Glossary

Section L ABBREVIATIONS AND ACRONYMS

A

ACCO	Army Central Control Office
acct	account
ACE	Analysis and Control Element
ACofS	Assistant Chief of Staff
ACR	armored cavalry regiment
ADA	air defense artillery
ADP	automated data processing
ADPSSEP	automatic data processing system security enhancement program
aer	aerial
Al	area of interest
AKA	also known as
AO	area of operations
AR	Army regulation
ARNG	Army National Guard
ARSOF	Army Special Operations Forces
ASAS	All-Source Analysis System
ASP	ammunition supply point
ASPP	Acquisition Systems Protection Program
attn	attention
AWOL	absent without leave

B

BDA	battle damage assessment
BE	basic encyclopedia
BI	background investigation
bn	battalion
BOS	Battlefield Operating System
BSA	brigade support area

C

C^2	command and control
C^3	command, control, and communications
CA	Civil Affairs
CARVE	criticality, accessibility, recuperability, vulnerability, and effect
cdr	commander
C-E	Communications-Electronics
CE	counterespionage
CFSO	CI force protection source operations
CG	commanding general
C-HUMINT	counter-human intelligence
CI	counterintelligence
CIA	Central Intelligence Agency
CIAC	CI Analysis Center
CIAS	counterintelligence analysis section
CIDC	Criminal investigation Command
C-IMINT	counter-imagery intelligence
CINC	Commander in Chief
CM	countermeasures
cmd	command
co	company
COA	course of action
COMINT	communications intelligence
comm	communications
COMSEC	communications security
CONUS	continental United States
CP	command post
C-RISTA	counterreconnaissance, intelligence, surveillance, and target acquisition
C-SIGINT	counter-signals intelligence
CSP	CI scope polygraph

D

DA	Department of the Army
DACAP	DA Cryptographic Access Program
DCID	Director of Central Intelligence Directive
DCII	Defense Central Index of Investigations
DCSINT	Deputy Chief of Staff, Intelligence

demo	demonstration
DF	direction finding
DHS	Defense HUMINT Services
DI	deception indicated
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual
DIS	Defense Investigative Service
DISCOM	Division Support Command
div	division
DIVARTY	division artillery
DM	Deutsche Mark
DOD	Department of Defense
DODD	Department of Defense Directive
DPA	Data Processing Activity
DPOB	date, place of birth
DS	direct support
DSO	defensive source operations
DTAC CP	division tactical CP
DTG	date-time group
DTOC	Division Tactical Operations Center

E

EA	electronic attack
EAC	echelons above corps
ECB	echelons corps and below
EEFI	essential elements of friendly information
ELINT	electronic intelligence
ELSEC	electronic security
EO	executive order
EOB	electronic order of battle
EP	electronic protection
EPB	electronic preparation of the battlefield
EPW	enemy prisoner of war
ES	electronic warfare support
EW	electronic warfare

F

FBI	Federal Bureau of Investigation
FEBA	forward edge of the battle area
FIS	foreign intelligence service
FLOT	forward line of own troops
FM	field manual; frequency modulation
FORSCOM	United States Army Forces Command
FSC	foreign SIGINT collector

G

G2	Assistant Chief of Staff, G2 (Intelligence)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
govt	government
GS	general support

H

HA	humanitarian assistance
HHOC	headquarters, headquarters and operations company
HPT	high-payoff target
HQ	headquarters
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
HVT	high-value target

I

I&S	intelligence and surveillance
I&W	indications and warning
ICF	intelligence contingency funds
ID	identification
IEW	intelligence and electronic warfare
IFF	identification, friend or foe
IMFR	Investigative Memorandum for Record
IMINT	imagery intelligence
INCL	inconclusive
inf	infantry
INS	Immigration and Naturalization Service

INSCOM	United States Army Intelligence and Security Command
intel	intelligence
intg	interrogation
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
IPW	prisoner of war interrogation
IR	information requirements
IRR	Investigative Records Repository

J

J	jamming
J2	Intelligence Directorate
JCS	Joint Chiefs of Staff
J-TENS	Joint Tactical Exploitation of National Systems
JTFCICA	Joint Task Force CI Coordinating Authority

K

KIA	killed in action

L

LAA	limited access authorization
LEA	law enforcement agency
LIC	low-intensity conflict
LLSO	low-level source operation
LNO	liaison officer
LOS	line of sight
LZ	landing zone

M

M	meter
MC	multichannel
MBA	main battle area
MDCI	multidiscipline counterintelligence
MDCISUM	MDCI summary
METT-T	mission, enemy, troops, terrain and weather, and time available
MI	military intelligence
MIJI	meaconing, intrusion, jamming, and interference
MO	modus operandi
MOS	military occupational specialty
MP	military police
MRE	meals ready to eat
MSE	mobile subscriber equipment
msg	message
MTI	moving target indicator
MTOE	modification table of organization and equipment

N

NAC	national agency check
NAI	named areas of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCIS	Naval Criminal Investigation Service
NCO	noncommissioned officer
NDI	no deception indicated
NGIC	National Ground Intelligence Center
NKSOF	North Korean Special Operations Forces
NO	no opinion
no	number
NRT	near-real time

O

OB	order of battle
OCONUS	outside continental United States
OJE	on-the-job experience
OOTW	operations other than war
ops	operations
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
OSI	Office of Special Investigations

P

PCS	permanent change of station
PFC	private first class
PIR	priority intelligence requirements

PL	phase line
plt	platoon
PSG	platoon sergeant
PSI	personnel security investigation
PSYOP	psychological operations

Q

qty	quantity

R

RAF	Royal Air Force
RC	Reserve Components
RDTE	research, development, test, and evaluation
RECCE	reconnaissance
REC	radio electronic combat
RF	radio frequency
RII	request for intelligence information
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
r q r	requirement

S

S2	Intelligence Officer (US Army)
S5	Civil Affairs Officer (US Army)
SA	special agent
SAEDA	Subversion and Espionage Directed Against US Army and Deliberate Security Violations
SALUTE	size, activity, location, unit, time, and equipment
SAP	special access program
SATRAN	see FM 34-5 (S) for classified identification
SCA	special category absentees
SCARF	standard collection asset request format
SCI	sensitive compartmented information
SCO	sub-control office
sec	section
sgt	sergeant
SIGINT	signals intelligence
SIGSEC	signals security
SJA	Staff Judge Advocate
SLAR	side looking airborne radar
SM	service member
SMU	special mission unit
SOFA	Status of Forces Agreement
SOP	standing operating procedure
spec	specialist
SSB	single sideband
SSBI	single scope background investigation
SSN	social security number
STANAG	Standardization Agreement
svc	service

T

tac	tactical
TAO	tactical agent operation
TDA	Tables of Distribution and Allowances
TDY	temporary duty
TEB	tactical exploitation battalion
TOC	tactical operations center
TOE	tables of organization and equipment
TRRIP	Theater Rapid Response Intelligence Package
TSCM	technical surveillance countermeasures
TTP	tactics, techniques, and procedures
TV	television

U

UAV	unmanned aerial vehicle
UCMJ	Uniform Code of Military Justice
US	United States (of America)
USAF	United States Air Force
USAI	United States Army Intelligence
USAIC&FH	US Army Intelligence Center and Fort Huachuca
USAR	United States Army Reserve
USMTF	US message text format

V

VCR	video cassette recorder

W

wpn	weapon

X

exploitation

Section II. TERMS

Analysis - A stage in the intelligence cycle in which information is subjected to review in order to identify significant facts and derive conclusions therefrom.

Assessment - Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity.

Collection Intelligence Cycle - Acquisition of information and the provision of the information to processing or production elements.

Communications Intelligence (COMINT) - Technical and intelligence 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. Communications security includes—cryptosecurity; transmission security; emission security; and physical security of communications security materials and information.

Compromising Emanations - Unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled, or otherwise processed by an information-processing system.

Counterintelligence (CI) - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs. Synonymous with Foreign Counterintelligence.

Counterintelligence (DOD, NATO) (JCS Pub 1) - Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism.

Counterintelligence (Inter-American Defense Board) (JCS Pub 1) - That phase of intelligence covering all activity devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, personnel against subversion, and installations or material against sabotage.

CI Liaison - The establishment and maintenance of personal contacts between CI liaison officers and personnel of organizations which have missions, responsibilities, information resources, or capabilities similar to those of US Army intelligence. It is conducted to promote cooperation, unity of purpose, and mutual understanding; coordinate actions and activities; and to exchange information and viewpoints. OCONUS CI liaison also includes overt collection of foreign intelligence and CI; acquisition from foreign sources of material and assistance not otherwise available; and the procedures used to gain access to individuals whose cooperation, assistance, or knowledge are desired.

Countermeasures - That form of military science that by the employment of devices or techniques, has as its objective the impairment of the operational effectiveness of enemy activity.

Counter-Signals Intelligence (C-SIGINT) - Those actions taken to determine enemy SIGINT capabilities and activities, the assessment of friendly operations to identify patterns and signatures, and the resulting vulnerabilities for subsequent development and recommendation of countermeasures. Recommendations to counter the foreign SIGINT collector (FSC) and EW threat are provided to the G3 by the G2. They can include offensive measures such as electronic attack, to include jamming or deception; or targeting for fire or maneuver.

Critical Node - An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations.

Cryptosecurity - The component of COMSEC which results from the provision of technically sound cryptosystems and their proper use.

Deception - Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce them to react in a manner prejudicial to their interests.

Doctrine - Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

Electronic Protection (EP) - That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Formerly known as electronic counter-countermeasures (ECCM).

Electronic Attack (EA) - That division of electronic warfare involving the use of the electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Formerly known as electronic countermeasures (ECM).

Electronic Deception - The deliberate radiation, reradiation, alteration, suppression, absorption, 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: manipulative electronic deception, simulated electronic deception, and imitative deception.

Electronic Jamming - The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment or systems.

Electronic Security (ELSEC) - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, for example, radar.

Electronics Intelligence (ELINT) - Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

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 electromagnetic spectrum.

Emission Control - The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize C^2 capabilities while minimizing, for OPSEC, detection by enemy sensors; to minimize mutual interference among friendly systems; or to execute a military deception plan.

Emission Security - That component of COMSEC which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crytoequipment and telecommunications systems.

Essential Elements of Friendly Information (EEFI) - Key questions about friendly intentions and military capabilities likely to be asked by opposing planners and decisionmakers in competitive circumstances.

Foreign SIGINT Collector (FSC)/EW - A foreign entity employing electromagnetic and SIGINT techniques to target friendly forces for the purposes of detecting, exploiting, or subverting the C-E environment of the friendly commander.

f-stop - A camera lens aperture setting indicated by an f-number.

Human Intelligence (HUMINT) - A category of intelligence information derived from human sources.

Imagery Intelligence (IMINT) - The collected products of imagery interpretation processed for intelligence purposes.

Indicator - (1) In intelligence usage, an item of information that reflects the intention or capability of a potential enemy to adopt or reject a COA. (2) Activities that can contribute to the determination of a friendly COA.

Intelligence - The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas.

Liaison - That contact or intercommunication maintained between elements of military forces to ensure mutual understanding and unity of purpose and action.

Liaison Contact - The act of visiting or otherwise contacting a liaison source.

Liaison Officer - A CI special agent (SA) assigned the mission of conducting CI liaison.

Liaison Source - An individual with whom liaison is conducted. This term applies regardless of whether the individual furnishes assistance or is contacted on a protocol basis.

Mission - (1) The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. (2) In common usage, especially when applied to lower military units, a duty assigned to an individual or unit to task.

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.

Patterns - Stereotyped actions which so habitually occur in a given set of circumstances that they cue an observer, well in advance, to either the type of military unit or activity, its identity, capabilities or intent. Stereotyping occurs in a variety of ways, such as communications deployment techniques or historical association. Patterns must be unique and detectable to be of military significance.

Profile - The picture formed through the identification and analysis of elements, actions, equipment, and details of military units or activity. Pattern plus signature equals profile.

Risk - A measure of the extent to which a recommended countermeasure has been historically effective in eliminating a vulnerability, given a certain level of susceptibility and threat.

Security - (1) Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or that may, impair its effectiveness. (2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (3) With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.

Signals Intelligence (SIGINT) - A category of intelligence information comprising all communications intelligence, electronic intelligence, and telemetry intelligence.

Signals Security (SIGSEC) - A generic term that includes both COMSEC and ELSEC.

Signature - The identification of a military unit or activity resulting from the unique and detectable visual, imagery, electromagnetic, olfactory, or acoustical display of key equipment normally associated with that type unit or activity.

source - (1) A point of origin or procurement. (2) One that initiates.

Source - Any person who furnishes intelligence information either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes.

SUBJECT - (1) A person who is the principal object of attention. (2) One who is under investigation.

Susceptibility - The degree to which a device, equipment, or weapons systems is open to effective attack due to one or more inherent weaknesses.

Threat - The technical and operational capability of a FSC or EW system to detect, exploit or subvert friendly signals and the demonstrated, presumed or inferred intent of that system to conduct such activity.

Vulnerability - Characteristics of a friendly C-E system or cryptosystem which are potentially exploitable by FSC or EW systems. As applied in this manual, vulnerability is a susceptibility in the presence of a threat. Susceptibility in the absence of a threat does not constitute a vulnerability.