

Glossary

Abbreviations and Acronyms

AM	amplitude modulated
AR	Army regulation
ARTEP	Army Training and Evaluation Program
attn	attention
AUTOVON	automatic voice network
BE	basic encyclopedia
BFO	beat frequency oscillator
bn	battalion
c	CONFIDENTIAL
CEOI	communications-electronics operation instructions (see SOI)
CEWI	combat electronic warfare and intelligence
COMINT	communications intelligence
COMSEC	communications security
CPT	captain
CW	continuous wave
C ³	command, control, and communications
C ³ CM	command, control, and communications countermeasures
DA	Department of the Army
DF	direction finder
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures

FM 24-33

E-O	electro-optics
EEFI	essential elements of friendly information
EPLRS	Enhanced Position Location Reporting System
ESM	electronic warfare support measures
EW	electronic warfare
FHMUX	frequency hopping multiplexer
FLOT	forward line of own troops
FM	frequency modulated/field manual (when used with a number)
G2	Assistant Chief of Staff, G2 (Intelligence)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
GEOREF	geographic reference
GHz	gigahertz
HF	high frequency
hi	high
HPBVWA	high-power broadband vehicular whip antenna
HQ	headquarters
IAW	in accordance with
IED	imitative electronic deception
inf	infantry
IHFR	intermediate high frequency radio
JEWC	Joint Electronic Warfare Center
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JTF	joint task force
JTIDS	Joint Tactical Information Distribution System

JUH-MTF	Joint User Handbook for Message Text Format
kHz	kilohertz
km	kilometer
MED	manipulative electronic deception
MHz	megahertz
MIJI	meaconing, intrusion, jamming, and interference
MSE	Mobile Subscriber Equipment
MSRT	mobile subscriber radiotelephone terminal
NAVAID	navigational aid
NCS	net control station
OADR	Originating Agency Determination Required
OPCODE	operations code
OPSEC	operations security
pam	pamphlet
PROWORD	procedure word
pwr	power
RATELO	radiotelephone operator
RAu	radio access unit
RDF	radio direction finding
REC	radio electronic combat
RWR	radar warning receiver
s	SECRET
S2	Intelligence Officer (US Army)
S3	Operations & Training Officer (US Army)
SED	simulative electronic deception

FM 24-33

SIGINT	signals intelligence
SINCGARS	Single-Channel Ground and Airborne Radio System
SNAP-1	steerable null antenna processor
SOI	signal operation instructions
SOP	standing operating procedure
TRADOC	United States Army Training and Doctrine Command
TX	Texas
U	unclassified
US	United States
VHF	very high frequency
Z	Zulu

Terms

AUTHENTICATION. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.

BREVITY CODE. A code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content.

COMMUNICATIONS-ELECTRONICS OPERATION INSTRUCTIONS (CEOI). (See signal operation instructions.)

COMMUNICATIONS INTELLIGENCE (COMINT). Intelligence and technical information derived from foreign communications by other than the intended recipients.

COMMUNICATIONS SECURITY (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

DECEPTION. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence in order to induce him to react in a manner prejudicial to his interests.

ELECTROMAGNETIC SPECTRUM. The frequencies present in a given electromagnetic radiation. A particular spectrum could include a single frequency or a wide range of frequencies.

ELECTRONIC COUNTER-COUNTERMEASURES (ECCM). That major subdivision of electronic warfare involving actions taken to retain friendly effective use of the electromagnetic spectrum.

ELECTRONIC COUNTERMEASURES (ECM). That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum.

ELECTRONIC WARFARE (EW). Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. Electronic warfare is divided into three categories - ESM, ECM, ECCM.

ELECTRONIC WARFARE SUPPORT MEASURES (ESM). That division of electronic warfare involving actions taken under the direct control of an operational commander to search for, intercept, locate, and identify sources of radiated electromagnetic energy for the purpose of immediate threat recognition.

EMISSION CONTROL. The management of the use of the electromagnetic spectrum by our forces.

ENCRYPT. To convert plain text into unintelligible form by means of a cryptosystem. This cryptosystem can be manual or electronic.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI). Items or activities associated with friendly planning which, if exposed to hostile intelligence activities, would serve as intelligence indicators and thus tend to compromise friendly intentions.

GUARDED FREQUENCIES. Frequencies restricted from friendly use or jamming operations. Guarded frequencies are the enemy's communications and electronics systems from which signals intelligence (SIGINT) and ESM information of tactical and technical importance is derived.

INTERCEPTION. As used in this manual, the act of listening to and/or recording signals intended for another party for the purpose of obtaining intelligence,

INTERFERENCE. Any electrical disturbance which causes undesirable responses in electronic equipment.

INTRUSION. The intentional insertion of electromagnetic energy into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

JAMMING. The deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy.

JOINT INTEROPERABILITY OF TACTICAL COMMAND AND CONTROL SYSTEMS (JINTACCS). A program which provides for information exchange on the battlefield among the military services, the Defense Intelligence Agency, and the National Security Agency. It uses standardized message formats, rules, and vocabulary. (Reference DA Pam 25-7.)

MEACONING. The transmission or retransmission of actual or simulated navigation signals to confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

NET CONTROL STATION (NCS). A station designated to control traffic and enforce circuit discipline within a given net.

OPERATIONS CODE (OPCODE). A code used to encrypt tactical information.

OPERATIONS SECURITY (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

OPERATIONS SECURITY INDICATORS. Actions or information, classified or unclassified, obtainable by an adversary that would result in adversary appreciations, plans, and actions harmful to achieving friendly intentions and preserving friendly military capabilities.

PREVENTIVE ECCM TECHNIQUES. Those measures taken to reduce the vulnerability of the friendly use of the electromagnetic spectrum to the efforts by the enemy to disrupt or destroy that use.

PROCEDURE WORD (PROWORD). A word or phrase limited to radio telephone procedure used to facilitate communications by conveying information in a condensed standard form. (Reference ACP 125.)

PROTECTED FREQUENCIES. Frequencies used by tactical friendly forces for a particular operational requirement that are restricted from friendly jamming operations.

RADIO LISTENING SILENCE. A period during which all or certain radio equipment is kept in a receive only mode on a given net except for the net control station.

RADIO SILENCE. A period during which all or certain radio equipment capable of radiation is kept inoperative.

REMEDIAL ECCM TECHNIQUES. Those actions taken to reduce or negate the effectiveness of enemy efforts to jam the friendly use of the electromagnetic spectrum.

SIGNAL OPERATION INSTRUCTIONS (SOI). A series of orders issued for the technical control and coordination of the signal activities of a command. Contains frequencies, call signs, and other information used to establish and maintain radio and other forms of communication.

SIGNAL-TO-JAMMING RATIO. The ratio at a selected point in a signal of the strength of a desired signal to that of a jamming signal.

SINGLE-CHANNEL GROUND AND AIRBORNE RADIO SYSTEM (SINCGARS). A new family of VHF-FM radios designed to provide the primary means of command and control for Infantry, Armor, and Artillery units. The radios can transmit and receive voice and tactical data while operating in a frequency hopping mode.

TABOO FREQUENCIES. Frequencies that are restricted from use or jamming by friendly forces. The following are some examples of these frequencies. Defense Communications System radar frequencies used for friendly early warning air defense; internationally controlled or treaty-governed frequencies, such as broadcast emergency frequencies and commercial air and shipping traffic control frequencies.

VOICE TEMPLATES. Standardized pre-formatted messages used with the JINTACCS message text procedures.