HANDBOOK

16-15

MAY 16

THE ELECTRONIC WARFARE SMARTBOOK

U.S. UNCLASSIFIED
FOR OFFICIAL USE ONLY

Handling Instructions for CALL Electronic Media and Paper Products

Center for Army Lessons Learned (CALL) authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S., coalition, and allied efforts.

The information contained in this product reflects the actions of units in the field and may not necessarily be approved U.S. Army policy or doctrine.

This product is designed for official use by U.S., coalition, and allied personnel and cannot be released to the public without the expressed written consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulation (AR) 380-5, section 5-2.

Official military and civil service/government personnel, to include all coalition and allied partners may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official products or research. However, integration of CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels and cannot be released to the public without the expressed written consent of CALL.

This product may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military and government officials have access to these products.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Department of Defense (DOD) Web sites that do not restrict access to authorized personnel. AR-25-1, 15 Jul 2005, Army Knowledge Management and Information Technology, paragraph 6-4 n (2) (b) and DOD Web Site Administration Policy and Procedures (11 Jan 2002), Part II, paragraph 3.6.1 require appropriate mechanisms to protect sensitive information.

When no longer needed, all CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CDROM destroyers.

To allied and coalition personnel:

This information is furnished with the understanding that it is to be used for defense purposes only, that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States, and that it is not to be revealed to another country or international organization without the written consent of CALL.

Electronic Warfare Smartbook

DIGITAL VERSION AVAILABLE

A digital version of this CALL publication is available to view, download, or reproduce from the CALL restricted website, <https://call2.army.mil>. Reproduction of this publication is welcomed and highly encouraged.

Common Access Card (CAC) or Army Knowledge Online (AKO) login is required to access the digital version.

Electronic Warfare Smartbook

Table of Contents

Center For Army Lessons Learned

Director	**COL Paul P. Reese**
CALL Analyst	**Bruce D. Adams**
Authors	**SFC Joshua J. Gendron**
	David L. Varner
	MSG Phillip E. Isbill (Editing)
Cyber Center of Excellence Contributors	**Rick San Miguel**
	Alonso Long

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, ADPs, ADRPs, ATPs, FMs, and TMs, must be obtained through your pinpoint distribution system.

Introduction

(U) Over the last decade of war, the U.S. military has experienced the impacts of electronic warfare (EW) on operations. In response, our forces have demonstrated EW capabilities during military operations in Iraq, Afghanistan, and in Europe. While EW is a complex joint enabler, it is often misunderstood by commanders and staffs, creating a challenge for effective employment and management of those EW capabilities in support of full spectrum operations. EW is a force multiplier and not limited to just radio frequencies (RF spectrum), but includes all aspects of spectrum use (optical, acoustical, and infrared emissions). We must control the electromagnetic spectrum and deny/exploit systems used by our adversaries.

(U) The Electronic Warfare Smartbook provides a reference guide for Soldiers and officers conducting EW operations and augments FM 3-38, *Cyber Electromagnetic Activities*, 12 February 2014; and JP 6-01, *Electromagnetic Spectrum Management Operations*, 20 March 2012. Developed by noncommissioned officers at the National Training Center (NTC), this smartbook is also a result of the lessons and best practices experienced by tactical and operational formations during Combat Training Center (CTC) rotations.

(U) The Electronic Warfare Smartbook provides doctrinal guidance to Army spectrum users and describes how spectrum managers support commanders through the warfighting functions, the military decisionmaking process, and in contributing to the common operational picture (COP). The smartbook will assist the commander and staff in integrating EW capabilities into operations, while assisting the EW planner in planning, preparation, execution, and assessment in support of full spectrum operations. The principal audience for the Electronic Warfare Smartbook is all members of the Profession of Arms to include commanders, staff, trainers, and educators throughout the Army.

Chapter 1

Electronic Warfare Staff Roles and Responsibilities

(U) This chapter identifies those assigned to an electronic warfare (EW) specialty, outlining the appropriate duties and products associated with each position. This chapter is not all inclusive of the specialties resident within cyber electromagnetic activities (CEMA).

The Electronic Warfare/Functional Area (FA) 29 Officer (O3-O6)

(U) The electronic warfare officer (EWO) serves as the principal staff officer for all responsibilities concerning EW. The EWO is a specially trained officer who performs EW duties and integrates CEMA. The EWO prepares a portion of Annex C (Operations) to the operation order (OPORD) or operation plan (OPLAN) and contributes to any section that has a CEMA subparagraph such as Annex N, (Space Operations).[1]

(U) According to the U.S. Army Cyber (ARCYBER) Center of Excellence (COE) Individual Critical Task List for 29A (EWO), 26 MAR 2014, the EWO:

- Serves as the principal staff officer for all responsibilities concerning EW.
- Integrates EW capabilities to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capabilities.
- Synchronizes and coordinates offensive and defensive EW throughout the operations process.
- Coordinates and synchronizes tactical EW with theater, strategic, and operational-level EW.
- Integrates intelligence from the G-2/S-2 into EW.
- Monitors execution of EW tasks to ensure friendly forces dominate the EW spectrum when needed.
- Plans, coordinates, and supports the execution of EW and other CEMA.
- Leads the EW working group.
- Plans, coordinates, and assesses EW offensive, defensive, and support requirements.

- Supports the G-2/S-2 during intelligence preparation of the battlefield.
- Supports the fire support coordinator to ensure electronic attack (EA) fires are integrated with all other effects.
- Plans, assesses, and implements friendly electronics security measures.
- Prioritizes EW effects and targets with the fire support coordinator.
- Plans and coordinates EW operations across functional and integrating cells.
- Deconflicts EW operations with the spectrum manager.
- Maintains a current assessment of available EW resources.
- Participates in other cells and working groups (as required) to ensure EW integration.
- Serves as EW subject matter expert (SME) on existing EW rules of engagement.
- When designated, serves as the jamming control authority.
- Prepares, submits for approval, and supervises the issuing and implementation of fragmentary orders for EW operations.

The Electronic Warfare Warrant Officer

(U) The EW warrant officer organizes, implements, monitors, and evaluates operations, threat environments, unit maintenance, and intermediate-level support maintenance of EW systems. The EW warrant provides advice on technical and tactical employment of EW systems.

(U) The EW warrant officer's duties include supervising maintenance of EW system equipment and components; monitoring the development of the enemy EW order of battle (OB); processing targeting information and intelligence generated by the OB section; and assisting in the production and application of target selection standards. Also, as per the ARCYBER COE Individual Critical Task List for 29A, the EW warrant officer:

- Serves as the unit's technical SME on EW.
- Provides advice on technical and tactical employment of EW systems.
- Evaluates the technical and tactical operations of EW sections.
- Monitors the process for support requests and reviews EW operational assessments.

- Recommends employment of, and directs the operation of, various EW resources.
- Creates and updates unit standard operating procedures (SOPs).
- Assists the EWO in the planning and targeting processes.
- Assists the electronic warfare sergeant with EW products as needed.

The Electronic Warfare Noncommissioned Officer, Military Occupational Specialty (MOS) 29E

(U) The ARCYBER COE Individual Critical Task List for the 29E (Electronic Warfare Specialist–Skill Level 2 through 5), 26 MAR 2014, outlines the duties and responsibilities of the EW noncommissioned officer (NCO) — the staff SME at all echelons. In this capacity, the MOS 29E NCO advises and assists the commander or command EWO on the use and integration of EW capabilities in order to control the EMS and defeat the enemy. The EW specialist field begins at the grade of E-5 (sergeant) through E-9 (sergeant major).

(U) The EW NCO is responsible for ensuring a successful EW program and battlefield survivability through the operation and integration of all EW systems. The EW NCO establishes an EW program through the integration of EW into operational assessments and the planning process; development and oversight of command EW training; fielding and maintenance of EW systems; and the development and execution of EW operations. EW NCOs also develop and maintain EW SOPs; tactics, techniques, and procedures (TTPs); and battle drills.

(U) Soldiers holding MOS 29E will establish a training program that contains standardized training objectives in the form of critical action lists. These critical objectives support unit missions during wartime. This individual critical task list applies to the Active Army, the Army National Guard, and the Army Reserve, unless otherwise stated. All tasks in the individual critical task list are related to 29E, EW specialist, skill level 2, Soldier duties and responsibilities.

29E Electronic Warfare Noncommissioned Officer in Charge (NCOIC)

(U) The senior EW NCO assists battalion (BN) level 29E personnel with career progression and is responsible for assigning incoming EW personnel to BNs as well as ensuring new EW Soldiers have adequate support when arriving at a new duty location. The senior EW NCO is also responsible for

the brigade (BDE) EW training program, training and certifying BN-level EW personnel. The senior EW NCO will sign for, maintain, and account for all BDE EW section equipment. The senior EW NCO will participate in the military decisionmaking process (MDMP) and assist the BDE EWO and BDE EW technician in the planning process.

Individual Critical Task List (E-8/29E50)

(U) Performs duties shown in the preceding skill level, provides guidance to subordinate Soldiers, and serves as the principal enlisted assistant to commanders and as a staff NCO for major commands at the division-level and higher. Supervises and synchronizes EW personnel and operations within the force. Develops plans to use resources and determines priorities and overall training requirements. Reviews and identifies intelligence requirements and products. Advises on electronic deception during the staff estimate process. Coordinates the employment of assigned EW systems.

Individual Critical Task List (E-7/29E40)

(U) Performs duties shown in the preceding skill level, provides guidance to subordinate Soldiers, and serves as the principal enlisted assistant to commanders and as a staff NCO for major commands at brigade-level or higher. Directs unit EW training and provides technical advice and assistance to commanders. Develops and executes EW policies and procedures for supported organizations. Coordinates external EW support mission requirements. Integrates EW operations into the MDMP. In addition, the 29E40 NCO will:

- Validate joint tactical air strike request (JTAR) and EA request forms.
- Prioritize JTAR and EA request forms.
- Coordinate division and above EW efforts within electronic warfare working groups (EWWG).
- Assist in the development of division and above EW target list.
- Assist in the management of EW assets.
- Revise EW SOPs.
- Produce EW products in support of the MDMP.
- Maintain situational awareness of EW activities.
- Assess EW execution.
- Adjust the EW plan.
- Evaluate event logs.

- Manage the EW reprogramming process.
- Evaluate measures of performance (MOPs) and measures of effectiveness (MOEs).
- Establish EW training plan.
- Integrate EW training requirements.
- Assess the EW training program.
- Advise the command on the EW training program.
- Participate in Army EW training development.
- Coordinate joint EW staff efforts.
- Participate in joint EW operations.
- Participate in the joint targeting process.
- Perform EW knowledge management.
- Perform administrative actions.
- Operate EW software programs.

Individual Critical Task List (E-6/29E30)

(U) Performs duties shown in the preceding skill level and provides guidance to subordinate Soldiers. Prepares and coordinates the EW appendix to the OPORD. Develops EW input to targeting products. Participates in targeting meetings. Analyzes situation and predicts needs. Assesses EW risks and vulnerabilities and recommends countermeasures. Assesses friendly capabilities and missions in EW terms. Determines electronic protection (EP) requirements and controls EW effects. Briefs friendly EW plan and vulnerabilities for each course of action.

Individual Critical Task List (E-5/29E20)

(U) Provides technical and tactical assistance to supported units. Maintains and assists in developing the EW staff estimate. Oversees EW pre-combat inspections/pre-combat checks. Serves as the EW master trainer. Assists and coordinates with the S-2 on electronic preparation of the battlefield.

(U) Coordinates with the S-6 for spectrum deconfliction. Disseminates common operational picture and EW information. At this skill level the EW specialist also:

- Administers the EW maintenance program.
- Determines intelligence requirements for EW.
- Coordinates EW efforts within the EWWG.
- Develops the EW target list.
- Determines EW assets.
- Deconflicts EW assets.
- Prepares EA request forms.
- Prepares EW input to OPLANs and OPORDs
- Prepares EW input for unit SOPs.
- Assesses EW execution.
- Coordinates the employment of assigned EW systems.
- Conducts reprogramming procedures.
- Operates test and measurement equipment.
- Interprets event logs.
- Implements the EW training program.
- Manages EW equipment employment.

Army Operational Electronic Warfare Personnel with the Additional Skill Identifier (ASI) 1J

(U) ASI 1J is awarded to individuals with a working foundation of EW for battalion and above operations, including Soldiers, Sailors, Airmen, and Marines, integrated and operating as members of the EW team. Each team member has a working knowledge of electronic fundamentals and the integration of EW into the military decisionmaking and targeting processes, how to analyze the electronic order of battle, EW targeting, and how to assess results. ASI 1J personnel apply knowledge to integrate EW across the full spectrum of military operations.

Endnote

1. Field Manual 6-0, *Commander and Staff Organization and Operations,* Change 2*,* 22 APR 2016, p. 2-18.

Chapter 2

Electronic Warfare Fundamentals

(U) As the modern battlefield becomes more technologically sophisticated, military operations continue to be executed in an increasingly complex electromagnetic environment. Planning for the integration of electronic warfare into operations requires an understanding of the operations process and associated electronic warfare (EW) considerations. The EW staff officer (EWO) is actively involved in the operations process. EW planning, preparation, execution, and assessment require collective expertise from operations, intelligence, signal, and mission command. The EWO integrates efforts across the warfighting functions to ensure that EW operations support the commander's objectives.[1]

Divisions of Electronic Warfare

(U) EW is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy.[2] EW is one of three capabilities of cyber electromagnetic activities (CEMA). The other activities are cyberspace operations and spectrum management operations.[3]

(U) EW is further composed of three divisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). Each division has its own purposes and effects that support unified land operations.[4]

(U) EA is a division of EW involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.[5]

(U) EP is a division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.[6]

(U) ES is a division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.[7]

Electronic Protection Fundamentals

(U) Understanding the threat to the EMS is the key to practicing sound EP techniques. As locations are determined and units are identified, enemy forces establish priorities to:

- Jam communication assets.
- Deceptively enter radio nets.
- Interfere with the normal flow of their enemy's communications.

(U) The more emphasis that is placed on EP, the greater the benefits, in terms of casualty reduction and combat survivability in a hostile environment. EW professionals' EP responsibilities include:

- Advising the S-2 of enemy capabilities that could be used to deny the unit effective use of the EMS.
- Exercising staff responsibility for EP, including ES and EA scenarios in all command post (CP) and field training exercises, and helping to evaluate EP techniques employed.
- Ensuring EP training is included in the unit training program.
- Aiding the S-6 in ensuring there are alternate means of communications for those systems most vulnerable to enemy jamming.

(U) Threats to friendly communications must be assessed during the planning process. Planning counters the enemy's attempts to take advantage of the vulnerabilities of friendly communications systems. At a minimum, four categories of EP planning must be considered: deployment, employment, replacement, and concealment.

Deployment

(U) Deployment involves placing and locating EW systems to best utilize those systems' capabilities to support operations. Because of the fluid nature of the operational environment (mobility), the locations of friendly emitters constantly change. Locations of friendly emitters should be analyzed by the J-6/G-6/S-6 in order to predict possible interference. Analysis results depend highly on the accuracy of data and the analytical technique used. Planners must also consider the following prior to deployment of EW assets:

- Communication systems perpendicular to the forward line of own troops (FLOT) enhance the enemy's ability to intercept communications because U.S. forces aim transmissions in the enemy's direction.

- If possible, U.S. forces must install terrestrial line of sight (LOS) communications parallel to the FLOT. This action supports keeping the primary strength of U.S. transmissions in friendly terrain.
- Locations of CPs must be carefully planned. CP locations determine antenna locations. Antennas and emitters should be dispersed and positioned at the maximum remote distance, terrain dependent from the CP, so that all of the unit's transmissions are not coming from one central location.
- Single-channel tactical satellite (TACSAT) systems reduce friendly CP vulnerability to enemy direction efforts.[8]

Employment

(U) Planning for the employment of EW capabilities includes determining how, when, and where EW capabilities are used to meet the commander's intent in support of operations. One of these employment capabilities is the establishment of alternate routes. Alternate routes enable friendly units to continue to communicate despite the enemy's effort to deny the use of friendly communications systems. Alternate routes also can be used by friendly units to transmit false messages and orders on the route that is experiencing interference, while transmitting the actual message and order through another route or means.[9]

(U) Three routing concepts can be used in communications:

- Straight-line system: provides no alternate routes of communications.
- Circular system: provides one alternate route of communications.
- Grid system: provides as many routes of communications as can be practically planned.[10]

(U) The number of friendly transmissions tends to increase or decrease according to the type of tactical operation being executed. Deceptive communication traffic can be executed using either false peaks or traffic leveling. False peaks are used to prevent the enemy from connecting an increase in communications with a tactical operation. Traffic leveling is accomplished by designing messages to be sent during decreases in transmission traffic, keeping transmissions fairly constant. Both techniques must be coordinated to avoid operational security violations, mutual interference, and confusion.[11]

(U) Frequency changing is a technique of changing frequencies often and at random, and has long been recognized as a key in confusing enemy traffic analysts. Change frequencies, network call signs, locations, and operators as often as possible and avoid establishing patterns of communication.[12]

Replacement

(U) Alternate means of communications should be used before enemy engagements to ensure the adversary cannot establish a database to destroy primary means of communications. Replacement involves establishing alternate routes and means of accomplishing what the commander requires. Frequency modulation (FM) voice communications are the most critical communications used by the commander during adversary engagements and are a target for the enemy to disrupt.[13]

(U) Primary systems must always be replaced with alternate means of communications if the primary means becomes significantly degraded. These replacements must be preplanned and carefully coordinated; if they are not, alternate means could be compromised and become worthless as a primary means of communications.[14]

(U) Users of communications equipment must know how and when to use the primary and alternate means of communications. This planning and knowledge ensures the most efficient use of communications systems.[15]

Concealment

(U) Most communications systems are difficult to conceal; however, installing antennas as low as possible on the backside of terrain features and behind man-made obstacles helps conceal communications equipment.[16]

Signal Security

(U) The goal of signal security is to ensure the enemy cannot exploit the friendly use of the EMS for communications. Signal security and EP should be based on the enemy's ability to gather intelligence and degrade friendly communications systems.[17]

Emission Control

(U) Transmitters should be turned on only when needed to accomplish the mission. Enemy intelligence analysts will look for patterns to turn into usable information. The enemy has no intelligence to work with if friendly transmitters are inactive (for example, radio silence or radio listening silence). Emission control should be a habitual exercise and transmissions should be kept to a minimum (20 seconds maximum, 15 seconds maximum is preferred).[18]

(U) Good emission control makes the use of communications equipment appear random and is therefore consistent with good EP practices. This technique will not eliminate the enemy's ability to find friendly transmitters; but when combined with other EP techniques, it makes locating a transmitter more difficult.[19]

Electronic Protection Techniques

(U) EP should be planned and applied to force the adversary to commit more jamming, information gathering, and deception resources to a target than it is worth. (Operating in a degraded system can provide some benefit in that the enemy will waste assets on the problematic degraded system that might be used to impair friendly communications elsewhere.) EP planning should be primarily focused on location (geometry) of radio systems and operating procedures.[20]

(U) The EW planner will focus on operating procedures. Effective jamming depends on knowing the frequencies and approximate locations of units to be jammed; the following techniques will reduce the vulnerability of communications from enemy disruption or destruction.[21]

Minimizing Transmissions

(U) The most effective preventive EP technique is to minimize both radio transmissions and transmission times. The high volume of radio communications that usually precedes a tactical operation makes the friendly force vulnerable to enemy interception, directional finding (DF), jamming, and deception. Traffic can be minimized by:

- Ensuring transmissions are necessary.
- Execution of the operation as per established SOPs.
- Preplanning messages before transmission. The Joint Interoperability of Tactical Command and Control Systems (JINTACCS) provides a standard vocabulary that can be used for message planning. JINTACCS voice templates are some of the best tools a radio operator can use to minimize transmission time.[22]

Electronic Protection Techniques For Minimizing Radio Transmissions

Clear and Concise Transmissions

(U) When a transmission is necessary, the radio operator should speak in a clear, well-modulated voice, using proper radio telephone procedures.

Using Equipment Capable of Data Burst Transmission

(U) This equipment is the most significant advantage of TACSAT communications systems. When messages are encoded on a digital entry device for transmission over satellite systems, the transmission time is greatly reduced.[23]

Using Alternate Means of Communications

(U) Alternate means of communications, such as cable, wire, or organic Soldiers performing as messengers, can be used to convey necessary directives and information. Use other means of communications as per unit's primary, alternate, contingency, and emergency (PACE) plan.[24]

Use of Brevity Codes

(U) A brevity code is a code that provides no security, but has as its sole purpose the shortening of messages, rather than the concealment of their content.[25]

Low Power

(U) In carefully planned and installed communications systems, users can normally operate on low power. Operating on low power decreases the range and makes it more difficult for the adversary to detect and intercept transmissions. Taking such action also reserves high power for penetrating enemy jamming.[26]

Radio Operator Procedures

(U) Many radio operators can be readily identified by certain voice characteristics or overused phrases. Strict adherence to the proper use of procedure words, outlined in the unit SOP, helps keep an operator's distinguishing characteristics to a minimum.[27]

(U) The adversary can gather information based on pattern and the content of radio communications. All reasonable measures should be taken to deny information to adversary intelligence analysts. Do not develop patterns through hourly radio checks, daily reports at specific times, or any other periodic transmissions. Periodic reports should be made by other means of communications.[28]

Authentication

(U) Authentication should be used in radio systems that do not use secure devices. Procedures for authentication are found in the supplemental instructions to the signal operating instructions (SOI). Authentication should be required in every instance in which an adversary attempts to deceptively enter nets to insert false information. Authentication is required if the user:

- Suspects the adversary is on their net.
- Transmits directions or orders that affect the tactical situation, such as change of locations, shift fire, or change frequencies.

- Talks about adversary contact, gives an early warning report, or issues a follow-up report.
- Tells a station to go to radio or listening silence.
- Cancels a message by radio or visual means, and the other station cannot recognize him.
- Resumes transmitting after a long period, or if this is the first transmission.
- Is authorized to transmit a classified message in the clear.
- Is forced, because of no response by a called station, to send a message in the blind.[29]

Remedial Electronic Protection Techniques

(U) Remedial EP techniques help reduce the effectiveness of enemy efforts to jam U.S. radio nets. EW specialists can:

- Identify jamming signals.
- Determine if the interference is obvious or subtle jamming.
- Recognize jamming and interference by:
    - ○ Determining whether the interference is internal or external to the radio.
    - ○ Determining whether the interference is jamming or unintentional interference.
    - ○ Reporting jamming and interference incidents.
- Overcome jamming and interference by adhering to the following techniques:
    - ○ Continue to operate.
    - ○ Improve the signal-to-jamming ratio.
    - ○ Adjust the receiver.
    - ○ Increase the transmitter power output.
    - ○ Adjust the antenna.
    - ○ Establish a wireless network extension station.
    - ○ Relocate the antenna.

- ○ Use an alternate route for communications.
- ○ Change the frequencies.
- ○ Acquire another satellite.[30]

Common Jamming Signals

(U) Jamming is an effective way for the enemy to disrupt friendly communications. An adversary only needs a transmitter tuned to a U.S. frequency, with enough power to override friendly signals, to jam U.S. systems. Jammers operate against receivers, not transmitters. The two modes of jamming are spot and barrage jamming. Spot jamming is concentrated power directed toward one channel or frequency. Barrage jamming is power spread over several frequencies or channels at the same time. It is important to recognize jamming, but it can be difficult to detect.[31] The following are the most common types of jamming signals.

(U) **Random Noise:** Synthetic radio noise is indiscriminate in amplitude and frequency. It is similar to normal background noise, and can be used to degrade all types of signals. Operators often mistake it for receiver or atmospheric noise, and fail to take appropriate EP actions.

(U) **Stepped Tones:** Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are normally used against single-channel amplitude modulation (SC AM) or FM voice circuits.

(U) **Spark:** Easily produced and one of the most effective jamming signals. Bursts are of short duration and high intensity; they are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications.

(U) **Gulls:** Generated by a quick rise and slow fall of a variable radio frequency (RF), and are similar to the cry of a sea gull. It produces a nuisance effect and is very effective against voice radio communications.

(U) **Random Pulse:** Pulses of varying amplitude, duration, and rate are generated and transmitted. They are used to disrupt teletypewriter, radar, and all types of data transmission systems.

(U) **Wobbler:** A single frequency, modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.

(U) **Recorded Sounds:** Any audible sound, especially of a variable nature, can be used to distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.

(U) **Preamble Jamming:** A tone resembling the synchronization preamble of the speech security equipment is broadcast over the operating frequency of secure radio sets. Results in all radios being locked in the receive mode. Especially effective when employed against radio nets using speech security devices.[32]

(U) **Note:** Subtle jamming is not obvious, as no sound is heard from the receivers. Although everything appears normal to the radio operator, the receiver cannot receive an incoming friendly signal. Often, users assume their radios are malfunctioning, instead of recognizing subtle jamming for what it is.[33]

Recognizing Jamming

(U) Radio operators must be able to recognize jamming. This is not always an easy task, as interference can be internal and external. If the interference or suspected jamming remains, after grounding or disconnecting the antenna, the disturbance is most likely internal and caused by a malfunction of the radio. Maintenance personnel should be contacted to repair it. If the interference or suspected jamming can be eliminated, or substantially reduced by grounding the radio equipment or disconnecting the receiver antenna, the source of the disturbance is most likely external to the radio. External interference must be checked further for enemy jamming or unintentional interference.[34]

(U) Interference may be caused by sources having nothing to do with enemy jamming. Unintentional interference may be caused by:

- Other radios (friendly and enemy).
- Other electronic or electric/electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.[35]

(U) The enemy is capable of using powerful unmodulated or noise-modulated jamming signals. Unmodulated jamming signals are identified by a lack of noise, while noise-modulated jamming signals feature obvious interference noise. If jamming is identified, unit SOPs should be consulted immediately for communication jamming battle drills. Regardless of whether the radio operator is able to overcome the effects of the jamming or interference, a joint spectrum interference resolution (JSIR) report must be submitted.[36]

Joint Spectrum Interference Resolution Report Information Requirements

(U) The JSIR report is used to document electromagnetic interference (EMI), thereby building situational understanding of the threat and aiding in the development of mitigation procedures. The report preparer provides a copy of the completed form to the EWO, spectrum manager, and G-6/S-6.

(U) Affected end users report EMI through JSIR-Online, if available. The JSIR-Online portal is located on the Secure Internet Protocol Network. Unit SOPs may also require a JSIR report be submitted through the chain of command using the JSIR format in Table D-1 of this handbook. The report preparer provides a copy of the completed form to the EWO, spectrum manager, and G-6/S-6.[37]

Endnotes

1. ATP 3-36, *Electronic Warfare Techniques*, 16 DEC 2014, p. 2-1.
2. Joint Publication (JP) 3-13.1, *Electronic Warfare*, 08 FEB 2012, p. GL-8.
3. ATP 3-36, *Electronic Warfare Techniques*, 16 DEC 2014, p. 1-1.
4. Ibid.
5. JP 3-13.1, *Electronic Warfare*, 08 FEB 2012, p. GL-8.
6. Ibid.
7. Ibid., GL-9.
8. ATP 6-02.53, *Techniques for Tactical Radio Operations*, 07 JAN 2016, p. 12-6.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid., pp. 12-13 though 12-14.
13. Ibid., p. 12-7.
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid., p. 12-8.
21. Ibid.
22. Ibid., pp. 12-8 through 12-9.
23. Ibid., p. 12-9.

24. Ibid.
25. Ibid.
26. Ibid.
27. Ibid., p. 12-10.
28. Ibid.
29. Ibid.
30. Ibid., p. 12-11.
31. Ibid.
32. Ibid., p. 12-12.
33. Ibid.
34. Ibid., p. 12-10.
35. Ibid. p. 12-12.
36. Ibid.
37. ATP 3-36, *Electronic Warfare Techniques*, 16 DEC 2014, pp. A-1 through A-2.

Chapter 3

Electronic Warfare and the Military Decisionmaking Process

(U) Electronic warfare (EW) planning minimizes fratricide and optimizes operational effectiveness during execution. Therefore, EW planning occurs concurrently with other operational planning during the military decisionmaking process (MDMP).[1] The electronic warfare officer (EWO) leads the cyber electromagnetic activities (CEMA) element in planning, integration, and synchronization of EW, cyberspace operations, and spectrum management.[2]

The Military Decisionmaking Process

(U) The MDMP consists of seven steps. Each step has various inputs and a series of processes that commanders and staffs conduct to produce the outputs. The outputs lead to an increased understanding of the situation, facilitating the next step of the MDMP. Commanders and staffs generally perform these steps sequentially; however, they may revisit several steps in an iterative fashion as they learn more about the situation before producing the plan or order.[3] The seven steps of the MDMP are:

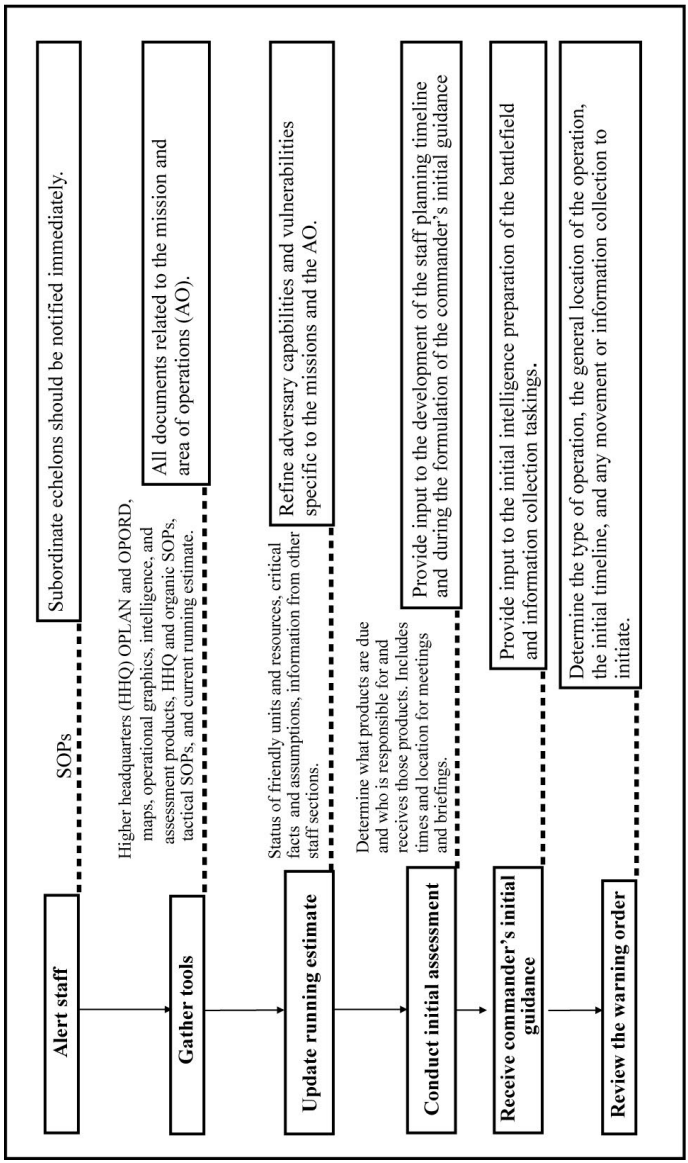
- Step 1: Receipt of mission.
- Step 2: Mission analysis.
- Step 3: Course of action (COA) development.
- Step 4: COA analysis.
- Step 5: COA comparison.
- Step 6: COA approval.
- Step 7: Orders production.

Receipt of the Mission (MDMP Step 1)

(U) Commanders initiate the MDMP upon receipt or in anticipation of a mission. Staff members responsible for planning and integrating **cyberspace operations** initiate coordination with higher headquarters (HHQ) staff counterparts to obtain information on current and future cyberspace operations, running estimates, and **other cyberspace operations planning products**. Actions during this step include:

- **EW staff lead** alerts subordinates (initial allocation of time).

- **EW lead** and staff begin to gather resources (target packets, enemy electronic order of battle [EOB]):
    - Publications, including Army Doctrine Reference Publication (ADRP) 1-02
    - HHQ operation plan (OPLAN), operation order (OPORD), maps, and operational graphics
    - HHQ and other organizations' intelligence and assessment products
    - Both HHQ and own organization's standard operating procedures (SOPs)
    - Current running estimates
    - Any Army design methodology products
- Update the cyberspace operations running estimate.
- Conduct initial assessment to help commander determine:
    - Time needed to plan and prepare for the mission for both headquarters and subordinate units.
    - Which outside agencies and organizations to contact and incorporate into the planning process.
    - The staff's experience, cohesiveness, and level of rest or stress.
- Issue the commander's initial guidance which includes, but is not limited to:
    - Initial time allocations.
    - A decision to initiate Army design methodology or go straight to MDMP.
    - Necessary coordination to exchange liaison officers.
    - Authorized movements and initiation of information collection.
    - Collaborative planning times and locations.
    - Initial information requirements.
    - Additional staff tasks.
- Issue the initial warning order.



(U) Figure 3-1. Receipt of the Mission Flow Diagram (Source: EW Observer, Coach, Trainer; National Training Center, in accordance with Army Doctrine Publication (ADP) 5-0, *The Operations Process*, and Field Manual (FM) 6-0, *Commander and Staff Organization and Operations*)

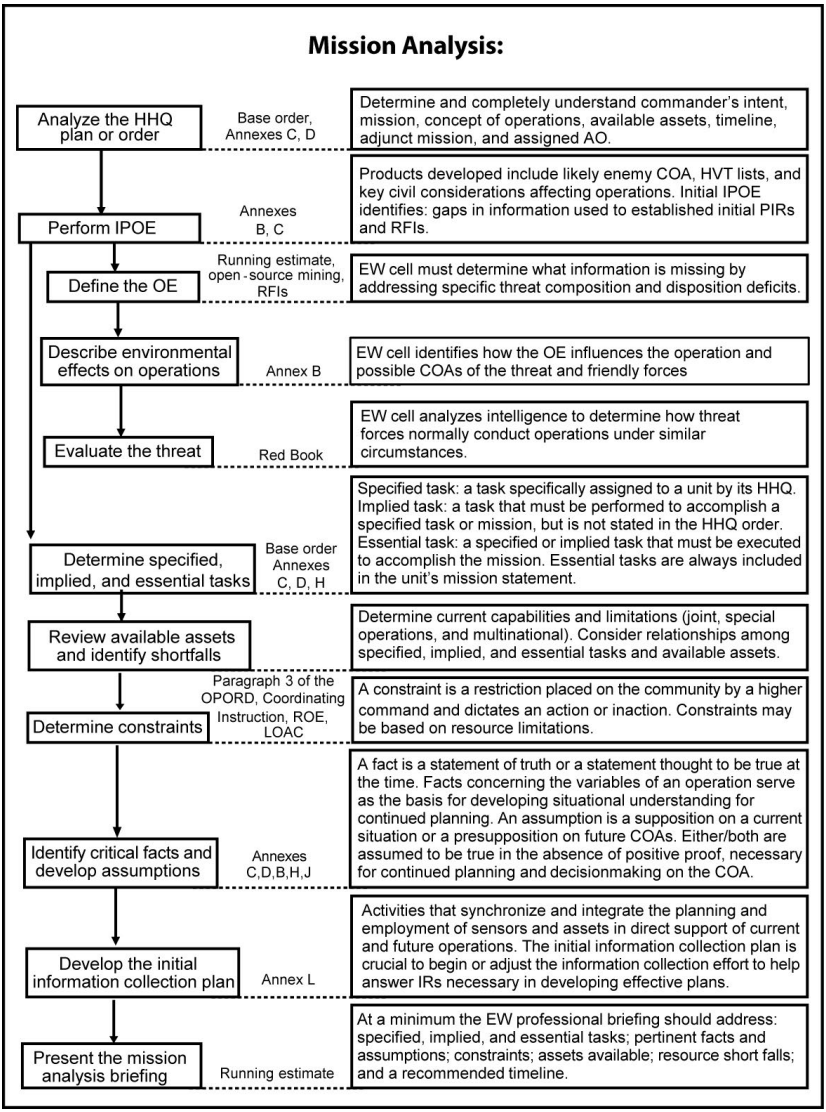
Mission Analysis (MDMP Step 2)

(U) Commanders and staffs conduct mission analysis to better understand the situation and problem. They identify "what" the command must accomplish (along with "when" and "where") and develop an understanding of the purpose of the operation – the "why." Staff members responsible for planning and integrating cyberspace operations gather, analyze, and synthesize information on current conditions of the operational environment with an emphasis on cyberspace, the electromagnetic spectrum (EMS), and the information environment. Figure 3-2 on page 28 provides an example of a mission analysis flow diagram.

(U) Key inputs into mission analysis are the commander's initial guidance and the HHQ plan or order:

- Identify commander's intent and end state (Annex C of the OPORD).
- Analyze the inputs and develop requests for **information relevant** to **cyberspace operations**.
- Perform initial intelligence preparation of the battlefield (IPB).
- Determine **cyberspace operations specified, implied, and essential tasks**.
- Determine **cyberspace limitations and constraints**, and identify **cyberspace critical facts and assumptions** (OPORD, all annexes' coordinating instructions).
    - Determine threat's dependence on the **EMS**.
    - Determine threat's **EW** capabilities.
    - Determine threat's intelligence collection capability.
    - Determine which threat vulnerabilities relate to the **EMS**.
    - Determine how an operational environment affects **EW operations** using operational and mission variables as appropriate.
    - Initiate, refine, and validate information requirements and requests for information (RFIs).
- Begin risk management process.
- Identify and nominate commander's critical information requirements (CCIR).
- Identify and nominate essential elements of friendly information.

- Provide initial input for the **combined information overlay**, relevant to **cyberspace operations**.
- Begin development of **cyberspace effects** request formats and evaluation request messages.
- Provide input for commander's initial planning guidance.
- Participate in the mission analysis brief.
- Provide **CEMA** input for the warning order.



(U) Figure 3-2. Mission Analysis Flow Diagram (Source: EW Observer, Coach, Trainer; National Training Center, in accordance with ADP 5-0, *The Operations Process*, and FM 6-0, *Commander and Staff Organization and Operations*)

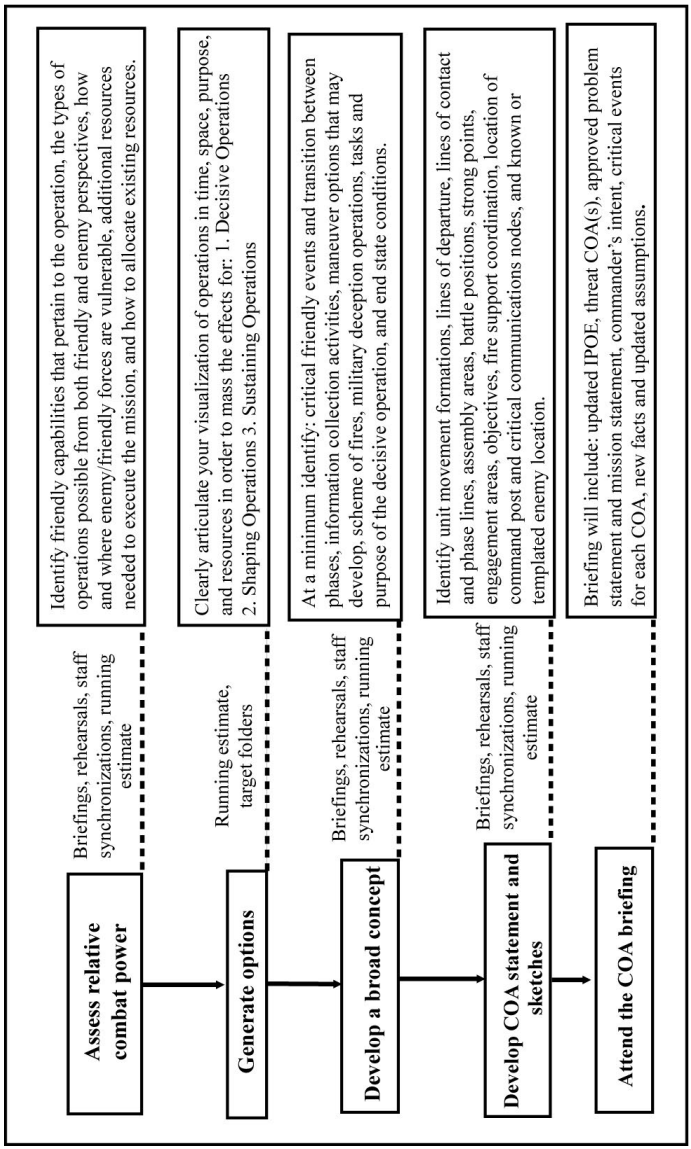
Course of Action Development (MDMP Step 3)

(U) COA development generates options for subsequent analysis and comparison that satisfy the commander's intent and planning guidance. Staff members responsible for planning and integrating cyberspace operations apply knowledge gained from the mission analysis step to assist with overall COA development. During COA development, these staff members develop an initial scheme of cyberspace operations consisting of cyberspace support tasks. The scheme of cyberspace operations describes how the commander intends to use cyberspace operations to support the concept of operations, with an emphasis on the scheme of maneuver. Figure 3-3 on page 31, depicts a COA development flow diagram.

(U) **EW planners** contribute to key inputs such as: commander's initial guidance, initial CCIR, updated IPB, CEMA specified and implied tasks relevant to cyberspace operations, list of high-value targets that may require effects by cyberspace operations capabilities, and updated cyberspace operations running estimate. EW planners' actions performed during COA development include:

- Determining friendly **EW capabilities** available to support the operation (organic and nonorganic), as well as possible friendly and threat **EW operations**.
- Identifying **EW tasks** required to support the COA:
    - **Electronic warfare support** to locate enemy **EMS** systems
    - **Electronic protection** against enemy capabilities
    - **Electronic attack** against enemy vulnerabilities
- Identifying EW tasks and their ties to triggers such as phase lines, critical times, and decision points.
- Identifying **EW tasks** with their task and purpose:
    - Task is threat-oriented.
    - Purpose is friendly-oriented.
    - Example: Degrade enemy counterfire radar in order to provide friendly freedom of fires.
- Briefing the fire support officer as early as possible and throughout the process on **EW capabilities**.
- Updating the **EW running estimates**:
    - Performing initial IPB.

- Providing **cyberspace operations** input to the information collection plan.
- Identifying **cyberspace operations**-related vulnerabilities of friendly, enemy, adversary, and neutral actors.
- Providing **cyberspace operations** input for the initial scheme of **CEMA** and fire support.
- Providing draft **cyberspace operations**-related input for the **combined information overlay**.
- Analyzing high-value targets and determining high-payoff targets that may require effects by **cyberspace capabilities**.
- Collaborating with **cyberspace operations** planners at HHQ to integrate existing **cyberspace operations** missions.
- Developing initial scheme of **cyberspace operations**.
- Developing and submitting **cyberspace effects** request formats and evaluation request messages.
- Providing **cyberspace operations** input for the development of the COA development brief as required.



(U) Figure 3-3. Course of Action Development Flow Diagram (Source: EW Observer, Coach, Trainer; National Training Center, in accordance with ADP 5-0, *The Operations Process*, and FM 6-0, *Commander and Staff Organization and Operations*)

COA analysis (MDMP Step 4)

(U) COA analysis enables commanders and staffs to identify difficulties or coordination problems, as well as probable consequences of planned actions for each COA being considered. The process helps planners think through the tentative plan. COA analysis may require commanders and staffs to revisit parts of a COA as discrepancies arise. COA analysis not only appraises the quality of each COA, but also uncovers potential execution problems, decisions required, and contingencies needed. In addition, COA analysis influences how commanders and staffs understand a problem and may require the planning process to restart.[4]

(U) The staff identifies the required assets of the warfighting functions to support the concept of operations, including those needed to synchronize sustaining operations. If requirements exceed available assets, the staff recommends priorities based on the situation, commander's intent, and planning guidance. To maintain flexibility, the commander may decide to create a reserve to maintain assets for unforeseen tasks or opportunities. Other tasks identified during COA analysis include:

- Likely times and areas for enemy use of weapons.
- Potential times or locations for committing reserves.
- Locations of commander and command posts.
- Requirements for supporting each warfighting function.
- Confirmation of locations of named areas of interest, target areas of interest, decision points, and intelligence requirements needed for support.

(U) The products the staff develops during mission analysis help commanders understand the situation and develop the commander's visualization. During COA development and COA comparison, the staff provides recommendations to support the commander in selecting a COA. The staff is integral to developing decision points, the synchronization matrix, and the decision support template and matrix. The staff determines whether the COA is feasible by considering:

- Requirements for military deception and surprise.
- The timing for concentrating forces and starting the attack or counterattack.
- The movement times and tables for critical assets, including information systems nodes.
- The estimated duration of the entire operation and each critical event.

- The projected percentage of enemy forces defeated in each critical event and overall.
- The percentage of minimum essential tasks that the unit can, or must, accomplish.
- The targeting requirements in the operation, to include identifying or confirming high-payoff targets and establishing attack guidance.
- The allocation of assets to subordinate commanders to accomplish their missions.

Course of Action Comparison (MDMP Step 5)

(U) COA comparison is an objective process to evaluate COAs independently and against set evaluation criteria approved by the commander and staff. The goal is to identify the strengths and weaknesses of COAs, enable selection of a COA with the highest probability of success, and further develop that COA into an OPLAN or OPORD. The commander and staff perform certain actions and processes that lead to key outputs:

- Give input to the high-payoff target list.
- Update target information folders: frequency range, datalinks, associated radars, maximum range, minimum range, maximum altitude, minimum altitude, associated weapons systems, and self-protection.
- Give input to the synchronization matrix.

Course of Action Approval (MDMP Step 6)

(U) After a decision briefing, the commander selects the COA to best accomplish the mission. If the commander rejects all COAs, the staff starts COA development again. If the commander modifies a proposed COA, or gives the staff an entirely different one, the staff war-games the new COA and presents the results to the commander with a recommendation. Once a COA is selected, EW planners:

- Update the mission command nodal analysis of the enemy, relevant to the selected COA.
- Tailor the EOB to the selected COA.
- Attain the updated collection assets and collection plan.

Orders Production (MDMP Step 7)

(U) The staff prepares the order or plan by turning the selected COA into a clear, concise concept of operations (CONOPS) with the required

supporting information. The COA statement becomes the CONOPS for the plan. The COA sketch becomes the basis for the operation overlay. If time permits, the staff may conduct a more detailed war game of the selected COA to more fully synchronize the operation and complete the plan.

The following annexes are developed or updated in accordance with the CONOPS:

- Final input to Annex C (Operations).
    - **Annex C, Appendix 12 (CEMA)**.
    - Annex C, Appendix 14 (Military Deception).
    - Annex C, Appendix 15 (Information Operations).
- Final input to Annex H (Signal).
    - Annex H, Appendix 1 (Defensive Cyberspace Operations).
    - Annex H, Appendix 2 (Information Network Operations).
    - Annex H, Appendix 6 (Spectrum Management Operations).

Endnotes

1. Army Techniques Publication (ATP) 3-36, *Electronic Warfare Techniques*, 16 DEC 2014, p. 2-1.

2. FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014, p. 2-2.

3. FM 6-0, *Operations*, 05 MAY 2014, p. 9-2.

4. Ibid., p. 9-26.

Chapter 4

Electronic Warfare Operations

(U) The operations process is a commander-centric activity informed by the mission command approach to planning, preparing, executing, and assessing military operations. These activities may occur sequentially or continuously throughout an operation, overlapping and recurring as required. The electronic warfare staff officer (EWO) is actively involved in the operations process. EW planning, preparation, execution, and assessment require collective expertise from operations, intelligence, signal, and mission command. The EWO integrates efforts across the warfighting functions to ensure that EW operations support the commander's objectives.[1]

Electronic Warfare Preparation

(U) Preparation consists of activities that units perform to improve their ability to execute an operation. Preparation includes, but is not limited to, plan refinement, rehearsals, information collection, coordination, inspections, and movement. Preparation creates conditions that improve friendly forces' opportunities for success. It facilitates and sustains transitions, including those to branches and sequels.[2] During preparation, actions are focused on:

- Revising and refining the running estimate and tasks in support of the overall plan.
- Rehearsing the synchronization of EW in support of the plan including integration into the targeting process, procedures for requesting assets, procedures for deconfliction, and asset determination and refinement.
- Synchronizing the collection plan and intelligence synchronization matrix with the attack guidance matrix and EW input to the operation plan or order annexes and appendixes.
- Assessing the planned task organization developed in support of EW, including liaison officers and organic and nonorganic capabilities, required by echelon.
- Coordinating procedures with information collection operational elements.
- Training the supporting staff of the cyber electromagnetic activities (CEMA) working group during rehearsals.
- Completing pre-combat checks and inspections of EW assets.
- Completing sustainment preparations for EW assets.

- Completing backbriefs by subordinate EW working groups on planned operations.
- Refining content and format for the EW element's portion of the operation update, assessment, and briefing.

Electronic Warfare Execution

(U) Execution puts a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions. Commanders focus their subordinates on executing the concept of operations (CONOPS) by issuing their commander's intent and mission orders.[3] During execution, the CEMA working group and EWO:

- Serve as EW experts for the commander.
- Maintain a running estimate for EW.
- Monitor CEMA in operations and recommend adjustments during execution.
- Recommend adjustments to the commander's critical information requirements based on the situation.
- Recommend adjustments to control measures and procedures related to EW.
- Maintain direct liaison with the fires, signal, and intelligence cells to ensure integration and deconfliction of EW.
- Coordinate and manage EW taskings to subordinate units or assets.
- Coordinate requests for nonorganic EW assets.
- Continue to assist the targeting working group in target development and in recommending targets to attack through cyberspace operations (CO) or electronic attack (EA) assets.
- Receive, process, and coordinate subordinate requests for EW assets during operations.
- Provide input to the overall assessment regarding the effectiveness of CO and EW missions.
- Maintain, update, and distribute the status of EW assets.

Electronic Warfare Assessment

(U) An assessment is the continuous monitoring and evaluating of the current situation and the progress of an operation. Commanders, assisted by

their staffs, continuously assess the operation and compare the results with the CONOPS, mission, and commander's intent. Based on their assessment, commanders direct adjustments, ensuring that the operation remains focused on the mission and higher commander's intent.[4] Assessments include three major tasks:

- Continuously assess the enemy's reactions and vulnerabilities.
- Continuously monitor the situation and the progress of electronic warfare support of the operation towards the commander's desired end state.
- Evaluate EW against measures of effectiveness (MOE) and measures of performance (MOP).

Support of the Warfighting Functions

(U) To exercise electromagnetic spectrum (EMS) control, commanders effectively apply and integrate EW operations across the warfighting functions: mission command, movement and maneuver, intelligence, fires, sustainment, and protection.

Mission Command

(U) Mission command develops and integrates those activities enabling a commander to balance the art of command and the science of control. EW supports the mission command warfighting function by:

- Protecting mission command systems.
- Executing frequency deconfliction.
- Tracking assets.
- Controlling EW effects during execution.
- Improving input to the common operational picture.
- Integrating, coordinating, deconflicting, and synchronizing EW operations.
- Monitoring and assessing EW operations.
- Developing MOP and MOE.

Movement and Maneuver

(U) Movement and maneuver consists of the related tasks and systems that move and employ forces to achieve a position of relative advantage

over the enemy and other threats. Direct fire and close combat is inherent in maneuver. EW enables the movement and maneuver of Army forces by:

- Suppressing and destroying integrated air defense systems.
- Denying information systems and information collection sensors.
- Designating target and range finding.
- Protecting friendly forces from effects of enemy EW.
- Providing effects against enemy combat capabilities.
- Providing threat warning and direction finding.
- Countering improvised explosive devices (IEDs).

Intelligence

(U) Intelligence consists of the related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations. It includes the synchronization of collection requirements with the execution of tactical tasks such as reconnaissance, surveillance, and related intelligence operations. EW enables the intelligence warfighting function by:

- Increasing abilities to search for, intercept, identify, and locate.
- Increasing access for intelligence collection assets by reducing anti-access, antipersonnel, and anti-stealth systems.
- Increasing threat recognition and threat warning.
- Providing indications and warning.
- Denying and destroying threat information collection systems.

Fires

(U) Fires includes the related tasks and systems that provide collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process. The integration and synchronization of CEMA is a task of this warfighting function. EW supports the fires warfighting function by:

- Detecting and locating surface targets.
- Providing radio frequency countermeasures.
- Providing electromagnetic (EM) deception.
- Providing EM intrusion.

- Providing EM jamming.
- Disrupting enemy sensors and mission command nodes.
- Disrupting and degrading enemy infrastructure.
- Destroying targeted enemy systems.

Sustainment

(U) Sustainment involves the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. EW supports the sustainment warfighting function by:

- Protecting friendly forces from adversary use of EW.
- Enhancing electromagnetic environment situational awareness through the interception, detection, identification, and location of adversary electromagnetic emissions used to provide indications and warning.
- Countering IEDs to support ground lines of communications.
- Providing spectrum deconfliction and emissions control.

Protection

(U) Protection consists of the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission. EW enables the protection warfighting function by:

- Enhancing EMS situational awareness through the interception, detection, identification, and location of adversary electromagnetic emissions to provide indications and warning.
- Denying, disrupting, or destroying EMS-triggered IEDs and enemy air defense systems.
- Deceiving enemy forces.
- Providing EW countermeasures for platform survivability.
- Protecting friendly personnel, equipment, and facilities from enemy EA, including friendly information systems and information.

Endnotes

1. Army Techniques Publication (ATP) 3-36, *Electronic Warfare Techniques*, 16 DEC 2014, p. 2-1.

2. Ibid, p. 3-1.

3. Ibid.

4. Ibid.

Chapter 5

Cyberspace Operations

(U) Cyberspace operations is the use of cyberspace capabilities to achieve the commander's intent and objectives in or through cyberspace. This chapter provides an understanding of cyberspace functions, cyberspace layers, threats, targeting, and the cyber effects request format (CERF). This chapter describes offensive, defensive, and Department of Defense (DOD) information network (DODIN) operations, as well as the physical network, logical network, and cyber persona layers. It provides an understanding and awareness of cyber threats and cyber electromagnetic activities (CEMA) operation activities. This chapter also provides the CERF form used to initiate planning, target development, and the delivery of fires.

Offensive Cyberspace Operations

(U) Offensive cyberspace operations (OCO) are intended to project power by the application of force in or through cyberspace.[1] A cyberspace attack consists of actions that create various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.[2]

Defensive Cyberspace Operations

(U) Defensive cyberspace operations (DCO) are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Defensive cyberspace operation response actions are deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DOD cyberspace capabilities or other designated systems.[3]

(U) Internal defensive measures are those DCO that occur within the DODIN. (See Joint Publication [JP] 3-12 (R), *Cyberspace Operations*, for more information on the DODIN).[4] Internal defensive measures may involve counter reconnaissance measures within LandWarNet to locate internal threats and respond to unauthorized activity or alerts and threat information.[5]

LandWarNet

(U) LandWarNet is a subset of the DODIN that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide.

LandWarNet includes all Army automated information systems and networks, including stand-alone, stovepipe networks supporting intelligence, sustainment, medical, Army National Guard, and U.S. Army Reserve.

(U) LandWarNet guides the installation, management, and protection of communication networks and information services. This guidance supports strategic, operational, and tactical forces in the collection, processing, storage, discovery, and dissemination of information.

(U) Network transport is a system of systems including the people, equipment, and facilities that provide the end-to-end communications connectivity for network components. Network transport enables Army units and organizations to transmit and receive voice, video, and data. As the physical network layer of the Army's portion of cyberspace, network transport encompasses the integrated space, aerial, and terrestrial capabilities that provide access from Soldier and sensor through joint and strategic levels.

Layers of Cyberspace

(U) **Physical Network Layer.** The physical network layer uses logical constructs as the primary method of security and integrity. The physical network layer includes both geographic and physical network components. The geographic component is the location in land, air, maritime, or space where elements of the network reside. The physical network component is composed of the hardware, system software, and infrastructure (wired, wireless, cable link, electromagnetic spectrum (EMS) link, satellite, and optical) that support the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers).

(U) **Logical Network Layer.** The logical network layer consists of those elements of the network related to one another in a way that is abstracted from the physical network (i.e., the form or relationships are not tied to an individual, specific path, or node). An example of this layer could include website information located on several servers accessed by users through a single uniform resource locator.

(U) **Cyber-Persona Layer.** The cyber-persona layer is an abstraction of the logical network and uses the rules of the logical network layer to develop a digital representation of an individual or entity identity in cyberspace.

Threats in Cyberspace

(U) The Army faces multiple, simultaneous, and continuous threats in cyberspace. A threat is any combination of actors, entities, or forces that have the capability and intent to harm U.S. forces, national interests, or the homeland.[6] Threats include state-supported actors, nation-state

actors, noncombatants, transnational corporations, criminal organizations, terrorists, hacker unions, mischievous hackers, and unwitting individuals who intend no malice. The diversity of threats ensures disparate agendas, alliances, and range of capabilities. Enemies and adversaries employ regular and irregular forces and use an ever-changing variety of conventional and unconventional tactics. Risks from insiders may be malicious or cause damage unintentionally. Risks from insiders that stem from noncompliance with policies and regulations create risk by causing vulnerabilities to the network.

Targeting Activities for Cyberspace Operations

(U) Targeting is the process of selecting and prioritizing targets and matching the appropriate response, taking into consideration operational requirements and capabilities.[7] Targeting is an integrating and iterative process that occurs throughout the major activities. Targeting activities for cyberspace operations, which involve the employment of cyberspace capabilities, OCO in particular, closely follow standard targeting processes. The functions of decide, detect, deliver, and assess (D3A) functions that define the targeting process occur simultaneously and sequentially during the operations process.

Decide

(U) Decide is the first step in the targeting process and begins with the military decisionmaking process (MDMP). This step does not end when the plan is completed, but rather continues throughout the operation.

(U) Designating targets that reside within cyberspace and the EMS depends heavily on the intelligence collection effort. Each designated target and its required effect is assigned to OCO, electronic attack (EA) fires, traditional physical fires, or a combination of each, in accordance with their capabilities.[8]

(U) An important part of the decide step in the targeting process is identifying potential fratricide situations and providing electronic protection and DCO to mitigate those situations. This mitigation requires intense coordination and synchronization on the part of the CEMA element. The spectrum management operations (SMO) component of CEMA is leveraged to ensure that EA does not cause unwanted interference on friendly systems or degrade friendly networks.[9]

(U) **Note:** The targeting team does not develop EA targets separately, the EA plan is integrated into the standard targeting products: high-payoff target list (HPTL), attack guidance matrix (AGM), and electronic warfare (EW) annex. Intelligence preparation of the operational environment (IPOE) plays a large role in the decide phase: define OE, effects of OE, evaluate threat, and determine threat COAs.

"Decide" key considerations

(U) The following is a list of basic targeting questions that should be considered and updated as necessary during the decide process:

- What targets should be acquired?
- When and where are the targets likely to be found?
- How long will the target remain once acquired?
- Who or what can locate the targets?
- What are the priorities for surveillance, reconnaissance, and target acquisition objectives and asset allocation?
- What intelligence requirements are essential to the targeting effort?
- How and by when must the information be collected, processed, and disseminated?
- When, where, how, and with what priority should targets be attacked?
- What are the measures of performance (MOPs) and measures of effectiveness (MOEs) that determine whether the target has been successfully attacked?
- Have the commander's desired effects been generated by doing so?
- Who or what can attack the targets? How should the attack be conducted to generate desired effects?
- What are the required assets/resources based on commander's guidance?
- What or who will obtain assessment or other information required for determining the success or failure of each attack?
- Who must receive and process that information, how rapidly, and in what format?

- Who has the decision-making authority to determine success or failure, and how rapidly must the decision be made and disseminated?
- What actions will be required if an attack is unsuccessful and who has the authority to direct those actions?

Detect

(U) Detect is the next critical function in targeting. The G-2/S-2 is responsible for directing the effort to detect specified target nodes in cyberspace identified in the decide portion of the targeting process. The capabilities that provide situational understanding of cyberspace provide situational data in the form of network topology, configuration, and enemy and adversary actions and intentions. Capabilities that provide situational understanding of the EMS provide situational data in the form of geospatial location, signal strength, system type, and frequency of target to focus effects on the intended target.[10] The detect process includes tasks involving reconnaissance and surveillance in and through specific portions of cyberspace to locate, track, and validate target nodes for follow-on action by friendly forces.

(U) **Note.** Electronic support (ES) assets are deployed to detect HPTs. Effective EA depends heavily on ES assets to detect critical data such as location, signal strength, frequency, etc., in order to establish vulnerabilities that EA can attack.

"Detect" key considerations

(U) The following are factors to consider during the detect process:

- Aircraft operating bases and dispersal sites, location, status, and disposition to include:
  - Number and type of enemy aircraft operating from each base.
  - Enemy sortie generation capability from each base.
  - Enemy munitions located at each base.
  - Enemy missile systems location, status, and disposition to include:
    - Infrastructure, storage, and launching locations.
    - Enemy concept of employment.
    - Launch platforms.
    - Command and control (C2) nodes.

        - Enemy integrated air defense system order of battle to include:
            - Aircraft, surface-to-air missiles, airfields, anti-aircraft artillery.
            - C2 systems.
            - Communications links.
            - Support facilities.
            - Signals intelligence capabilities and EW assets.

- Sensor coverage requirements. Factors to consider include:
    - Enemy threat systems.
    - Threat locations.
    - Likely threat avenues of approach.
    - Threat altitude, radar cross-section, required detection range, and terrain.
    - Intelligence generated through reconnaissance and surveillance.
- Synchronization of reconnaissance and surveillance, linking acquisition assets to:
    - Find specific enemy formations.
    - Provide required information to answer the commander's information requirements.
    - Focal points.
    - Develop named areas of interest (NAIs) and target areas of interest (TAIs).
    - Integrate focal points into the collection management (CM) plan. The CM plan drives signals intelligence (SIGINT).

(U) During the detect process the SIGINT team performs two major collection activities:

- Signals intercepts (intercept and identify EM signals for immediate threat recognition)
    - Direction finding (approximation of the location of the threat's signals)

        - Movement of threat personnel
        - Locations of emitters associated with weapons systems
        - New and confirmed emitter locations
    - Friendly targets the threat might intend to attack

(U) SIGINT collection provides data on threat capabilities, disposition, composition, and intentions, as well as informing the targeting process.

Deliver

(U) Attack guidance for target nodes is initiated as a result of the detect process and executed as planned. Close coordination is required between those engaged in detecting targets and those engaged in delivering effects upon target nodes in designated cyberspace. Integration and synchronization is vitally important during the delivery function, as tailored cyberspace capabilities are employed and the possibility for unintended consequences exists.

(U) CEMA ensures the full coordination, integration, deconfliction, and employment of cyberspace operations and physical fires in accordance with the commander's time-phased scheme of maneuver. Close coordination between collecting assets (sensor) and other assets delivering fires (shooter) is critical during the engagement to avoid unintended effects.[11]

(U) **Note:** Execution of EA against targets is identified in the HPTL, AGM, and EW Annex. Synchronization of fires is accomplished through the AGM; Intelligence, Surveillance, and Reconnaissance; and EW Annex.

"Deliver" key considerations

(U) Delivery occurs primarily during execution and must satisfy attack guidance from the "decide" step of the targeting process.

(U) Offensive actions:

- Disrupt enemy counterattacks.
- Obscure enemy observation or screen friendly movement.
- Seal-off objective areas.
- Disrupt, destroy, or damage enemy defenses through preparation fire.

- Protect assaulting troops – planned targets destroy, neutralize, or suppress enemy communications and non-communications sensors.
- Target enemy reinforcements during attack.

(U) Defensive actions:

- Engage critical enemy elements before the attack.
- Plan effects against enemy indirect fire sensors attacking critical friendly elements.
- Apply constant pressure to enemy mission command structure; plan the acquisition and attack of HPTs throughout the battlefield.
- Integrate with lethal fires in synchronization with maneuver in the conduct of decisive and shaping operations.
- Plan counter-preparation effects to disrupt enemy preparations for an attack.
- Delay movement of reinforcements; disrupt the enemy's command, communications, and observation; and decrease the effectiveness of artillery preparation.
- Plan targets on avenues of approach to disrupt enemy attacks by striking the enemy during his assault.

Assess

(U) Assessment occurs throughout the operations process. Targeting in cyberspace is continuously refined and adjusted between the commander and staff during the operation. Assessment in cyberspace provides information on the effectiveness of the decide and detect functions and whether the target nodes need re-engaging.

(U) Execution of CEMA is often dependent on intelligence. Effects produced by CEMA are not always physically visible or apparent. The intelligence community operates many airborne and ground-based sensors that provide raw data. Intelligence is the primary contributor to the assessment of effects produced by CEMA on enemies and adversaries and their reactions to counter these effects. Intelligence allows for the adjustment of the targeting process. For more information on intelligence see Army Doctrine Publication (ADP) 2-0, *Intelligence*, 31 AUG 2012; Army Doctrine Reference Publication (ADRP) 2-0, *Intelligence*, 31 AUG 2012; Field Manual (FM) 2-0, *Intelligence Operations*, 15 APR 2014; and FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014.

(U) **Note.** Determination of the effectiveness during military operations involves three elements of assessment: munitions effectiveness assessment (MEA), battle damage assessment (BDA), and reattack recommendations.

"Assess" key considerations

(U) Key considerations during the assessment process include:

- MOPs and MOEs. (commander, staff, and fires cell at each echelon determine MOPs and MOEs during planning).
- Criterion assessing friendly actions that is tied to measuring task accomplishment.
- Criterion assessing changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.
- MEA and BDA.
- Reattack recommendation.

Endnotes

1. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 FEB 2016, p. 412.

2. FM 3-38, *Cyber Electromagnetic Activities,* 12 FEB 2014, p. 31.

3. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 FEB 2016, p. 63.

4. JP 3-12 (R), *Cyberspace Operations*, 5 FEB 2013, p. II-3.

5. FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014, p. 3-6.

6. ADRP 3-0, *Unified Land Operations*, 16 MAY 2012, p. GL-6.

7. JP 3-0, *Joint Operations*, 11 AUG 2011, p. GL-17.

8. FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014, p. 6-12.

9. Ibid.

10. Ibid.

11. Ibid.

Appendix A

Friendly Electronic Warfare Equipment

(U) This appendix provides information on Army and other Service electronic warfare (EW) capabilities. It is not an all-inclusive list, due to the evolving nature of EW equipment and systems. This information is perishable and should be augmented, updated, and maintained by the unit EW officer.

(FOUO) **Airborne electronic attack** is an EW capability that delivers electronic attack from aerial platforms. Although some of these platforms are organic to the Army, much of the capability resides in other Services creating a truly joint operation. Effective airborne electronic attack requires good integrating procedures and communications between the EW element and the airborne electronic attack asset owner.[1]

(FOUO) Figure A-1 depicts the following airborne electronic attack platforms:

- EC-130H Compass Call
- EC-130J Commando Solo
- EA-6B Prowler
- EA-18G Growler

EC 130H Compass Call

Performance
Branch: Air Force
# of Airframes: 14
Crew: 13
Maximum Speed: 300 mph
Range: 1.9K nm (2,295 miles)
Ceiling: 25,000 ft
Communications: HF, VHF, UHF, SATCOM, HAVE QUICK
Mission: EA, SEAD, Offensive Counterinformation
Armament
Hardpoints: 2
Nonkinetic Energy Waveforms

EC 130J Commmando Solo

Performance
Branch: Air Force
# of Airframes: 3
Crew: 5
Maximum Speed: 416 mph
Range: 4,173 nm (4,803 miles)
Ceiling: 28,000 ft
Communications: HF, VHF, UHF, SATCOM, HAVE QUICK
Mission:
IO, MISO, CA in AM, FM, HF, TV, and military bands
Armament: N/A

Airborne Electronic Attack Platforms

EW Aviation

EA-6B Prowler

Performance
Branch: Navy
# of Airframes: 55
Crew: 4
Maximum Speed: 566 knots (651 mph)
Range: 1,757 nm (2,022 miles)
Ceiling: 37,730 ft
Communications: HF, VHF (AM/FM), UHF, HAVE QUICK, SINCGARS
Mission: SEAD, SOJ
Armament
Hardpoints: 5
AN/ALQ-99 Tactical Jamming System
AN/USQ-218 Tactical Jamming System Receiver
AN/USQ-113 Communications Jamming System
AN/ALE-43(V) Bulk Chaff Dispensing System Pod
2 x U.S. 300-gallon fuel tanks
4 x AGM-88 HARM

EA-18G Growler

Performance
Branch: Navy
# of Airframes: 108
Crew: 2
Maximum Speed: Mach 1.8 (1,190 mph)
Range: 1,266 nm (1,458 miles)
Ceiling: 50,853 ft (15,500 meters)
Communications: VHF (AM/FM), UHF
Mission: SEAD, SOJ
Armament
Hardpoints: 11
AN/ALQ-218 Detection Pods (wingtips)
AN/ALQ-99 High Band Jamming Pods
AN/ALQ-99 Low Band Jamming Pods
2 x 480 U.S. gallon fuel drop tanks
2 x AGM-88 HARM
2 x AIM-120 AMRAAM
2 x AGM-154 JSOW

(FOUO) Figure A-1. Airborne Electronic Attack Platforms

(FOUO) **Intelligence, surveillance, and reconnaissance (ISR).** An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing; exploitation; and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.[2]

(FOUO) Figure A-2 depicts the following airborne ISR platforms:

- U-2
- Joint Surveillance Target Attack Radar System (JSTARS)
- RC-135 Rivet Joint
- EC-130E Senior Scout

U-2

Performance
Branch: Air Force
# of Airframes: 36
Crew: 1
Maximum Speed: 475 mph
Range: 6,082 nm (7,000 miles)
Ceiling: 84,974 ft
Communications: HF, VHF, UHF
Mission: EO/IR and wet film imagery, SIGINT, MTI, MASINT
Armament: N/A
Nonkinetic Energy Waveforms

JSTARS

Performance
Branch: Air Force
# of Airframes: 17
Crew: 4-18
Maximum Speed: 587 mph
Range: 9 hours
Ceiling: 42,000 ft
Communications: HF, VHF, UHF, SATCOM, HAVE QUICK
Mission: Radar ground tracking/surveillance/ C2
Armament: N/A

Airborne ISR Platforms

Military Intelligence Aviation

Surveillance Aviation

Command and Control Aviation

RC-135 Rivet Joint

Performance
Branch: Air Force
Crew: 4-19
Maximum Speed: 580 mph
Range: 2,900 nm (3,450 miles)
Ceiling: 50,000 ft
Communications: HF, HAVE QUICK (clear), VHF, UHF, SATCOM (clear/secure), Datalink, IBS-I, IDM, Secret/SCI chat
Mission: ISR
Armament: N/A

EC-130E Senior Scout

Performance
Branch: Air Force
# of Shelters/Containers: 3
Maximum Speed: 410 mph
Range: 2,300 nm (2,646 miles)
Ceiling: 28,000 ft
Comms: HF, UHF, VHF, SATCOM
Mission: SIGINT
Armament: N/A

(FOUO) Figure A-2. Airborne ISR Platforms

(FOUO) **Signals intelligence (SIGINT)** is intelligence gained by exploiting an adversary's use of the electromagnetic spectrum (EMS) with the aim of gaining undetected firsthand intelligence on the adversary's intentions, dispositions, capabilities, and limitations.

(FOUO) Figure A-3 depicts the following airborne and ground-based SIGINT platforms:

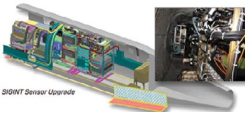
- Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS)
- RC-12X Guardrail Aerial Common Sensor
- Green Dart
- Prophet

EMARSS

Performance
Branch: Army
# of Airframes: 15
Crew: 3-6
Maximum Speed: 360 mph
Range: 1,089 miles
Ceiling: 35,000 ft
Communications: UHF, VHF, HF, INMARSAT
Mission: SIGINT, EO/IR imagery, FMV
Armament: N/A

RC-12X Guardrail Aerial Common Sensor

Performance
Branch: Army
# of Airframes: 14
Crew: 1-5
Maximum Speed: 300 mph
Range: 215 miles
Ceiling: 35,105 ft
Communications: VHF, UHF, AM/FM, SSB, Continuous Wave, FDM
Mission: SIGINT
Armament:
N/A



Signals Intelligence Platforms

Signals Intelligence

Green Dart

Performance
Branch: Army
# of Airframes: 15
Crew: Unknown
Maximum Speed: Unknown
Range: Unknown
Ceiling: Unknown
Communications: Unknown
Mission: ISR
Armament: N/A

Prophet

Performance
Branch: Army
# of Platforms: 83
Platforms: Prophet Control, Prophet Air, Prophet Ground (mounted and dismounted)
Crew: Dependent on use of system
Maximum Speed: N/A
Range: 150 km wide by 120 km deep
Communications: N/A
Mission: Signal Intercept and DF in the 20-20,000 MHz frequency range providing signal characteristics and LOB data on SOIs
Armament: N/A

(FOUO) Figure A-3. Airborne and Ground-Based SIGINT Platforms

(FOUO) **Airborne early warning (AEW)** is the detection of enemy air or surface units by radar or other equipment carried in an airborne vehicle and the transmitting of a warning to friendly units.[3]

(FOUO) Figure A-4 depicts the following AEW platforms:

- E-2 Hawkeye
- E-3 Sentry Airborne Warning and Control System (AWACS)

E-2 Hawkeye

Performance
# of Airframes: 75
Crew: 5
Maximum Speed: 375 mph
Range: 1,394 nm (1,605 miles)
Ceiling: 30,807 ft
Communications: HF, VHF-AM, VHF
Mission: Airborne C2, Battle space management
Armament: N/A

E-3 Sentry AWACS

Performance
# of Airframes: 68
Crew: 4-19
Maximum Speed: 530 mph
Range: 3,995 nm (4,598 miles)
Ceiling: 41,000 ft
Communications: HF, VHF-AM, VHF
Mission: Airborne C2, Aircraft control and deconfliction
Armament: N/A

Airborne Early Warning Platforms

Surveillance Aviation

C2

Command and Control Aviation

(FOUO) Figure A-4. AEW Platforms

(FOUO) **Unmanned aircraft systems (UAS).** One technology that has seen the greatest expansion of research, development, and fielding activity in recent years is UAS. According to the International Institute for Strategic Studies there are currently over 800 UAS in use today. This number is projected to see steady growth as users seek the versatility, robustness, and feasibility of UAS. Reasons for the expanded use of UAS are that these systems can extend our vision and reach over any terrain, against any force, with fewer restrictions, dangers, and support requirements than manned aircraft systems. Since UAS are unmanned, they can go into areas where risk to crews might hinder a mission.[4]

(FOUO) Figure A-5 depicts the following UAS platforms:

- MQ-1 Predator
- MQ-9 Reaper (Predator B)
- Avenger (Predator C)
- Guardian

(FOUO) Figure A-6 depicts the following UAS platforms:

- RQ-20 Puma
- RQ-4 Global Hawk
- AAI RQ-7 Shadow
- RQ-170 Sentinel

(FOUO) Figure A-7 depicts the following UAS platforms:

- RQ-5 Hunter
- MQ-1C Gray Eagle

MQ-1 Predator

Performance
# of Airframes: 360
Crew: 3
Maximum Speed: 135 mph
Range: 454 miles
Ceiling: 25,000 ft
Mission: Unarmed reconnaissance or missile armed hunter
Armament:
2 x AGM-114 Hellfire laser-guided anti-tank missiles or 2 x AIM-92 Stinger short-range anti-aircraft missiles

MQ-9 Reaper (Predator B)

Performance
# of Airframes: 33
Crew: 3
Maximum Speed: 230 mph
Range: 3,682 miles
Ceiling: 50,000 ft
Mission: Armed reconnaissance
Armament:
2 x AGM-114 Hellfire anti-tank missiles
2 x GBU-12 JDAM
2 x GBU-38 JDAM

Unmanned Aircraft Systems

Unmanned Aircraft System

Unmanned Aircraft System Fixed Wing

Avenger (Predator C)

Performance
# of Airframes: 4
Crew: 3
Maximum Speed: 463 mph
Range: Undetermined
Ceiling: 60,000 ft
Mission: Intelligence gathering, target identification, and reconnaissance
Armament:
Will be held in an internal weapons bay. AGM-114 Hellfire anti-tank missile, GBU-24 Paveway III guided bomb, GBU-31 JDAM guided bomb, GBU-38 Small diameter bomb

Guardian

Performance
# of Airframes: 2
Crew: 0
Maximum Speed: 298 mph
Range: 1,150 miles
Ceiling: 49,869 ft
Mission: Surveillance, intelligence gathering, and reconnaissance
Armament: N/A

(FOUO) Figure A-5. Unmanned Aircraft Systems

RQ-20 Puma

Performance
# of Airframes: 1,000
Crew: 2
Maximum Speed: 52 mph
Range: 9 miles
Ceiling: 499 ft
Mission: Intelligence, surveillance, reconnaissance, and targeting (ISRT)
Armament: N/A

RQ-4 Global Hawk

Performance
# of Airframes: 47
Crew: N/A
Maximum Speed: 404 mph
Range: 13,809 miles
Ceiling: 65,000 ft
Mission: Intelligence gathering, target identification, and reconnaissance
Armament: N/A

Unmanned Aircraft Systems

Unmanned Aircraft System

Unmanned Aircraft System Fixed Wing

AAI RQ-7 Shadow

Performance
# of Airframes: 88
Crew: N/A
Maximum Speed: 129 mph
Range: 48 miles
Ceiling: 14,993 ft
Mission: Target acquisition/reconnaissance and surveillance
Armament: N/A

RQ-170 Sentinel

Performance
# of Airframes: 20
Crew: N/A
Maximum Speed: Classified
Range: Classified
Ceiling: 49,213 ft
Mission: Reconnaissance and surveillance of enemy elements
Armament: N/A

(FOUO) Figure A-6. Unmanned Aircraft Systems

RQ-5 Hunter

Performance
# of Airframes: 13
Crew: 2
Maximum Speed: 127 mph
Range: 162 miles
Ceiling: 15,000 ft
Mission: Observation and reconnaissance providing real-time imagery, target acquisition, artillery adjustment, and general surveillance of the battlefield
Hardpoints: 0
Armament:
Observation, communications, and countermeasures equipment

MQ-1C Gray Eagle

Performance
# of Airframes: 61
Crew: 3
Maximum Speed: 155 mph
Range: Unknown
Ceiling: 29,003 ft
Mission: Intelligence gathering, target identification, and reconnaissance
Hardpoints: 4
Armament:
Any combination of the following:
4 x Hughes AGM 114 Hellfire anti-tank missiles
8 x AIM-92 Stinger short-range anti-aircraft missiles
4 x GBU-44B Viper Strike guided bombs

Unmanned Aircraft Systems

Unmanned Aircraft System

Unmanned Aircraft System Fixed Wing

(FOUO) Figure A-7. Unmanned Aircraft Systems

(FOUO) **Counterfire radar.** The counterfire radar capability of detecting, tracking, classifying, and identifying aerial objects (including manned and unmanned aircraft; ballistic and cruise missiles; and rocket, artillery, and mortar projectiles) is a core competency of the fires warfighting function. The continuous growth of UAS, both friendly and threat, further justifies the need for airspace coverage.

(FOUO) Figure A-8 depicts the following counterfire radar systems:

- AN/TPQ-36
- AN/TPQ-37
- AN/TPQ-53

AN/TPQ-36

Capabilities:
- Locates mortars, artillery, and rocket launchers
- Locates 10 weapons simultaneously
- Locates targets on first round
- Interfaces with tactical fire
- Predicts impact of hostile projectiles

Specifications:
Setup Time: 15 minutes
Location: 3-6 km behind FLOT
Maximum Range: 24 km
Effective Range:
Mortar: 18 km
Artillery: 14.5 km
Rockets: 24 km
Azimuth Sector: 90°
Frequency: X-band, 32 frequencies
Prime Power: 115/200 VAC, 400 Hz, 3-phase, 8 kW
Features: Permanent storage for 99 targets, digital data interface, remote operations

AN/TPQ-37

Capabilities:
- Locates mortars, artillery, and rocket launchers
- Locates 10 weapons simultaneously
- Locates targets on first round
- Interfaces with tactical fire
- Predicts impact of hostile projectiles

Specifications:
Setup time: 30 minutes
Location: 8-12 km behind FLOT
Maximum Range: 50 km
Effective Range:
Mortar: 30 km
Rockets: 50 km
Azimuth Sector: 90°
Frequency: S-band, 15 frequencies
Prime Power: 115/200 VAC, 400 Hz, 3-phase, 43 kW
Features: Permanent storage for 99 targets, digital data interface

Counterfire Radar

RADAR

AN/TPQ-53

Capabilities:
- Locates mortars, artillery, and rocket launchers
- Locates 10 weapons simultaneously
- Locates targets on first round
- Interfaces with tactical fire
- Predicts impact of hostile projectiles

Specifications: 2 vehicles needed to operate
Setup Time: 5 minutes
Take Down: 2 minutes
Location: 8-12 km behind FLOT
Maximum Range: 60 km
Effective Range:
Mortar: 30 km
Artillery: 20 km
Rockets: 60 km
Azimuth Sector: 90°, 360°
Frequency: S-band

(FOUO) Figure A-8. Counterfire Radar Systems

(FOUO) **Tactical Internet (TI) and wireless communications systems.** The electromagnetic environment (EME) is described as the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic (EM) emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. EME is the sum of electromagnetic interference; electromagnetic pulse; hazards of EM radiation to personnel, ordnance, volatile materials; and natural phenomena effects of lightning and precipitation static. Essentially, the EME is the global EM background.

Upper TI lists

Army Battle Command Systems (ABCS):

- Command Post of the Future (CPOF)/Mission Command Information Systems (MCIS)
- Distributed Common Ground System-Army (DCGS-A)
- Advanced Field Artillery Tactical Data System (AFATDS)
- Battle Command Sustainment Support System (BCS3)
- Tactical Airspace Integration System (TAIS)
- Air and Missile Defense Workstation (AMDWS)
- SECRET Internet Protocol Router Network (SIPRNET)
- Nonsecure Internet Protocol Router Network (NIPRNET)

Standard Army Management Information System (STAMIS):

- Combat Service Support (CSS) Automated Information Systems Interface (CAISI)
- CSS SATCOM Very Small Aperture Terminal (VSAT),
- Medical Communications for Combat Casualty Care (MC4)
- Property Book Unit Supply Enhanced (PBUSE)
- Standard Army Maintenance System-Enhanced (SAMA-E)
- Transportation Coordinators' Automated Information for Movements System II (TC-AIMS II)

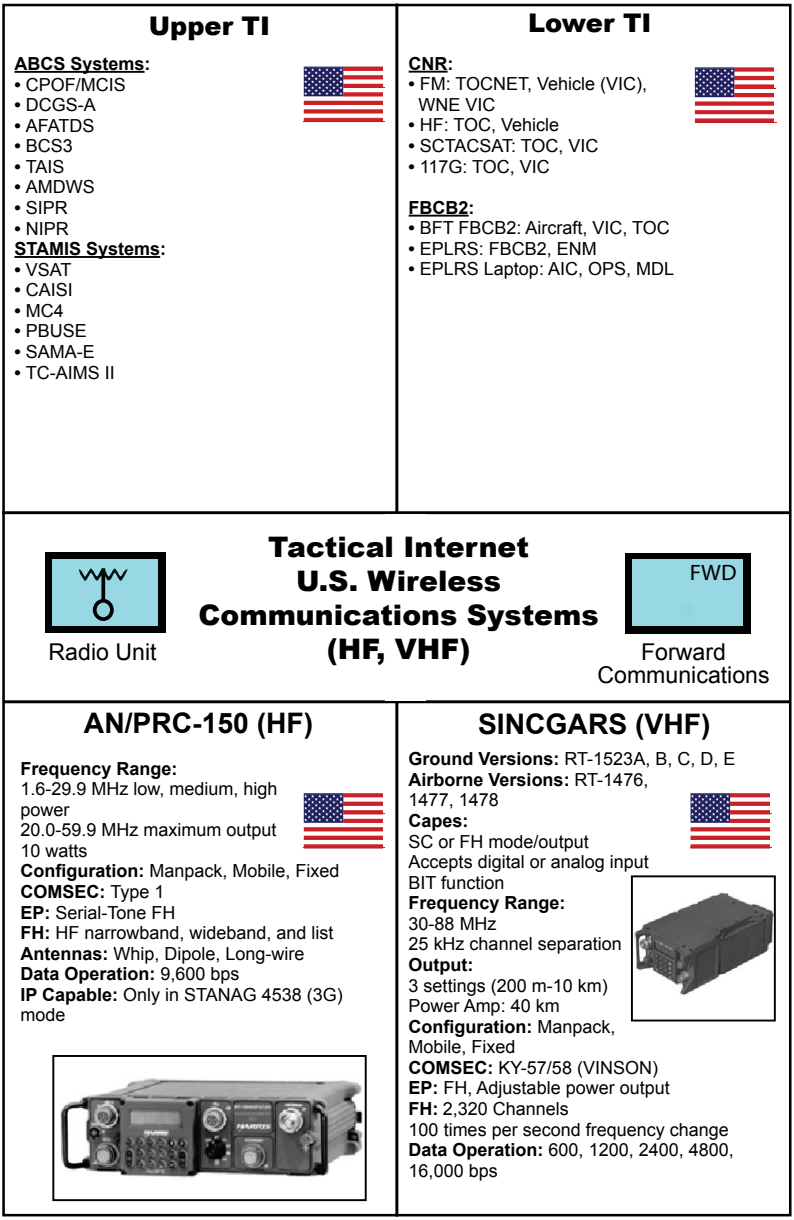
Lower TI lists

Combat Net Radio (CNR) and Force XXI Battle Command—Brigade and Below (FBCB2)

AN/PRC-150 (HF)

Single-Channel Ground and Airborne Radio System (SINCGARS) (VHF)

(FOUO) Figure A-9 depicts TI and wireless communications equipment.



(FOUO) Figure A-9. Tactical Internet and U.S. Wireless Communications Systems (HF, VHF)

(FOUO) The goal of tactical spectrum operations is to control the electromagnetic spectrum so that it serves the needs of friendly forces while denying use to the enemy so that he is unable to command, control, or otherwise employ his forces effectively.

(FOUO) Figure A-10 provides examples of VHF and UHF equipment:

- AN/PRC-148 Multiband Inter/Intra Team Radio (MBITR)
- AN/PRC-152
- FBCB2
- Enhanced Position Location Reporting System (EPLRS).

(FOUO) Figure A-11 provides examples of UHF equipment:

- Blue Force Tracker
- AN/VRC-108, Near-term Digital Radio (NTDR)
- Tactical Digital Information Link J (TADIL-J)
- Joint Tactical Information Distribution System (JTIDS)

(FOUO) Figure A-12 provides examples of single-channel tactical satellite (SC TACSAT) equipment:

- Lightweight Satellite Transceiver (LST)-5B, 5C, 5D
- AN/PSC-11
- AN/PSC-5, Spitfire

(FOUO) Figure A-13 provides examples of TACSAT and airborne radio equipment:

- AN/PSC-5I and AN/PSC-5D
- AN/PRC-117F, G
- AN/ARC-231
- AN/ARC-164

(FOUO) Figure A-14 provides examples of TACSAT and airborne radio equipment:

- AN/ARC-210
- AN/ARC-220
- AN/VRC-83
- AN/ARC-186

AN/PRC-148 MBITR (VHF)

Frequency Range: 30-512 MHz, 0.1-5 watts
Configuration: Handheld
Capes:
Operates in clear (analog) and secure (digital)
Stores up to 100 channels
SINCGARS, HAVE QUICK I/II, and ANDVT interoperable
Data Operations: 12-16 kbps
COMSEC: KYK-13, KYX-15, KOI-18, AN/CYZ10

AN/PRC-152 (VHF)

Frequency Range:
VHF Low Band: 30.0-89.9 MHz
VHF High Band: 90.0-224.9 MHz
UHF Band: 225-511.9 MHz
Configuration: Handheld
Capes:
SC multiband radio
SINCGARS, HAVE QUICK II, VHF/UHF AM and FM interoperable
Data Operations: 16 kbps
COMSEC: KY-57/ VINSON, ANDVT/KYV-5, KG-84C, DS-101, DS-102

U.S. Wireless Communications Systems (VHF, UHF)

Radio Unit

FWD

Forward Communications

FBCB2 (UHF)

(Force XXI Battle Command Brigade and Below)

Capes:
Automatically disseminates COFOR locations, reported enemy locations, and graphics
Configuration:
Computers
GPS equipment
Communication systems
Communications:
Terrestrial (EPLRS)
Satellite (BFT)

EPLRS (UHF)

(Enhanced Position Location Reporting System)

Capes:
Alternate data communications link between C2 platforms at brigade and battalion level
Primary data communications link between company/platoon platforms
3-10 km between each radio
Frequency Range: 420-450 MHz
FH: 512 times per second
COMSEC: TRANSEC
Configuration:
Manpack,
Surface VIC radio set,
Airborne radio set, Grid reference radio set

(FOUO) Figure A-10. U.S. Wireless Communications Systems (VHF, UHF)

BFT (UHF)
(Blue Force Tracker)

Frequency Range:
L-band SATCOM
Capes:
GPS enabled tracking of COFOR
Population of data amongst all users
Detailed information up to 5,000 miles
Configuration:
Computer hardware and software
Interconnecting cables
L-band satellite transceiver
PLGR
Mission data loader

No photo available

AN/VRC-108, NTDR (UHF)

Capes:
10-20 km range
Incorporates GPS to provide MGRS position
Frequency Range:
225-450 MHz
Configuration (typically):
Battle command VIC
C2 vehicles
Selected M1068 TOC and TAC platforms
UH-60 helicopters equipped with A2C2S
EP: Sequence spreading at a chip rate of 8 MHz
Data Operation: 288 kbps

U.S. Wireless Communications Systems (UHF)

Radio Unit

Forward Communications

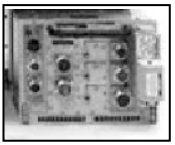
TADIL J (UHF)
(Tactical Digital Information Link J)

Configuration:
Uses EPLRS for data distribution
Capes:
Near equivalent to Link 16
Protocol for joint (U.S. only) AMDS and battle management
Communications, navigation and ID system
FH: Secure, FH, jam-resistant, high-capacity link
Users of TADIL J:
FA-19
AWACS
E-2C
SHORAD
Patriot
AMDC
JTAGS

No photo available

JTIDS (UHF)
(Joint Tactical Information Distribution System)

Frequency Range: 960-1215 MHz
Configuration:
Class 2M terminal, terminal controller, antenna; Uses tactical datalink to provide secure, jam-resistant, high-capacity interoperable voice and data communications for tactical platforms and weapon systems; Army uses as the medium to defense broadcast and receive an enhanced joint air picture



(FOUO) Figure A-11. U.S. Wireless Communications Systems (UHF)

SC TACSAT Introduction

Operates in the UHF band
No planning range required
Depends on LOS and satellite location
Provides half duplex operations
56 kbps on 25 kHz wideband channels
9.6 kbps on 5 kHz narrowband channels
Limited resources for SC TACSAT
DAMA Networks:
Matches users demands to available satellite time
RTO does not notice a difference
Increases satellite by 4-20 times

LST-5B, 5C, 5D (VHF, UHF)

Capes:
Modulate in AM and FM voice, cipher, data, and beacon
Frequency Range:
225-399.995 MHz
5 kHz and 25 kHz channel spacing
Configuration:
Manpack
Vehicle
Shipboard
Airborne
EP: Embedded encryption for voice and data
Data Operation: 16 kbps

Single-Channel Tactical Satellite

Radio Unit

Tactical Satellite Radio Unit

AN/PSC-11 (SHF, EHF)

Capes:
Single-channel anti-jam man-portable terminal
Must establish the satellite path prior to use
Point-to-point or Broadcast
Provides range extension to the SINCGARS
Frequency Range:
Uplink, 43.5-45.5 GHz (Q Band)
2 GHz bandwidth
Configuration:
Manpack
EP: Embedded COMSEC
Data Operation: 24 kbps

AN/PSC-5, Spitfire (HF-UHF)

Capes:
Operates in SATCOM and DAMA modes
Half duplex operation
Capable of scanning five presets in PT voice or CT voice
Provides range extension for SINCGARS
Frequency Range:
30-87.995 MHz
108-129.995 MHz
130-148.995 MHz
156-173.995 MHz
225-399.995 MHz
5 kHz channel spacing
Configuration:
Manpack
EP: Embedded COMSEC
Data Operation: 16-24 kbps (depending on mode)

(FOUO) Figure A-12. Single-Channel TACSAT

AN/PSC-5I

Shadowfire (HF-UHF)
Upgrade to the Spitfire

Additional Capes:
HAVE QUICK I and II
SINCGARS anti-jam
30-420 MHz frequency range

AN/PSC-5D (HF- UHF)

Upgrade to the Shadowfire

30-512 MHz frequency range

AN/PRC-117F, G (HF-UHF)

Capes:
LOS
SATCOM
ECCM
FH (SINCGARS and HAVE QUICK)
Frequency Range:
30-512 MHz
VHF Low band: 30-89.9
VHF High band: 90-224.9
UHF band: 225-511.9
UHF SATCOM: 243-270 MHz,
292-318 MHz
Configuration:
Manpack
Vehicle
EP: COMSEC fills TEKs, TSKs, KEKs

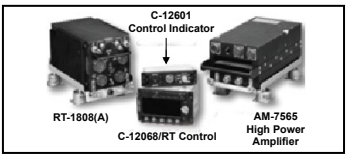
Single-Channel Tactical Satellite Airborne Radios

Radio Unit

Tactical Satellite Radio Unit

AN/ARC-231 (HF-UHF)

Capes:
HAVE QUICK I/II and SINCGARS modes
DAMA and SATCOM modes
Used in A2C2S to provide C2 mission capabilities to Corps, Division maneuver brigades, and tactical command posts
Frequency Range:
30-511.995 MHz
Channel Spacing:
8.33 kHz
Configuration:
Airborne
EP: Embedded COMSEC



AN/ARC-164 (UHF)

Capes:
Operates in SC or FH mode
Provide anti-jam, secure communications links for the JTF and Army aviation missions
7,000 channel capacity
UHF-AM mode
Frequency Range:
225-399.975 MHz
Configuration:
Airborne x 3
Ground x 1
EP: Embedded COMSEC

(FOUO) Figure A-13. Single-Channel TACSAT/Airborne Radios

AN/ARC-210 (VHF, UHF)

Capes:
Operates in SC and FH
Frequency Range:
30-512 MHz
121.5 and 243 MHz guard channels
Channel Spacing:
25 kHz (30-512 MHz)
8.33 kHz (118-137 MHz)
12.5 kHz (400-512 MHz)
Configuration:
Airborne
EP: Embedded COMSEC
Data Operation:
80 kbps (SATCOM)
100 kbps (LOS)

AN/ARC-220 (MF, HF)

Capes:
Operates in SC and FH
Frequency Range:
2-29.9 MHz
Channel Spacing:
100 Hz steps
Configuration:
Airborne
EP: Anti-jam functions

Airborne Radios

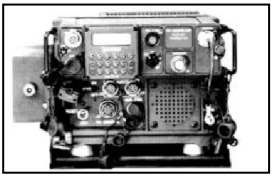
Radio Unit

FWD

Forward Communications

AN/VRC-83 (VHF, UHF)

Capes:
Two band VHF AM and UHF AM
Short-range air-to-air and air-to-ground communications
Frequency Range:
VHF: 116-149.975 MHz; 1,360 channels
UHF: 225-399.875; 7,000 channels
Channel Spacing:
25 kHz
Configuration:
Airborne
EP: Embedded COMSEC



AN/ARC-186 (VHF)

Capes:
Used primarily as an administrative VHF AM/FM radio to communicate with the ATC;
Used as a secondary means of secure communications to overcome SINCGARS and HAVE QUICK II LOS constraints
Frequency Range:
AM Tx/Rx: 116-151.975
AM Rx: 108-115.975
FM Tx/Rx: 30-87.975
Channel Spacing:
25 kHz
20 channels
Configuration:
Airborne
EP: Embedded COMSEC

(FOUO) Figure A-14. Airborne Radios

Endnotes

1. Army Techniques Publication, *Electronic Warfare Techniques*, 16 DEC 2014, p. 3-4.

2. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 FEB 2016, p. A-39.

3. Ibid, p. 5.

4. Training and Doctrine Command G-2 Intelligence Support Activity (TRISA) World Equipment Guide Volume Two, *Airspace and Air Defense Systems*, AUG 2014, p. 4-1.

Appendix B

Electronic Warfare Threat Systems

(U) This appendix provides information on electronic warfare (EW) threat capabilities. It is not an all-inclusive list due to the evolving nature of EW equipment and systems. This information is perishable and should be augmented, updated, and maintained by the unit EW officer.

Electronic Warfare Threat Equipment

(FOUO) The following figures depict surface-to-air missile (SAM) launcher systems that are known to be used by adversaries as EW threat capabilities.

(FOUO) Figure B-1 depicts the following SAM launcher systems: the SA-2/ GUIDELINE; SA-3/GOA, Pechora-2M; SA-4b/GANEF; and the SA-5/ GAMMON.

(FOUO) Figure B-2 depicts the SA-6/ GAINFUL, SA-8b/GECKO, SA-9/ GASKIN, and the SA-10b/GRUMBLE.

(FOUO) Figure B-3 depicts the SA-10c/GRUMBLE, SA-12a/ GLADIATOR, SA-12b/GIANT, and the SA-20a/GARGOYLE.

(FOUO) Figure B-4 depicts the SA-20b/Favorit, SA-21a/GROWLER, SA-11/GLADFLY, and the SA-13b/GOPHER.

(FOUO) Figure B-5 depicts the SA-15b/ GAUNTLET, SA-17/ GRIZZLY, French Crotale 5000/Chinese FM-90, and the European Crotale (New Generation).

SA-2/GUIDELINE

Performance
Missile: GUIDELINE
Range: 18.8 nm (35 km)
Maximum Altitude: 16.1 nm (30 km)
Minimum Altitude: 100 m
FC Radar: FAN SONG
Frequency: E, F, G Bands (2-6 GHz)
Range: 64.7 nm (120 km)
TA/EW Radar: SPOONREST
Frequencyuency: A, B Bands (.2-.5 GHz)
Range: 148 nm (275 km)
HF Radar: SIDE NET
Frequency: E Band (2-3 GHz)
Range: 97 nm (180 km)
EW Radar: KNIFE REST
Frequencyuency: A Band (.03-.3 GHz)
Range: 199 nm (370 km)

Targets: FW, RW, Cruise Missile
Combat Load: One missile (six launchers per battery)
Notes: The SA-2/GUIDELINE is a two-stage medium- to high altitude, radar-tracking SAM. It is fired from a single-rail ground-mounted launcher that can be moved by a truck. Limitations include limited effectiveness against updated ECM, restricted mobility, and limited effectiveness against low-altitude targets.
Proliferation: Azerbaijan, Bulgaria, China, Cuba, Egypt, Iran, Kyrgyzstan, Libya, Mongolia, Burma, North Korea, Pakistan, Romania, Sudan, Syria, Tajikistan, Vietnam, Yemen, Zimbabwe

SA-3/GOA, Pechora-2M

Performance
Missile: Pechora
Range: 13.4 nm (25 km)
Maximum Altitude: 9.7 nm (18.3 km)
Minimum Altitude: 1.5 nm (2.4 km)
FC Radar: LOW BLOW
Frequency: I Band (8-10 GHz)
Range: 59.3 nm (110 km)
TA Radar: FLAT FACE
Frequencyuency: C Band (.5-1 GHz)
Range: nm (250 km)
TA Radar: SQUAT EYE
Frequency: C Band (.5-1 GHz)
Range: 69.1 nm (128 km)

Targets: FW, RW, Cruise Missile,
Combat Load: Two or four missiles depending on variant
Notes: The SA-3/GOA is a two-stage, low- to medium-altitude SAM. Two ready missiles travel in tandem on a modified truck or tracked vehicle from which the crew loads the missiles onto a ground-mounted, trainable launcher for firing. The SA-3 is not mobile. It is movable, with considerable displacement time. Pechora-2M is a highly mobile system and is picking up sales.
Proliferation: Azerbaijan, Bulgaria, China, Cuba, Egypt, Iran, Kyrgyzstan, Libya, Mongolia, Burma, North Korea, Pakistan, Romania, Sudan, Syria, Tajikistan, Vietnam, Yemen, Zimbabwe

SAM Launcher Systems

Air Defense Missile

SA-4b/GANEF

Performance
Missile: GANEF
Range: 26.9 nm (50 km)
Maximum Altitude: 12.9 nm (24.5 km)
Minimum Altitude: 150 m
Missile Guidance: PAT HAND
Frequency: H Band (6-8 GHz)
Range: 70.1 nm (130 km)
TA Radar: LONG TRACK
Frequency: E Band (2.6 GHz)
Range: 80.9 nm (150 km)
HF Radar: THIN SKIN
Frequency: H Band (6-8 GHz)
Range: 129 nm (240 km)

Targets: FW, RW, Cruise Missile
Combat Load: Two missiles
Notes: A variety of more modern automated control complexes, such as Polyana, can be used to upgrade the system and process data more rapidly. Batteries may use a mix of SA-4a and SA-4b missiles to maximize range, altitude, and guidance modes available, while reducing dead space.

SA-5/GAMMON

Performance
Missile: GAMMON
Range: 134 nm (250 km)
Maximum Altitude: 15.6 nm (29 km)
Minimum Altitude: 300 m
FC Radar: SQUARE PAIR
Frequency: H Band (6.62-6.94)
Range: 188 nm (350 km)
TA Radar: BAR LOCK B
Frequency: E Band (2-2.5 GHz)
Range: 210 nm (390 km)
EW Radar: TALL KING
Frequency: A Band (150-180 MHz)
Range: 323 nm (600 km)

Targets: FW, Cruise Missile
Combat Load: One missile
Notes: The SA-5/GAMMON is a long-range, strategic, semi-active guided missile system for targeting medium-to-high altitude high-speed aircraft.

(FOUO) Figure B-1. SAM Launcher Systems

SA-6/GAINFUL

Performance
Missile: GAINFUL
Range: 13.4 nm (25 km)
Maximum Altitude: 7.5 nm (14 km)
Minimum Altitude: 30 m
FC Radar: TV
Range: 16.1 nm (30 km)
TA Radar: STRAIGHT FLUSH
Frequency: G, H, I (4-10 GHz)
Range: 48.5 nm (90 km)
EW Radar: LONG TRACK
Frequency: E Band (2.6 GHz)
Range: 91 nm (167 km)
HF Radar: THIN SKIN
Frequency: H Band (6-8 GHz)
Range: 129 nm (240 km)
Targets: Low- to medium-altitude FW and RW
Combat Load: 3 missiles
Notes: Two or more battery missiles may be launched at a target during an engagement. Has radio-command guidance with semi-active radar terminal homing. The associated STRAIGHT FLUSH fire control/target acquisition radar vehicle uses the same chassis as the SA-6a TEL.

SA-8b/GECKO

Performance
Missile: GECKO
Range: 5.4 nm (10 km)
Maximum Altitude: 2.7 nm (5 km)
Minimum Altitude: 25 m
FC Radar: EO w/IR assist
Range: 3.2 nm (6 km)
TA Radar: LAND ROLL
Frequency: TA: H Band (6-8 GHz), FC: J Band (14.2-14.8 GHz)
Range: 13.4 nm (25 km)
Targets: FW, RW, Cruise Missile, ASM, UAV
Combat Load: 6 missiles
Notes: This is one of the longest-range fielded amphibious systems in the world. This system is also air-transportable and cross-country capable. One transloader vehicle (carrying 18 missiles boxed in sets of three) supports two TELARs.

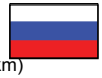
SAM Launcher Systems

Air Defense Missile

SA-9/GASKIN

Performance
Missile: GASKIN
Range: 2.1 nm (4.2 km)
Maximum Altitude: 1.6 nm (3.5 km)
Minimum Altitude: 30 m
FC Radar: EO/IR
Range: 3.2 nm (6.4 km)
TA Radar: DOG EAR
Frequency: F, G Band (3-6 GHz)
Range: 43.1 nm (80 km)
Targets: FW, RW
Combat Load: 6 missiles
Notes: Generally, the system would be expected to have the FLAT BOX-A, but not the GUN DISH radar in the platoon. The insensitive missile seeker was difficult to lock on target and was fairly easily countermeasured from any aspect except the tail aspect.

SA-10b/GRUMBLE



Performance
Missile: GRUMBLE
Range: 40.4 nm (75 km)
Maximum Altitude: 13.4 nm (25 km)
Minimum Altitude: 25 m
TA Radar: FLAP LID
Frequency: I, J Band (8-20 GHz)
Range:107 nm (200 km)
EW/TA Radar: BIG BIRD
Frequency: F Band (3-4 GHz)
Range: 161 nm (300 km)
Targets: FW, RW, Cruise Missile, ASM, UAV
Combat Load: 4 missiles in canisters, 2 SA-16 manpads
Notes: Although many SA-10b units were fielded with 36D6/TIN SHIELD TA radars, most were later replaced with 76N6/CLAM SHELL.

(FOUO) Figure B-2. SAM Launcher Systems (continued)

SA-10c/GRUMBLE

Performance
Missile: GRUMBLE
Range: 48.5 nm (90 km)
Maximum Altitude: 14.5 nm (27 km)
Minimum Altitude: 25 m
TA Radar: CLAM SHELL
Frequency: I Band (8-10 GHz)
Range: 64.7 nm (120 km)
EW/TA Radar: BIG BIRD
Frequency: F Band (3-4 GHz)
Range: 161 nm (300 km)
Targets: FW, RW, Cruise Missile, ASM, UAV
Combat Load: 4 missiles, 2 SA-18 manpads
Notes: Most units use TELs only, not semi-trailer MELs. Chinese upgrades similar to SA-10c are called HQ-10 and HQ-15.

SA-12a/GLADIATOR

Performance
Missile: GLADIATOR
Range: 43.1 nm (80 km)
Maximum Altitude: 13.4 nm (25 km)
Minimum Altitude: 25 m
EW/TA Radar: BILL BOARD
Frequency: F Band (3-4 GHz) phased array
Range: 134 nm (250 km)
TA/FC Radar: GRILL PAN
Frequency: INA 3-D phased array
Range: 80.9 nm (150 Km)
Targets: FW, RW, TBM, Cruise Missile, ASM, UAV
Combat Load: 4 missiles, 2 SA-18 manpads
Notes: The system generally does not target helicopters, but will for self-defense. The Nebo-SV/BOX SPRING counter-stealth radar can also be used.

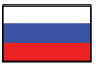
SAM Launcher Systems

Air Defense Missile

SA-12b/GIANT

Performance
Missile: GIANT
Range: 59.3 nm (100 km)
Maximum Altitude: 16.1 nm (30 km)
Minimum Altitude: .54 nm (1 km)
EW/TA Radar: BILL BOARD
Frequency: F Band (3-4 GHz) phased array
Range: 134 nm (250 km)
TA/FC Radar: GRILL PAN
Frequency: INA 3-D phased array
Range: 80.9 nm (150 km)
Targets: FW, RW, TBM, Cruise Missile, ASM, UAV
Combat Load: 4 missiles, 2 SA-18 manpads
Notes: The system generally does not target helicopters, but will for self-defense. The Nebo-SV/BOX SPRING counter-stealth radar can also be used.

SA-20a/GARGOYLE



Performance
Missile: GARGOYLE
Range: 80.9 nm (150 km)
Maximum Altitude: 14.5 nm (27 km)
Minimum Altitude: 6 m
EW/TA Radar: BIG BIRD
Frequency: F Band (3-4 GHz) phased array
Range: 161 nm (300 km)
TA/FC Radar: TOMBSTONE
Frequency: I, J Band (8-20 GHz) phased array
Range: 161 nm (300 km)
Targets: FW, RW, TBM, Cruise Missile, ASM, UAV
Combat Load: 4 missiles, 2 SA-18 manpads
Notes: The "big missile" could be replaced with 48N6M/48N6E2. Although 30N6E1 dual-mode radar may not be able to use the full 200 km missile range against some smaller aerial targets, it can use the improved range against larger targets.

(FOUO) Figure B-3. SAM Launcher Systems (continued)

SA-20b/Favorit

Performance
Missile: Favorit
Range: 107 nm (200 km)
Maximum Altitude: 14.5 nm (27 km)
Minimum Altitude: 6 m
EW/TA Radar: BIG BIRD
Frequency: F Band (3-4 GHz) phased array
Range: 161 nm (300 km)
TA/FC Radar: TOMBSTONE
Frequency: I, J Band (8-20 GHz) phased array
Range: 161 nm (300 km)
Targets: FW, MRBM, RW, Cruise Missile, ASM, UAV, Artillery Rocket
Combat Load: 7 missiles (3 "big," 4 "small") 2 SA-18 manpads
Notes: By shifting from 1 small missile pod per launcher to 2-4, the number of missiles per launcher can increase from 7 to 10, 13, or 16. Strategic ABM units have only big missiles.

SA-21a/GROWLER

Performance
Missile: GROWLER
Range: 215 nm (400 km)
Maximum Altitude: 26.9 nm (50 km)
Minimum Altitude: 5 m
EW/TA Radar: BIG BIRD
Frequency: F Band (3-4 GHz) phased array
Range: 161 nm (300 km)
TA/FC Radar: GRAVESTONE
Frequency: I/J Band (8-20 GHz) phased array
Range: 215 nm (400 km)
Targets: FW, IBRN, RW, Cruise Missile, ASM, UAV, Artillery Rocket
Combat Load: 7 missiles, 2 SA-18 manpads
Notes: There are also reports of a system in development called S-500, with longer range and a design velocity of 10,000 m/s. No details are available.

SAM Launcher Systems

Air Defense Missile

SA-11/GLADFLY

Performance
Missile: GLADFLY
Range: 19.4 nm (36 km)
Maximum Altitude: 11.8 nm (22 km)
Minimum Altitude: 5 m
FC Radar: TV
Range: 10.7 nm (20 km)
FC/TA Radar: FIRE DOME
Frequency: H, I Band (6-10 GHz)
Range: 43.1 nm (80 km)
Battery TA Radar: SNOW DRIFT
Frequency: Centimetric 3-D phased array
Range: 80.9 nm (150 km)
Targets: FW, RW, Cruise Missile, UAV, Guided Bomb, Artillery Rocket, Ground Targets, Ships
Combat Load: 8 missiles
Notes: TELARs can operate autonomously. Launcher-loader can launch with TELAR command. SA-11 can launch SAMs against ground targets.

SA-13b/GOPHER

Performance
Missile: GOPHER
Range: 3.7 nm (7 km)
Maximum Altitude: 1.6 nm (3.5 km)
Minimum Altitude: 10 m
FC Radar: EO/IR
Range: 5.4 nm (10 km)
Radar: SNAP SHOT
Frequency: K Band (20-40 GHz)
Range: 5.4 nm (10 km)
Radar: FLAT BOX
Frequency: Passive radio DF system
Range: 16.1 nm (30 km)
Targets: FW, RW, Cruise Missile, UAV
Combat Load: 8 missiles, 2,000 7.62-mm MG RPK
Notes: The SA-13a replaced SA-9 with an updated launcher mounted on a different chassis. The MT-LB hull offers half the protection of the SA-9 BRDM-2 chassis, but with more mobility. The battery set uses centralized digital target warning net, but each launcher must individually acquire and launch against targets. The platoon command launcher (9A35M/TELAR-1) has a FLAT BOX-B, and can pass data to the other launchers (9A34M/TELAR-2).

(FOUO) Figure B-4. SAM Launcher Systems (continued)

SA-15b/ GAUNTLET

Performance
Missile: GAUNTLET
Range: 6.4 nm (12 km)
Maximum Altitude: 3.2 nm (6 km)
Minimum Altitude: 10 m
FC Radar: EO TV
Range: 10.7 nm (20 km)
TA Radar: SCRUM HALF
Frequency: G, H Band (4-8 GHz)
Range: 13.4 nm (25 km)
Targets: FW, RW, Cruise Missile, UAV
Combat Load: 8 missiles
Notes: Completely autonomous air defense system (at division level), capable of surveillance, command and control, missile launch, and guidance functions from a single vehicle. The basic combat formation is the firing battery consisting of four TLARs and the Rangir battery command post. The TLAR carries 8 ready missiles stored in 2 containers holding 4 missiles each. The SA-15b has the capability to automatically track and destroy 2 targets simultaneously in any weather or at any time of day.

SA-17/ GRIZZLY

Performance
Missile: GRIZZLY
Range: 22.6 nm (42 km)
Maximum Altitude: 13.4 nm (25 km)
Minimum Altitude: 0 m
FC Radar: Laser range-finder
Range: 8.0 nm (15 km)
FC/TA Radar: FIRE DOME
Frequency: H, I Band (6-10 GHz)
Range: 43.1 nm (80 km)
Battery TA Radar: SNOW DRIFT
Frequency: Centimetric 3-D phased array
Range: 80.9 nm (150 km)
Targets: FW, RW, Cruise Missile, UAV, ASM, Artillery Rocket, Ships, Ground Targets
Combat Load: 8 missiles
Notes: The Buk-M1-2 is a multi-role system for SAM and SSM ground/sea target attack missions.

SAM Launcher Systems

Air Defense Missile

French Crotale 5000 Chinese FM-90

Performance
Missile: R440
Range: 5.4 nm (10 km)
Maximum Altitude: 2.7 nm (5 km)
Minimum Altitude: 15 m
FC Radar: TV
Range: 7.5 nm (14 km)
TA Radar: Mirador IV pulse doppler
Frequency: E Band (2-3 GHz)
Range: 9.7 nm (18.5 km)
Targets: FW, RW, Cruise Missile, ASM
Combat Load: 8 missiles
Notes: The all-weather system is deployed in platoons. A platoon includes an Acquisition and Coordination Unit (ACU) vehicle and 2-3 "firing units" (launcher vehicles). A battery includes 2 platoons. Battery reloads are delivered on trucks. An ACU uses the same P4R chassis and a surveillance radar, IFF interrogator, battle management computer, digital RF data link, and VHF radios. With RF datalink, interval can be up to 10 km between ACUs, and up to 3 km between ACU and launcher vehicles. Off-chassis remote control system can be used to guide the missile.

European Crotale– New Generation

Performance
Missile: VT-1
Range: 5.9 nm (11 km)
Maximum Altitude: 3.2 nm (6 km)
Minimum Altitude: 5 m
FC Radar: CCD TV
Range: 8 nm (15 km)
TA Radar: GRIFFON
Frequency: S Band
Range: 10.7 nm (20 km)
Targets: FW, RW, Cruise Missile, ASM, UAV
Combat Load: 8 missiles
Notes: Russian Fakel VL-VT-1 launcher gives the VT-1 hypervelocity missile vertical 40 m rise before pitch-over to target. It permits 360° launch, without need to reorient the vehicle, and a shorter reaction time.

(FOUO) Figure B-5. SAM Launcher Systems (continued)

(FOUO) Figure B-6 depicts the ZSU-23-4 23-mm self-propelled anti-aircraft gun and the 2S6M1 30-mm self-propelled anti-aircraft gun/missile system.

ZSU-23-4 23-mm Self-Propelled Anti-Aircraft Gun

Performance
Missile: GROUSE
Range: 3.2 nm (6 km)
Maximum Altitude: 1.6 nm (3.5 km)
Minimum Altitude: 10 m
TA/FC Radar: GUNDISH
Frequency: J Band (14.8-15.6 GHz)
Range: 10.7 nm (20 km)
Targets: Low flying aircraft, mobile ground targets
Combat Load: 2,000 23-mm
Possible SA-18 Grouse manpad
Notes: Ammunition is normally loaded with a ratio of three HE rounds to one AP round. ZSU 23-4 is capable of acquiring, tracking, and engaging low-flying aircraft (as well as mobile ground targets while either in place or on the move). Resupply vehicles carry an estimated additional 3,000 rounds for each of the four ZSUs in a typical battery.

2S6M1 30-mm Self-Propelled Anti-Aircraft Gun/Missile System

Performance
Missile: GRISON
Range: 5.4 nm (10 km)
Maximum Altitude: 3.2 nm (6 km)
Minimum Altitude: 0 m
FC Radar: Stabilized EO Sight
Range: 9.7 nm (18 km)
TA Radar: HOT SHOT
Frequency: E Band (2-3 GHz)
Range: 8.6 nm (16 km)
Targets: FW, RW, Cruise Missile, UAV, and Ground Targets
Combat Load: 1,904 30-mm
10 missiles
Notes: Main operating mode is radar mode, with day/night capability. Other modes offer reduced radar signature. Thermal sight listed is optional, representing a rational upgrade to existing 2S6M and is standard on 2S6M1 system.

Self-Propelled Anti-Aircraft Gun/Gun-Missile System

Air Defense Gun

(FOUO) Figure B-6. Self-Propelled Anti-Aircraft Gun/Gun-Missile Systems

(FOUO) Figure B-7 depicts threat unmanned aerial vehicles (UAVs): the Aisheng ASN-209 Silver Eagle, the CASIC WJ-600, the Chengdu Pterodactyl I (Wing Loong), and the Guizhou Soar Eagle/Soar Dragon.

(FOUO) Figure B-8 depicts the Guizhou SparrowHawk II, the Guizhou WZ-2000 (WuZhen-2000/WZ-9), the ASN-104/105, and the ASN-207.

(FOUO) Figure B-9 depicts the Pchela-1K; Tupolev Tu-143, 243, 300; Searcher I/II; and the Heron.

(FOUO) Figure B-10 depicts the Mohajer IV, a threat UAV.

Aisheng ASN-209 Silver Eagle

Performance
# of Airframes: 24
Crew: 0
Maximum Speed: 112 mph
Range: 124 miles
Ceiling: 16,406 ft
Mission:
Target designation, ELINT, target tracking, EW, or serve as a communication relay station
Hardpoints: 0
Armament: N/A

CASIC WJ-600

Performance
# of Airframes: 6
Crew: 0
Maximum Speed: 447 mph
Range: 1,305 miles
Ceiling: 32,808 ft
Mission:
Synthetic Aperture Radar
Electronic Surveillance
Hardpoints: 2
Armament:
Precision-guided munitions
Conventional drop ordnance
Reconnaissance-minded payloads

Unmanned Aerial Vehicles

Chengdu Pterodactyl I (Wing Loong)

Performance
# of Airframes: 4
Crew: 0
Maximum Speed: 174 mph
Range: 3,107 miles
Ceiling: 16,404 ft
Mission:
Synthetic Aperture Radar
Forward-Looking Infrared
Hardpoints: 2
Armament:
Sensor equipment
Air-to-surface weaponry

Guizhou Soar Eagle/ Soar Dragon

Performance
# of Airframes: 1
Crew: 0
Maximum Speed: 466 mph
Range: 3,495 miles
Ceiling: 59,055 ft
Mission:
Anti-ship missile and cruise-missile support for ranged precision attack
Hardpoints: 2
Armament: Initially none, limited to reconnaissance sorties

(FOUO) Figure B-7. Threat Unmanned Aerial Vehicles (UAV)

Guizhou Sparrow Hawk II

Performance
# of Airframes: 1
Crew: 0
Maximum Speed: Unknown
Range: 1,802 miles
Ceiling: 27,887 ft
Mission:
Possible development of air-to-surface guided munitions in the form of x2 missiles or similar drop/launched ordnance
Hardpoints: 0
Armament: Optical and sensors payload

Guizhou WZ-2000 (WuZhen-2000/WZ-9)

Performance
# of Airframes: 20
Crew: 0
Maximum Speed: 497 mph
Range: 1,491 miles
Ceiling: 59,055 ft
Mission:
Attack UAV with built-in surveillance capabilities
Hardpoints: 2
Armament:
Air-to-surface ordnance (conventional drop and precision-guided)

Unmanned Aerial Vehicles

ASN-104/105

Performance
# of Airframes: Unknown
Crew: 0
Maximum Speed: 127 mph
Range: 37 miles
Ceiling: 1,049 ft
Mission:
Surveillance
Hardpoints: 0
Armament:
Panoramic camera
Low-light television

ASN-207

Performance
# of Airframes: Unknown
Crew: 0
Maximum Speed: 130 mph
Range: 372 miles
Ceiling: 19,685 ft
Mission:
EW
ECM
Hardpoints: 0
Armament:
JN-1102 suite which can scan, intercept, analyze, monitor, and jam enemy ground-to-air communications at 20-500 MHz.

(FOUO) Figure B-8. Threat UAV (continued)

Pchela-1K

Performance
# of Airframes: Unknown
Crew: 2
Maximum Speed: 86 mph
Range: 37 miles
Ceiling: 9,842 ft
Mission:
Surveillance
Hardpoints: 0
Armament: Video camera, TV, IR

Tupolev Tu-143, 243, 300

Performance
# of Airframes: 950
Crew: 0
Maximum Speed: 590 mph
Range: 125 miles
Ceiling: 16,400 ft
Mission:
Surveillance
Hardpoints: 0
Armament:
Panaromic camera, Low-light-level TV, IR, and radiation detection equipment

Unmanned Aerial Vehicles

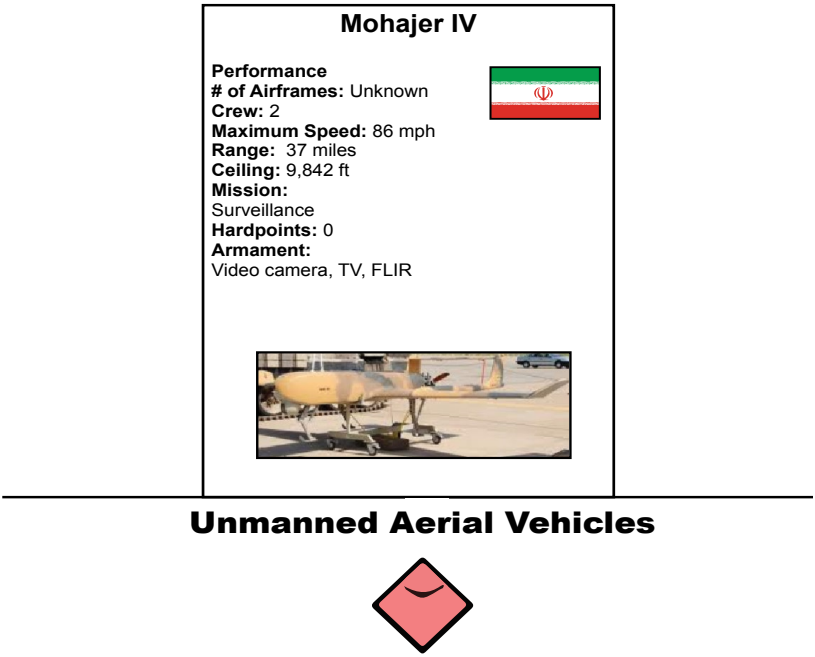
Searcher I/II

Performance
# of Airframes: 200 produced in Israel (unclear how many were purchased by India)
Crew: 0
Maximum Speed: 124 mph
Range: Unknown
Ceiling: 20,013 ft
Mission:
Reconnaissance
Hardpoints: 0
Armament: Payload consists of optics and sensors

Heron

Performance
# of Airframes: 206 produced in Israel (unclear how many were purchased by India)
Crew: 6
Maximum Speed: 129 mph
Range: 217 miles
Ceiling: 30,512 ft
Mission:
Surveying enemy movement and identifying potential targets
Hardpoints: 0
Armament:
Payload consists of specialized equipment only

(FOUO) Figure B-9. Threat UAV (continued)



(FOUO) Figure B-10. Threat UAV (continued)

(FOUO) Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units. Soldiers use ground-based EW capabilities to support continuous operations and to respond quickly to the ground commander's EW requirements.

(FOUO) Figures B-11 through B-14 provide examples of threat ground-based EW equipment.

Meerkat-S

Performance
Description: ESM and ELINT
Tier: One
Frequency Range (MHz): 2-40,000
Degrade GPS: Yes
Degrade FH: Yes
Range: 500 km
Power Output: Passive

No photo available

Weasel 2000

Performance
Description: ESM and ELINT
Tier: Two
Frequency Range (MHz): .5-40,000
Degrade GPS: No
Degrade FH: Yes
Range: 500 km
Power Output: Passive

No photo available

Ground-Based Electronic Warfare Support Measures (ESM)

EW Direction Finding

EW Intercept

MCS90 Tamara

Performance
Description: ELINT
Tier: Three
Frequency Range (MHz): 820-18,000
Degrade GPS: Unknown
Degrade FH: No
Range: 450 km
Power Output: Passive

R-703/709

Performance
Description: ESM
Tier: Four
Frequency Range (MHz): 1.5-2,000
Degrade GPS: No
Degrade FH: N/A
Range: Unknown
Power Output: Unknown

No photo available

(FOUO) Figure B-11. Threat Ground-Based EW Equipment

Cicada-C

Performance
Description: Mounted ESM/ECM, HF/VHF/UHF
Tier: One
Frequency Range (MHz): .525–3,000
Degrade GPS: Yes
Degrade FH: Yes
Range: 100 km
Power Output: 10 kW

No photo available

TRC-274

Performance
Description: Mounted ESM/ECM, HF/VHF/UHF
Tier: Two
Frequency Range (MHz): 20-3,000
Degrade GPS: Yes
Degrade FH: Yes
Range: 150 km
Power Output: 4 kW (1.2 kW on the move)

Ground-Based Electronic Attack

EW Jamming

Pelena-6

Performance
Description: Mounted ECM, HF/VHF/UHF
Tier: Three
Frequency Range (MHz): 20-1,000
Degrade GPS: Yes
Degrade FH: No
Range: 60 km
Power Output: 60 W

No photo available

R-330 T/B

Performance
Description: Mounted ECM, HF/VHF
Tier: Four
Frequency Range (MHz): 1.5-100
Degrade GPS: No
Degrade FH: No
Range: 60 km
Power Output: 1 kW

(FOUO) Figure B-12. Threat Ground-Based EW Equipment (continued)

Cicada-R

Performance
Description: Mounted ESM/ECM, HF/VHF/UHF
Tier: One
Frequency Range (MHz): .525-3,000
Degrade GPS: Yes
Degrade FH: Yes
Range: 100 km
Power Output: 10 kW

GSY 1800

Performance
Description: Mounted ESM/ ECM, HF/VHF/UHF
Tier: Two
Frequency Range (MHz): 1-3,000
Degrade GPS: Yes
Degrade FH: Yes
Range: 100 km
Power Output: 1 kW

No photo available

Tactical Satellite Electronic Attack

EW Direction Finding

EW Intercept

Liman P2

Performance
Description: Mounted ECM, HF/VHF/UHF
Tier: Three
Frequency Range (MHz): 20-1,000
Degrade GPS: Yes
Degrade FH: No
Range: 60 km
Power Output: 60 W

R-934B

Performance
Description: Mounted ECM, VHF/UHF
Tier: Four
Frequency Range (MHz): 100-400
Degrade GPS: No
Degrade FH: No
Range: 50 km
Power Output: 500 W

(FOUO) Figure B-13. Threat Ground-Based EW Equipment (continued)

BOQ-X300

Performance
Description: Mounted ECM, S, C, X, Ku, K
Tier: One
Frequency Range (MHz): 2-40,000
Degrade GPS: Yes
Degrade FH: N/A
Range: Unknown
Power Output: Unknown

No photo available

CBJ-40 Bome

Performance
Description: Mounted ECM, S, C, X, Ku
Tier: Two
Frequency Range (MHz): 2-20,000
Degrade GPS: Yes
Degrade FH: N/A
Range: Unknown
Power Output: Unknown

No photo available

Radar Electronic Attack

EW Jamming

Pelena-1

Performance
Description: Mounted ECM, S, C
Tier: Three
Frequency Range (MHz): 1,000-4,000
Degrade GPS: Yes
Degrade FH: N/A
Range: 250 km
Power Output: Unknown

SPN-2/4

Performance
Description: Mounted ECM, X, K
Tier: Four
Frequency Range (MHz): 6,000-17,500
Degrade GPS: No
Degrade FH: No
Range: 130 km
Power Output: 1 kW (ECM)

(FOUO) Figure B-14. Threat Ground-Based EW Equipment (continued)

HANDBOOK

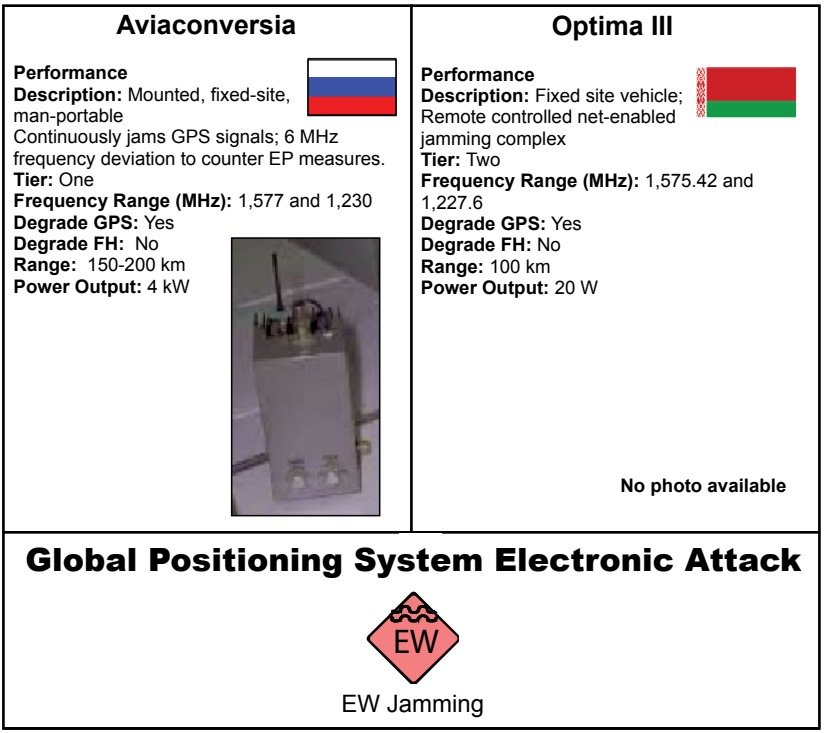
16-15

MAY 16

THE ELECTRONIC WARFARE SMARTBOOK

U.S. UNCLASSIFIED
FOR OFFICIAL USE ONLY

(FOUO) Figure B-15 shows examples of the threat GPS jammers: Aviaconversia and Optima III.



(FOUO) Figure B-15. Threat GPS Jammers

(FOUO) Figures B-16 and B-17 display examples of threat counterfire radar.

PRP-4MU (Val)

Performance
Tier: 1
Crew: 5, including 2 scouts for dismounted operations
Radios: R-123M on PRP-3
Sensors: Passive IR night sight
Radar: SMALL FRED
Frequency Range: 36.2-37 GHz (K Band)
Detection Range: 20 km
Tracking Range: 7-12 km

Variants
Radios: R-173, R-163-50
Sensors: LLLTV sight, 1PN59 thermal sight
Radar: TALL MIKE
Frequency Range: (I Band)
Detection Range: 10-15 km (vehicles) 3 km (personnel)
Tracking Range: 40 km
Note: This radar can be dismounted for tripod mount in a remote OP.

SNAR 10 (BIG FRED)

Performance
Tier: 3-4
Crew: 5
Radios: R-123M, 2 each
Sensors: N/A
Radar: BIG FRED
Frequency Range: 34.55-35.25 GHz (K Band)
Detection Range: 16 km (vehicles) 10 km (shell impact)
Tracking Range: 40 km
Note: Primary mission of the BIG FRED radar is to detect and track both moving ground and water surface targets. The radar is used additionally to provide friendly fire correction data to artillery units.

Counterfire (Artillery Locating) Radar

Artillery Target Acquisition Radar

Artillery Target Acquisition

ARK-1M Rys

Performance
Tier: 3
Crew: 4
Radios: R-123M
Sensors: N/A
Radar: ARK-1M Rys
Frequency Range: Unknown
Detection Range:
Mortar: 13 km
Howitzer: 8 km
MLRS: 25 km
Tactical Missile: 30 km
Tracking Range: Unknown
Maximum number of targets: 3

BL-904 (704 and 704M)

Performance
Tier: 2-3
Crew: 4
Radios: Unknown
Sensors: N/A
Radar: BL-904
Frequency Range: 8-12 GHz
Detection Range (Wide Scan Mode):
82-mm Mortar: 15 km
122-mm Howitzer: 16 km
155-mm Howitzer: 8 km
Detection Range (Narrow Scan Mode):
122-mm Mortar: 20 km
155-mm Howitzer: 25 km
273-mm Howitzer: 30 km

(FOUO) Figure B-16. Threat Counterfire Radar

1L219 (Zoopark-1)

Performance
Tier: 1-3
Crew: 3
Radios: R-123M
Sensors: N/A
Radar: Zoopark-1
Frequency Range: 6-8 GHz
Detection Range:
81-mm Mortar: 12 km
120-mm Howitzer: 15 km
105-mm Howitzer: 8 km
155-mm Mortar: 10 km
122-mm Howitzer: 12 km
220-mm Howitzer: 20 km
Tactical Missile: 35 km

Note: The Zoopark-1 is capable of tracking friendly artillery fire. The system calculates the impact error of friendly artillery rounds and provides automatic correction parameters for increased accuracy. The radar is capable of conducting air traffic control around an airfield. The radar tracks and establishes the current position of aircraft and provides real-time data transmissions to the air control center.

1L220 (Zoopark-2)

Performance
Tier: 1-2
Crew: Unknown
Radios: Unknown
Sensors: N/A
Radar: Zoopark-2
Frequency Range: 3-4 GHz
Detection Range:
Mortar: 30 km
Tube Artillery: 20 km
Rocket: 40 km
Tactical Missile: 55 km

No photo available

Counterfire (Artillery Locating) Radar

Artillery Target Acquisition Radar

Artillery Target Acquisition

(FOUO) Figure B-17. Threat Counterfire Radar (continued)

Appendix C

National Training Center (NTC) Electronic Warfare Metrics and Maps for Success

(U) The metrics and maps to success are document tools used by the NTC "Critter teams" for the evaluation of success. Rotational training units are measured for effectiveness by the observer coach trainers under the supervision of the NTC Commander, Operations Group (COG).

Metrics and Purpose

(U) A metric is a system or standard of measurement that provides important information about how a process is functioning and provides a basis for improvements. Metrics are used to drive improvements and help the EW professional focus efforts and resources on what is important. Metrics are gathered based on organizational and Army priorities, providing a window on performance.

(FOUO) The metrics on the following pages will help tell the EW planner:

- How the electronic warfare cell (EWC) is performing.
- If measurable progress is being made toward a goal.
- To focus on what is being accomplished.
- When the organization reaches its target.

(FOUO) Table C-1. EW and TOC Functions Metrics

TOC Function	0	1	2	3	4	5
Receive Information	Not Observed	SOP does not exist	SOP in draft format	SOP exists, but is not enforced	SOP exists and is routinely enforced	SOP exists, routinely enforced, and minimize reporting
		Information recording tools do not exist	Information recording tools exist, but are not used	Information recording tools exist, but are not integrated	Information recording tools exist and are integrated	Information recording tools exist, are integrated, and result in information sharing
Distribute Information	Not Observed	No PACE plan	PACE plan established, but does not address all echelons	PACE plan established, addresses all echelons and MC nodes, but not routinely enforced	PACE plan established, addresses all echelons and MC nodes, and routinely enforced	PACE plan established, addresses all echelons and mission command nodes, but not routinely enforced; triggers to switch methods planned and understood
		No system for disseminating information within the TOC	EW plan disseminated information, but does not achieve full dissemination within the TOC	EW plan disseminated information across the warfighting functions	EW plan disseminated info across the warfighting functions; information disseminated to all MC nodes, subordinate CPs	EW plan disseminated information across the warfighting functions; information disseminated to all MC nodes. subordinate CPs, and adjacent units, as applicable
Analyze Information	Not Observed	No analysis conducted on information received	Analysis conducted, but stovepiped within warfighting functions	Analysis conducted across warfighting functions	Analysis conducted across warfighting functions, synchronized with other MC nodes	Analysis conducted across warfighting functions, synchronized with other MC nodes, validated by subordinate units and HHQ
		No battle rhythm	Battle rhythm exists, but not routinely executed	Battle rhythm exists, routinely executed, absent analysis/ assessment	Battle rhythm exists, routinely executed, analysis/assessment provided	Battle rhythm exists, routinely executed, analysis/ assessment provided; battle rhythm leads to continued analysis/ planning/ provides running estimates that drive planning, incorporated into the TOC 2-minute drill

(FOUO) Table C-1. EW and TOC Functions Metrics (continued)

TOC Function	0	1	2	3	4	5
Make Recommendations	Not Observed	MDMP not followed for mission planning	MDMP loosely followed, but not synced with warfighting functions representatives	MDMP loosely followed and synced with warfighting functions representatives	MDMP conducted to standard	MDMP conducted to standard and within 1/3-2/3 rule planning timelines
		EW battle drills not developed	EW battle drills developed, but not understood by TOC staff	EW battle drills developed; understood by TOC staff, but not rehearsed	EW battle drills developed, understood by TOC staff, and rehearsed	EW battle drills successfully employed to manage current operations fight
Integrate Resources	Not Observed	EW plan does not have visibility on assets available	EW plan has visibility of assets available from HHQ, but fails to request additional enablers from HHQ	EW plan has visibility of assets available from HHQ; requests additional enablers, but not within timelines	EW plan has visibility of assets available from HHQ; requests additional enablers within timelines	EW plan has visibility of assets available from HHQ; requests additional enablers within timelines; provides appropriate task and purpose
		MC nodes employed without purpose	MC nodes employed with purpose	MC nodes employed with purpose; resourced according to purpose	MC nodes employed with purpose; resourced according to purpose; triggers for transitioning MC planned and understood	MC nodes employed with purpose; resourced according to purpose; triggers for transitioning MC planned and understood; authorities of MC nodes identified
Synchronize Resources	Not Observed	EW produces analog graphics only	EW produces analog and digital graphics	EW produces analog and digital graphics; shares with subordinate units and HHQ; fails to incorporates FSCM	EW produces analog and digital graphics; shares with subordinate units and HHQ; incorporates FSCM	EW produces analog and digital graphics; shares with subordinate units and HHQ; incorporates FSCM; receives bottom up refinement
		EW does not participate in rehearsals	EW participates in CAR	EW participates in CAR; EW covers all identified friction points and decision points	EW participates in CAR; EW covers all identified friction points and decision points; EW participates in fires technical rehearsal	EW participates in all necessary rehearsals (fires, CAR, IC, sustainment); EW covers all identified friction points and decision points
		EW does not have system to track changes	EW disseminates changes to operations without FRAGORDs	EW disseminates changes through FRAGORDs	EW disseminates changes through FRAGORDs; changes made without consideration of second/third order of effects	EW disseminates changes through FRAGORDs; changes synced across the warfighting functions

(FOUO) Table C-2. EW and BIG SEVEN Metrics

Task	1	2	3	4	5
Orders/ Planning Process	No annex issued	Failure to develop essential tasks and does not follow 1/3-2/3 rule	Clearly identifies essential tasks and follows 1/3-2/3 rule	All subordinates have a full understanding of the EW plan and full understanding of the commander's intent	All subordinates and enablers have a full understanding of the plan and time to implement, allowing full understanding of commander's intent at the lowest level
Risk Management	Not done	Risks identified (only safety focused), but not mitigated; no control measures; process not conducted to standard	RM (safety and tactical risk considered); process conducted to standard and briefed	Tactical and safety risk considered and mitigated as part of the planning process; RM used throughout all phases of mission; risk considered and updated during mission	Risk considered in the AAR and lessons learned incorporated into future planning
Rehearsals	Does not attend	Incorrect or inadequate rehearsal technique executed	Technique selected is appropriate, reinforces the unit's task and purpose; schemes of maneuver, fires, support and the EMLCOA; prepared and concise in briefing	Includes all elements identified in the "GREEN" column; multiple COAs are identified and considerations are given to adjacent unit missions	Includes all elements identified in the "GREEN" and "BLUE" columns; subordinates, to include all enablers, achieve complete understanding and synchronization from rehearsal
Common Operating Picture and Graphics	Graphics not used	Graphics not refined to unit's operation	Graphics are consistent with maneuver, fires, and MC	Includes all elements identified in the "GREEN" column to include graphics support branches and sequels; include obstacles, SITEMP, and CSS	Unit/EW plan is using automated graphical updates and consolidated common graphic with subordinate refinements
Information Collection	No contribution to the R&S plan	Sporadic synchronization or coordination	Synchronizes information with the S-2 to enhance the development of the R&S and ISR plans	Uses NAIs for nonlethal fires planning; contributes to the threat template; shares information with subordinates and superiors	Plans are tied to PIRs, NAIs, and TAIs and fully synchronized higher to lower; utilizes all available assets from higher, in concert with internal assets
Fires Planning and Execution	EW is not aware of FSCM; targets are not established	Targets established, but not distributed; priority of fires and observers not identified	EW targets are distributed; observers are identified	Nonlethal fires plan established; targets are distributed using task, purpose, trigger, and targets	Fires plan rehearsed both technically and tactically with incorporated EW; targets complete using task, purpose, execution, assessment
Security and Force Protection	No plan	Unaware of compromises	Designated plan	Adjusts security plans to encountered threats; EW is checking all patrolling elements prior to start point	Security plans rehearsed to standard; patrolling elements include all necessary equipment and coordination to be effective

(FOUO) Table C-3. EW and Intelligence Support Metrics

Task	1	2	3	4	5
Collect	Does not possess or collect on any PIR	Possesses initial set of unit's PIRs, SIRs, and SORs	Aids in developing PIR/SIR; aids in requesting higher-level ISR assets	Refines objectives based on patrol debriefs and integrates higher-level assets/ enablers into ISR plan; gives bottom-up refinement to ISR plan covering the unit's AO	Recommends PIR refinements based on answered SIRs at the CO and BN level; EW contributions result in enhanced intelligence-driven operations
Disseminate	Does not have KM plan; executes ad hoc information sharing	Has CO KM plan for intelligence reporting	COISTs participate in intelligence sync meetings with BN S-2 daily; intelligence support teams produce company INTSUM which goes to both BN and PLTs	Intelligence sharing with coalition partners; DOMEX passed to BN and PLTs; collaborative intelligence sync meeting between all intelligence support teams and BN S-2	IST conducts time sensitive reporting based on actionable intelligence; initial analysis of DOMEX
Conduct Patrol Pre-brief and Debrief	Does not conduct pre-briefs and debriefs	Pre-brief conducted; debrief conducted; has standardized formats, dissemination to all platoons and attachments less than 50 percent	Pre-brief conducted using situation map, pattern analysis, and previous patrol information; disseminate "be on the lookout" list; pre-briefs provide collection requirements (PIR, SIR, SOR); debrief format addresses PIR/SIRs, SIGACTs, KLE, route analysis and an overall assessment 50-79 percent	Debriefs provide answers to collection requirements, along with patrol assessment, that result in operational or collection refinements; intelligence identified in debriefs communicated to BN with analysis 80-100 percent	Pre-briefs incorporate higher-level analysis and ISR; analysis from debriefs are fused and incorporated into company INTSUMs and feed the BN AO assessment and future patrol pre-briefs
Intelligence Support to Lethal Targeting	Has no CO or BN lethal HPTL; no target folders	Possesses higher threat HPTL and targeting folders	Create CO-level HPTL using available intelligence and analysis; HPTL nested with BN; COIST integrates into BN targeting i.e., intelligence support team recommends BN HPTL refinement; uses nonlethal means i.e., MISO and CA to neutralize lethal targets (HPTs, IDF points of origin, IED EAs)	Develop target folders and conduct CO HPTL refinement as intelligence develops; request and plan (with BN S-2) for targeting enablers such as low-level SIGINT and HCTs	Immediately exploits and analyzes current target leads to follow-on targeting i.e., "Domino Effect"; creates CO-level target sync matrix, includes lethal targets that result in successful intelligence-driven operations

(FOUO) Table C-3. EW and Intelligence Support Metrics (continued)

Task	1	2	3	4	5
Intelligence Support to Nonlethal Targeting	Has no CO or BN nonlethal HPTL; no target folders	Possesses higher HPTL and targeting folders (SOI and projects); COIST aware of reward money and micro-grants	Tracks key SOIs, promises made/kept, use of rewards and micro-grants; provides patrols with higher IO messages/talking points and MISO products; refines BN nonlethal HPTL; establishes and disseminates consequence management/IO battle drill	Implements consequence management (mitigates poor actions and exploits successes); recommends projects; develops proactive recommendations for using reward money and micro-grants; integrates nonlethal enablers (provincial reconstruction teams, MISO, human terrain team, HCT)	Creates company-level target sync matrix including nonlethal targets that result in successful intelligence-driven operations

Maps for Success

(FOUO) Table C-4. Fires Planning and Execution

1	2	3	4	5
Inaccurate graphics and FSCMs; targets not established; Class V status not known	Graphics and FSCMs not complete; fires plan not complete; targets established, but not distributed; priority of fires and observers not identified	Graphics and FSCMs distributed; fires plan exists; priority targets distributed to firing elements and observers with priority of fires identified	Unit meets five requirements for accurate predicted fires; all graphics and FSCMs are in place; fires plan established; targets distributed using TPEA	Unit consistently meets five requirements for accurate predicted fires; all graphics and FSCMs are in place and tracked at HHQ; fires plan rehearsed, both technical and tactical; targets completed using TPEA

(FOUO) Table C-5. Direct Fire and Planning and Execution

1	2	3	4	5
No apparent deliberate direct fire plan	Plans direct fires, but plan does not demonstrate the ability to fully focus, distribute, or shift overwhelming mass of direct fires due to shortcomings in the fundamental principles	Unit meets the standard; unit plan effectively accounts for the eight fundamental principles of direct fire control according to standards listed below: in execution, focuses, distributes, and shifts the overwhelming mass of direct fire capability at critical locations and times	Unit meets the standard, plus planners are strong in planning principles; execution of the direct fire plan is exceptional at adjusting to battlefield conditions and capitalizing on surprise, concentration, audacity, tempo, and flexibility	Units meets all requirements for Level 4, plus understands where they succeeded and failed/how to improve for next engagement

Appendix D

Forms, Reports, and Messages

(U) The electronic warfare (EW) staff uses several different forms, reports, and messages in the performance of its duties. The form, message, and report formats contained in this appendix are in addition to those found in Field Manual (FM) 6-99, *U.S. Army Report and Message Formats*, and represent those most commonly used by EW personnel during unified land operations. Techniques for completing each may be modified to fit individual unit needs.

Joint Spectrum Interference Resolution (JSIR) Report

(FOUO) Affected end-users report electromagnetic interference (EMI) through JSIR-Online, if available.

(FOUO) Table D-1. JSIR Information Requirements

Item Number	Data Input
1	Frequencies affected by the interference.
2	Locations of systems experiencing the interference.
3	The affected system name, nomenclature, manufacturer (with model number), or other system description. If available, include the equipment characteristics of the victim receiver, such as bandwidth, antenna type, and antenna size.
4	The operating mode of the affected system. If applicable, include the following: frequency agile, pulse Doppler, search, and upper and lower sidebands.
5	The characteristics of the interference (noise, pulsed, continuous, intermittent, frequency, or bandwidth).
6	The description of the interference effects on victim performance (reduced range, false targets, reduced intelligibility, or data errors).
7	Enter the dates and times the interference occurred. Indicate whether the duration of the interference is continuous or intermittent, the approximate repetition rate of the interference, and whether the amplitude of the interference is varying or constant. Indicate if the interference is occurring at a regular or irregular time of day and if the occurrence of the interference coincides with any ongoing local activity.
8	The location of possible interference sources (coordinates or line-of-bearing [if known], otherwise, state as unknown).

(FOUO) Table D-1. JSIR Information Requirements (continued)

Item Number	Data Input
9	A listing of other units affected by the interference (if known) and their location/distance and bearing from the reporting site.
10	A clear and concise narrative summary of what is known about the interference and any local actions that have been taken to resolve the problem. The operator is encouraged to provide any other information, based on observation or estimation that is pertinent in the technical or operational analysis of the incident. Identify whether the information being furnished is based on actual observation/measurement or is being estimated. Avoid the use of Army or program jargon and acronyms.
11	Reference message traffic that is related to the interference problem being reported. Include the message date-time group, originator, action addressees, and subject line.
12	Indicate whether the problem has been identified or resolved.
13	Indicate if JSIR technical assistance is desired or anticipated.
14	Point of contact information, including name, unit, and contact phone numbers.

Cyber Effects Request Format

(FOUO) Below is an example of a cyber effects request format (CERF) taken from FM 6-99:

CYBER EFFECTS REQUEST FORMAT (CERF)

REPORT NUMBER: C090

GENERAL INSTRUCTIONS: Use to initiate planning, target development, and the delivery of fires in and through cyberspace in support of a commander's strategic end state, operational objectives, and tactical tasks.[1]

LINE 1 – REQUESTING UNIT INFORMATION_____(unit making report)

LINE 2 – DATE AND TIME_____(DTG)

LINE 3 – SUPPORTED COMMAND_____(supported major command)

LINE 4 – REQUESTING UNIT_____(unit requesting data)

LINE 5 – POINT OF CONTACT_____(individual initiating request)

LINE 6 – SUPPORTED OPERATION INFORMATION_____(supported operation data)

LINE 7 – OPLAN/CONPLAN/ORDER_____(number or name of supported OPLAN, CONPLAN, ORDER)

LINE 8 – MISSION STATEMENT_____(commander's mission statement)

LINE 9 – COMMANDER'S INTENT_____(specific item of commander's intent)

LINE 10 – COMMANDER'S END STATE_____(specific item of commander's end state)

LINE 11 – CONCEPT OF OPERATION_____ (concept of operation)

LINE 12 – OBJECTIVE_____ (STRAT/OP/TACT)

LINE 13 – OBJECTIVE/TASK_____ (tactical objective/task)

LINE 14 – COMPUTER NETWORK OPERATIONS INFORMATION_____ (network and target data)

LINE 15 – TYPE OF TARGET_____ (on-call/scheduled)

LINE 16 – TARGET PRIORITY_____(emergency/priority/routine)

LINE 17 – TARGET NAME_____ (TGT name: MIDB/EID, or O-suffix/BE number)

LINE 18 – TARGET LOCATION_____ (TGT location: IP, MAC, physical location, any or all known)

LINE 19 – TARGET DESCRIPTION_____ (facility, individual, virtual, equipment, or organization)

LINE 20 – TARGET FUNCTION_____ (target primary function)

LINE 21 – TARGET SIGNIFICANCE_____ (TGT's importance to the adversary TGT systems)

LINE 22 – CONCEPT OF CYBER OPERATION_____ (OCO: describe how cyber fires contribute to commander's objectives; DCO: assessments/detection, containment, response, investigation)

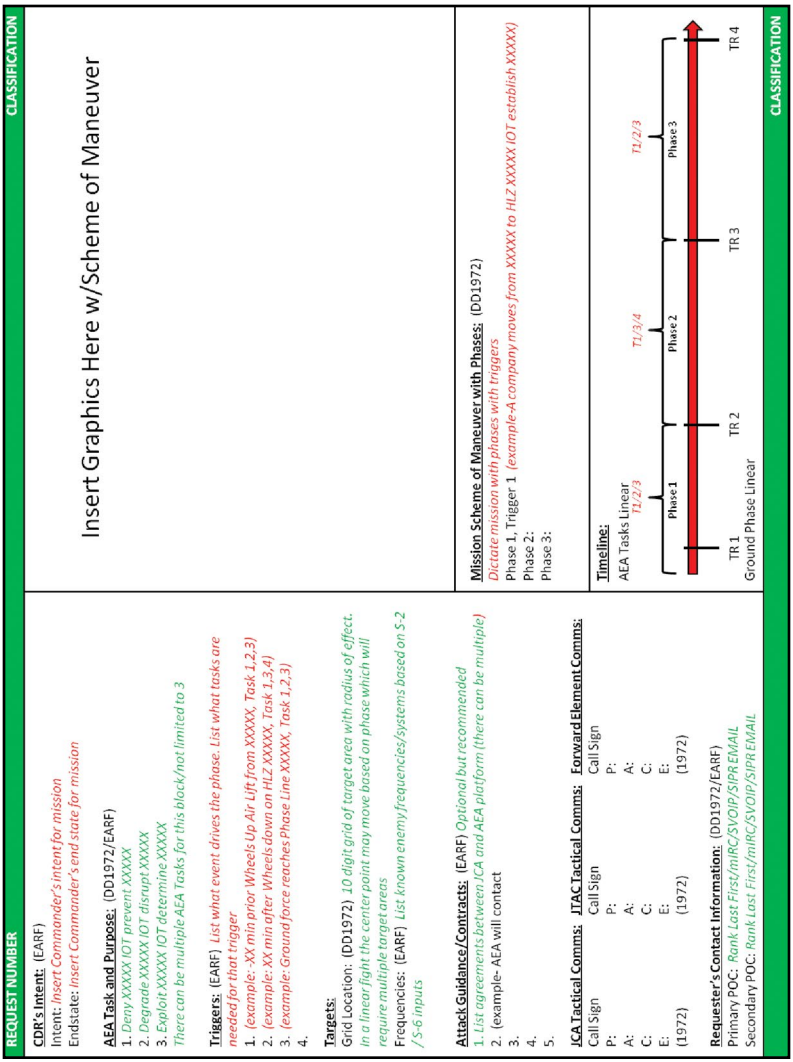
LINE 23 – TARGET EXPECTATION STATEMENT_____ (describe end state for targeting)

LINE 24 – REMARKS_____ (amplifying information)

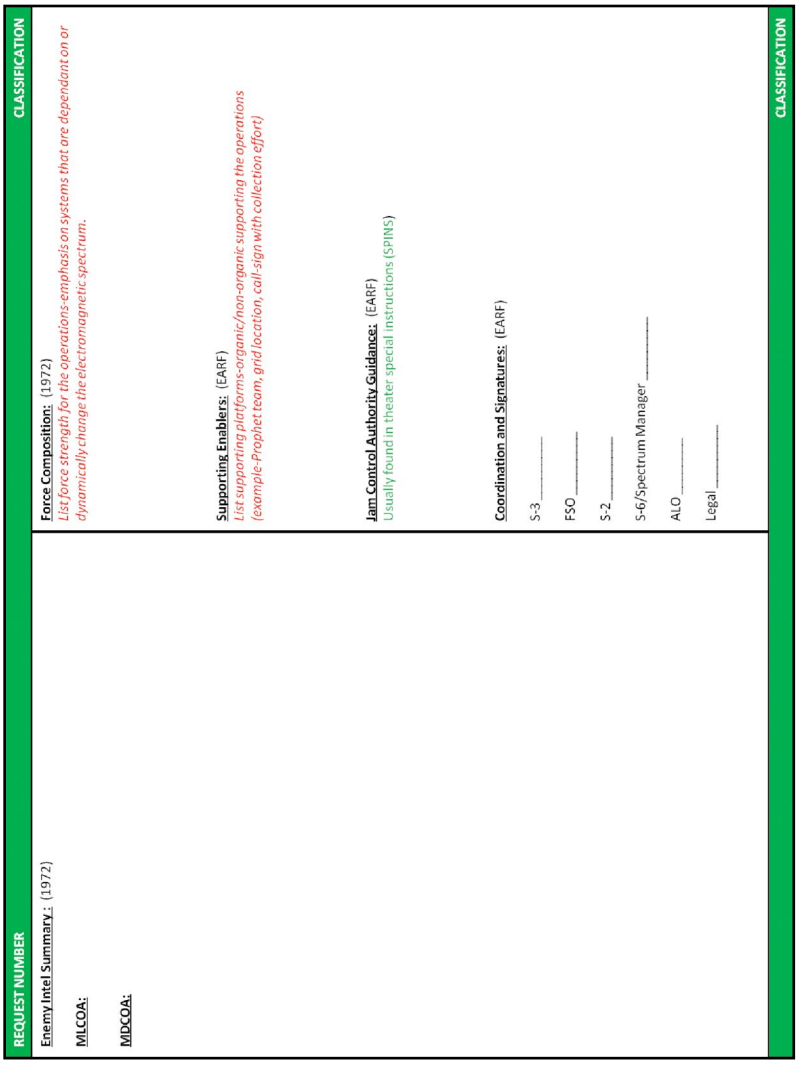
LINE 25 – AUTHENTICATION_____ (report authentication)

(FOUO) Table D-2. CERF acronym and abbreviation list

BE	**basic encyclopedia**
CONPLAN	**concept plan**
DCO	**defensive cyberspace operations**
DTG	**date-time group**
EID	**electrically initiated device**
IP	**initial point**
MAC	**media access control**
MIDB	**modernized integrated database**
OCO	**offensive cyberspace operations**
OP	**operational**
OPLAN	**operation plan**
STRAT	**strategic**
TACT	**tactical**
TGT	**target**



(FOUO) Figure D-1. DD 1972–Joint Tactical Air Strike Request Form



(FOUO) Figure D-2. Electronic Attack Request Form

OPLAN or OPORD

(FOUO) The following table (Table D-3) lists the attachments (annexes, appendixes, tabs, and exhibits) to the base OPLAN or OPORD and identifies the staff officers responsible for developing each attachment.

(FOUO) Table D-3. List of attachments and responsible staff officers

ANNEX A–TASK ORGANIZATION (G-5 or G-3 [S-3])
ANNEX B–INTELLIGENCE (G-2 [S-2])
Appendix 1–Intelligence Estimate Tab A–Terrain (Engineer Officer) Tab B–Weather (Staff Weather Officer) Tab C–Civil Considerations Tab D–Intelligence Preparation of the Battlefield Products Appendix 2–Counterintelligence Appendix 3–Signals Intelligence Appendix 4–Human Intelligence Appendix 5–Geospatial Intelligence Appendix 6–Measurement and Signature Intelligence Appendix 7–Open-Source Intelligence
ANNEX C–OPERATIONS (G-5 or G-3 [S-3])
Appendix 1–Army Design Methodology Products Appendix 2–Operation Overlay Appendix 3–Decision Support Products • Tab A–Execution Matrix • Tab B–Decision Support Template and Matrix Appendix 4–Gap Crossing Operations • Tab A–Traffic Control Overlay Appendix 5–Air Assault Operations • Tab A–Pickup Zone Diagram • Tab B–Air Movement Table • Tab C–Landing Zone Diagram Appendix 6–Airborne Operations • Tab A–Marshalling Plan • Tab B–Air Movement Plan • Tab C–Drop Zone/Extraction Zone Diagram Appendix 7–Amphibious Operations • Tab A–Advance Force Operations • Tab B–Embarkation Plan • Tab C–Landing Plan • Tab D–Rehearsal Plan Appendix 8–Special Operations (G-3 [S-3]) Appendix 9–Battlefield Obscuration (chemical, biological, radiological, and nuclear [CBRN] Officer)

(FOUO) Table D-3. List of attachments and responsible staff officers (continued)

Appendix 10–Airspace Control (G-3 [S-3] or Airspace Control Officer) • Tab A–Air Traffic Services Appendix 11–Rules of Engagement (Staff Judge Advocate) • Tab A–No-Strike List • Tab B–Restricted Target List (G-3 [S-3] with Staff Judge Advocate) Appendix 12– Cyber Electromagnetic Activities/Electronic Warfare Officer • Tab A–Offensive Cyberspace Operations • Tab B–Defensive Cyberspace Operations–Response Actions • Tab C–Electronic Attack • Tab D–Electronic Protection • Tab E–Electronic Warfare Support Appendix 13–Military Information Support Operations (Military Information Support Officer) Appendix 14–Military Deception (Military Deception Officer) Appendix 15–Information Operations (Information Operations Officer)
ANNEX D–FIRES (Chief of Fires/Fire Support Officer)
Appendix 1–Fire Support Overlay Appendix 2–Fire Support Execution Matrix Appendix 3–Targeting • Tab A–Target Selection Standards • Tab B–Target Synchronization Matrix • Tab C–Attack Guidance Matrix • Tab D–Target List Work Sheets • Tab E–Battle Damage Assessment (G-2 [S-2]) Appendix 4–Field Artillery Support Appendix 5–Air Support Appendix 6–Naval Fire Support Appendix 7–Air and Missile Defense (Air and Missile Defense Officer) • Tab A–Enemy Air Avenues of Approach • Tab B–Enemy Air Order of Battle • Tab C–Enemy Theater Ballistic Missile Overlay • Tab D–Air and Missile Defense Protection Overlay
ANNEX E–PROTECTION (Chief of Protection/Protection Officer as designated by the commander)
Appendix 1–Operational Area Security Appendix 2–Safety (Safety Officer) Appendix 3–Operations Security Appendix 4–Intelligence Support to Protection Appendix 5–Physical Security Appendix 6–Antiterrorism Appendix 7–Police Operations (Provost Marshal) Appendix 8–Survivability Operations Appendix 9–Force Health Protection (Surgeon)

(FOUO) Table D-3. List of attachments and responsible staff officers (continued)

Appendix 10–Chemical, Biological, Radiological, and Nuclear Defense (CBRN Officer) Appendix 11–Explosive Ordnance Disposal (EOD) (EOD Officer) Appendix 12–Coordinate Air and Missile Defense (Air Defense Officer) Appendix 13–Personnel Recovery (Personnel Recovery Officer) Appendix 14–Detainee and Resettlement
ANNEX F–SUSTAINMENT (Chief of Sustainment [S-4])
Appendix 1–Logistics (G-4 [S-4]) • Tab A–Sustainment Overlay • Tab B–Maintenance • Tab C–Transportation ○ Exhibit 1–Traffic Circulation and Control (Provost Marshal) ○ Exhibit 2–Traffic Circulation Overlay ○ Exhibit 3–Road Movement Table ○ Exhibit 4–Highway Regulation (Provost Marshal) • Tab D–Supply • Tab E–Field Services • Tab F–Distribution • Tab G–Contract Support Integration • Tab H–Mortuary Affairs Appendix 2–Personnel Services Support (G-1 [S-1]) • Tab A–Human Resources Support (G-1 [S-1]) • Tab B–Financial Management (G-8) • Tab C–Legal Support (Staff Judge Advocate) • Tab D–Religious Support (Chaplain) • Tab E–Band Operations (G-1 [S-1]) Appendix 3–Health Service Support (Surgeon)
ANNEX G–ENGINEER (Engineer Officer)
Appendix 1–Mobility/Countermobility • Tab A–Obstacle Overlay Appendix 2–Survivability Appendix 3–General Engineering Appendix 4–Geospatial Engineering Appendix 5–Environmental Considerations • Tab A–Environmental Assessments • Tab B–Environmental Assessment Exemptions • Tab C–Environmental Baseline Survey
ANNEX H–SIGNAL (G-6 [S-6])
Appendix 1–Defensive Cyberspace Operations Appendix 2–Information Network Operations Appendix 3–Voice, Video, and Data Network Diagrams

(FOUO) Table D-3. List of attachments and responsible staff officers (continued)

Appendix 4–Satellite Communications Appendix 5–Foreign Data Exchanges Appendix 6–Spectrum Management Operations Appendix 7–Information Services
ANNEX I–Not Used
ANNEX J–PUBLIC AFFAIRS
Appendix 1–Public Affairs Running Estimate Appendix 2–Public Affairs Guidance
ANNEX K–CIVIL AFFAIRS OPERATIONS (G-9 [S-9])
Appendix 1–Execution Matrix Appendix 2–Populace and Resources Control Plan Appendix 3–Civil Information Management Plan
ANNEX L–INFORMATION COLLECTION (G-3 [S-3])
Appendix 1–Information Collection Plan Appendix 2–Information Collection Overlay
ANNEX M–ASSESSMENT (G-5 [S-5] or G-3 [S-3])
Appendix 1–Nesting of Assessment Efforts Appendix 2–Assessment Framework Appendix 3–Assessment Working Group
ANNEX N–SPACE OPERATIONS (Space Operations Officer)
ANNEX O–NOT USED
ANNEX P–HOST-NATION SUPPORT (G-4 [S-4])
ANNEX Q–KNOWLEDGE MANAGEMENT (Knowledge Management Officer)
Appendix 1–Knowledge Management Decision Support Matrix Appendix 2–Common Operational Picture Configuration Matrix Appendix 3–Mission Command Information Systems Integration Matrix Appendix 4–Content Management Appendix 5–Battle Rhythm
ANNEX R–REPORTS (G-3 [S-3], G-5 [S-5], and Knowledge Management Officer)
ANNEX S–SPECIAL TECHNICAL OPERATIONS (Special Technical Operations Officer)
Appendix 1–Special Technical Operations Capabilities Integration Matrix Appendix 2–Functional Area I Program and Objectives Appendix 3–Functional Area II Program and Objectives
ANNEX T–SPARE
ANNEX U–INSPECTOR GENERAL (Inspector General)

(FOUO) Table D-3. List of attachments and responsible staff officers (continued)

ANNEX V–INTERAGENCY COORDINATION (G-3 [S-3] and G-9 [S-9])
ANNEX W–OPERATIONAL CONTRACT SUPPORT (G-4 [S-4])
ANNEX X–SPARE
ANNEX Y–SPARE
ANNEX Z–DISTRIBUTION (G-3 [S-3], Knowledge Management Officer)

(U) Table D-4. Kilometer to Nautical Mile Converter

kilometer (km)	nautical mile (nm)	kilometer (km)	nautical mile (nm)	kilometer (km)	nautical mile (nm)	kilometer (km)	nautical mile (nm)	kilometer (km)	nautical mile (nm)
1	0.540	34	18.359	67	36.177	100	53.996	133	71.814
2	1.080	35	18.898	68	36.717	101	54.536	134	72.354
3	1.620	36	19.438	69	37.257	102	55.076	135	72.894
4	2.160	37	19.978	70	37.797	103	55.616	136	72.434
5	2.700	38	20.518	71	38.337	104	56.156	137	73.974
6	3.240	39	21.058	72	38.877	105	56.695	138	74.514
7	3.780	40	21.598	73	39.417	106	57.235	139	75.054
8	4.320	41	22.138	74	39.957	107	57.775	140	75.594
9	4.860	42	22.678	75	40.497	108	58.315	141	76.134
10	5.400	43	22.218	76	41.037	109	58.855	142	76.674
11	5.940	44	23.758	77	41.577	110	59.395	143	77.214
12	6.479	45	24.298	78	42.117	111	59.935	144	77.754
13	7.019	46	24.838	79	42.657	112	60.475	145	78.294
14	7.559	47	25.378	80	43.197	113	61.015	146	78.834
15	8.099	48	25.918	81	43.737	114	61.555	147	79.374
16	8.639	49	26.458	82	44.276	115	62.095	148	79.914
17	9.179	50	26.998	83	44.816	116	62.635	149	80.454
18	9.719	51	27.538	84	44.356	117	63.175	150	80.994
19	10.259	52	28.078	85	45.896	118	63.715	151	81.533
20	10.799	53	28.618	86	45.436	119	64.255	152	82.073
21	11.339	54	29.158	87	46.976	120	64.795	153	82.613
22	11.879	55	29.698	88	47.516	121	65.335	154	83.153
23	12.419	56	30.238	89	48.056	122	65.875	155	83.693
24	12.959	57	30.778	90	48.596	123	66.415	156	84.233
25	13.499	58	30.317	91	49.136	124	66.955	157	84.773
26	14.039	59	31.857	92	49.676	125	67.495	158	85.313
27	14.579	60	32.397	93	50.216	126	68.035	159	85.853
28	15.119	61	32.937	94	50.756	127	68.035	160	86.393
29	15.659	62	33.477	95	51.296	128	69.114	161	86.933
30	16.199	63	34.017	96	51.836	129	69.654	162	87.473
31	16.739	64	35.557	97	52.376	130	70.194	163	88.013
32	17.279	65	35.097	98	52.916	131	70.734	164	88.553
33	17.819	66	35.637	99	53.456	132	71.274	165	89.093

(U) Table D-5. United States Zulu Time Converter

UTC	PST & ALDT	PDT & MST	MDT & CST	CST & EST	EDT & AST	ALST	HST
0000	1600	1700	1800	1900	2000	1500	1400
0100	1700	1800	1900	2000	2100	1600	1500
0200	1800	1900	2000	2100	2200	1700	1600
0300	1900	2000	2100	2200	2300	1800	1700
0400	2000	2100	2200	2300	0000	1900	1800
0500	2100	2200	2300	0000	0100	2000	1900
0600	2200	2300	0000	0100	0200	2100	2000
0700	2300	0000	0100	0200	0300	2200	2100
0800	0000	0100	0200	0300	0400	2300	2200
0900	0100	0200	0300	0400	0500	0000	2300
1000	0200	0300	0400	0500	0600	0100	0000
1100	0300	0400	0500	0600	0700	0200	0100
1200	0400	0500	0600	0700	0800	0300	0200
1300	0500	0600	0700	0800	0900	0400	0300
1400	0600	0700	0800	0900	1000	0500	0400
1500	0700	0800	0900	1000	1100	0600	0500
1600	0800	0900	1000	1100	1200	0700	0600
1700	0900	1000	1100	1200	1300	0800	0700
1800	1000	1100	1200	1300	1400	0900	0800
1900	1100	1200	1300	1400	1500	1000	0900
2000	1200	1300	1400	1500	1600	1100	1000
2100	1300	1400	1500	1600	1700	1200	1100
2200	1400	1500	1600	1700	1800	1300	1200
2300	1500	1600	1700	1800	1900	1400	1300
2400	1600	1700	1800	1900	2000	1500	1400

UTC	Coordinated Universal Time	UTC	CDT	Central Daylight Time	UTC - 5 hours
PST	Pacific Standard Time	UTC - 8 hours	EST	Eastern Standard Time	UTC - 5 hours
ALDT	Alaskan Daylight Time	UTC - 8 hours	EDT	Eastern Daylight Time	UTC - 4 hours
PDT	Pacific Daylight Time	UTC - 7 hours	AST	Atlantic Standard Time	UTC - 4 hours
MST	Mountain Standard Time	UTC - 7 hours	ALST	Alaskan Standard Time	UTC - 9 hours
MDT	Mountain Daylight Time	UTC - 6 hours	HST	Hawaiian Standard Time	UTC - 10 hours
CST	Central Standard Time	UTC - 6 hours			

(U) Table D-6. World Zulu Time Converter

UTC	CET	EET	BT	ZP4	ZP5	ZP6	WAST	CCT	JST	SBT	IDLE	IDLW	NT	NST	AT	WAT
0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	2100	2200	2300
0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	2200	2300	0000
0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	2300	0000	0100
0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	0000	0100	0200
0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	0100	0200	0300
0500	0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	0200	0300	0400
0600	0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	0300	0400	0500
0700	0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	0400	0500	0600
0800	0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	0500	0600	0700
0900	1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	0600	0700	0800
1000	1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0700	0800	0900
1100	1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0800	0900	1000
1200	1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0900	1000	1100
1300	1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	1000	1100	1200
1400	1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	1100	1200	1300
1500	1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	1200	1300	1400
1600	1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	1300	1400	1500
1700	1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	1400	1500	1600
1800	1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	1500	1600	1700
1900	2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	1600	1700	1800
2000	2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1700	1800	1900
2100	2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1800	1900	2000
2200	2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1900	2000	2100
2300	0000	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	2000	2100	2200
2400	0100	0200	0300	0400	0500	0600	0700	0800	0900	1000	1100	1200	1300	2100	2200	2300

CET	Central European Time	JST	Japan Standard Time
EET	Eastern European Time	SBT	Solomon Island Time
BT	Baghdad	IDLE	International Date Line East
ZP4		IDLW	International Date Line West
ZP5		NT	Nome Time
ZP6		NST	Newfoundland Standard Time
WAST	West Africa Time Zone	AT	Azores Time
CCT	China Coast Time	WAT	West Africa Time

(FOUO) Brevity Codes

ANGELS: …….....…….....Altitude

ARIZONA:….....……..No anti-radiation missiles remaining

AS FRAG'ED: ……...….....Exactly as stated in ATO

BENT/BROKEN: …….....System indicated is inoperative

BINGO:…….....Fuel state needed for recovery

BUZZER:…….…..Electronic communications jamming

CHATTERMARK:……...…..……Begin using briefed radio procedures

FADED:……..Radar contact is lost on non-friendly air/surface contact, any positional information is estimated

FURBALL:……...……Non-friendly and friendly aircraft are in close proximity

GADGET:…….....……..Radar of emitter equipment

GO CLEAR:……...……..Use unencrypted voice communications

GO SECURE:……...……...Use encrypted voice communications

JOKER:…….....….Bug out/event termination due to fuel

MAGNUM:…….…….Launch of friendly anti-radiation missile

MUSIC:…….....……..Radar electronic jamming

PLAYTIME:……..…..Amount of time aircraft can remain on station

PUSH:…….....……Go to designated frequency

ROLEX:……..….....…….Timeline adjustment in minutes

SICK:…….....……..System indicated is degraded

SINGER:…….....……Informative call of radar warning receiver indication of surface-to-air missile launch

STRANGER:……...…….Unidentified traffic, not participant in action in progress

WINCHESTER:…….....……No ordnance remaining

Endnotes

1. FM 6-99, *U.S. Army Report and Message Formats*, 19 AUG 2013, pp. A-74 through A-75.

Appendix E

Army Universal Tasks Related to Electronic Warfare (EW)

Conduct Direct Fires (ART 1.4)[1]		
Conduct Nonlethal Direct Fire Against a Surface Target (ART 1.4.2)		
No.	**Scale**	**Measure**
1	Yes/ No	Direct fires contributed to accomplishing the unit mission.
2	Yes/ No	Conduct of nonlethal direct fires against surface target was done per rules of engagement, to include receipt of the approval of weapons released from a competent authority.
3	Time	To develop nonlethal direct fire options after receiving warning order.
4	Time	To complete nonlethal direct fire attack on target (after initiation).
5	Percent	Of all targets evaluated as candidates for nonlethal direct fire attack.
6	Percent	Of nonlethal direct fire attacks on selected targets that achieve desired effect.
7	Percent	Of nonlethal direct fire attacks without lethal results.
8	Percent	Of nonlethal direct fire attacks that require lethal fires to achieve desired operational effects.
9	Percent	Of nonlethal direct fire attacks that result in collateral damage
10	Percent	Of threat actions that are denied, stopped, moved, diverted, suppressed, and/or disabled due to nonlethal direct fire attack.
11	Percent	Of nonlethal direct fire attacks that result in friendly or neutral casualties.
12	Number	Of nonlethal direct fire attacks that result in friendly or neutral casualties.
13	Number	Of nonlethal direct fire attacks that result in collateral damage

Support to Situational Understanding (ART 2.2)[2]		
Evaluate the Threat (ART 2.2.1.3)		
No.	**Scale**	**Measure**
1	Yes/ No	The threat's capabilities were stated in the intelligence preparation of the battlefield process and accounted for in the military decisionmaking process.
2	Yes/ No	Unit used pattern analysis, event analysis, and intelligence from higher headquarters and other organizations to create threat templates, models, and methods of operation and identify high-payoff targets and high-value targets.
3	Time	Required to incorporate new intelligence data and products into ongoing threat evaluations.
4	Time	To identify threat capabilities and limitations.
5	Time	To update or create threat templates, models, and methods of operation.
6	Time	To disseminate updated threat templates, models, and methods of operation.
7	Percent	Of correctly identified threat templates, models, and methods of operations; capabilities and limitations; high-payoff targets; high-value targets; and threat models.
8	Percent	Of new, processed intelligence integrated to update broad courses of action (COAs).

Determine Threat Courses of Action (ART 2.2.1.4)		
No.	**Scale**	**Measure**
1	Yes/ No	The entire staff, under the direction of the intelligence staff, assessed the effects of friendly actions on threat COAs.
2	Yes/ No	The threat's likely objectives and desired end state were identified, beginning with the threat command level at one echelon above the friendly unit and ending the process at two echelons below.
3	Yes/ No	Unit staff identified opportunities and constraints that the operational environment offers or affords to threat and friendly forces.

4	Yes/ No	Unit staff assessed effects of friendly actions on threat COAs.
5	Yes/ No	Units considered threat capabilities, effects of the operational environment, and the threat's preference in operations.
6	Yes/ No	Units determined most probable and most dangerous COAs and other threat COAs to a micro level of detail as time permitted.
7	Yes/ No	Units disseminated threat COAs to lower, adjacent, and next higher echelon.
8	Yes/ No	Units delivered threat COAs in time to be of value for developing friendly COAs.
9	Yes/ No	The G-3 or S-3 led staff war-gaming with full staff participation to validate and update assessments.
10	Time	Required to identify likely threat objectives and desired end states at different threat echelons of command.
11	Time	To identify and analyze the feasibility of each threat COA in terms of time, space, resources, and force ratios required to accomplish its objective.
12	Time	To evaluate and prioritize each identified threat COA.
13	Percent	Of new intelligence integrated to update threat COAs.

Provide Intelligence Support to Targeting and Information-Related Capabilities (ART 2.4)[3]		
Provide Intelligence Support to Targeting (ART 2.4.1)		
No.	**Scale**	**Measure**
1	Yes/ No	The intelligence officer identified threat command and control nodes, to include all aspects.
2	Yes/ No	The intelligence officer identified threat communication systems, to include all aspects.
3	Yes/ No	The intelligence officer identified threat computer systems, to include all aspects.
4	Yes/ No	The intelligence officer identified threat personnel.

5	Yes/ No	The fire support coordinator, information operations officer, and EW officer received information and intelligence support for targeting of the threat's forces through lethal and nonlethal means.
6	Yes/No	Risks to targeting cultural, historic sites, religious centers, medical facilities, natural resources, hazard areas (such as nuclear power plants, chemical facilities, and oil refineries) were assessed and included in target nomination criteria.
7	Time	To detect all aspects of the threat command and control nodes.
8	Time	To detect all aspects of the threat communications systems.
9	Time	To detect all aspects of the threat computer systems.
10	Time	To provide the fire support coordinator information operations officer, electronic warfare officer information and intelligence support for targeting of the threat's forces through fires and nonlethal capabilities, to include updates.
11	Percent	Of threat command and control nodes vulnerable to electronic attack (EA) and electronic support.
12	Percent	Of threat computer systems vulnerable to computer network attack and computer network exploit.
13	Percent	Of threat command and control nodes disrupted and degraded.
14	Percent	Of threat command and control nodes monitored.
15	Percent	Of threat computer systems compromised.
16	Percent	Of threat computer systems monitored.

Provide Intelligence Support to Command and Control Warfare (ART 2.4.2.3)

No.	Scale	Measure
1	Yes/ No	Unit identified threat command and control nodes.
2	Yes/ No	Unit identified threat communications systems.
3	Yes/ No	Unit identified threat computer systems.
4	Yes/ No	Intelligence support required for EA identified through intelligence preparation of the battlefield and support to targeting.

5	Yes/ No	Unit identified the threat's assets, processes, patterns, and means vulnerable to EA.
6	Yes/ No	Unit provided intelligence support to locate targets for EA.
7	Yes/ No	Unit provided intelligence support to determine if desired effects were achieved.
8	Yes/ No	Unit provided information regarding target capabilities and vulnerabilities.
9	Yes/ No	Unit provided information regarding which enemy systems are available against which to perform EA.
10	Yes/ No	Unit completed combat assessment for EA.
11	Time	To determine support required for EA.
12	Time	To determine specific information requirements for EA.
13	Time	To provide combat assessments in support of EA.
14	Percent	Of threat command and control nodes vulnerable to EA.
15	Percent	Of threat command and control nodes vulnerable to electronic exploitation.
16	Percent	Of threat computer systems vulnerable to computer network attack.
17	Percent	Of threat command and control nodes disrupted and degraded.
18	Percent	Of threat computer systems compromised.
19	Percent	Of personnel, facilities, or equipment degraded, denied, disrupted, or destroyed by EA.

Integrate Fires (ART 3.1)[4]		
Nominate Electronic Attack Targets (ART 3.1.4)		
No.	**Scale**	**Measure**
1	Yes/ No	Targets selected were required for accomplishing the unit mission and commander's intent.
2	Yes/ No	Unit nominated EA targets following rules of engagement.
3	Time	To submit EA targets to operational echelons.
4	Time	To receive and assess results of EA.

5	Percent	Of enemy systems not engaged by EA that are targeted for physical attack.
6	Percent	Of enemy systems not engaged by EA that are targeted for collection or exploitation.

Conduct Cyber Electromagnetic Activities (CEMA) (ART 5.9)[5]

No.	Scale	Measure
1	Yes/ No	Unit integrated and synchronized the functions and capabilities of cyberspace operations, electronic warfare, and electromagnetic spectrum operations.
2	Yes/ No	Unit developed the commander's overall situational awareness and situational understanding to support decision-making processes.
3	Yes/ No	Unit planned, coordinated, integrated, and conducted (as applicable) cyberspace operations to affect personnel, facilities, physical and logical networks, equipment, and organizations.
4	Yes/ No	Unit conducted electronic warfare to include electronic attack using electromagnetic energy, directed energy, or antiradiation capabilities to affect personnel, facilities, or equipment.
5	Yes/ No	Unit efficiently used the electromagnetic spectrum while in a joint environment that enabled operational planning and execution.
6	Yes/ No	Unit integrated and synchronized across all command echelons and warfighting functions as part of the operations process.
7	Yes/ No	Unit coordinated electronic warfare and cyberspace operations that ensured synergistic application and maximum effectiveness.

Conduct Cyberspace Operations (ART 5.9.1)

No.	Scale	Measure
1	Yes/ No	Unit planned, coordinated, and integrated offensive cyberspace operations in and through cyberspace to create and achieve desired effects in support of the commander's objectives.

2	**Yes/ No**	**Unit conducted and coordinated, as required, defensive cyberspace operations in and through cyberspace and effectively detected, identified, and responded to enemy and adversary actions against friendly force networks and information resident in these networks.**
3	**Yes/ No**	**Unit coordinated network operations within Department of Defense information networks and LandWarNet to support cyberspace operations.**
4	**Yes/ No**	**Unit performed cyberspace support actions enabling cyberspace operations and the accomplishment of the mission.**
5	**Yes/No**	**Unit developed cyberspace situational awareness by effectively gathering, processing, and communicating relevant information that resulted in the transfer of knowledge into situational understanding.**

Integrate Offensive Cyberspace Operations (ART 5.9.1.1)

No.	Scale	Measure
1	**Yes/ No**	**Unit performed planning and targeting processes and identified, selected, and developed targets for engagement by offensive cyberspace operations means.**
2	**Yes/ No**	**Unit reviewed selected targets for compliance with rules of engagement and authorities specific to cyberspace operations.**
3	**Yes/ No**	**Unit developed and submitted cyber effects request formats for selected targets.**
4	**Yes/ No**	**Unit coordinated and conducted information collection in support of offensive cyberspace operations to gain and maintain access to physical and logical networks and to prepare for follow-on offensive cyberspace operations.**
5	**Yes/ No**	**Unit planned, coordinated, integrated, and conducted (as applicable) cyberspace attacks and achieved simultaneous and complementary effects in support of the scheme of maneuver.**

6	Yes/ No	Unit obtained and applied combat and battle damage assessments for targets engaged by cyberspace attack means.

Conduct Defensive Cyberspace Operations (ART 5.9.1.2)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit employed tactics, techniques, and procedures to detect intrusions and cyber attacks into the Army's portion of the Department of Defense information networks called LandWarNet.
2	Yes/ No	Unit coordinated, deconflicted, and conducted defensive cyberspace operation response actions outside the LandWarNet.
3	Yes/ No	Unit coordinated, deconflicted, and employed internal defensive measures inside the LandWarNet.
4	Yes/ No	Unit conducted rehearsals to react to enemy cyber attacks on friendly networks and per operation order, battle drills, and standard operating procedures.
5	Yes/ No	Unit coordinated and conducted information collection in support of defensive cyberspace operations.
6	Yes/ No	Unit developed and submitted cyber effects request formats as required in support of defensive cyberspace operations.

Coordinate Network Operations (ART 5.9.1.3)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit enabled and facilitated cyberspace operations inside friendly force networks.
2	Yes/ No	Unit enabled and facilitated cyberspace operations outside friendly force networks.
3	Yes/ No	Unit enforced cyber electromagnetic policies and standards that guided the development, deployment, and management of personnel, products, and processes.

Conduct Cyberspace Support (ART 5.9.1.4)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit performed development, engineering, and analysis that enabled the enterprise network.
2	Yes/ No	Unit conducted legal, regulatory, and policy analysis and coordination.
3	Yes/ No	Unit performed vulnerability assessments.
4	Yes/ No	Unit performed remediation in response to unauthorized intrusions or attacks.

Conduct Electronic Warfare (ART 5.9.2)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit conducted EA to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.
2	Yes/ No	Unit conducted electronic protection (EP) using actions to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.
3	Yes/ No	Unit conducted ES to intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.
4	Yes/ No	Unit integrated, analyzed, and fused collected data and information to provide targetable intelligence in support of EW.
5	Yes/ No	Unit conducted a legal review of EW operations.

Conduct Electronic Attack (ART 5.9.2.1)		
No.	**Scale**	**Measure**
1	Yes/ No	Targets selected were required for accomplishing the unit mission and commander's intent.
2	Yes/ No	Unit nominated EA effects on targets following rules of engagement.

3	Time	To submit electronic attack effects on targets to operational echelons.
4	Time	To receive and assess results of EA.
5	Percent	Of enemy systems not engaged by electronic attack that were targeted for physical attack.
6	Percent	Of enemy systems not engaged by EA that were targeted for collection or exploitation.

Perform Electronic Protection Actions (ART 5.9.2.2)

No.	Scale	Measure
1	Yes/ No	Unit course of action was not compromised by enemy offensive information operations.
2	Yes/ No	EW mission spectrum requirements were deconflicted with the unit spectrum manager.
3	Yes/ No	EW system emission security compromises degraded, delayed, or modified unit operations.
4	Time	For friendly information collection sensor system managers, operators, and emergency response teams or contact teams to respond, identify, and correct system failures attributed to enemy offensive information operations.
5	Time	To identify, determine appropriate response, and implement changes in response to a possible threat to information systems.
6	Percent	Of time units in the area of operations (AO) were in restrictive information operations condition.
7	Percent	Of information systems hardware, software components, and databases backed up by replacement components or backup files in case of failure or compromise.
8	Percent	Of identified friendly vulnerabilities in the AO exploited by enemy actions.
9	Percent	Of friendly emitters in the AO exploited by the enemy.
10	Percent	Of friendly operations conducted in a restrictive emission control environment.
11	Percent	Of emission control procedures that had improved from previous assessments.

12	Percent	Of successful EW system reprogramming events.
13	Percent	Of friendly systems affected by friendly EW systems.
14	Percent	Of friendly systems affected by enemy EW systems.
15	Number	Of frequency interference issues.
16	Number	Of EW systems operating on assigned frequencies.
17	Number	Of EW systems detected by enemy sensors.
18	Number	Of emission security violations in the AO in a given time.
19	Number	Of instances when frequency allocation or frequency management failed to prevent signal fratricide.
20	Number	Of EW system reprogramming events.
21	Number	Of instances when EW system reprogramming was unsuccessful.
22	Number	Of friendly systems affected by friendly or enemy EW systems.

Provide Electronic Warfare Support (ES) (ART 5.9.2.3)

No.	Scale	Measure
1	Yes/ No	Unit developed a support plan for ES operations.
2	Yes/ No	Unit disseminated EW reprogramming information.
3	Yes/ No	Unit had assets available to satisfy ES requirements.
4	Yes/ No	Unit identified intelligence support requirements for ES.
5	Yes/ No	Unit had procedure in place to request intelligence support to satisfy ES requirements.
6	Yes/ No	Unit had procedure in place for rapid electronic warfare reprogramming.

Conduct Electromagnetic Spectrum Operations (ART 5.9.3)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit provided appropriate guidance and necessary coordination to deconflict interference with other friendly uses of the EMS.
2	Yes/ No	Unit obtained clearance (or approval) from host nation for the use of the EMS (through existing coordination procedures).
3	Yes/ No	Unit ensured assigned military forces were authorized sufficient use of the EMS to accomplish their designated missions.
4	Yes/ No	Unit developed and distributed plans for appropriately using EMS that included frequency reuse and sharing schemes for specific frequency bands.
5	Yes/ No	Unit maintained the necessary database that contained information on all friendly, available, adversary, and selected neutral or civil spectrum emitters or receivers.
6	Yes/ No	Unit established and maintained a close working relationship with the frequency management personnel.

Perform Spectrum Management (ART 5.9.3.1)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit managed spectrum to satisfy mission requirements and met commander's intent.
2	Yes/ No	All systems operated with no interference.
3	Yes/ No	Unit maintained databases.
4	Time	To convert raw data to a useable format.
5	Time	To deconflict spectrum assignments.
6	Time	To evaluate environmental effects.
7	Time	To resolve frequency interference.
8	Time	To coordinate EW issues.
9	Time	To process interference report.
10	Time	To coordinate, develop, and publish a joint restricted frequency list.

11	Time	To coordinate with network managers.
12	Number	Of frequency assignments managed.
13	Number	Of systems requiring EMS.

Perform Frequency Assignment (ART 5.9.3.2)

No.	Scale	Measure
1	Yes/ No	Unit requested sufficient frequencies to meet mission requirements.
2	Yes/ No	Sufficient frequencies were available to meet mission requirements.
3	Yes/ No	Unit utilized frequency reuse plans to efficiently use the electromagnetic spectrum.
4	Time	To generate radio load sets and frequency plans.
5	Time	To build communications-electronics operating instructions.
6	Time	Between request for frequencies.
7	Time	To obtain frequency approval.
8	Time	To design the frequency plan for area networks.

Perform Host Nation Electromagnetic Coordination (ART 5.9.3.3)

No.	Scale	Measure
1	Yes/ No	Unit established relationship with host nation agency responsible for radio frequency spectrum.
2	Yes/ No	Commander was informed of host nation restrictions on spectrum use.
3	Time	To process frequency request
4	Time	To obtain frequency approval.
5	Percent	Of frequency requests filled.
6	Percent	Of mission degradation due to inadequate spectrum.

Monitor Spectrum Management Policy Adherence (ART 5.9.3.4)

No.	Scale	Measure
1	Yes/ No	Unit observed all spectrum policies, regulations, and rules.

2	Yes/ No	Commander was aware of policy, regulations, and rules affecting operations.
3	Time	To complete DD 1494 (Application for Equipment Frequency Allocation).
4	Time	To get approval from the Military Communications-Electronics Board.
5	Time	To disseminate spectrum supportability guidance.
6	Number	Of systems not meeting spectrum certification compliance.

Conduct the Operations Process (ART 5.1)[6]		
Receive the Mission (ART 5.1.1.2.1)		
No.	**Scale**	**Measure**
1	Yes/ No	Staff collected materials for analysis.
2	Yes/ No	Commander provided adequate initial guidance.
3	Time	After receipt of mission to issue initial planning guidance.
4	Time	To alert staff of receipt of new mission.
5	Time	To issue warning order.

Perform Mission Analysis (ART 5.1.1.2.2)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit developed mission analysis briefing for presentation to the commander.
2	Yes/ No	Unit developed and approved restated mission, commander's guidance, commander's intent, commander's critical information requirements (CCIR), use of available time, and warning order.
3	Yes/ No	Unit developed reconnaissance and surveillance plan, initial themes and messages, a proposed problem statement, and the course of action evaluation criteria.
4	Yes/ No	Mission statement included who, what, when, where, and why of the mission.
5	Yes/ No	Unit performed time or distance analysis.

6	**Yes/ No**	**Unit developed assumptions to replace missing or unknown facts necessary for continued planning.**
7	**Yes/ No**	**Commander issued planning guidance to staff and subordinate commands.**
8	**Yes/ No**	**Staffs developed and maintained running estimate pertaining to their areas of expertise.**
9	**Yes/ No**	**Unit issued a warning order.**
10	**Time**	**To initiate preliminary movement.**
11	**Time**	**To update operational timeline.**
12	**Percent**	**Of critical information and running estimates reviewed before mission analysis.**
13	**Percent**	**Of major topics within the intelligence preparation of the battlefield for which assessments were completed.**
14	**Percent**	**Of assumptions that proved to be either invalid or unrealistic and significantly affected the operation.**
15	**Percent**	**Of constraints identified that affected the operation significantly.**
16	**Percent**	**Of specified tasks derived in mission analysis and carried into planning.**
17	**Percent**	**Of implied tasks derived in mission analysis and carried into planning.**
18	**Percent**	**Of essential tasks derived in mission analysis and carried into planning.**
19	**Percent**	**Of specified and implied tasks identified as essential tasks and included in the mission statement, commander's intent, or concept of operations paragraphs of the operation order.**
20	**Percent**	**Of forces identified as required to perform the essential tasks.**
21	**Percent**	**Of commander's guidance (coverage of functional responsibilities) completed.**
22	**Percent**	**Of planning time used to issue guidance.**
23	**Percent**	**Of rules of engagement clearly understood.**
24	**Percent**	**Of subordinates accepting commander's intent without requests for clarification.**

25	Number	Of amendments issued to planning guidance (due to requests for clarification).
26	Number	Of requests for clarification of planning guidance received from subordinate headquarters.
27	Number	Of misunderstood rules of engagement.
28	Number	Of revisions to commander's intent.

Develop Courses of Action (ART 5.1.1.2.3)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit developed distinguishable and complete COAs in terms of feasibility, suitability, and acceptability for mission accomplishment if executed.
2	Time	To provide the commander with suitable, feasible, and acceptable COAs after receipt of operation order or warning order.
3	Time	To prepare complete COA statements and sketches.
4	Percent	Of COAs that were complete.
5	Percent	Of nonselected COAs considered for military deception
6	Percent	Of COAs suitable—solve the problem and are legal and ethical.
7	Percent	Of COAs feasible—fit within available resources.
8	Percent	Of COAs acceptable—worth the cost or risk.
9	Percent	Of COAs distinguishable—differ significantly from other solutions.
10	Percent	Of COAs presented to commander that were suitable, feasible, acceptable, and distinct from one another.
11	Number	Of COAs developed as per commander's guidance.

Analyze Courses of Action (ART 5.1.1.2.4)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit identified advantages and disadvantages of COAs, measures of effectiveness (MOE), or measures of performance (MOP) for evaluation.
2	Yes/ No	Unit reviewed and revised CCIR, as necessary, during the war-gaming process.
3	Yes/ No	Unit developed risk management plan for COA analysis.
4	Yes/ No	Unit applied evaluation criteria (MOE or MOP) to the war-gaming analysis.
5	Yes/ No	Methods applied during war-gaming analysis included belt, box, or avenue-in-depth.
6	Yes/ No	Unit used synchronization matrix or sketch note worksheet during war-gaming analysis.
7	Time	To complete COA analysis (war-gaming).
8	Percent	Of completeness of COAs (war-gaming).
9	Percent	Of conformance of analysis (war-gaming) to doctrine.
10	Percent	Of branches and sequels experienced identified in COAs.
11	Percent	Of capabilities ultimately required identified in COA analysis (war-gaming).
12	Percent	Of COAs analyzed against potential enemy COAs.
13	Number	Of limitations (ultimately identified during execution) identified during analysis.
14	Number	Of criteria of comparison and success identified during COA analysis (war-gaming).
15	Number	Of decision points and critical events identified and applied to CCIR during war-gaming.

Compare Courses of Action (ART 5.1.1.2.5)		
No.	**Scale**	**Measure**
1	Yes/ No	Previously selected comparison criteria allowed for definitive comparison of COAs.

2	**Yes/ No**	**Unit developed risk management plan used during COA comparison.**
3	**Percent**	**Of comparison criteria eliminated before comparison.**
4	**Percent**	**Of comparison criteria eventually used, defined, and weighted before comparison began.**

Approve Course of Action (ART 5.1.1.2.6)		
No.	**Scale**	**Measure**
1	**Yes/ No**	**COA brief developed and presented to commander.**
2	**Yes/ No**	**Commander evaluated COAs, selected a COA, and modified or rejected all presented COAs.**
3	**Yes/ No**	**Modified COA or new COA created a new war game to consider products deriving from that COA.**
4	**Yes/ No**	**Revised commander's intent adequately addressed key tasks for force as whole, wider purpose; it is expressed in four to five sentences or bullets.**
5	**Yes/ No**	**Commander decided level of risk to accomplish the mission and approved control measures.**
6	**Time**	**To issue warning orders.**

Produce Plan or Order (ART 5.1.1.2.7)		
No.	**Scale**	**Measure**
1	**Yes/ No**	**Orders or plans accomplished the mission and commander's intent. They were communicated effectively and completed with sufficient time for the force to complete required preparatory actions before execution.**
2	**Yes/ No**	**Commander's intent refined and adequately addressed key tasks for the force as a whole, wider purpose; it was expressed in four to five sentences.**

3	Time	To issue warning orders, as required.
4	Time	Before execution to reissue commander's intent and concept of operations.
5	Time	To prepare plans and orders (after deciding on mission concept and commander's intent).
6	Time	To obtain approval of plans and orders.
7	Time	To issue plan or order (after approved).
8	Percent	Of functional responsibilities covered in operation plan.
9	Percent	Of accurate information in plans and orders issued and disseminated to subordinate units.
10	Percent	Of accurate information in operation order or plan to meet established objectives.
11	Number	Of instances where the operation plan or order conflicted with standards established under the law of war and international conventions.

Integrate Requirements and Capabilities (ART 5.1.1.4)		
No.	**Scale**	**Measure**
1	Yes/ No	Unit established MOPs.
2	Yes/ No	Combinations and timings of forces and warfighting functions contributed to mission accomplishment.
3	Yes/ No	Unit integrated information superiority contributors to enhance rapid and accurate situational understanding that initiate or govern actions to accomplish tactical missions.
4	Yes/ No	Unit leveraged information superiority contributors that support making more precise and timely decisions than the enemy does.
5	Yes/ No	Unit integrated operations security and military deception causing the enemy to make inappropriate, untimely, or irrelevant decisions.
6	Yes/ No	Unit planned transition operations.
7	Yes/ No	Unit planned monitoring.

8	Time	Delay in initiating phase of operation.
9	Time	Before execution for force to execute matrix with sequence and timing of each subordinate task throughout the operation.
10	Time	To modify plans and actions due to operational contingencies.
11	Percent	Of assigned and supporting forces coordinated to synchronize operation in right place at right time.
12	Number	Of potential cross-boundary fratricides identified and eliminated by force headquarters.
13	Number	Of uncoordinated element or activity actions causing disruption or delay of U.S. or multinational plans and objectives.

Evaluate Situation or Operation (ART 5.1.4.2)[7]		
No.	**Scale**	**Measure**
1	Yes/ No	Evaluation reflected reality of the degree of mission accomplishment and forecasted the degree of mission accomplishment.
2	Time	To evaluate progress or situation and determine type of decision.
3	Time	To complete evaluation of situation or progress.
4	Percent	Of accuracy of evaluation of situation or progress.
5	Percent	Of accurate friendly evaluations.
6	Number	Of opportunities or threats recognized.

Develop Running Estimates (ART 5.1.4.2.1)		
No.	**Scale**	**Measure**
1	Yes/ No	Running estimates were accurate and supported the commander's visualization of the operation.
2	Time	Into future that planning branches have been developed.

3	**Time**	**From receipt of information to complete or update running estimate.**
4	**Percent**	**Of decision points that have branches.**
5	**Percent**	**Of enemy actions or operations that affected course of battle, but not forecast.**
6	**Percent**	**Of forecast branches that appeared at execution.**

Endnotes

1. Army Doctrine Reference Publication (ADRP) 1-03, *The Army Universal Task List*, 2 OCT 2015, pp. 1-25 through 1-26.

2. Ibid., pp. 2-18 through 2-19.

3. Ibid., pp. 2-43 through 2-50.

4. Ibid., pp. 3-1 through 3-4.

5. Ibid., pp. 5-61 through 5-66.

6. Ibid., pp. 5-2 through 5-9.

7. Ibid. p. 5-23.

Appendix F

Key Abbreviations and Acronyms

A	
A2C2S	Army Airborne Command and Control System
AADC	Area air defense commander
AAR	After action review
ABCS	Army Battle Command Systems
ABM	Antiballistic missile
ACM	Airspace coordinating measure
AEW	Airborne early warning
AFATDS	Advanced Field Artillery Tactical Data System
AGM	Attack guidance matrix, air-to-ground missile
ALO	Air liaison officer
AM	Amplitude modulation
AMDC	Air and missile defense commander
AMDS	Autonomous Mine Detection System
AMDWS	Air and Missile Defense Workstation
Amp	Ampere
AMRAAM	Advanced medium-range air-to-air missiles
ANDVT	Advanced Narrowband Secure Voice Terminal
AO	Area of operation
AP	Antipersonnel
ASI	Additional skill identifier
ASM	Anti-ship missile
ATACMS	Army Tactical Missile System
ATO	Air tasking order
AWACS	Airborne Warning and Control System
B	
BCS3	Battle Command Sustainment Support System

BDA	**Battle damage assessment**
BDE	**Brigade**
BE	**Basic encyclopedia**
BFT	**Blue Force Tracker**
BN	**Battalion**
bps	**Bits per second**
C	
C2	**Command and control**
C3	**Command, control, and communications**
CA	**Civil affairs**
CAR	**Combined arms rehearsal**
CCIR	**Commander's critical information requirements**
CEMA	**Cyber electromagnetic activities**
CERF	**Cyber effects request format**
CM	**Collection manager**
CNR	**Combat Net Radio**
CO	**Cyberspace operations**
COA	**Course of action**
COG	**Commander of Operations Group**
COIST	**Company intelligence support team**
COMSEC	**Communications Security**
CONPLAN	**Concept plan**
COP	**Common operational picture**
CP	**Command post**
CPOF	**Command Post of the Future**
CSS	**Combat Service Support**
CAISI	**Combat Service Support Automated Information Systems Interface**
D	
D3A	**Decide, detect, deliver, and assess**
DAMA	**Demand assigned multiple access**
DCGS-A	**Distributed Common Ground System-Army**
DCO	**Defensive cyberspace operations**

DCO-RA	**Defensive cyberspace operation response actions**
DF	**Directional finding**
DOD	**Department of Defense**
DOMEX	**Document and media exploitation**
DTG	**Date-time group**
E	
EA	**Engagement area; Electronic attack**
ECCM	**Electronic counter-countermeasures**
ECM	**Electronic countermeasures**
EHF	**Extremely high frequency**
ELINT	**Electronic intelligence**
EM	**Electromagnetic**
EMARSS	**Enhanced Medium Altitude Reconnaissance and Surveillance System**
EME	**Electromagnetic environment**
EMLCOA	**Enemy most likely course of action**
EMS	**Electromagnetic spectrum**
EO/IR	**Electro-optical/infrared**
EOB	**Electronic order of battle**
EP	**Electronic protection**
EPLRS	**Enhanced Position Location Reporting System**
ES	**Electronic warfare support**
ESM	**Electronic warfare support measures**
EW	**Electronic warfare**
EWC	**Electronic warfare cell**
EWWG	**Electronic warfare working group**
F	
FBCB2	**Force XXI Battle Command—Brigade and Below**
FDM	**Frequency detection multiplexing**
FEZ	**Fighter engagement zone**
FH	**Frequency hop**
FLIR	**Forward-looking infrared**

FLOT	**Forward line of own troops**
FM	**Frequency modulation; Field manual**
FRAGORD	**Fragmentary order**
FSCM	**Fire support coordination measure**
FSO	**Fire support officer**
ft	**Feet; foot**
FTX	**Field training exercise**
FW	**Fixed wing**
G	
GHz	**Gigahertz**
GPS	**Global Positioning System**
H	
HARM	**High-speed anti-radiation missiles**
HCT	**Human intelligence (HUMINT) collection team**
HE	**High explosives**
HF	**High frequency**
HHQ	**Higher headquarters**
HPT	**High-payoff target**
HPTL	**High-payoff target list**
HQ	**HAVE QUICK; headquarters**
HVT	**High-value target**
Hz	**Hertz**
I	
IADS	**Integrated air defense system**
IBS	**Integrated broadcast service**
IC	**Intelligence community**
ICC	**Information coordination central**
IDF	**Indirect fire**
IDM	**Improved Data Modem**
IED	**Improvised explosive device**
IFF	**Identification, friend or foe**
INMARSAT	**International maritime satellite**
INTSUM	**Intelligence summary**
IO	**Information operations**

IP	**Internet protocol; initial point**
IPB	**Intelligence preparation of the battlefield**
IPOE	**Intelligence preparation of the operational environment**
IR	**Incident report; information rate; information requirement; infrared; intelligence requirement**
ISR	**Intelligence, surveillance, and reconnaissance**
ISRT	**Intelligence, surveillance, reconnaissance, and targeting**
IST	**Intelligence support team**
J	
JCA	**Jamming control authority**
JDAM	**Joint direct attack munitions**
JDN	**Joint data network**
JEZ	**Joint engagement zone**
JFACC	**Joint force air component commander**
JICO	**Joint interface control officer**
JINTACCS	**Joint Interoperability of Tactical Command and Control Systems**
JOA	**Joint operations area**
JSIR	**Joint spectrum interference resolution**
JSOW	**Joint stand-off weapon**
JSTARS	**Joint Surveillance Target Attack Radar System**
JTAGS	**Joint Tactical Ground Station**
JTAR	**Joint tactical air strike request**
JTF	**Joint task force**
JTIDS	**Joint Tactical Information Distribution System**
K	
kbps	**Kilobits per second**
KEK	**Key encryption key**
kHz	**Kilohertz**

KLE	**Key leader engagement**
Km	**Kilometer**
KM	**Knowledge management**
kW	**Kilowatt**
L	
LOAC	**Law of armed conflict**
LOB	**Line of bearing**
LOS	**Line of sight**
LST	**Lightweight Satellite Transceiver**
M	
MAC	**Media access control**
MASINT	**Measurement and signature intelligence**
MBITR	**Multiband Inter/Intra Team Radio**
MC	**Mission command**
MC4	**Medical Communications for Combat Casualty Care**
MCIS	**Mission Command Information Systems**
MDCOA	**Most dangerous course of action**
MDMP	**Military decisionmaking process**
MEA	**Munitions effect assessment**
MEL	**Mobile erector launcher**
MEZ	**Missile engagement zone**
MGRS	**Military grid reference system**
MHz	**Megahertz**
MIDB	**Modernized integrated database**
MISO	**Military information support operations**
MLCOA	**Most likely course of action**
MLRS	**Multiple launch rocket system**
MOE	**Measure of effectiveness**
MOP	**Measure of performance**
MOS	**Military occupational specialty**
mph	**Miles per hour**

MRBM	**Medium-range ballistic missile**
MTI	**Moving target indicator**
N	
NAI	**Named area of interest**
NATO	**North Atlantic Treaty Organization**
NIPRNET	**Nonsecure Internet Protocol Router Network**
Nm	**Nautical mile**
NTC	**National Training Center**
NTDR	**Near-term digital radio**
O	
OB	**Order of battle**
OCO	**Overseas contingency operations; offensive cyberspace operations**
OE	**Operational environment**
OP	**Observation post**
OPLAN	**Operation plan**
OPORD	**Operation order**
P	
PACE	**Primary, alternate, contingency, and emergency**
PBUSE	**Property Book Unit Supply Enhanced**
PIR	**Priority intelligence requirement**
PLGR	**Precision lightweight GPS receiver**
PLT	**Platoon**
PNT	**Position, navigation, and timing**
PPLI	**Precise participant location and identification**
PRT	**Provincial reconstruction team**
PT/CT	**Plain text/cipher text**
R	
R&S	**Reconnaissance and surveillance**
RADC	**Regional air defense commander**
RF	**Radio frequency**
RFI	**Request for information**

RM	**Risk management**
ROA	**Restricted operations area**
ROE	**Rules of engagement**
ROZ	**Restricted operating zone**
RTO	**Radio telephone operator**
RW	**Rotary-wing**
S	
SADC	**Sector air defense commander**
SAM	**Surface-to-air missile**
SAMA-E	**Standard Army Maintenance System-Enhanced**
SATCOM	**Satellite communications**
SC	**Single-channel**
SCI	**Sensitive compartmented information**
SEAD	**Suppression of enemy air defenses**
SHF	**Super high frequency**
SHORAD	**Short range air defense**
SIGACT	**Significant activity**
SIGINT	**Signals intelligence**
SINCGARS	**Single-Channel Ground and Airborne Radio System**
SIPRNET	**SECRET Internet Protocol Router Network**
SIR	**Specific information requirement**
SITEMP	**Situation template**
SME	**Subject matter expert**
SMO	**Spectrum management operations**
SOI	**Security operating instruction; signal operating instructions**
SOJ	**Stand-off jammer**
SOP	**Standard operating procedure**
SOR	**Statement of requirement**
SPINS	**Special instructions**
SSB	**Single side band**
SSM	**Surface-to-surface missile**

STAMIS	**Standard Army Management Information System**
Sync	**Synchronization**
T	
TA/FC	**Target acquisition/fire control**
TA	**Target acquisition**
TACSAT	**Tactical satellite**
TADIL J	**Tactical Digital Information Link J**
TAIS	**Tactical Airspace Integration System**
TBM	**Theater ballistic missile**
TC-AIMS	**Transportation Coordinators' Automated Information for Movements System II**
TEK	**Traffic encryption key**
TEL	**Transporter erector launcher**
TELAR	**Transporter erector launcher and radar**
TI	**Tactical internet**
TLAR	**Transporter launcher and radar**
TOC	**Tactical operations center**
TPEA	**Task, purpose, execution, and assessment**
TRANSEC	**Transmission security**
TRISA	**Training and Doctrine Command G-2 Intelligence Support Activity**
TSK	**Transmission security key**
TTP	**Tactics, techniques, and procedures**
U	
UAS	**Unmanned aircraft system**
UAV	**Unmanned aerial vehicle**
UHF	**Ultrahigh frequency**
V	
VHF	**Very high frequency**
VIC	**Vehicular intercommunication set**
VSAT	**Very small aperture terminal**

W	
WARNORD	**Warning order**
WEG	**Worldwide equipment guide**
X	
XO	**Executive Officer**

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, the Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL website (CAC login required). The CALL website is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

https://call2.army.mil

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL restricted website (CAC login required): "RFI or Request Pubs" or "Contact CALL."

PROVIDE LESSONS AND BEST PRACTICES OR SUBMIT AN AFTER ACTION REVIEW (AAR)

If your unit has identified lessons or best practices or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

CALL Restricted Website <https://call2.army.mil> (CAC login required):

- **Select "Submit Observations, Best Practices, or AARs" tab at the top of the page.**
- **Under "Document Identification," enter AAR subject in "Subject of Lesson or TTP" block.**
- **Identify whether or not the AAR is classified in the "Is it Classified?" block.**
- **Select the "Browse" button by "File to Upload" block and upload the AAR file.**
- **Enter questions or comments in the "Comments/Questions" block.**
- **Press "Submit Form" button.**

Mailing Address: **Center for Army Lessons Learned**
ATTN: Chief, Collection and Analysis Division
10 Meade Ave., Bldg. 50
Fort Leavenworth, KS 66027-1350

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at <https://call2.army.mil>. Mouse over the "RFI or Request Pubs" tab and select "Request for Publication." Please fill in all the information, including your unit name and street address. Please include building number and street for military posts.

NOTE: Some CALL publications are no longer available in print. Digital publications are available by using the "Products" tab on the CALL restricted website.

PRODUCTS AVAILABLE ONLINE

CENTER FOR ARMY LESSONS LEARNED

Access and download information from CALL's restricted website. CALL also offers Web-based access to the CALL archives. The CALL restricted website address is:

https://call2.army.mil

CALL produces the following publications on a variety of subjects:

- **Handbooks**
- **Bulletins, Newsletters, and Trends Reports**
- **Special Studies**
- ***News From the Front***
- **Training Lessons and Best Practices**
- **Initial Impressions Reports**

You may request these publications by using the "RFI or Request Pubs" tab on the CALL restricted website. (**NOTE**: Some CALL publications are no longer available in print. Digital publications are available by using the "Products" tab on the CALL restricted website.)

COMBINED ARMS CENTER (CAC)
Additional Publications and Resources

The CAC home page address is:

http://usacac.army.mil

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <http://usacac.army.mil/cac2/cal>.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history. Find CSI products at <http://usacac.army.mil/cac2/csi/csipubs.asp>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <http://www.apd.army.mil> or the Central Army Registry (formerly known as the Reimer Digital Library) <http://www.adtdl.army.mil>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <http://fmso.leavenworth.army.mil>.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <http://usacac.army.mil/cac2/militaryreview>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA at <https://atn.army.mil/media/dat/TRISA/trisa.aspx> (CAC login required).

Capability Development Integration Directorate (CDID)

CDID conducts analysis, experimentation, and integration to identify future requirements and manage current capabilities that enable the Army, as part of the Joint Force, to exercise Mission Command and to operationalize the Human Dimension. Find CDID at <http://usacac.army.mil/organizations/mccoe/cdid>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <https://jcisfa.jcs.mil/Public/Index.aspx>.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

CENTER FOR ARMY LESSONS LEARNED
10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350

www.leavenworth.army.mil

US Army
Combined
Arms Center
"Intellectual Center of the Army"