

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

DOD Military Intelligence

U.S. Department of Defense


1978

Glossary of Intelligence Terms

W. S. Liptak Cmdr

Robert Bolin , depositor

Follow this and additional works at: <https://digitalcommons.unl.edu/dodmilintel>

 Part of the [Defense and Security Studies Commons](#), [Military and Veterans Studies Commons](#), [Other Engineering Commons](#), [Peace and Conflict Studies Commons](#), and the [Soviet and Post-Soviet Studies Commons](#)

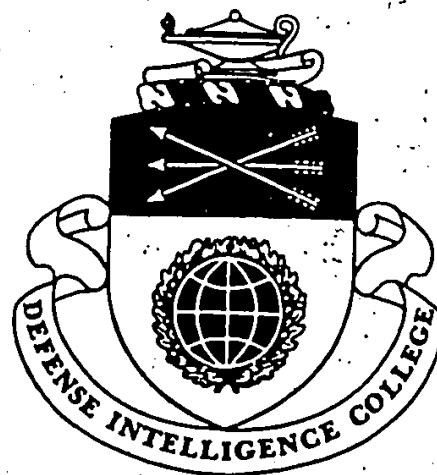
This Article is brought to you for free and open access by the U.S. Department of Defense at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in DOD Military Intelligence by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

00167

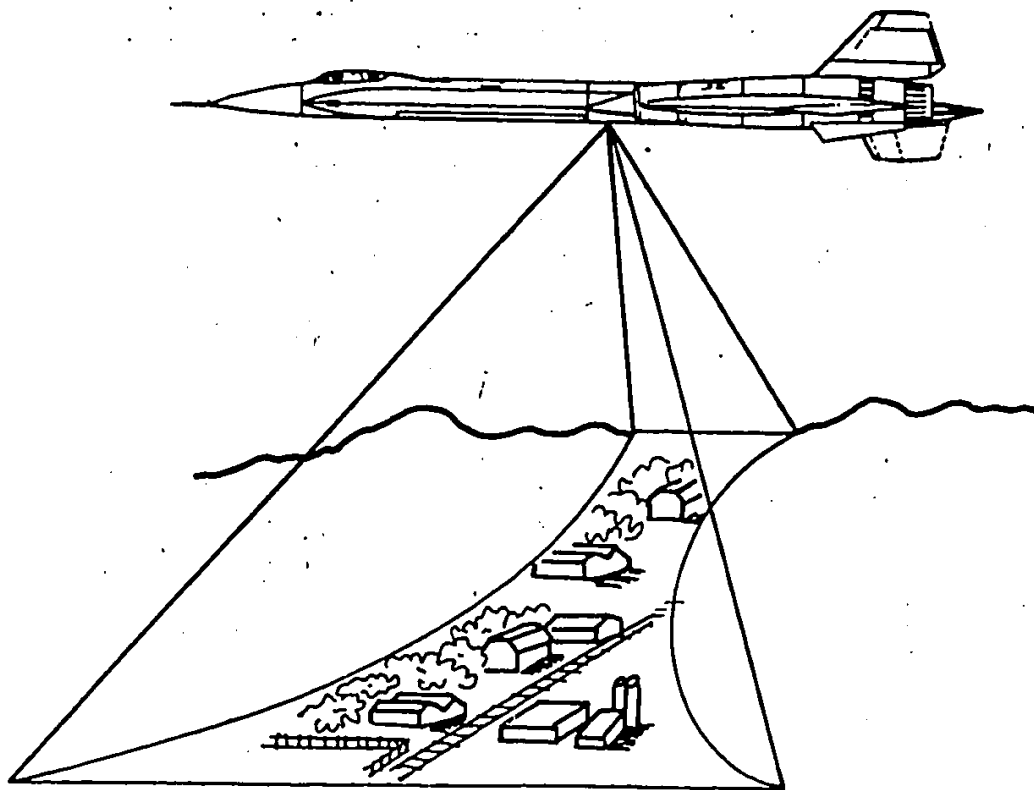
1990/00/00

FOR INSTRUCTIONAL USE ONLY

**SEMINAR ON
RECONNAISSANCE
AND TECHNICAL
INFORMATION
COLLECTION (SORTIC)**



**GLOSSARY OF
INTELLIGENCE TERMS**



Defense Intelligence College Washington, D.C. 20301-6111

FOR INSTRUCTIONAL USE ONLY

GLOSSARY OF
INTELLIGENCE TERMS
EDITED BY
CDR W.S. LIPTAK

METHODOLOGY

The definitions in this glossary have been devised by intelligence officers, not by philologists or semanticists. Some definitions, therefore, may have limited applicability outside the Intelligence Community, while other definitions may be restricted to the single use of a word which has intelligence significance, as, for example, in the word *source*. Insofar as possible, however, the definitions included here contain a measure of consistency of form, and an attempt has been made to establish relationships among important intelligence words and terms. A basic example exists in the relationships to be found among the terms *information*, *intelligence information* and *intelligence*. William R. Corson, in his *The Armies of Ignorance*, observed.

A word of caution about the term *intelligence* is in order. Too often it is used synonymously or interchangeably with *information*. This is inaccurate and quite misleading. Information until and unless it has been analyzed and evaluated remains nothing more than a fact. Information may be interesting, amusing, or hitherto unknown to the person receiving it, but by and in itself it is inappropriate to call it intelligence. The three terms *intelligence*, *intelligence information*, and *information* need to remain distinct. Intelligence by itself refers to the meaning of, or a conclusion about, persons, events, and circumstances which is derived from analysis and/or logic. Intelligence information consists of facts bearing on a previously identified problem or situation, the significance of which has not been completely established. And information is made of raw-facts whose relationship to other phenomena has yet to be considered or established. Similarly, the methods involved in acquiring information and/or intelligence information by any means and turning it into intelligence constitute the intelligence process or cycle. The distinctions between these terms are important to remember. . . .

This glossary makes similar distinctions. *information* is unevaluated material of every description, *intelligence information* is information of potential intelligence value, and *intelligence* is the knowledge derived from a cyclical processing of information. The articulation of these differences is fundamental to the repeated use of these terms in defining other terms. One will find, for example, that nuclear intelligence is defined as *intelligence* derived from the collection and analysis of radiation etc., whereas communications intelligence is defined as technical and *intelligence information* derived from the intercept of foreign communications, etc. (not yet analyzed, it is not yet *intelligence*). Such fine distinctions are expected to contribute to a broader understanding of the common meanings of many such terms.

Arriving at a suitable definition for the word *intelligence* is a challenge unto itself. In Sherman Kent's *Strategic Intelligence for American World Policy*, *intelligence* is characterized as having three definitional subsets: knowledge, organization, and activity. This concept is particularly useful in establishing the fact that *intelligence* in the current context has multiple meanings.

Intelligence, he says, is the knowledge that our nation must possess regarding other nations in order to assure itself that its interests will not fail because of planning or decisionmaking done in ignorance, and upon which knowledge our national foreign

policy is based. *Intelligence* is also an institution, a physical organization of living people which pursues the special kind of knowledge at issue. And *intelligence* is the activity which the organization performs, research, analysis, collection, evaluation, study, presentation, and myriad others.

As helpful as they are, Kent's definitions are excessively delimiting for purposes of this glossary. In the sense that intelligence is knowledge, for example, one cannot assume that all intelligence is "our" intelligence. It is necessary, therefore, to fashion the most basic definition possible for the word *intelligence* in this sense of its meaning, trusting in the utilizer's ability to select a proper modifier to give the word more precise meaning when that is necessary. More definitional flexibility results from such an approach.

But *intelligence* is more than the knowledge contained in an intelligence product. It encompasses the intelligence organizations and activities that Kent refers to, and other activities—and their resultant products—which are known as *counterintelligence*. For these reasons, one might be tempted to define *intelligence* simply as a generic term which encompasses both foreign intelligence and foreign counterintelligence, thence to formulate separate definitions for each of those terms. One quickly discovers, however, that such a simplistic approach is insufficiently satisfying because it fails to provide for several shades of meaning and subsequent use.

The problem is compounded by the scores of different types of intelligence that are used commonly and which must be broadly understood, and by the variety of headings under which these types of intelligence are classified. Some types of intelligence are source-oriented (such as human intelligence or signals intelligence), some form-oriented (as in raw or unfinished intelligence), some system-oriented (electronic or telemetric), some subject-oriented (medical, economic), some use-oriented (military, tactical), and a probable host of others. But the point to be made here is how essential the basic definition of *intelligence* is to further understanding of the many, many ways in which it can be used. The definition of *intelligence* as it appears in this glossary attempts to account for all of the foregoing.

SOME TYPES OF INTELLIGENCE

| | |
|---|---|
| Acoustic(al) Intelligence (ACOUSTINT or ACINT) | Imagery Intelligence (IMINT) |
| Actionable Intelligence | Joint Intelligence |
| Basic Intelligence | Laser Intelligence (LASINT) |
| Biographic(al) Intelligence | Measurement and Signature Intelligence (MASINT) |
| Cartographic Intelligence | Medical Intelligence (MEDINT) |
| Combat Intelligence | Military Intelligence (MI) |
| Communications Intelligence (COMINT) | National Intelligence |
| Counterintelligence | Nuclear Intelligence (NUCINT) |
| Critical Intelligence | Nuclear Proliferation Intelligence |
| Current Intelligence | Operational Intelligence (OPINTEL) |
| Department(al) Intelligence | Optical Intelligence (OPTINT) |
| Economic Intelligence | Photographic Intelligence (PHOTINT) |
| Electro-Optical Intelligence (ELECTRO-OPTINT) | Political Intelligence |
| Electronic Intelligence (ELINT) | Positive Intelligence |
| Energy Intelligence | Radar Intelligence (RADINT) |
| Estimative Intelligence | Radiation Intelligence (RINT) |
| Evasion and Escape Intelligence | Raw Intelligence |
| Finished Intelligence | Scientific and Technical (S&T) Intelligence |
| Foreign Counterintelligence (FCI) | Signals Intelligence (SIGINT) |
| Foreign Instrumentation Signals Intelligence (FISINT) | Special Intelligence (SI) |
| Foreign Intelligence (FI) | Strategic Intelligence |
| Foreign Materiel (FORMAT) Intelligence | Tactical Intelligence (TACINTEL) |
| Geographic(al) Intelligence | Target Intelligence |
| Human Intelligence (HUMINT) | Technical Intelligence (TI) |
| | Telemetry Intelligence (TELINT) |

The reader will notice frequent cross-referencing between terms and their definitions. In addition to providing an intelligence lexicon, the glossary purports to be tutorial, inasmuch as it is possible, and frequent cross-referencing is a technique employed intentionally to that end.

The term cross-referenced most often is *intelligence cycle* which, with its separately defined steps, is conceptually fundamental to understanding the vocabulary of intelligence. The definitional technique is to list the steps in the cycle as subsets of it (rather than in their normal alphabetical order in the glossary), and to refer many related terms to the cycle and its various steps. The desired result is to keep the reader's focus on the intelligence cycle in order to maintain the conceptual integrity of its component steps.

The drafters of the definitions contained in this glossary were not constrained by existing definitions or by the narrow meaning of terms where broader significance could be achieved by redefinition. Known definitions were nevertheless accommodated to the greatest extent possible. The primary objective of the drafters was to define those terms that lacked definition and to improve on those definitions extant.

GLOSSARY OF INTELLIGENCE TERMS AND DEFINITIONS

acoustical intelligence* (ACOUSTINT): Intelligence information derived from analysis of acoustic waves radiated either intentionally or unintentionally by the target into the surrounding medium. (In Naval usage, the acronym *ACINT* is used and usually refers to intelligence derived specifically from analysis of underwater acoustic waves from ships and submarines.)

actionable intelligence: Intelligence information that is directly useful to customers without having to go through the full intelligence production process; it may address strategic or tactical needs, close-support of U.S. negotiating teams, or action elements dealing with such matters as international terrorism or narcotics.

administratively controlled information: Privileged but unclassified material bearing designations such as **FOR OFFICIAL USE ONLY**, or **LIMITED OFFICIAL USE**, to prevent disclosure to unauthorized persons.

advisory tasking: A non-directive statement of intelligence interest or a request for intelligence information which is usually addressed by an element of the Intelligence Community to departments or agencies having information collection capabilities or intelligence assets not a part of the National Foreign Intelligence Program.

agent*: A person who engages in clandestine intelligence activity under the direction of an intelligence organization but who is not an officer, employee, or co-opted worker of that organization.

agent of influence*: A person who is manipulated by an intelligence organization to use his position to influence public opinion or decisionmaking in a manner which will advance the objective of the country for which that organization operates.

alert memorandum: A document issued by the Director of Central Intelligence to National Security Council-level policymakers to warn them of possible developments abroad, often of a crisis nature, of major concern to the U.S.; it is coordinated within the Intelligence Community to the extent time permits.

analysis*: A process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions therefrom. (Also see *intelligence cycle*.)

assessment*: (1) (*General use*) Appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. When used in contrast with *evaluation* assessment implies a weighing against resource allocation, expenditure, or risk. (See *evaluation*.) (2) (*Production context*) See *intelligence assessment*. (Also see *net assessment*.)

asset*: See *intelligence asset*. (Also see *national intelligence asset* and *tactical intelligence asset*.)

authentication: (1) A communications security measure designed to provide protection against fraudulent transmission and hostile imitative communications-deception by establishing the validity of a transmission, message, station, or designator. (2) A means of identifying or verifying the eligibility of a station, originator, or individual to receive specific categories of information. (Also see *communications deception*.)

automatic data processing system security: All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy; it includes: all hardware/software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at the central computer facility; remote computer and terminal facilities, management constraints, physical structures and devices; and the personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system.

basic intelligence*: Comprises general reference material of a factual nature which results from a collection of encyclopedic information relating to the political, economic, geographic, and military structure, resources, capabilities, and vulnerabilities of foreign nations.

biographical intelligence: Foreign intelligence on the views, traits, habits, skills, importance, relationships, health, and curriculum vitae of those foreign personalities of actual or potential interest to the United States Government.

cartographic intelligence: Intelligence primarily manifested in maps and charts of areas outside the United States and its territorial waters.

case officer*: A professional employee of an intelligence organization who is responsible for providing direction for an agent operation. (See *agent*.)

*See Appendix B, Alternate Definitions.

Central Intelligence Agency Program (CIAP): See *National Foreign Intelligence Program*.

cipher*: A cryptographic system in which the cryptographic treatment (i.e., the method of transforming plain text by predetermined rules to obscure or conceal its meaning) is applied to plain text elements such as letters, digits, polygraphs, or bits which either have no intrinsic meaning or are treated without regard to their meaning in cases where the element is a natural-language word.

clandestine: Secret or hidden; conducted with secrecy by design.

clandestine activity: Secret or hidden activity conducted with secrecy by design. (The phrase *clandestine operation* is preferred. Operations are *pre-planned activities*.)

clandestine collection: The acquisition of intelligence information in ways designed to assure the secrecy of the operation.

clandestine communication: Any type of communication or signal originated in support of clandestine operations. (Also see *illicit communication*.)

clandestine operation*: A pre-planned secret intelligence information collection activity or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses both clandestine collection and covert action.

Clandestine Services: That portion of the Central Intelligence Agency (CIA) that engages in clandestine operations; sometimes used as synonymous with the CIA Operations Directorate.

classification: The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is normally termed a *security classification*. (Also see *declassification*.)

classification authority: Those officials within the Executive Branch who have been authorized pursuant to an Executive Order to originally classify information or material.

classified information*: Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

code*: A cryptographic system in which the cryptographic equivalents (usually called *code groups*), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements such as words, phrases, or sentences.

code word*: (Generally, a word or term which conveys a prearranged meaning other than the conventional one; specifically, a word or term chosen to conceal the identity of a function or action, as distinguished from a *cover name* which conceals the identity of a person, organization, or installation. (Also see *cover*.)

CODEWORD*: Any of a series of designated words or terms used with a security classification to indicate that the material so classified was derived through a sensitive source or method, constitutes a particular type of sensitive compartmented information (SCI), and is therefore accorded limited distribution.

collateral: All national security information classified under the provisions of an Executive Order for which special Intelligence Community systems of compartmentation (i.e., *sensitive compartmented information*) are not formally established.

collection*: See *intelligence cycle*.

collection guidance: See *guidance*.

collection requirement: An expression of an intelligence information need which requires collection and carries at least an implicit authorization to commit resources in acquiring the needed information. (Also see *intelligence requirement*.)

combat information: Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the customer's tactical intelligence requirements.

combat intelligence: That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Also see *tactical intelligence*.)

Committee on Exchanges (COMEX): See *Director of Central Intelligence Committee*. (Also see DCID 2/6.)

Committee on Imagery Requirements and Exploitation (COMIREX): See *Director of Central Intelligence Committee*. (Also see DCID 1/13.)

communications cover: See *manipulative communications cover*.

communications deception: The deliberate transmission, retransmission, alteration, absorption, or reflection of telecommunications in a manner intended to cause a misleading interpretation of these telecommunications. It includes:

*See Appendix B, Alternate Definitions

imitative communications deception: Intrusion into foreign communications channels for the purpose of deception by introducing signals or traffic in imitation of the foreign communications.

b. manipulative communications deception: The alteration or simulation of friendly telecommunications for the purpose of deception.

communications intelligence* (COMINT): Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the intercept of communications obtained during the course of counterintelligence investigations within the United States.

communications security* (COMSEC): The protection resulting from any measures taken to deny unauthorized persons information of value which might be derived from telecommunications, or to ensure the authenticity of such telecommunications.

communications security signals acquisition and analysis: The acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required but does not include acquisition of information carried on the system; it is one of the techniques of communications security surveillance. (Also see *communications security surveillance*.)

communications security surveillance: The systematic examination of telecommunications and automatic data processing systems to determine the adequacy of communications security measures; to identify communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation.

Community On-Line Intelligence System (COINS): A network of Intelligence Community computer-based information storage and retrieval systems that have been interconnected for interagency sharing of machine formatted files.

compartmentation*: Formal systems of restricted access to intelligence activities, such systems established by and/or managed under the cognizance of the Director of Central Intelligence to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. (Also see *decompartmentation*.)

compromise*: The exposure of classified official information or activities to persons not authorized access thereto; hence, *unauthorized disclosure*. (Also see *classified information*.)

*See Appendix B, Alternate Definitions

compromising emanations: Unintentional emissions which could disclose information being transmitted, received, or handled by any information-processing equipment.

computer security*: The computer-driven aspects of automatic data processing system security encompassing the mechanisms and techniques that control access to or use of the computer or information stored in it (Also see *automatic data processing system security*.)

Consolidated Cryptologic Program (CCP): See *National Foreign Intelligence Program*.

Consolidated Intelligence Resources Information System (CIRIS): The automated management information system used to identify and display the expected distribution of all intelligence resources within the National Foreign Intelligence Program.

consumer*: See *customer*

co-opted worker: A national of a country but not an officer or employee of the country's intelligence service who assists that service on a temporary or regular basis. (In most circumstances a co-opted worker is an official of the country but might also be, for example, a tourist or student.)

coordination: (1) *(In general)* The process of seeking concurrence from one or more groups, organizations, or agencies regarding a proposal or an activity for which they share some responsibility, and which may result in contributions, concurrences, or dissents. (2) *(In intelligence production)* The process by which producers gain the views of other producers on the adequacy of a specific draft assessment, estimate, or report; it is intended to increase a product's factual accuracy, clarify its judgments, resolve disagreement on issues that permit, and sharpen statements of disagreement on major unresolved issues.

counterintelligence*: See *foreign counterintelligence*.

cover: Protective guise used by a person, organization, or installation to prevent identification with clandestine operations.

covert: See *clandestine*.

covert action: A clandestine operation designed to influence foreign governments, events, organizations, or persons in support of United States foreign policy; it may include political, economic, propaganda, or paramilitary activities. Covert action is referred to in Executive Order No. 12036 as *special activities*. (See *special activities*.)

covert operation: See *clandestine operation* (preferred term) A covert operation encompasses covert action and clandestine collection.

Critical Collection Problems Committee (CCPC): See *Director of Central Intelligence Committee*. (Also see DCID 7/2)

critical intelligence*: Intelligence information or intelligence of such urgent importance to the security of the United States that it is transmitted at the highest priority to the President and other national decisionmaking officials before passing through regular evaluative channels.

Critical Intelligence Communications System (CRITCOMM): Those communications facilities under the operational and technical control of the Director, National Security Agency which have been allocated for the timely handling of critical intelligence. (Also see *critical intelligence*.)

critical intelligence message* (CRITIC): A message designated as containing critical intelligence. (Also see *critical intelligence*.)

cryptanalysis (CA): The steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system or key employed in the encryption.

CRYPTO: A designation which is applied to classified, cryptographic information which involves special rules for access and handling. (Also see *cryptographic information*.)

cryptographic information: All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial ("significantly descriptive" means that the information could, if made known to unauthorized persons, permit recovery of specific cryptographic features of classified crypto-equipment, reveal weaknesses of associated equipment which could allow recovery of plain text or of key, aid materially in the cryptanalysis of a general or specific cryptosystem, or lead to the cryptanalysis of an individual message, command, or authentication). (Also see *CRYPTO*.)

cryptographic security: The component of communications security that results from the provision of technically sound cryptographic systems and which provides for their proper use.

cryptographic system: All associated items of cryptomaterial (e.g., equipment and their removable components which perform cryptographic functions, operating instructions, and maintenance manuals) that are used as a unit to provide a single means of encryption and decryption of plain text so that its meaning may be concealed; also any mechanical or electrical device or method used for the purpose of disguising, authenticating, or concealing the contents, significance, or meanings of communications; short name *cryptosystem*.

cryptography*: The branch of cryptology used to provide a means of encryption and deception of plain text so that its meaning may be concealed.

cryptologic activities: The activities and operations involved in the production of signals intelligence and the maintenance of signals security.

cryptology: The science of producing signals intelligence and maintaining signals security. (Also see *cryptanalysis* and *cryptography*.)

cryptomaterial*: All material (including documents, devices, or equipment) that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.

cryptosecurity: Shortened form of *cryptographic security*. See above.

cryptosystem: Shortened form of *cryptographic system*. See above.

current intelligence*: Intelligence of all types and forms of immediate interest to the users of intelligence; it may be disseminated without the delays incident to complete evaluation, interpretation, analysis, or integration.

customer: An authorized person who uses intelligence or intelligence information either to produce other intelligence or directly in the decisionmaking process; it is synonymous with *consumer* and *user*.

damage assessment: (1) (*Intelligence Community context*.) An evaluation of the impact of a compromise in terms of loss of intelligence information, sources, or methods, and which may describe and/or recommend measures to minimize damage and prevent future compromises. (2) (*Military context*.) An appraisal of the effects of an attack on one or more elements of a nation's strength (military, economic, and political) to determine residual capability for further military action in support of planning for recovery and reconstitution.

DCID 1/2 Attachment: An annual publication by the Director of Central Intelligence (DCI) which establishes a priorities classification system; it presents requirements categories and foreign countries in a geographical matrix, against which priorities are assigned which provide the Intelligence Community with basic substantive priorities guidance for the conduct of all U.S. foreign intelligence activities; it includes a system for adjusting priorities between annual publications; priorities are approved by the DCI with the advice of the National Foreign Intelligence Board. (Also see *priority*.)

deception: Those measures designed to mislead a foreign power, organization, or person by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Also see *communications deception*, *electronic countermeasures*, and *manipulative deception*.)

*See Appendix B Alternate Definitions

declassification: Removal of official information from the protective status afforded by security classification; it requires a determination that disclosure no longer would be detrimental to national security. (Also see *classification*.)

decode: To convert an encoded message into plain text.

decompartmentation: The removal of information from a compartmentation system without altering the information to conceal sources, methods, or analytical procedures. (Also see *compartmentation*.)

decrypt: To transform an encrypted communication into its equivalent plain text.

decipher: To convert an enciphered communication into its equivalent plain text.

defector*: A national of a designated country who has escaped from its control or who, being outside its jurisdiction and control, is unwilling to return and who is of special value to another government because he is able to add valuable new or confirmatory intelligence information to existing knowledge about his country. (Also see *emigre*, *refugee*, and *disaffected person*.)

Defense Intelligence Community*: Refers to the Defense Intelligence Agency (DIA), the National Security Agency (NSA) and the Military Services' intelligence offices including Department of Defense (DoD) collectors of specialized intelligence through reconnaissance programs.

departmental intelligence*: Foreign intelligence produced and used within a governmental department or agency in meeting its assigned responsibilities.

direction finding (DF): A procedure for obtaining bearings on radio frequency emitters with the use of a directional antenna and a display unit on an intercept receiver or ancillary equipment.

Director of Central Intelligence (DCI): The President's principal foreign intelligence adviser appointed by him with the consent of the Senate to be the head of the Intelligence Community and Director of the Central Intelligence Agency and to discharge those authorities and responsibilities as they are prescribed by law and by Presidential and National Security Council directives.

Director of Central Intelligence Committee: Any one of several committees established by the Director of Central Intelligence (DCI) to advise him and to perform whatever functions he shall determine; DCI Committees usually deal with Intelligence Community concerns, and their terms of reference ordinarily are specified in DCI Directives; members may be drawn from all components of the Intelligence Community. (Also see *Director of Central Intelligence Directive*.)

Director of Central Intelligence Directive (DCID): A directive issued by the Director of Central Intelligence which outlines general policies and procedures to be followed by intelligence agencies and organizations which are under his direction or overview.

disaffected person: A person apparently disenchanted with his current situation who may therefore be exploitable for intelligence purposes, e.g., by the willingness to become an *agent* or *defector*. (Also see *walk-in*.)

disclosure: The authorized release of classified information through approved channels.

dissemination*: See *intelligence cycle*.

domestic collection: The acquisition of foreign intelligence information within the United States from governmental or nongovernmental organizations or individuals who are witting sources and choose to cooperate by sharing such information.

double agent*: An agent who is cooperating with an intelligence service of one government on behalf of and under the control of an intelligence or security service of another government, and is manipulated by one to the detriment of the other.

downgrade: To change a security classification from a higher to a lower level.

economic intelligence*: Foreign intelligence concerning the production, distribution and consumption of goods and services, labor, finance, taxation, and other aspects of the international economic system.

Economic Intelligence Committee (EIC): See *Director of Central Intelligence Committee*. (Also see DCID 3/1.)

electro-optical intelligence (ELECTRO-OPTINT): Intelligence information derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far (long wavelength) infrared (1,000 micrometers). (Also see *optical intelligence*.)

electronic countermeasures (ECM): That division of electronic warfare involving actions taken to prevent or reduce an adversary's effective use of the electromagnetic spectrum. Electronic countermeasures include *electronic jamming*, which is the deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the uses of electronic equipment used by an adversary; and *electronic deception*, which is similar but is intended to mislead an adversary in the interpretation of information received by his electronic system.

electronic counter-countermeasures (ECCM): The division of electronic warfare involving actions taken to ensure the effective use of the electromagnetic spectrum despite an adversary's use of electronic countermeasures. (Also see *electronic warfare*.)

* See Appendix B, Alternate Definitions

electronic emission security: Those measures taken to protect all transmissions from interception and electronic analysis.

electronic intelligence* (ELINT): Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than atomic detonation or radioactive sources.

electronic order of battle* (EOB): A listing of noncommunications electronic devices including site designation, nomenclature, location, site function, and any other pertinent information obtained from any source and which has military significance when related to the devices.

electronic security* (ELSEC): The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from their intercept and analysis of noncommunications electromagnetic radiations; e.g., radar.

electronic surveillance*: Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

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. (The three divisions of electronic warfare are: *electronic warfare support measures*, *electronic countermeasures*, and *electronic counter-countermeasures*.)

electronic warfare support measures (ESM): That division of electronic warfare involving actions to search for, intercept, locate, record, and analyze radiated electromagnetic energy for the purpose of exploiting such radiations in support of military operations; thus, electronic warfare support measures provide a source of electronic warfare information which may be used for immediate action involving conduct of electronic countermeasures, electronic counter-countermeasures, threat detection and avoidance, target acquisition, homing, and other combat support measures.

emanations security (EMSEC): The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from other than cryptographic equipment and telecommunications systems. (Also see *emission security*.)

emigre: A person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (Also see *refugee* and *defector*.)

emission security: The component of communications security resulting from all measures taken to deny to unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (Also see *emanations security*.)

encode: To convert plain text into a different form by means of a code.

encipher*: To encrypt plain text by means of a cipher. (Also see *cipher*.)

encrypt*: To convert plain text into a different form in order to conceal its meaning.

end product: See *finished intelligence*. (Also see *product*.)

energy intelligence: Intelligence relating to the technical, economic and political capabilities and programs of foreign countries to engage in development, utilization, and commerce of basic and advanced energy technologies; it includes: the location and extent of foreign energy resources and their allocation; foreign government energy policies, plans, and programs; new and improved foreign energy technologies; and economic and security aspects of foreign energy supply, demand, production distribution, and utilization.

espionage*: Intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed.

essential elements of information (EEI): Those items of intelligence information essential for timely decisions and for enhancement of operations and which relate to foreign power, forces, targets, or the physical environment.

estimative intelligence: A category of intelligence which attempts to project probable future foreign courses of action and developments and their implications for U.S. interests; it may or may not be coordinated and may be either national or departmental intelligence.

evaluation*: Appraisal of the worth of an intelligence activity, information, or product in terms of its contribution to a specific goal; or the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. Evaluation may be used without reference to cost or risk, particularly when contrasted with *assessment*. (Also see *assessment*.) It is also a process in the production step of the intelligence cycle. (See *intelligence cycle*.)

evasion and escape (E&E): The procedures and operations whereby military personnel and other selected individuals are enabled to emerge from enemy held or hostile areas to areas under friendly control.

* See Appendix B, Alternate Definitions.

evasion and escape intelligence: Processed intelligence information prepared to assist personnel to avoid capture if lost in enemy-dominated territory or to escape if captured.

exploitation*: The process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes. (Also see *source*.)

finished intelligence: The result of the production step of the intelligence cycle; the intelligence product. (Also see *intelligence cycle* and *end product*.)

foreign affairs community: Those U.S. Government departments, agencies, and other organizations which are represented in U.S. diplomatic missions abroad, and those which may not be represented abroad but are significantly involved in international activities with the governments of other nations.

foreign counterintelligence (FCI): Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations or persons; it does not include personnel, physical, document, or communications security programs.

foreign instrumentation signals (FIS): Electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and sub-surface systems which may have either military or civilian application; it includes but is not limited to the signals from telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links.

foreign instrumentation signals intelligence (FISINT): Technical and intelligence information derived from intercept of foreign instrumentation signals (see above).

foreign intelligence* (FI): The product resulting from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the United States, and which is provided by a government agency that is assigned an intelligence mission (i.e., an *intelligence agency*). (Also see *intelligence cycle*.)

foreign intelligence service: An organization of a foreign government which engages in intelligence activities.

foreign materiel (FORMAT) intelligence: Intelligence derived from the exploitation of foreign materiel.

foreign official: A person acting in an official capacity on behalf of a foreign power, attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or employed by a public international organization

forward-looking infrared (FLIR) system: An infrared imaging system which raster scans the scene viewed by internal means, both horizontally and vertically; it can be spaceborne, airborne, seaborne, mounted on a ground vehicle, or placed at a fixed site; and its field of view is determined by the optics used, the scanning mechanism, and the dimensions of the detector array

fusion: The blending of intelligence information from multiple sources to produce a single intelligence product.

fusion center: A term used within the Department of Defense referring to an organization having the responsibility of blending both compartmented intelligence information with all other available information in order to support military operations. (Also see *actionable intelligence* and *tactical intelligence*.)

General Defense Intelligence Program (GDIP): See *National Foreign Intelligence Program*.

geographic(al) intelligence: Foreign intelligence dealing with the location, description, and analysis of physical and cultural factors of the world, (e.g. terrain, climate, natural resources, transportation, boundaries, population distribution) and their changes through time.

general medical intelligence (GMI): See *medical intelligence*.

guidance*: Advice which identifies, interprets, clarifies, and/or expands upon an information need. (Also see *information need*.)

human intelligence (HUMINT): A category of intelligence information derived from human sources. (Also see *human source reporting* and *human resources collection*.)

human resources collection: All activities which attend collection of intelligence information from human sources. (See *human intelligence* and *human source*.)

Human Resources Committee (HRC): See *Director of Central Intelligence Committee*. (Also see DCID 1/17.)

human source: A person who wittingly or unwittingly conveys by any means information of potential intelligence value to an intelligence activity.

human source reporting: The flow of intelligence information from those who gather it to the customer; it may come from information gathering activities either within or outside the Intelligence Community. (A form of the term is also used to denote an item of information being conveyed, as in *human source report*.) (Also see *human intelligence*)

illegal: An officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he is connected or with the government operating that intelligence organization

* See Appendix B, Alternate Definitions

illegal agent: An agent operated by an illegal residency or directly by the headquarters of an intelligence organization. (Also see *illegal residency*.)

illegal communication: An electronic communication or signal made without the legal sanction of the nation where it originates.

illegal residency: An intelligence apparatus established in a foreign country and composed of one or more intelligence officers, and which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (Also see *legal residency*.)

illicit communication: An electronic communication or signal originated in support of clandestine operations; it is a type of clandestine communication.

imagery: Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

imagery intelligence (IMINT): The collected products of imagery interpretation processed for intelligence use. (Also see *imagery interpretation* below.)

imagery interpretation (II): The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented by imagery; it includes *photographic interpretation*.

imitative communications deception: See *communications deception*.

imitative deception: The introduction into foreign channels of electromagnetic radiations which imitate his own emissions.

Intelligence and warning (I&W): Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to U.S. or allied military, political, or economic interests, or to U.S. citizens abroad. It encompasses forewarning of: enemy hostile actions or intentions; the imminence of hostilities; serious insurgency; nuclear/nonnuclear attack on the U.S., its overseas forces, or allied nations; hostile reactions to U.S. reconnaissance activities, terrorist attacks; and other similar events.

information: Unevaluated material of every description, at all levels of reliability, and from any source which may contain intelligence information. (Also see *intelligence information*.)

information handling: Management of data or information which may occur in connection with any step in the intelligence cycle; such management may involve activities to transform, manipulate, index, code, categorize, store, select, retrieve, associate or display intelligence materials; it may involve the use of printing, photographic, computer or communications equipment, systems or networks; it may include software programs to operate computers and process data and/or information; and may include information contained in reports, files, data bases, reference services and libraries.

information security: Safeguarding knowledge against unauthorized disclosure; or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure or release to the public, information the protection of which is authorized by executive order or statute.

information need: The requirement of an official involved in the policymaking process or the intelligence production process for the best available information and intelligence on which to base policy decisions, recommendations, or intelligence production.

infrared imagery: A likeness or impression produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared portion of the electromagnetic spectrum.

integration*: A process in the production step of the intelligence cycle in which a pattern is formed through the selection and combination of evaluated intelligence information. (Also see *intelligence cycle*.)

intelligence*: (1) A body of evidence and the conclusions drawn therefrom which is acquired and furnished in response to the known or perceived requirements of customers; it is often derived from information which is concealed or not intended to be available for use by the acquirer; it is the product of a cyclical process. (Also see *intelligence cycle*.)

Examples:

- Policy development requires good *intelligence*.
- Timely *intelligence* is important to informed decisionmaking.

(2) A term used to refer collectively to the functions, activities, or organizations which are involved in the process of planning, gathering, and analyzing information of potential value to decisionmakers and to the production of intelligence as defined in (1) above. (Also see *foreign intelligence* and *foreign counterintelligence*.)

Examples:

- Human source collection is an important *intelligence* activity
- Central Intelligence Agency
- *Intelligence* is a demanding profession.

* See Appendix B, Alternate Definitions

intelligence activities)*: A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations. (Also see *intelligence organization*.)

intelligence agency: A component organization of the Intelligence Community. (Also see *Intelligence Community*.)

intelligence assessment: A category of intelligence production that encompasses most analytical studies dealing with subjects of policy significance; it is thorough in its treatment of subject matter--as distinct from building-block papers, research projects, and reference aids--but unlike estimative intelligence need not attempt to project future developments and their implications; it is usually coordinated within the producing organization but may not be coordinated with other intelligence agencies. (Also see *estimative intelligence*.)

intelligence asset: Any resource--person, group, instrument, installation, or technical system--at the disposal of an intelligence organization.

intelligence collector: A phrase sometimes used to refer to an organization or agency that engages in the collection step of the intelligence cycle. (Also see *intelligence cycle*.)

Intelligence Community (IC): A term which, in the aggregate, refers to the following Executive Branch organizations and activities: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research (INR) of the Department of State; intelligence elements of the military services; intelligence elements of the Federal Bureau of Investigation (FBI); intelligence elements of the Department of Treasury; intelligence elements of the Department of Energy; intelligence elements of the Drug Enforcement Administration; and staff elements of the Office of the Director of Central Intelligence.

Intelligence Community Staff (IC Staff): A term referring to an organization under the direction and control of the Director of Central Intelligence (DCI) formed to assist the DCI in discharging his responsibilities relating to the Intelligence Community.

intelligence consumer: See *customer*.

intelligence cycle*: The processes by which information is acquired and converted into intelligence and made available to customers. There are usually five steps in the cycle:

a. **planning and direction**--determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection entities, and a continuous check on the productivity of collection entities.

b. **collection***--acquisition of information or intelligence information and the provision of this to processing and/or production elements.

c. **processing***--conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence.

d. **production***--conversion of information or intelligence information into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements.

e. **dissemination***--conveyance of intelligence in suitable form to customers.

intelligence estimate*: The product of *estimative intelligence*.

intelligence information*: Information of potential intelligence value concerning the capabilities, intentions, and activities of any foreign power, organization, or associated personnel.

Intelligence Information Handling Committee (IHC): See *Director of Central Intelligence Committee*. (Also see DCID 1/4.)

intelligence information report: A product of the collection step of the intelligence cycle. (Also see *intelligence report*.)

intelligence officer: A professional employee of an intelligence organization who is engaged in intelligence activities.

intelligence organization: A generic term used to refer to any organization engaged in intelligence activities; it may include either an intelligence agency or a foreign intelligence service, or both. (Also see *intelligence agency* and *foreign intelligence service*.)

Intelligence Oversight Board (IOB): A body formed by appointment of the President to provide him and the Attorney General with reports and advice on the legality and propriety of intelligence activities; membership and duties are expressed in Executive Order No. 12036.

intelligence producer: A phrase usually used to refer to an organization or agency that participates in the production step of the intelligence cycle. (Also see *intelligence cycle*.)

intelligence related activities (IRA): Those activities specifically excluded from the National Foreign Intelligence Program which: respond to departmental or agency tasking for time-sensitive information on foreign activities, respond to national Intelligence Community advisory tasking of collection capabilities which have a primary mission of supporting departmental or agency missions or operational forces, of training personnel for intelligence duties, or are devoted to research and development for intelligence and related capabilities.

* See Appendix B, Alternate Definitions.

intelligence report*: A product of the production step of the intelligence cycle. (Also see *intelligence information report*.)

intelligence requirement*: Any subject, general or specific, upon which there is a need for the collection of intelligence information or the production of intelligence. (Also see *collection requirement*.)

Intelligence Research and Development Council (IR&DC): See *Director of Central Intelligence Committee*. (Also see DCID 1/12.)

intelligence user: See *customer*.

Interagency Defector Committee (IDC): See *Director of Central Intelligence Committee*. (Also see DCID 4/1.)

interagency intelligence memorandum (IIM): A national intelligence assessment or estimate issued by the Director of Central Intelligence with the advice of appropriate National Foreign Intelligence Board components.

intercept(ion)*: Acquisition for intelligence purposes of electromagnetic signals (such as radio communications) by electronic collection equipment without the consent of the signallers.

intercept station: A station which intercepts communications or non-communications transmissions for intelligence purposes.

international lines of communications (ILC): Those communications services which are under the supervision of the International Telecommunication Union and which carry paid public communications traffic between different countries; also known as: International Civil Communications, International Commercial Communications, Internationally-Leased Communications, International Service of Public Correspondence, and commercial communications.

international terrorist activity*: The calculated use of violence, or the threat of violence, to attain political goals through fear, intimidation or coercion; usually involves a criminal act, often symbolic in nature, and is intended to influence an audience beyond the immediate victims. *International terrorism* transcends national boundaries in the carrying out of the act, the purpose of the act, the nationalities of the victims, or the resolution of the incident; such an act is usually designed to attract wide publicity in order to focus attention on the existence, cause, or demands of the perpetrators.

interpretation: A process in the production step of the intelligence cycle in which the significance of information or intelligence information is weighed relative to the available body of knowledge. (Also see *intelligence cycle*.)

Joint Atomic Energy Intelligence Committee (JAEIC): See *Director of Central Intelligence Committee*. (Also see DCID 3/3.)

joint intelligence: (1) (*Military context*.) Intelligence produced by elements of more than one military service of the same nation. (2) (*Intelligence Community context*.) Intelligence produced by intelligence organizations of more than one country.

laser intelligence (LASINT): Technical and intelligence information derived from laser systems; it is a subcategory of *electro-optical intelligence*. (See *electro-optical intelligence*.)

legal residency: An intelligence apparatus in a foreign country and composed of intelligence officers assigned as overt representatives of their government but not necessarily identified as intelligence officers. (Also see *illegal residency*.)

manipulative communications cover: Those measures taken to alter or conceal the characteristics of communications so as to deny to any enemy or potential enemy the means to identify them. Also known as *communications cover*.

manipulative communications deception: See *communications deception*.

manipulative deception: The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

measurement and signature intelligence* (MASINT): Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same.

medical intelligence* (MEDINT): Foreign intelligence related to all aspects of foreign natural and man-made environments which could influence the health of military forces; it incorporates general medical intelligence which is concerned with foreign biological medical capabilities and health situations, and medical scientific and technical intelligence which assesses and predicts technological advances of medical significance, to include defense against Chemical, Biological, Radiological Warfare. It applies to both tactical and strategic planning and operations, including military and humanitarian efforts. (Also see *biographical intelligence*.)

* See Appendix B, Alternate Definitions.

military intelligence (MI): Basic, current, or estimative intelligence on any foreign military or military-related situation or activity.

monitor: To observe, listen to, intercept, record, or transcribe any form of communication or media for collection of intelligence information or communications security purposes, either overtly or covertly.

multi-level security: (For automatic data processing (ADP) systems.) Provisions for the safeguarding of all information within a multilevel information handling system. The multilevel information handling system permits various levels, categories, and/or compartments of material to be concurrently stored and processed in a remotely-accessed resource-sharing ADP system, while simultaneously permitting material to be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. Security measures are therefore aimed at ensuring proper matches between information security and personnel security. (Also see *uni-level security*.)

national estimate: See *national intelligence estimate*.

National Foreign Assessment Center (NFAC): An organization established by and under the control and supervision of the Director of Central Intelligence, which is responsible for production of national intelligence.

National Foreign Intelligence Board (NFIB): A body formed to provide the Director of Central Intelligence (DCI) with advice concerning: production, review, and coordination of national foreign intelligence; the National Foreign Intelligence Program budget; inter-agency exchanges of foreign intelligence information; arrangements with foreign governments on intelligence matters; the protection of intelligence sources or methods; activities of common concern; and such other matters as are referred to it by the DCI. It is composed of the DCI (chairman), and other appropriate officers of the Central Intelligence Agency, the Office of the DCI, Department of State, Department of Defense, Department of Justice, Department of the Treasury, Department of Energy, the offices within the Department of Defense for reconnaissance programs, the Defense Intelligence Agency, the National Security Agency, and the Federal Bureau of Investigation; senior intelligence officers of the Army, Navy, and Air Force participate as observers; a representative of the Assistant to the President for National Security Affairs may also attend meetings as an observer

National Foreign Intelligence Program (NFIP): Includes the programs listed below, but its composition shall be subject to review by the National Security Council and modification by the President.

(a) The programs of the Central Intelligence Agency;

(b) The Consolidated Cryptologic Program, the General Defense Intelligence Program, and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance except such elements as the Director of Central Intelligence and the Secretary of Defense agree should be excluded;

(c) Other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence and the head of the department or by the President as national foreign intelligence or counterintelligence activities;

(d) Activities of the staff elements of the Office of the Director of Central Intelligence.

(e) Activities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

national intelligence*: Foreign intelligence produced under the aegis of the Director of Central Intelligence and intended primarily to be responsive to the needs of the President, the National Security Council, and other Federal officials involved in the formulation and execution of national security, foreign political, and/or economic policy.

national intelligence asset: An intelligence asset funded in the National Foreign Intelligence Program, the primary purpose of which is the collection or processing of intelligence information or the production of national intelligence. (Also see *intelligence asset* and *national intelligence*.)

National Intelligence Estimate* (NIE): A thorough assessment of a situation in the foreign environment which is relevant to the formulation of foreign, economic, and national security policy, and which projects probable future courses of action and developments; it is structured to illuminate differences of view within the Intelligence Community; it is issued by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board. (Also see *Special National Intelligence Estimate*.)

National Intelligence Officer (NIO): The senior staff officer of the Director of Central Intelligence (DCI) and the DCI's Deputy for National Intelligence for an assigned area of substantive responsibility; he manages estimative and interagency intelligence production on behalf of the DCI; he is the principal point of contact between the DCI and intelligence consumers below the cabinet level; he is charged with monitoring and coordinating that portion of the National Foreign Assessment Center's production that involves more than one office or that is interdisciplinary in character; and is a primary source of national-level substantive guidance to Intelligence Community planners, collectors, and resource managers.

* See Appendix B, Alternate Definitions

National Intelligence Tasking Center (NITC): The central organizational mechanism established under the direction, control and management of the Director of Central Intelligence for coordinating and tasking national foreign intelligence collection activities, and for providing advisory tasking to other intelligence and information gathering activities.

national security: The territorial integrity, sovereignty, and international freedom of action of the United States. (*Intelligence activities relating to national security* encompass all the military, economic, political, scientific and technological, and other aspects of foreign developments which pose actual or potential threats to U.S. national interests.)

national/tactical interface: A relationship between national and tactical intelligence activities encompassing the full range of fiscal, technical, operational, and programmatic matters.

near-real-time: The brief interval between the collection of information regarding an event and reception of the data at some other location, caused by the time required for processing, communications, and display.

net assessment: A comparative review and analysis of opposing national strengths, capabilities, vulnerabilities, and weaknesses. (*An intelligence net assessment* involves only foreign countries.)

nuclear intelligence (NUCINT): Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources.

nuclear proliferation intelligence: Foreign intelligence relating to (1) scientific, technical, and economic capabilities and programs and the political plans and intentions of nonnuclear weapons states or foreign organizations to acquire nuclear weapons and/or to acquire the requisite special nuclear materials and to carry on research, development, and manufacture of nuclear explosive devices, and; (2) the attitudes, policies, and actions of foreign nuclear supplier countries or organizations within these countries toward provision of technologies, facilities, or special nuclear materials which could assist nonnuclear weapons states or foreign organizations to acquire or develop nuclear explosive devices.

official: See *foreign official*.

official information: Information which is subject to the control of the United States Government.

open source information: A generic term describing information of potential intelligence value (i.e., *intelligence information*) which is available to the general public.

operational control (OPCON): (*military context*) The authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location; to deploy the forces concerned; and to retain or assign tactical control of those forces. (It does not, of itself, include administrative or logistic control)

* See Appendix B, Alternate Definitions

operational intelligence* (OPINTEL): Intelligence required for planning and executing operations.

operations security (OPSEC): Those measures designed to protect information concerning planned, ongoing, and completed operations against unauthorized disclosure.

optical intelligence (OPTINT): That portion of electro-optical intelligence that deals with visible light. (Also see *electro-optical intelligence*)

order of battle (OB): Intelligence pertaining to identification, strength, command structure, and disposition of the personnel, units, and equipment of any foreign military force. (Also see *technical intelligence*.)

overt: Open; done without attempt at concealment.

overt collection: The acquisition of intelligence information from public media, observation, government-to-government dialogue, elicitation, and from the sharing of data openly acquired; the process may be classified or unclassified; the target and host governments as well as the sources involved normally are aware of the general collection activity although the specific acquisition, sites, and processes may be successfully concealed.

penetration: (1) (clandestine operations.) The recruitment of agents within or the infiltration of agents or introduction of technical monitoring devices into an organization or group or physical facility for the purpose of acquiring information or influencing its activities. **(2) (automatic data processing (ADP) operations.)** The unauthorized extraction and identification of recognizable information from a protected ADP system.

personnel security: The means or procedures--such as selective investigations, record checks, personal interviews, and supervisory controls--designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy.

photographic intelligence (PHOTINT): The collected products of photographic interpretation classified and evaluated for intelligence use; it is a category of *imagery intelligence*.

photographic interpretation (FI): The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented on photography; it is a category of *imagery interpretation*.

physical security*: Physical measures--such as safes, vaults, perimeter barriers, guard systems, alarms and access controls--designed to safeguard installations against damage, disruption or unauthorized entry; information or material against unauthorized access or theft; and specified personnel against harm.

plain text*: Normal text or language, or any symbol or signal, that conveys information without any hidden or secret meaning

planning and direction: See *intelligence cycle*

Policy Review Committee (As pertains to intelligence matters) (PRC(I)): A committee established under the National Security Council which when meeting under the chairmanship of the Director of Central Intelligence is empowered to establish requirements and priorities for national foreign intelligence and to evaluate the quality of the intelligence product; it is sometimes referred to as the *Policy Review Committee (Intelligence)*; its specific duties are defined in Executive Order No. 12036.

political intelligence*: Intelligence concerning the dynamics of the internal and external political affairs of foreign countries, regional groupings, multilateral treaty arrangements and organizations, and foreign political movements directed against or impacting upon established governments or authority.

positive intelligence: A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence.

priority: A value denoting a preferential rating or precedence in position which is used to discriminate among competing entities; the term normally used in conjunction with intelligence requirements in order to illuminate importance and to guide the actions planned, being planned, or in use, to respond to the requirements.

processing*: See *intelligence cycle*.

product: (1) An intelligence report disseminated to customers by an intelligence agency. (2) In SIGINT usage, intelligence information derived from analysis of SIGINT materials and published as a report or translation for dissemination to customers. (Also see *production* in Appendix B.)

production*: See *intelligence cycle*.

proprietary: A business entity owned, in whole or in part, or controlled by an intelligence organization and operated to provide private commercial cover for an intelligence activity of that organization. (Also see *cover*.)

radar intelligence (RADINT): Intelligence information derived from data collected by radar.

radiation intelligence* (RINT): The functions and characteristics derived from information obtained from unintentional electromagnetic energy emanating from foreign devices; excludes nuclear detonations or radioactive sources.

raw intelligence: A colloquial term meaning collected intelligence information which has not yet been converted into intelligence. (Also see *intelligence information*.)

reconnaissance (RECCE or RECON): An operation undertaken to obtain by visual observation or other detection methods information relating to the activities, resources or forces of a foreign nation, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

recruitment-in-place: A person who agrees to become an agent and retain his position in his organization or government while reporting on it to an intelligence or security organization of a foreign country.

RED/BLACK Concept: The separation of electrical and electronic circuits, components, equipment, and systems which handle classified plain language information in electric signal form (RED) from those which handle encrypted or unclassified information (BLACK); RED and BLACK terminology is used to clarify specific criteria relating to and differentiating between such circuits, components, equipment, and systems and the areas in which they are contained.

refugee: A person who is outside the country or area of his former habitual residence and who, because of fear of being persecuted or because of hostilities in that country or area, is unwilling or unable to return to it. (Also see *defector* and *emigre*.)

report: See *intelligence report* and *intelligence information report*.

requirement*: See *intelligence requirement* or *collection requirement*.

residency: See *illegal residency* and *legal residency*.

sabotage: Action against material, premises or utilities, or their production, which injures, interferes with, or obstructs the national security or ability of a nation to prepare for or carry on a war.

safe house: A house or premises controlled by an intelligence organization that affords—at least temporarily—security for individuals involved or equipment used in clandestine operations.

sanitization: The process of editing or otherwise altering intelligence information or reports to protect sensitive intelligence sources, methods, capabilities, analytical procedures, or privileged information in order to permit wider dissemination.

scientific and technical (S&T) intelligence*: Intelligence concerning foreign development in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapon systems and their capabilities and characteristics; it also includes intelligence which requires scientific or technical expertise on the part of the analyst, such as medicine, physical health studies, and behavioral analyses.

* See Appendix B, Alternate Definitions

Scientific and Technical Intelligence Committee (STIC): See *Director of Central Intelligence Committee*. (Also see DCID 3/5.)

security: Establishment and maintenance of protective measures which are intended to ensure a state of inviolability from hostile acts or influences.

TYPES OF SECURITY

Automatic Data Processing System Security
Communications Security
Computer Security
Cryptographic Security
Electronic Emission Security
Electronic Security
Emanation Security
Emission Security
Information Security
Multi-level Security
National Security
Operations Security
Personnel Security
Physical Security
Signals Security
Transmission Security
Uni-level Security

security classification: See *classification*.

Security Committee (SECOM): See *Director of Central Intelligence Committee*. (Also see DCID 3/11.)

sensitive*: Requiring special protection from disclosure to avoid compromise or threat to the security of the nation.

sensitive compartmented information* (SCI): All information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established. (Also see *compartmentation*.)

sensitive intelligence sources and methods: A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support U.S. intelligence activities.

Service Cryptologic Agencies (SCA): See *Service Cryptologic Elements*.

* See Appendix B, Alternate Definitions

Service Cryptologic Elements: A term used to designate separately or together those elements of the U.S. Army, Navy, and Air Force which perform cryptologic functions, also known as Service Cryptologic Agencies and Service Cryptologic Organizations.

Service Cryptologic Organizations (SCO): See *Service Cryptologic Elements*.

sensor: (1) A technical device designed to detect and respond to one or more particular stimuli and which may record and/or transmit a resultant impulse for interpretation or measurement, often called a *technical sensor*. (2) *special sensor:* An unclassified term used as a matter of convenience to refer to a highly classified or controlled technical sensor.

side-looking airborne radar (SLAR): An airborne radar, viewing at right angles to the axis of the vehicle, which produces a presentation of terrain or targets.

SIGINT activity: Any activity conducted for the purpose of producing signals intelligence. (Also see *SIGINT-related activity*.)

SIGINT Committee: See *Director of Central Intelligence Committee*. (Also see DCID 6/1.)

SIGINT-related activity: Any activity primarily intended for a purpose(s) other than signals intelligence (SIGINT), but which can be used to produce SIGINT, or which produces SIGINT as a by-product of its principal function(s). (Also see *SIGINT activity*.)

SIGINT technical information: Information concerning or derived from intercepted foreign transmissions or radiations which is composed of technical information (as opposed to intelligence) and which is required in the further collection or analysis of signals intelligence.

signal*: Anything intentionally transmitted by visual and other electromagnetic, nuclear, or acoustical methods for either communications or non-communications purposes.

signals intelligence* (SIGINT): Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

signals security (SIGSEC): A term which includes communications security and electronics security and which encompasses measures intended to deny or counter hostile exploitation of electronic emissions.

signals security acquisition and analysis: The acquisition of electronic emissions and subsequent analysis to determine numerically the susceptibility of the emission to interception and exploitation by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required, but does not include acquisition of information carried on the system; it is one of the techniques of *signals security surveillance*. (Also see *signals security surveillance*.)

signals security surveillance: The systematic examination of electronic emissions to determine the adequacy of signals security measures, to identify signals security deficiencies, to provide data from which to predict the effectiveness of proposed signals security measures, and to confirm the adequacy of such measures after implementation.

source*: A person, device, system, or activity from which intelligence information is obtained. (Also see *human source* and *sensitive intelligence sources and methods*.)

special activities: As defined in Executive Order No. 12036, activities conducted abroad in support of national foreign policy objectives which are designed to further official United States programs and policies abroad and which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but not including diplomatic activity or the collection and production of intelligence or related support functions; also known as *covert action*. (Also see *covert action*.)

Special Activities Office(r) (SAO): A control point for certain categories of compartmented information. (The acronym is often used to refer to the compartmented information itself.)

Special Coordination Committee (SCC): A committee established under the National Security Council which deals *inter alia* with the oversight of sensitive intelligence activities, such as covert actions, which are undertaken on Presidential authority.

special intelligence (SI): An unclassified term used to designate a category of sensitive compartmented information (SCI). (Also see *sensitive compartmented information*.)

special intelligence communications* (SPINT-COMM): A communications network for the handling of all special intelligence and consisting of those facilities under the operational and technical control of the chief of intelligence of each of the military departments, under the management of the Defense Intelligence Agency, and under the technical and security specification criteria established and monitored by the National Security Agency.

Special National Intelligence Estimate (SNIE): National Intelligence Estimates (NIEs) which are relevant to specific policy problems that need to be addressed in the immediate future. SNIEs are generally unscheduled, shorter, and prepared more quickly than NIEs and are coordinated within the Intelligence Community to the extent that time permits. (Also see *National Intelligence Estimate*.)

Special Security Office(r) (SSO): A control point for security procedures within any activity authorized access to sensitive compartmented information.

special sensor*: See *sensor*.

strategic intelligence: Intelligence which is required for the formulation of policy and military plans at national and international levels; it differs primarily from tactical intelligence in level of use, but may also vary in scope and detail.

strategic warning: Intelligence information or intelligence regarding the threat of the initiation of hostilities against the U.S. or in which U.S. forces may become involved; it may be received at any time prior to the initiation of hostilities.

Support for the Analysts' File Environment (SAFE): A joint CIA/DIA project to develop a new computer/microfilm system to support production analysts in reading, filing, and routing cable traffic; building and searching private and central files; and writing, editing, and routing intelligence memoranda and reports.

surveillance: The systematic observation or monitoring of places, persons, or things by visual, aural, electronic, photographic, or other means.

tactical intelligence* (TACINTEL): Foreign intelligence produced under the aegis of the Secretary of Defense and intended primarily to be responsive to the needs of military commanders in the field to maintain the readiness of operating forces for combat operations and to support the planning and conduct of combat operations. (Also see *combat intelligence*.)

tactical intelligence asset: An intelligence asset funded in Department of Defense programs, the primary purpose of which is the collection or processing of intelligence information or the production of tactical intelligence. (Also see *tactical intelligence* and *intelligence asset*.)

target: A country, area, installation, organization, weapon system, military force, situation (political or economic), signal, person, or other entity against which intelligence operations are conducted.

target intelligence: Intelligence which portrays and locates the components of a target or target complex and indicates its identification, vulnerability, and relative importance.

tasking: The assignment or direction of an individual or activity to perform in a specified way to achieve an objective or goal.

technical intelligence (TI): Intelligence on the characteristics and performance of foreign weapons and equipment; a part of *scientific and technical intelligence* and distinct from *order of battle*.

technical sensor: See *sensor*.

technical SIGINT: Intelligence information which provides a detailed knowledge of the technical characteristics of a given emitter and thus permits estimates to be made about its primary function, capabilities, modes of operation (including malfunctions), and state-of-the-art, as well as its specific role within a complex weapon system or defense network; it is a contributor to *technical intelligence*.

* See Appendix B, Alternate Definitions

telecommunications: Any transmission, emission, or reception of signs, signals, writing, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

telemetry intelligence (TELINT): Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of *foreign instrumentation signals intelligence*.

teleprocessing: The overall function of an information transmission system which combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole.

TEMPEST: An unclassified term referring to technical investigations for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emission security.

terrorist organization: A group that engages in terrorist activities. (Also see *international terrorist activity*.)

traffic analysis (TA): The cryptologic discipline which develops information from communications about the composition and operation of communications structures and the organizations they serve. The process involves the study of traffic and related materials, and the reconstruction of communication plans, to produce signals intelligence.

transmission security (TRANSEC): The component of communications security which results from all measures designed to protect transmissions from interception and from exploitation by means other than cryptanalysis.

unauthorized disclosure: See *compromise*.

uni-level security: (*For automatic data processing systems*) Provision for the safeguarding of all material within a single information handling system in accordance with the highest level of classification and most restrictive dissemination caveats assigned to any material contained therein, as distinguished from multilevel security. (Also see *multi-level security*.)

United States Signals Intelligence System (USSS): An entity that is comprised of the National Security Agency (including assigned military personnel); those elements of the military departments and the Central Intelligence Agency performing signals intelligence activities; and those elements of any other department or agency which may from time to time be authorized by the National Security Council to perform signals intelligence activities during the time when such elements are so authorized; it is governed by the *United States Signals Intelligence Directives (USSID)* system.

upgrade: To determine that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher degree. (Also see *classification*.)

user: See *customer*.

validation: A process normally associated with the collection of intelligence information which provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not previously been satisfied. (Also see *collection requirement*.)

walk-in: A person who on his own initiative makes contact with a representative of a foreign country and who volunteers intelligence information and/or requests political asylum. (Also see *disaffected person*.)

Weapon and Space Systems Intelligence Committee (WSSIC): See *Director of Central Intelligence Committee*. (Also see *DCID 3/4*.)

Appendix A

ACRONYMS AND ABBREVIATIONS

| | |
|----------------|---|
| ACINT | Acoustical Intelligence (Naval acronym, see definition.) |
| ACOUSTINT | Acoustical Intelligence |
| A-31 | Assistant Chief of Staff/Intelligence (Army or Air Force) |
| CA | Cryptanalysis |
| CAMS | COMIREX Automated Management System |
| CCF | Collection Coordination Facility |
| CCP | Consolidated Cryptologic Program |
| CCPC | Critical Collection Problems Committee |
| CI | Counterintelligence |
| CIA | Central Intelligence Agency |
| CIAP | Central Intelligence Agency Program |
| CIFAX | Enciphered Facsimile |
| CIPHONY | Enciphered Telephone |
| CIRIS | Consolidated Intelligence Resources Information System |
| CIVISION | Enciphered Television |
| COINS | Community On-Line Intelligence System |
| COMEX | Committee on Exchanges |
| COMINT | Communications Intelligence |
| COMIREX | Committee on Imagery Requirements and Exploitation |
| COMSEC | Communications Security |
| CONTEXT | Conferencing and Text Manipulation System |
| CRITIC | Critical Intelligence Message |
| CRITICOMM | Critical Intelligence Communications System |
| CRYPTO | CRYPTO (See definition) |
| DAO | Defense Attache Office |
| DCI | Director of Central Intelligence |
| DCID | Director of Central Intelligence Directive |
| DEA | Drug Enforcement Administration |
| DEFSMAC | Defense Special Missile and Astronautic Center |
| DF | Direction Finding |
| DIA | Defense Intelligence Agency |
| DNI | Director of Naval Intelligence |
| ECCM | Electronic Counter-Countermeasures |
| ECM | Electronic Countermeasures |
| EEL | Essential Elements of Information |
| E&E | Evasion and Escape |
| EIC | Economic Intelligence Committee |
| ELECTRO-OPTINT | Electro-optical Intelligence |
| ELINT | Electronic Intelligence |
| ELSEC | Electronic Security |
| EMSEC | Emanations Security |
| EOB | Electronic Order of Battle |
| ESM | Electronic Warfare Support Measures |
| EW | Electronic Warfare |
| FBI | Federal Bureau of Investigation |
| FBIS | Foreign Broadcast Information Service |

Appendix A (Continued)

| | |
|----------|--|
| FCI | Foreign Counterintelligence |
| FI | Foreign Intelligence |
| FIS | Foreign Instrumentation Signals |
| FISINT | Foreign Instrumentation Signals Intelligence |
| FLIR | Forward-looking infrared |
| FORMAT | Foreign Materiel |
| GDIP | General Defense Intelligence Program |
| GMI | General Medical Intelligence |
| HPSCI | House Permanent Select Committee on Intelligence |
| HRC | Human Resources Committee |
| HUMINT | Human Intelligence |
| IC | Intelligence Community |
| ICRS | Imagery Collection Requirements Subcommittee (COMIREX) |
| IDC | Interagency Defector Committee |
| IHC | Intelligence Information Handling Committee |
| II | Imagery Interpretation |
| IIM | Interagency Intelligence Memorandum |
| ILC | International Lines of Communications |
| IMINT | Imagery Intelligence |
| INR | Bureau of Intelligence and Research, Department of State |
| IOB | Intelligence Oversight Board |
| IRA | Intelligence-Related Activities |
| IR&DC | Intelligence Research & Development Council |
| I&W | Indications and Warning |
| JAEIC | Joint Atomic Energy Intelligence Committee |
| JINTACCS | Joint Interoperability Tactical Command and Control System |
| LASINT | Laser Intelligence |
| MASINT | Measurement and Signature Intelligence |
| MEDINT | Medical Intelligence |
| MI | Military Intelligence |
| NFAC | National Foreign Assessment Center |
| NFIB | National Foreign Intelligence Board |
| NFIP | National Foreign Intelligence Program |
| NIE | National Intelligence Estimate |
| NIO | National Intelligence Officer |
| NITC | National Intelligence Tasking Center |
| NMIC | National Military Intelligence Center |
| NOIWON | National Operations and Intelligence Watch Officers Network |
| NPHR | National Foreign Intelligence Plan for Human Resources |
| NPIC | National Photographic Interpretation Center |
| NSA | National Security Agency |
| NSCID | National Security Council Intelligence Directive |
| NSOC | National SIGINT Operations Center |
| NSRL | National SIGINT Requirements List |
| NTPC | National Telemetry Processing Center |
| NUCINT | Nuclear Intelligence |

Appendix A (Continued)

| | |
|------------------|--|
| OB | Order of Battle |
| OPCON | Operational Control |
| OPINTEL | Operational Intelligence |
| OPSEC | Operations Security |
| OPTINT | Optical Intelligence |
| PARPRO | Peacetime Airborne Reconnaissance Program |
| PHOTINT | Photographic Intelligence |
| PI | Photographic Interpretation or Photographic Interpreter |
| PRC(I) | Policy Review Committee (Intelligence) |
| RADINT | Radar Intelligence |
| RECCE or RECON | Reconnaissance |
| RINT | Radiation Intelligence |
| S&T | Scientific and Technical |
| SA | Signals Analysis |
| SAFE | Support for the Analysts' File Environment |
| SAO | Special Activities Office |
| SCA | Service Cryptologic Agencies |
| SCC | Special Coordination Committee |
| SCI | Sensitive Compartmented Information or Source Code Indicator |
| SCO | Service Cryptologic Organizations |
| SECOM | Security Committee |
| SI | Special Intelligence |
| SIGINT | Signals Intelligence |
| SIGINT Committee | Signals Intelligence Committee |
| SIGSEC | Signals Security |
| SIRVES | SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee) |
| SLAR | Side-Looking Airborne Radar |
| SNIE | Special National Intelligence Estimate |
| SOSUS | Sound Surveillance System |
| SOTA | SIGINT Operational Tasking Authority |
| SPINTCOMM | Special Intelligence Communications |
| SSCI | Senate Select Committee on Intelligence |
| SSO | Special Security Officer |
| STIC | Scientific and Technical Intelligence Committee |
| TA | Traffic Analysis |
| TACINTEL | Tactical Intelligence |
| TI | Technical Intelligence |
| TELINT | Telemetry Intelligence |
| TRANSEC | Transmission Security |
| USSID | United States Signals Intelligence Directive |
| USSS | United States Signals Intelligence System |
| WWMCCS | Worldwide Military Command and Control Systems |
| WSSIC | Weapon and Space Systems Intelligence Committee |

Appendix B

ALTERNATE DEFINITIONS

acoustical intelligence: The technical and intelligence information derived from foreign sources which generate waves. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

agent: 1) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*). 2) In intelligence usage, one who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

agent of influence: An individual who can be used to influence covertly foreign officials, opinion molders, organizations, or pressure groups in a way which will generally advance United States Government objectives, or to undertake specific action in support of United States Government objectives. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

analysis: In electronic warfare, a study of electromagnetic radiations to determine their technical characteristics and their tactical or strategic use. (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*).

assessment: Judgment of the motives, qualifications, and characteristics of present or prospective employees or "Agent." (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

asset: Any resource—a person, group, relationship, instrument, installation, or supply—at the disposition of an intelligence agency for use in an operational or support role. The term is normally applied to a person who is contributing to a CIA clandestine mission, but is not a fully controlled agent of CIA. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

basic intelligence: 1) General reference material for use in planning concerning other countries which pertains to capabilities, resources or potential theaters of operations. See also -- intelligence---. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*). 2) Factual, fundamental, and generally permanent information about all aspects of a nation—physical, social,

economic, political, biographical, and cultural—which is used as a base for intelligence products in support of planning, policymaking, and military operations. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*). 3) "Fundamental intelligence concerning the general situation, resources, capabilities and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject." (*Recommended Changes to JCS Pub 1, 25 July 1977*).

case officer: A staff employee of the CIA who is responsible for handling agents. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

cipher: Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

clandestine operations: 1) Intelligence, counterintelligence, or other information collection activities and covert political, economic, propaganda and paramilitary activities, conducted so as to assure the secrecy of the operation. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*). 2) Activities to accomplish intelligence, counterintelligence, 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 identity of sponsor.) (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

classified information: "Classified information" means information or material (hereinafter collectively termed "information") that is owned by, produced for or being in the possession of or under the control of the United States Government that has been determined by proper authority to require protection against unauthorized disclosure in the interest of national security and is so designated (*Classification and Declassification of National Security Information and Material; (Executive Order No. 11652 as amended, Nov 1977)*).

code: A system of communication in which arbitrary groups of symbols represent units of plain text. Codes may be used for brevity or for security. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

Appendix B (Continued)

code word: 1) A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a planned operation. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*). 2) A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. (*Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73, (U)*). 3) A word which conveys a meaning other than its conventional one. Prearranged by the correspondents. Its aim is to increase security. (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*).

CODEWORD: 1) A cryptonym used to identify sensitive intelligence data. (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*). 2) A single word selected from those listed in joint Army, Navy, Air Force publication (JANAP) 299 and subsequent volumes, and assigned a classified meaning by appropriate authority to insure proper security concerning intentions, and to safeguard information pertaining to actual, real world military plans or operations classified as Confidential or higher. (*Modern Data Communications Concepts, Language and Media (U), William P. Davenport, Hayden Book Co., Inc., 1971, (U)*).

collection: 1) Any one or more of the gathering, analysis, dissemination or storage of non-publicly available information without the informed express consent of the subject of the information. (*USSID 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U), NSA, 26 May 76*). 2) The act of employing instruments and/or equipment to obtain qualitative or quantitative data from the test or operation of foreign systems. (*Defense Intelligence Collection Requirements Manual (C), DIA, 27 Jan 75*). 3) Used in ELINT to mean the gathering or collection of the unevaluated and uninterpreted information about the enemy or potential enemy, specifically the collection of data from noncommunications radiators such as radars, navigation aids or countermeasures equipments. (*Basic Manual (U), ELINT Collection Analysis Guide (U), National Cryptologic School, 1965, (S)*).

communications intelligence (COMINT): 1) Technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications. However transmitted, COMINT shall not include:

1. Intercept and processing of unencrypted written communications, except the processing of written plain text versions of communications which have been encrypted or are intended for subsequent encryption.

2. Intercept and processing of press, propaganda and other public broadcasts, except for processing encrypted or "hidden meaning" passages in such broadcasts.

3. Oral and wire interceptions conducted under DoD Directive 5200.24.

4. Censorship. (*Signals Intelligence (SIGINT) (U), DOD, 25 Jan 73*).

2) Technical and intelligence information derived from foreign communications by other than the intended recipients:

A. Foreign Communications are all communications except: (1) Those of the governments of the U.S. and the British Commonwealth, (2) Those exchanged among private organizations and nationals, acting in a private capacity of the U.S. and the British Commonwealth. (3) Those of nationals of the U.S. and British Commonwealth appointed or detailed by their governments to serve in the international organizations.

B. COMINT activities are those which produce COMINT by collecting and processing foreign communications passed by radio, wire, or other electromagnetic means, and by the processing of foreign encrypted communications. However transmitted, collection comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of the plaintext, the fusion of these processes, and the reporting of results.

C. Exceptions to COMINT and COMINT activities. COMINT and COMINT activities as defined here do not include: (1) Intercept and processing of unencrypted written communications, except written plaintext versions of communications which have been encrypted or are intended for subsequent encryption. (2) Intercept and processing of press, propaganda and other public broadcasts, except for encrypted or "hidden meaning" passages in such broadcasts (3) Operations conducted by U.S., U.K. or Commonwealth security authorities. (4) Censorship. (5) The interception and study of non-communications transmissions (ELINT). (*USSID 3, SIGINT Security (U), NSA, 24 Aug 72*).

3) Technical and intelligence information derived from foreign communications by someone other than the intended recipient. It does not include foreign press, propaganda, or public broadcasts. The term is sometimes used interchangeably with SIGINT. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

Appendix B (Continued)

communications security (COMSEC): 1) Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications. (*U.S. Intelligence Activities, Executive Order No. 12036, Jan 1978.*) 2) The protection of United States telecommunications and other communications from exploitation by foreign intelligence services and from unauthorized disclosure. COMSEC is one of the mission responsibilities of NSA. It includes cryptosecurity, transmission security, emission security, and physical security of classified equipment, material, and documents. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976.*) 3) The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunications and from application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value which might be derived from the possession and study of such telecommunications or to insure the authenticity of such telecommunications. (*Glossary of Communications Security and Emanations Security Terms (U), U.S. Communications Security Board, Oct. 74.*) 4) 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. Also called COMSEC. Communications security includes: A. Cryptosecurity; B. Transmission Security; C. Emission Security; and D. Physical Security of Communications Security materials and information.

A. Cryptosecurity—The component of communications security which results from the provision of technically sound cryptosystems and their proper use.

B. Transmission Security—The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

C. Emission Security—The component of communications security 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 crypto-equipment and telecommunications systems.

D. Physical Security—The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U).*)

compartmentation: 1) The practice of establishing special channels for handling sensitive intelligence information. The channels are limited to individuals with a specific need for such information and who are

therefore given special security clearances in order to have access to it. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976.*) 2) 1. In SIGINT, special protection given to the production and distribution of SIGINT material of especially sensitive nature because of its source, method of processing, or content. 2. In COMSEC, restricting the use of specific primary cryptovariables to specific operational units grouped together on the basis of their geographical area or their common participation in a mission or operation for the purpose of limiting the information protected by these cryptovariables and thus limiting the adverse impact of a compromise of these variables. (*Basic Cryptologic Glossary (U), NSA, 1971*) 3) 1. Establishment and management of an intelligence organization so that information about the personnel, organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*)

compromise: 1) The loss of control over any COMINT or information related to COMINT or COMINT activities resulting in a reasonable assumption that it could have, or confirmation of the fact that it has, come to the knowledge of an unauthorized person. (*USSID 3, SIGINT Support to Military Commanders (U), NSA, 1 Jul 74.*) 2) The known or suspected exposure of classified information or material in whole or in part to unauthorized persons through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing, or any other means. (*Basic Cryptologic Glossary (U), NSA, 1971*)

computer security: The protection resulting from all measures designed to prevent either deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of classified information in a computer system. (*Basic Cryptologic Glossary (U), NSA, 1971.*)

consumer: An obsolete term for customer. (*Basic Cryptologic Glossary (U), NSA, 1971.*)

counterintelligence: 1) Information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities or assassination: conducted for or on behalf of foreign powers, organizations or persons, but not including personnel, physical, document, or communications security programs. (*U.S. Intelligence Activities, Executive Order No. 12036, Jan 1978.*) 2) Information concerning the protection of foreign intelligence or of national security information and its collection from detection or disclosure. (*USSID 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U), NSA, 26 May 76.*) 3) That phase of intelligence covering all activity devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against

Appendix B. (Continued)

espionage, personnel against subversion, and installations or material against sabotage. See also counter-espionage, countersabotage, countersubversion. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74, 3*) That aspect of intelligence activity which is devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, individuals against subversion, and installations or material against sabotage. See also counterespionage, countersabotage, countersubversion. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

critical intelligence: Intelligence which is critical and requires the immediate attention of the commander. It is required to enable the commander to make decisions which will provide a timely and appropriate response to actions by the potential/actual enemy. It includes but is not limited to the following:

A. Strong indications of the imminent outbreak of hostilities of any type (warning of attack):

B. Aggression of any nature against a friendly country:

C. Indications or use of nuclear-biological chemical weapons (targets): and

D. Significant events within potential enemy countries that may lead to modification of nuclear strike plans. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

critical intelligence message (CRITIC): A message containing information indicating a situation or possibility of a situation which affects the security or interests of the United States or its allies to such an extent that it may require the immediate attention of the President. (*Defense Special Security Communications System (DSSCS) Operating Instructions System Procedures (U), NSA, 6 Feb 73*).

cryptography: The enciphering of plain text so that it will be unintelligible to an unauthorized recipient. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

cryptomaterial: All COMSEC material bearing the marking CRYPTO or otherwise designated as incorporating cryptographic information. Classified cryptoequipments, their classified subdivisions and keying material are considered cryptomaterial even though they do not bear the CRYPTO marking. (*Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73*).

current intelligence: Summaries and analyses of recent events. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

defector: A person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the United States Government. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

Defense Intelligence Community: The Defense Intelligence Agency, National Security Agency, and the intelligence components of the unified and specified command. (*DIHS Glossary of Common Acronyms, Codes, Abbreviations, and Terms Used in Dept. of Defense Intelligence Data Handling Systems (DIHS) Documents (U), DIA, 1970*).

departmental intelligence: 1) Intelligence which any department or agency of the Federal Government requires to execute its own mission. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*). 2) The intelligence which Government departments and agencies generate in support of their own activities. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

dissemination: The distribution of intelligence products (in oral, written, or graphic form) to departmental and agency intelligence consumers. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

double agent: Agent in contact with two opposing intelligence services only one of which is aware of the double agent contact or quasi-intelligence services. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

economic intelligence: Intelligence regarding foreign economic resources, activities, and policies. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

electronic intelligence (ELINT): 1) That technical and intelligence information derived from foreign electromagnetic noncommunications transmissions by other than the intended recipients. (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*). 2) The intelligence information product of activities engaged in the collection and processing for subsequent intelligence purposes of foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations and radioactive sources. (*Basic Cryptologic Glossary (U), NSA, 1971*). 3) Technical and intelligence information derived from the collection (or interception) and processing of foreign electromagnetic radiations (noncommunications) emanating from sources such as radar. ELINT is part of the NSA/CSS Signals Intelligence Mission. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

Appendix B (Continued)

electronic order of battle (EOB): A document summarizing the deployment of enemy noncommunications and communications emitters in a given area. In addition to deployment, the EOB also contains data as to the function of each emitter. (*Basic Manual (U), ELINT Collection Analysis Guide (U), National Cryptologic School, 1965*).

electronic security: The detection, identification, evaluation, and location of foreign electromagnetic radiations. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

electronic surveillance: Surveillance conducted on a person, group, or other entity by electronic equipment which is often highly sophisticated and extremely sensitive. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

encipher: To convert a plain text message into unintelligible form by the use of a cipher system. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

encrypt: To convert a plain text message into unintelligible form by means of a cryptosystem; this term covers the meanings of encipher and encode. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

espionage: Clandestine intelligence collection activity. This term is often interchanged with "clandestine collection." (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

evaluation: 1) Appraisal of an item of information in terms of credibility, reliability, pertinency, and accuracy. Appraisal is accomplished at several stages within the intelligence process with progressively different contexts. Initial evaluations made by case officers and report officers are focused upon the reliability of the source and the accuracy of the information as judged by data available at or close to their operational levels. Later evaluations by intelligence analysts are primarily concerned with verifying accuracy of information and may, in effect, convert information into intelligence. Appraisal or evaluation of items of information or intelligence is indicated by a standard letter-number system. The evaluation of the reliability of sources is designated by a letter from A through F, and the accuracy of the information is designated by numeral 1 through 6. These are two entirely independent appraisals, and these separate appraisals are indicated in accordance with the system indicated below. Thus, information adjudged to be "probably true" received from a "usually reliable source" is designated "B-2" or "B2" while information of which the "truth cannot be judged" received from a "usually reliable source" is designated "B-6" or "B6."

Reliability of source:

A- Completely reliable; B- Usually reliable; C- Fairly reliable; D- Not usually reliable; E- Unreliable; F- Reliability cannot be judged.

Accuracy of information:

1- Confirmed by other sources; 2- Probably true; 3- Possibly true; 4- Doubtful; 5- Improbable; 6- Truth cannot be judged.

(*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

2) In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinency, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. (*Recommended Change to JCS Pub 1, 25 July 1977*).

exploitation: In SIGINT, the production of information from messages that are encrypted in systems whose basic elements are known. Exploitation includes decryption, translation, and the solution of specific controls such as indicators and specific keys (*Basic Cryptologic Glossary (U), NSA, 1971*).

foreign intelligence: 1) Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities. (*U.S. Intelligence Activities, Executive Order No. 12036, Jan 1978*.) 2) a. Information concerning the capabilities, intentions and activities of any foreign power, or of any non-United States person, whether within or outside the United States or concerning areas outside the United States. b. Information relating to the ability of the United States to protect itself against actual or potential attack or other hostile acts of a foreign power or its agents. c. Information with respect to foreign powers or non-United States persons which because of its importance is deemed essential to the security of the United States or to the conduct of its foreign affairs. d. Information relating to the ability of the United States to protect itself against the activities of foreign intelligence services. (*USSID 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U), NSA, 25 May 76*.) 3) Intelligence concerning areas not under control of the power sponsoring the collection effort. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

guidance: The general direction of an intelligence effort, particularly in the area of collection. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*)

Appendix B (Continued)

integration: In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or, the process by which several photographic images are combined into a single image. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)*).

intelligence: 1) Foreign intelligence and counterintelligence. (*U.S. Intelligence Activities, Executive Order No. 12036, Jan 78.*) 2) The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976.*) 3) The product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to foreign activities and to foreign or enemy-held areas. This processing includes the evaluation and collation of the information obtained from all available sources, and its analysis, synthesis, and interpretation. (*Basic Cryptologic Glossary (U), NSA, 1971.*) 4) The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operations and which is immediately or potentially significant to military planning and operations. (*Dictionary of Military and Associated Terms, Dept. of Defense (U) the Joint Chiefs of Staff, 3 Sep 74. (U)*).

intelligence activities: Sec 14. (a) As used in this resolution, the term "intelligence activities" includes (1) the collection, analysis, production, dissemination, or use of information which relates to any foreign country, or any government, political group, party, military force, movement, or other association in such foreign country, and which relates to the defense, foreign policy, national security, or related policies of the United States, and other activity which is in support of such activities; (2) activities taken to counter similar activities directed against the United States; (3) covert or clandestine activities affecting the relations of the United States with any foreign government, political group, party, military force, movement or other association; (4) the collection, analysis, production, dissemination, or use of information about activities of persons within the United States, its territories and possessions, or nationals of the United States abroad whose political and related activities pose, or may be considered by any department, agency, bureau, office, division, instrumentality, or employee of the United States to pose, a threat to the internal security of the United States, and covert or clandestine activities directed against such persons. Such term does not include tactical foreign military intelligence serving no national policymaking function (*Senate Resolution 400, June 1977.*)

intelligence cycle: 1) The steps by which information is assembled, converted to intelligence, and made available to users. These steps are in four phases:

A. Planning and direction. Determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection agencies, and a continuous check on the productivity of collection agencies.

B. Collection: The exploitation of sources of information by collection agencies and the delivery of this information to the proper intelligence processing unit for use in the production of intelligence.

C. Processing: The step whereby information becomes intelligence through evaluation, analysis, integration, and interpretation.

D. Dissemination: The conveyance of intelligence in suitable form (oral, graphic, or written) to agencies needing it. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)*). 2) The steps by which information is assembled, converted into intelligence, and made available to consumers. The cycle is composed of four basic phases: (1) direction: the determination of intelligence requirements, preparation of a collection plan, tasking of collection agencies, and a continuous check on the productivity of these agencies; (2) collection: the exploitation of information sources and the delivery of the collected information to the proper intelligence processing unit for use in the production of intelligence; (3) processing: the steps whereby information becomes intelligence through evaluation, analysis, integration, and interpretation; and (4) dissemination: the distribution of information or intelligence products (in oral, written, or graphic form) to departmental and agency intelligence consumers. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976.*)

intelligence estimate: An appraisal of the elements of intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the probable order of their adoption. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)*).

intelligence information: 1) In SIGINT, information which is of intelligence use to customers whose primary mission does not include SIGINT operations of technical SIGINT information. (*Basic Cryptologic Glossary (U), NSA (PI), 1971.*) 2) The unevaluated and uninterpreted information about the enemy or potential enemy. (*Basic manual (U), ELINT Collection Analysis Guide (U), National Cryptologic School, 1965.*)

intelligence report: A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74 (U)*).

intelligence requirement: A consumer statement of information needed which is not already at hand. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

interception: The act of searching for and listening to and/or recording communications and/or electronic transmissions for the purpose of obtaining intelligence. (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*).

international terrorist activities: Means any activity or activities which: (a) involves killing, causing serious bodily harm, kidnapping, or violent destruction of property, or an attempt or credible threat to commit such acts; and (b) appears intended to endanger a protectee of the Secret Service or the Department of State or to further political, social, or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its cause; and (c) transcends national boundaries in terms of the means by which it is accomplished, the civilian population, government, or international organization it appears intended to coerce or intimidate, or the locale in which its perpetrators operate or seek asylum. (*U.S. Intelligence Activities, Executive Order No. 12036, 26 Jan 1978*.)

measurement and signature intelligence (MASINT): MASINT is obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependent, modulation, plasma, and hydromagnetic) derived from sensing instruments other than those normally associated with human communications, electronics intelligence (HUMINT, COMINT, ELINT) or imagery collection. MASINT includes, but is not limited to, the following disciplines: Radar intelligence (RADINT); Nuclear intelligence (NUCINT); Unintentional Radiation intelligence (RINT); Acoustic intelligence (Non-Compressible fluids -- ACINT; Compressible Fluids -- ACOUSTINT); Electro-Optic intelligence (Electro-OPTINT); Event-related dynamic measurements photography (OPTINT); and debris collection. Telemetry intelligence (TELINT) is a special category of signals intelligence (SIGINT) that provides measurement data on foreign instrumentation signals (FIS). Requirements for collection will be expressed as MASINT requirements. The term MASINT should be used when referring to the above categories of special sensor disciplines in aggregate. (*Defense Intelligence Collection Requirements Manual (C), DIA, 27 Jan 75*).

medical intelligence: That category of intelligence which concerns itself with man as a living organism and those factors affecting his efficiency, capability, and well-being. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74, (U)*).

national intelligence: 1) Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74, (U)*). 2) Intelligence produced by the CIA which bears on the broad aspects of United States national policy and national security. It is of concern to more than one department or agency. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

National Intelligence Estimate: A strategic estimate of capabilities, vulnerabilities, and probable courses of action of foreign nations which is produced at the national level as a composite of the views of the Intelligence Community. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74, (U)*).

operational intelligence: 1) Intelligence required for planning and executing all types of military operations. 2) Intelligence required to support the activities of intelligence agencies under the National Security Council. (*Basic Cryptologic Glossary (U), NSA, 1971*).

physical security: 1) The component of security which results from all physical measures necessary to safeguard classified equipment and material from access by unauthorized persons. (*Basic Cryptologic Glossary (U), NSA, 1971*). 2) The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons. (*Glossary of Communications Security and Emanations Security Terms (U), U.S. Communications Security Board, Oct 74*). 3) The element of communications security that results from all physical measures necessary for safeguarding classified equipment, material, and documents from access or observation by unauthorized persons. (*Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73*). 4) That part of security concerned with physical measures designed to safeguard personnel to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. See also communications security. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74*).

plain text: Unencrypted communications; specifically, the original message of a cryptogram, expressed in ordinary language. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

political intelligence: Intelligence concerning foreign and domestic policies of governments and the activities of political movements. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74*).

Appendix B (Continued)

processing: 1) The manipulation of collected raw information to make it usable in analysis to prepare for data storage or retrieval. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*) 2) Treatment of copy in accordance with predetermined and generalized criteria so as to produce all or some of the information contained in it in a new medium or a new form. (The main types of processing are conversion, scanning, extraction, digestion and diarization). (*Basic Cryptologic Glossary (U), 1971*). 3) Further handling, manipulation, consolidation, compositing, etc., of information to convert it from one format to another or to reduce it to manageable and/or intelligible information. (*Communications-Electronics Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73*). 4) In photography, the operations necessary to produce negatives, diapositives or prints from exposed films, plates or paper. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74*).

production: 1) Intelligence product means the estimates, memoranda and other reports produced from the analysis of available information. (*Executive Order No. 12036, 26 Jan 1978*.) 2) The preparation of reports based on an analysis of information to meet the needs of intelligence users (consumers) within and outside the Intelligence Community. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

radiation intelligence: Intelligence derived from the collection and analysis of non-information bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipments, and systems excluding those generated by the detonation of automatic/nuclear weapons. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74*).

requirement: A general or specific request for intelligence information made by a member of the Intelligence Community. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

scientific and technical intelligence: The product resulting from collection, evaluation, analysis and interpretation of foreign scientific and technical information which covers: A. Foreign developments in basic and applied research and in applied engineering techniques; and B. Scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems and material. The research and development related thereto, and the production methods employed for their manufacture (*USSID 40, ELINT Operating Policy (U), NSA, 24 Oct 75*).

sensitive: Something which requires special protection from disclosure, which could cause embarrassment, compromise, or threat to the security of the sponsoring power. (*Final Report, Senate Select Committee on Intelligence, 26 April 1976*).

sensitive compartmented information: The term as used in this manual is identified with its use in DCID 1/14. It is intended to include all information and material bearing special Intelligence Community controls indicating restricted handling within Community intelligence collection programs and their end products for which Community systems of compartmentation are formally established. The term does not include restricted data as defined in section 11, Atomic Energy Act of 1954, as amended. (*Security of Compartmented Computer Operations (U), DIA, 14 Jan 75*).

signal: 1) In electronics, any transmitted electric impulse which is of interest in the particular context; and 2) Anything intentionally transmitted by visual, acoustical, or electrical methods, which is intended to convey a meaning to the recipient. (*Basic Cryptologic Glossary (U), NSA, 1971*). 3) A visual, audible, electrical, or other indication used to convey information; and 4) The message or effect to be conveyed over a communication system. (*Glossary of Machine Processing Terms (U), NSA (Office of Machine Processing), 1964*). 5) Event, phenomenon or electrical quality that conveys information from one point to another; and 6) Operationally, a type of message that is conveyed or transmitted by visual, acoustical, or electric means. The text consists of one or more letters, words, characters, signal flags, visual displays, or special sounds with prearranged meanings. (*Communications-Electronic Terminology (U), U.S. Dept. of the Air Force, 15 Nov 73*).

signals intelligence (SIGINT): 1) A generic term which includes both communications intelligence (COMINT) and electronic intelligence (ELINT). (*Glossary of Communications-Electronics Terms (U), JCS, Dec 74*). 2) A generic term including communications intelligence and electronic intelligence, abbr. SIGINT. (SIGINT refers to the combination of COMINT and ELINT or to either when one of them is not specifically identified). (*Basic Cryptologic Glossary (U), NSA, 1971*). 3) A generic term which includes both communication intelligence and electronic intelligence. Also called SIGINT. See also intelligence. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74, (U)*). 4) A category of intelligence information comprising all communications intelligence (COMINT), electronics intelligence (ELINT), and telemetry intelligence (TELINT). (*Signals Intelligence (SIGINT) (U), DOD, 25 Jan 73*).

source: 1) A person, thing, or activity which provides intelligence information. In clandestine activities, the term applies to an agent or asset, normally a foreign national, being used in an intelligence activity for intelligence purposes. In interrogations, it refers to a person who furnishes intelligence information with or without knowledge that the information is being used for intelligence purposes. 2) In interrogation activities, any person who furnished intelligence that the information is being used for intelligence purposes. In

Appendix B (Continued)

this context, a controlled source is in the employment or under the control of the intelligence activity and knows that his information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)*).

special intelligence communications (SPINTCOMM): SPINTCOMM was established by Secretary of Defense Memorandum, dated 4 November 1964. It consists of those communications facilities under the operational and technical control of the chief of intelligence of each of the military departments and under the management of the Defense Intelligence

Agency. (*Defense Special Security Communications System (DSSCS) Operating Instructions System/ Data Procedures (U), NSA, 8 Oct 75*).

special sensor: Equipment on instrumented platforms and in installations designed to collect measurement and signature data that can be further processed into data usable by intelligence analysts. (*Defense Intelligence Collection Requirements Manual DIA, 27 Jan 75*).

tactical intelligence: Intelligence which is required for the planning and conduct of tactical operations. Essentially tactical intelligence and strategic intelligence differ only in scope, point of view and level of employment. (*Dictionary of Military and Associated Terms, Dept. of Defense (U), the Joint Chiefs of Staff, 3 Sep 74. (U)*).

Appendix C

INDEX OF OTHER INTELLIGENCE GLOSSARIES

Other publications, many of which contain classified information, also contain definitions of intelligence terms. An index of some of these publications appears below.

- Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.* Army Regulation 380-13. September 1971
- ADP Security Manual, Techniques and Procedures for Implementing Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems.* DoD. January 1973
- Basic Cryptologic Glossary.* NSA. 1971
- Charter of DCI SIGINT Committee.* DCID No. 6/1. May 1976
- Classification and Declassification of National Security Information and Material.* Executive Order No. 11652. March 1972 and as amended.
- Combat Intelligence.* Army Field Manual 30-5. October 1973
- Communications-Electronics Terminology Handbook.* Public Affairs Press. 1965
- Communications-Electronics Terminology.* U.S. Dept. of the Air Force. November 1973
- Communications Glossary.* Range Commanders Council, White Sands Missile Range. March 1966
- Communications Security.* Army Regulation 530-2. March 1976
- Control of Compromising Emanations.* Army Regulation 530-4. June 1971
- Coordination of U.S. Clandestine Foreign Intelligence and Activities Abroad.* DCID No. 5/1. May 1976
- Coordination of U.S. Clandestine Foreign Intelligence and Counterintelligence Liaison.* DCID No. 5/2. May 1976
- Counterintelligence Operations.* Army Field Manual 30-17. January 1972
- Counterintelligence Special Operations.* Army Field Manual 30-17A. February 1973
- DCI Policy on Release of Foreign Intelligence to Contractors.* DCID No. 1/7. May 1976
- DoD Human Resource Intelligence Collection Implementation Plan.* 1966
- Data Standardization for the Intelligence Community.* DCID No. 1/5. May 1976
- Defector Program, The.* NSCID No. 4. February 1972
- Defector Program Abroad, The.* DCID No. 4.2. May 1976
- Defense Intelligence Collection Requirements Manual.* DIA. January 1975
- Defense Special Security Communications System (DSSCS) Operating Instructions System/Data Procedures.* NSA. October 1975
- Definitions of Search and Analysts Terms.* Appendix D to "Selected Electronic Emitters for Target Countries." June 1964
- Department of the Army Supplement to DoD 5200 I-R.* Army Regulation 38-05. July 1974
- Dictionary of Military and Associated Terms.* JCS Pub 1. September 1974
- Dictionary of Telecommunications.* 1970

Appendix C (Continued)

- Dictionary of United States Army Terms*. Army Regulation 310-25 June 1972
- Domestic Exploitation Program*. Army Regulation 381-15 July 1974
- Electronic Security*. Army Regulation 530-3 June 1971
- Electronic Warfare*. Army Regulation 105-87. August 1976
- ELINT Operating Policy*. USSID 40. October 1975
- ELINT Collection Analysis Guide*. National Cryptologic School. 1965
- Enemy Prisoners of War, Civilian Internees, and Detained Persons*. Army Field Manual 19-40. February 1976
- Engineer Intelligence*. Army Field Manual 5-30. September 1967
- Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Together with Additional Supplemental and Separate Views*. April 1976
- Foreign Intelligence Production*. NSCID No. 3. February 1972
- Glossary of Basic TA Terminology*. National Cryptologic School. 1969
- Glossary of Communications-Electronics Terms*. December 1974
- Glossary of Communications Security and Emanations Security Terms*. U.S. Communications and Security Board. October 1974
- Glossary for Computer Systems Security*. National Bureau of Standards. February 1976
- Glossary of Machine Processing Terms*. September 1964
- Handling of Critical Information*. DCID No. 7/1. May 1976
- House Resolution 658*. (Establishes House Permanent Select Committee on Intelligence). November 1977
- IDHS Glossary of Common Acronyms, Codes, Abbreviations, and Terms Used in Dept. of Defense Intelligence Data Handling Systems (IDHS) Documents*. 1970
- Information Security Regulation*. DoD 5200.1-R
- Intelligence Collection Operations*. Army Field Manual 30-18. November 1973
- Intelligence Cover and Operational Support Activities*. Army Regulation 361-102. November 1973
- Intelligence Interrogation*. Army Field Manual 30-15. June 1973
- Intelligence Support*. Army Regulation 381-19. March 1977
- Limitations and Procedures in Signals Intelligence Operations of the USSR*. USSID 18. May 1976
- List of Terminology Used in Foreign Counterintelligence and Counterespionage Investigations*. December 1973
- Meteorological Support for the U.S. Army*. Army Regulation 115-10. June 1970
- Military Geographic Intelligence (Terrain)*. Army Field Manual 30-10. March 1972
- Military Intelligence Officer Excepted Career Program*. Army Regulation 614-115. January 1975
- Military Intelligence Organizations*. Army Field Manual 30-9. October 1973
- Modern Data Communications Concepts, Language and Media*. Wm. P. Davenport, Hayden Book Co., Inc. 1971
- National Foreign Intelligence Plan for Human Resources*. NFIB D/27 7/5. 1977
- NATO Glossary of Terms and Definitions for Military Use (AAP-6)*

National SIGINT Requirements System Handbook. December 1976

Naval Intelligence System Architectural Management Plan for 1978 (NISAM-78)
(Draft)

Offensive CI Operations (OFCCO). Army Regulation 381-47 April 1976

Operations. Army Field Manual 100.5. July 1976

Operations Security. Army Regulation 530-1. May 1976

Physical Security. Army Field Manual 19-30. November 1977

Point Weather Warning Dissemination. Army Regulation 115-1. February 1975

Security Committee. DCID No. 1/11. May 1976

Security, Use and Dissemination of Communications Intelligence, The. Army Regulation 380-35. March 1973

Security, Use and Dissemination of Communications Intelligence, The. DoD Directive S-5200.17 (M-2)

Security, Use and Dissemination of Communications Intelligence, The. USAFINTEL 201-1.

Senate Resolution 400. (Establishes the Senate Select Committee on Intelligence). June 1977

SIGINT Security. NSA. USSID 3. August 1972

Signals Intelligence. NSCID No 6. February 1972

Signal Intelligence (SIGINT). Army Field Manual 30-21 August 1975

Signals Intelligence. DoD Directive S-3115.7

SIGSEC Techniques. Army Field Manual 32-6 February 1977

Soviet Naval Threat Circa 2000, The. August 1976

Special Security Officer System, The. Army Regulation 380-28 October 1971

Statement of Intelligence Interest. DoD Document No. 05990

Surveillance, Target Acquisition and Night Observation (STANO) Operations. Army Field Manual 31-100. May 1971

Technical Intelligence. Army Field Manual 30-16. August 1972

Telemetry Terminology, Missile Intelligence Agency, Huntsville, Alabama. January 1975

Threat Analysis. Army Regulation 381-11. August 1974

Title Classified. DCID No. 6/2. May 1976

Title Classified. DoD Directive TS-500.12 (M-1)

Title Classified (USAFINTEL 201-4)

United States Air Force Dictionary, Woodford Agee Heflin (Editor), Research Studies Institute, Air University Press, Maxwell Air Force Base, Alabama 1956

United States Intelligence Activities. Executive Order No 12036. January 1978

U.S. Air Force Glossary of Standardized Terms. (Air Force Manual 11-1)

U.S. Army Requirements for Weather Service Support. Army Regulation 115-12 August 1976

U.S. Clandestine Foreign Intelligence and Counterintelligence Activities Abroad. NSCID No 5 February 1972