GLOSSARY

ACRONYMS AND ABBREVIATIONS

admin	administration
APC	armored personnel carrier
ASPS	all-source production section
arty	artillery
BAT-D	battlefield deception
BBC	British Broadcasting Corporation
bde	brigade
bn	battalion
C3	command, control and communications
C3CM	command, control, and communications countermeasures
CAA	combined arms army
C-E	communications-electronics
CESO	C-E staff officer
CEWI	combat electronic warfare intelligence
CI	counterintelligence
co	company
comd	command
COMINT	communications intelligence
comm	communications
COMSEC	communications security
cons	consideration
CP	command post
CS	combat support
CSS	combat service support
CTOC	corps tactical operations center
DA	Department of the Army
D-day	a day set for launching an operation, specifically, June 6, 1944, on which Allied forces began the invasion of France in World War II.
div	division
DOD	Department of Defense
EAC	echelons above corps
ECB	echelons corps and below
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EEFI	essential elements of friendly information
EW	electronic warfare

FEBA	forward edge of the battle area
FLOT	forward line of own troops
FM	field manual
FRAGO	fragmentary order
FSE	fire support element
FTI	fixed target indicators
G1	Assistant Chief of Staff, G1 (Personnel)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
HHC	headquarters, headquarters company
HUMINT	human intelligence
HVT	high value target
ICD	imitative communications deception
IED	imitative electronic deception
IMINT	imagery intelligence
INCD	imitative noncommunications deception
intel	intelligence
inf	infantry
IPB	intelligence preparation of the battlefield
IR	information requirements
J3	Operations Directorate
JTF	Joint Task Force
LIC	low intensity conflict
LOC	lines of communication
log	logistics
LOS	line of sight
MCCD	multispectral close contact decoy
MCD	manipulative communications deception
MED	manipulative electronic deception
METT-T	mission, enemy, terrain, troops, and time available
MI	military intelligence
MNCD	manipulative noncommunications deception
MOP	Memorandum of Policy
MTI	moving target indicators
MTOE	modified table of equipment
MSD	multispectral decoy

NBBS	New British Broadcast Station
NCA	National Command Authority
NLT	not later than
no	number
obsn	observation
OIC	officer in charge
OMG	operation maneuver group
op	operation
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
photo	photographic
PIR	priority intelligence requirements
POL	petroleum, oils, and lubricants
prelim	preliminary
PSYOP	psychological operations
PWE	Political Warfare Executive
RAF	Royal Air Force
recon	reconnaissance
RF	radio frequency
RTO	radio telephone operator
S1	Adjutant (United States Army)
S3	Operations and Training Officer (United States Army)
S4	Supply Officer (United States Army)
SALUTE	size, activity, location, unit, time, equipment
SAM	surface-to-air missile
SED	simulative electronic deception
SIGINT	signals intelligence
SIGSEC	signal security
sit	situation
SOP	standing operating procedures
TAC-D	tactical deception
tech	technical
TDSE	tactical deception support element
TOC	tactical operations center
TRADOC	Training and Doctrine Command
UAV	unmanned air vehicles
US	United States
USSR	Union of Soviet Socialist Republics
vol	volume

DEFINITIONS

acoustical intelligence (JCS Pub 1-DOD)	Technical and intelligence information derived from foreign sources that generate acoustical waves.
acoustical surveillance (JCS Pub 1-DOD)	Employment of electronic devices including sound recording, receiving, or transmitting equipment for the collection of information.
battlefield deception (DA) (AR 310-25)	Those operations or measures conducted at echelons Theater and below to purposely mislead enemy forces by distorting, concealing, or falsifying indicators of friendly intent.
camouflage (JCS Pub 1-DOD, IADB)	The use of concealment and disguise to minimize the possibility of detection and/or identification of troops, materiel, equipment, and installations. Includes taking advantage of the natural environment as well as application of natural and artificial materials.
chaff (JCS Pub 1-DOD, IADB)	Radar reflectors, which consist of thin, narrow metallic strips of various lengths and frequency responses, used to reflect echoes to confuse opponents.
clandestine operation (JCS Pub 1-DOD, IADB)	An activity to accomplish intelligence, CI, and other similar activities sponsored or conducted by governmental departments or agencies, in such a way as to assure secrecy or concealment. (It differs from covert operations in that emphasis is placed on concealment of the operation rather than on concealment of the identity of sponsor.)
code (JCS Pub 1-DOD, IADB)	a. Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or for security. b. A cryptosystem in which cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements that are primarily words, phrases, or sentences.

code word (JCS Pub 1-DOD, NATO, IADB)	a. A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. b. A cryptonym used to identify sensitive intelligence data.
collection (acquisition) (JCS Pub 1-DOD)	Obtaining information in any manner, including direct observation, liaison with official agencies, or soliciting from official, unofficial, or public sources.
collection (intelligence)	Exploiting information sources by the proper intelligence processing unit to produce and report intelligence. Collection is divided into four main functions: guidance, coverage, reporting, and selection.
command, control, and communications countermeasures (C^3CM)	Integrated use of OPSEC, military deception, jamming, and physical destruction supported by intelligence to deny information to the enemy, to influence, degrade, or destroy adversary C^3 capabilities, and to protect friendly C^3 against such actions.
communications cover and communications deception (or communications cover and deception) (JCS MOP 116-DOD)	Terms that broadly identify deception and cover activities in communications. Communications cover encompasses activities not considered deception: a. Communications cover (JCS MOP 116-DOD). The technique of concealing or altering the characteristics of communication patterns for the purpose of denying valuable information to an enemy. b. Communications deception (JCS MOP 116-DOD). Deliberate transmission, retransmission, or alteration of communications in a manner intended to cause a misleading interpretation. (1) ICD. Introduction by unauthorized parties of signals or traffic, which imitate valid messages, into communications channels to deceive authorized users of the communications system. (2) MCD. Alteration or simulation of friendly communications for purposes of deception.

communications intelligence (COMINT) (JCS Pub 1-DOD, IADB)	Technical and intelligence information derived from foreign communications by other than the intended recipients.
communications security (COMSEC) (JCS Pub 1-DOD, IADB)	The protection resulting from all measures designed to deny to unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such study. Also called COMSEC, communications security includes: a. Crypto security. The component of COMSEC that results from providing technically sound crypto systems and their proper use. b. Transmission security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. c. Emission security. The component of COMSEC that results from all measures taken to deny unauthorized persons information of value which might be derived from interception and analysis of compromising emanations from crypto equipment and telecommunications systems. d. Physical security. The component of COMSEC which results from all physical measures needed to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.
communications security monitoring (JCS Pub 1-DOD, IADB)	The act of listening to, copying, or recording transmissions of one's own circuits (or when specially agreed, such as, in allied exercise, those of friendly forces) to provide material for COMSEC analysis in order to determine the degree of security being provided to those transmissions. In particular, the purposes include providing a basis for advising

	commanders on the security risks resulting from their transmissions, improving the security of communications, and planning and conducting MCD operations.
concealment (JCS Pub 1-DOD)	Protection from observation or surveillance.
confusion reflector (JCS Pub 1-DOD, NATO)	A reflector of electromagnetic radiation used to create echoes for confusion purposes. Radar confusion reflectors include such devices as chaff, rope, and corner reflectors.
corner reflector (JCS Pub 1-DOD, NATO)	a. A device, normally consisting of three metallic surfaces or screens perpendicular to one another, designed to act as a radar target or marker. b. In radar interpretation, an object that, by means of multiple reflections from smooth surfaces, produces a radar return of greater magnitude than might be expected from the physical size of the object.
counterdeception (JCS Pub 1-DOD)	Efforts to negate, neutralize, and diminish the effects of, or gain advantage from, a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations.
cover (JCS Pub 1-DOD, NATO)	a. The action by land, air, or sea forces to protect by offense, defense, or threat of either or both. b. Shelter or protection, either natural or artificial. c. Protection guise used by a person, organization, or installation to prevent identification with clandestine activities.
covert operations (JCS Pub 1-DOD, IADB)	Operations that are so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. They differ from clandestine operations in that emphasis is placed on concealment of the identity of sponsor rather than on concealment of the operation.

deception (JCS Pub 1-DOD, IADB)	Those measures designed to mislead enemy forces by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.
deception concept (JCS MOP 116-DOD)	Ideas or potential courses of action for using deception.
deception means (JCS Pub 1-DOD)	Methods, resources, and techniques that can be used to convey or deny information to a foreign power. There are three categories of deception means: a. Administrative means. Resources, methods, and techniques designed to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. b. Physical means. Activities and resources used to convey or deny selected information to a foreign power. Examples include military operations, including exercises; reconnaissance, training activities, and movement of forces; the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; and test and evaluation activities. c. Technical means. Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, reradiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or supression of nuclear particles.
deception objectives (JCS MOP 116-DOD)	The ultimate purpose of a deception plan in terms of the action or lack of action desired from the target against whom the deception is directed.
deception plan	A complete plan which details and formalizes a deception operation and, when approved, authorizes execution.

	a. Deception measures (DA). The deliberate provision of false indicators to meet enemy EEI. Deception measures are visual, sonic, electronic, and olfactory. b. Deception story (DA). False information provided to the enemy to lead him to an incorrect estimate of our capabilities and intentions. c. Deception tasks (DA). The directions given to subordinate units to carry out their roles in the projection of the deception story. Units are directed to conduct feints, demonstrations, ruses, and displays.
deception target	Foreign decision makers against whom deception operations are ultimately directed.
decoy (JCS Pub 1-DOD, NATO, IADB)	An imitation in any sense of person, object, or phenomemon that is intended to deceive enemy surveillance devices or mislead enemy evaluation.
demonstration (JCS Pub 1-DOD, NATO, IADB)	An attack or a show of force on a front where a decision is not sought, made with the aim of deceiving the enemy.
dissimulation	Altering or hiding physical, technical, or administrative evidence by concealing or protecting it from enemy observation.
diversion (JCS Pub 1-DOD)	a. The act of drawing the attention and forces of an enemy from the point of the principal operation; an attack alarm or feint that diverts attention. b. A change made in a prescribed route for operational or tactical reasons.
diversionary attack (JCS Pub 1-DOD, NATO, IADB)	An attack wherein a force attacks, or threatens to attack, a target other than the main target for the purpose of drawing enemy defenses away from the main effort.
dummy	A simulated object used to camouflage an installation, serve as a decoy, or lend reality to a decoy situation.

dummy message (JCS Pub 1-DOD, NATO, IADB)	A message sent for some purpose other than its content, which may consist of dummy groups or meaningless text.
electromagnetic intrusion (JCS Pub 1-DOD)	The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or causing confusion.
electronic warfare (EW) (JCS Pub 1-DOD)	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. There are three divisions within electronic warfare. a. Electronic countermeasures (ECM). That division of EW involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Electronic countermeasures include: (1) Electronic jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems. (2) Electronic deception. The deliberate radiation, reradiation, alteration, suppression, absorbtion, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. Among the types of electronic deception are: (a) Imitative electronic deception (IED). The introduction of radiations into unfriendly channels that imitate hostile emissions. (b) Manipulative electronic deception (MED). Actions to eliminate revealing, or convey misleading, telltale indicators that may be used by hostile forces.

(c) Simulative electronic deception (SED). Actions to represent friendly notional or actual capabilities to hostile forces.

b. Electronic counter-countermeasures (ECCM). That division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW.

c. EW support measures. That division of EW involving actions taken under direct control of an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Thus EW support measures provide a source of information required for immediate decisions involving ECM, ECCM, avoidance targeting, and other tactical employment forces. EW support-measures data can be used to produce SIGINT, both COMINT and ELINT.

electronics intelligence (ELINT) (JCS Pub 1-DOD, IADB) — Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

enemy capabilities (JCS Pub 1-DOD, NATO, IADB) — Those courses of action which the enemy is physically capable of and that, if adopted, will affect accomplishment of our mission. The term "capabilities" includes not only the general courses of action open to the enemy such as attack, defense, or withdrawal, but also all the particular courses of action possible under each general course of action. "Enemy capabilities" are considered in the light of all known factors affecting military operations, including time, space, weather, terrain, and the strength and disposition of enemy forces. In strategic thinking, the capabilities of a nation represent the courses of action within the power of the nation for accomplishing its national objectives in peace and war.

essential elements of friendly information (EEFI) (JCS Pub 1-DOD)	Key questions about friendly intentions and military capabilities likely to be asked by opposing planners and decision makers in competitive circumstances.
execution schedule	Chronological schedule of actions required to execute a deception plan.
feint (Webster's New World Dictionary)	Something feigned or intended to deceive to gain advantage; a false or deceptive act or trick; a mock blow or attack on or toward one area in order to distract the opposition while one attacks another area.
imitative electronic deception (IED)	The introduction of radiation into unfriendly channels that imitate hostile emissions.
infrared deception	The use of sources of infrared energy for purposes of deception.
indicator (JCP Pub 1-DOD, NATO)	In intelligence usage, an item of information that reflects the intention or capability of a potential enemy to adopt or reject a course of action.
meaconing (JCS Pub 1-DOD)	A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.
military deception (JCS Pub 1-DOD).	Actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. There are three categories of military deception: a. Strategic military deception. Military deception planned and executed to result in foreign national policies and actions that

	support the originator's national objectives, policies, and strategic military plans. b. Tactical military deception. Military deception planned and executed by and in support of operational commanders against the pertinent threat, to result in opposing operational actions favorable to the originator's plans and operations. c. Battlefield deception (Army Only). Those operations or measures conducted at echelons Theater and below to purposely mislead enemy forces by distorting, concealing, or falsifying indicators of friendly intent. d. Departmental/service military Deception. Military deception planned and executed by military services about military systems, doctrine, tactics, techniques, personnel, or service operations, or other activities to result in foreign actions that increase or maintain the originator's capabilities relative to adversaries.
minimize (JCS Pub 1-DOD, IADB)	A condition wherein normal message and telephone traffic is drastically reduced so that messages connected with an actual or simulated emergency shall not be delayed.
misinformation (Webster's New World Dictionary)	Information which is false, partially false, or correct, but calculated to mislead; a technique used to mislead, confuse, or otherwise present an enemy with a seemingly authentic story which is actually false and of no real intelligence value.
notional (Webster's New World Dictionary)	Imaginary; not actual (to inhabit a notional world). The adjective "notional" is used to modify such military terms as "plans," "weapons," and "order of battle," when referring to false objects or plans that the friendly force seeks to make the enemy accept as real.
observable (Webster's New World Dictionary)	Anything that is noteworthy or unusual, capable of being observed, discerned, detected, or noticed.

operations security (OPSEC) (JCS Pub 1-DOD).	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.
psychological warfare (JCS Pub 1-DOD IADB).	The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives.
radio deception (JCS Pub 1-DOD, IADB)	The employment of radio to deceive the enemy. Radio deception includes sending false dispatches, using deceptive headings, and employing enemy call signs.
repeater-jammer (JCS Pub 1-DOD, NATO)	A receiver-transmitter device that amplifies, multiplies, and retransmits signals received for purposes of deception or jamming.
ruse	A stratagem or trick usually intended to deceive.
signals intelligence (SIGINT) (JCS Pub 1-DOD, IADB)	A category of intelligence information comprising all communications intelligence, electronics intelligence, and telemetry intelligence.
simulation	Using fabricated or imitative, physical, technical, or administrative evidence to deceive enemy surveillance (detection, identification, and analysis). (Simulate what isn't, mask what is.)
sonic deception	Use of special sonic equipment to simulate such sounds as troop and equipment movements, landing force operations, and gunfire, to cause the target to react in a specific manner.
spot jamming (JCS Pub 1-DOD, NATO, IADB)	The jamming of a specific channel or frequency.
vulnerability (JCS Pub 1-DOD, IADB)	a. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.

b. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.