a variety of target acquisition, surveillance, and electronic radars. Each class of equipment produces an individual signature. The OPFOR uses repeaters, transponders, and reflectors that substitute an altered or generated-signal in imitation of the radar's normal return echo to deceive it. Successful deception requires a much better understanding of the technical characteristics of the enemy radar than that required for jamming.

---

[1] In addition, the potential exists for the use of the high-powered, fixed broadcast facilities located throughout the State to disrupt enemy strategic communications in the HF and lower radio frequency bands.

SIGN IN