

10 April 1978

MEMORANDUM FOR: Members, National Foreign Intelligence Board

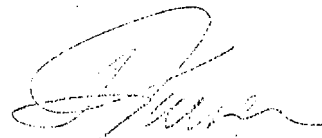
SUBJECT: Intelligence Definitions

REFERENCE: NFIB 24.1/14, Subject: Definitions of Intelligence,
dated 13 September 1977

1. The Intelligence Definitions Working Group, which was established by the reference, has completed the initial task of devising definitions appropriate for inclusion in an unclassified intelligence glossary. You are asked to comment on:

- The substance of the definitions;
- Any terms which should be included (with proposed definitions) or any terms which you deem inappropriate and believe should be omitted;
- The draft Preface, Methodology, and Maintenance chapters (which will be part of the publication containing the glossary); and
- The draft list of acronyms and abbreviations.

2. While this coordination is underway, the Working Group will continue to develop supporting annexes designed to enhance the glossary when it is published (to include an index of other glossaries, graphic relationships of words and terms, and duplicate definitions and sources of intelligence terms). In connection with the latter, please bear in mind that the definitions in this glossary may not and need not coincide precisely with definitions used elsewhere for departmental or special legal purposes. I welcome any suggestions you have which will move the glossary closer to publication.



STANSFIELD TURNER
Chairman

Attachments:

1. draft Preface, etc.
2. draft Glossary of Intelligence
Terms and Definitions

GLOSSARY OF INTELLIGENCE TERMS AND DEFINITIONS

Acoustical intelligence (ACOUSTINT): Technical 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 addressed by an authorized 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 review in order to identify significant facts and derive conclusions therefrom. (See intelligence cycle.)

Assessment: 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. When used in contrast with evaluation assessment implies a weighing against resource allocation, expenditure, or risk. (See evaluation.)

Asset: See intelligence asset and national 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 and military structure, resources, capabilities and vulnerabilities of foreign nations.

Biographical intelligence: Foreign intelligence on the views, traits, habits, skills, importance, relationships 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.)

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: See illicit communication.

Clandestine operation: A pre-planned secret intelligence information collection activity or covert political, economic, propaganda or paramilitary activity 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 pre-arranged 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. (See cover.)

CODEWORD: A word or term used with a security classification to indicate that the material so classified was derived from a sensitive source 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 intelligence information needs 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 sensor 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 user'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. (See tactical intelligence.)

Committee on Exchanges (COMEX): See Director of Central Intelligence Committee.

Committee on Imagery Requirements and Exploitation (COMIREX): See Director of Central Intelligence Committee.

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:

a. Imitative communications deception--Intrusion into the enemy's communications channels for the purpose of deceiving him by introducing signals or traffic in imitation of his own communications.

b. Manipulative communications deception--Regulated insertion of misleading material into one's own telecommunications channels for the purpose of presenting a false picture to the enemy.

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 the application of 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. (See communications security surveillance.)

Communications security surveillance: The systematic examination of telecommunications 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 Network 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 established and/or managed by 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.)

Compromising emanations: Unintentional data-related or intelligence-bearing signals which could disclose classified 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. (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 activities.

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. (Also known as "special activities" as defined in Executive Order No. 12036; see Appendix _____.)

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.

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 (CRITICOMM): 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. (See critical intelligence.)

Critical intelligence message (CRITIC): A message designated as containing critical intelligence. (See critical intelligence.)

Cryptanalysis: 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. (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, lead to the cryptanalysis of an individual of a message, command, or authentication); it is normally identified by the bold letter marking "CRYPTO" and is subject to the special safeguards required by that marking. (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 communications security.

Cryptology: The branch of knowledge which treats the principles of cryptography and cryptanalysis and is used to produce signals intelligence and maintain communications security. (See cryptography and cryptanalysis.)

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: A 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 a nation's military forces to determine residual military capability and to support 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; presents requirements categories and foreign countries in a geotopical 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. (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.

Declassification: Removal of official information from the protective status afforded by security classification; requires a determination that disclosure no longer bears on 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.

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 order to meet the unique requirements of the department or agency mission.

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 of 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. (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 who either through inducement or voluntary action has indicated the willingness or desire to defect.

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.

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

Electronic countermeasures (ECM): That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Electronic 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 enemy; and electronic deception, which is similar but is intended to mislead an enemy 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 enemy's use of electronic countermeasures. (See electronic warfare.)

25X1

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 non-communicat 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 non-communications electromagnetic radiations; e.g., radar.

Electronic surveillance: The acquisition of a non-public communication by electronic means without the consent of a person who is a party to the communication, but not including radio direction finding used 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 counter-measures, 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, and homing.

Emanations: See noncommunications emanations.

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 emis-sion security.)

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

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.

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

Encipher: To encrypt plain text by means of cipher. (See cipher.)

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 illegal in the territory in which it takes place.

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

Estimative intelligence: A category of intelligence production which attempts to project future foreign 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. (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.

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

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

Finished intelligence: The result of the production step of the intelligence cycle; the intelligence product. (See intelligence cycle.)

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, interrogators, track/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 of collection, processing, and analysis 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).

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

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

Foreign official: A foreign national 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): An airborne system used for producing infrared ground images the dimensions of which are determined by the forward motion of the aircraft and by scanning across its flight path.

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. (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.

Guidance: Advice which identifies, interprets, clarifies, and/or expands upon an information need. (See information need.)

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

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.") (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.

Illegal agent: An agent operated by an illegal residency or directly by the headquarters of an intelligence organization.

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 also called clandestine communication.

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

Imagery intelligence: The collected products of imagery interpretation processed for intelligence use. (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 enemy channels of electromagnetic radiations which imitate his own emissions.

Indications 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/non-nuclear 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. (See intelligence information.)

Information handling: Management of data and 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 to process data and/or information; and may include information contained in reports, files, data bases, reference services and libraries.

Information Handling Committee (IHC): See Director of Central Intelligence Committee.

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. (See intelligence cycle.)

Intelligence: (1) Knowledge acquired and furnished in response to the known or perceived requirements of decision-makers which is derived principally from information which is normally concealed or not intended to be available for use by the acquirer; it is the product of a cyclical process. (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. (See foreign intelligence and foreign counterintelligence.)

Examples:

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

Intelligence activity(ies): A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations. (See intelligence organization.)

Intelligence agency: A component organization of the Intelligence Community. (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 estimates may not attempt to project future developments and their implications; it may or may not be coordinated.

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. (See intelligence cycle.)

Intelligence Community (IC): A term which, in the aggregate, refers to those Executive Branch organizations and activities composed of: 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 users. 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 into intelligence information and a form suitable to 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 user requirements.

e. Dissemination--conveyance of intelligence in suitable form to users.

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 report: A report which disseminates foreign intelligence information.

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. (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 12036.

Intelligence producer: A phrase usually used to refer to an organization or agency that participates in the production step of the intelligence cycle. (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 to support departmental or agency missions or operational forces, train personnel for intelligence duties, or are devoted to research and development for intelligence and related capabilities.

Intelligence report: A product of the analysis of foreign intelligence information.

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 user: See customer.

Interagency Defector Committee (IDC): See Director of Central Intelligence Committee.

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 communicators.

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

Interdepartmental intelligence: Integrated departmental intelligence required by departments and agencies of the U.S. government for the execution of their missions but which transcends the competence or interest of a single department or agency.

International lines of communications (ICL): 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. (See intelligence cycle.)

Joint Atomic Energy Intelligence Committee (JAEIC): See Director of Central Intelligence Committee.

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.

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 dependent, 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 (GMI), 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 (CBR) Warfare; it applies to both tactical and strategic planning and operations, including military and humanitarian efforts.

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 multi-level information handling system. The multi-level 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; interagency 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): A program aggregating the programs of the Central Intelligence Agency; the Consolidated Cryptologic Program; 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); the elements of the General Defense Intelligence Program; and other programs of agencies within the Intelligence Community designated by the President or jointly by the Director of Central Intelligence and the head of the department as national foreign intelligence or national foreign counterintelligence activities; and activities of the staff elements of the Office of the Director of Central Intelligence.

National intelligence: Foreign intelligence collected by assets funded in the NFIP and then evaluated 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, the primary purpose of which is the collection, or processing of intelligence information and the production of national intelligence. (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.

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 he is a primary source of national-level substantive guidance to Intelligence Community planners, collectors, and resource managers.

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.)

Noncommunications emanations: That class of radiations which are emitted intentionally or unintentionally by electrical or electronic equipment for purposes other than communications; e.g., by radars, navigational aids, jammers, or remote control systems.

Nuclear intelligence (NUCINT): Intelligence derived from the collection and analysis of radiation and other effects resulting from the detonation of nuclear devices or 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 weapon states (NNWS) or foreign organizations to acquire nuclear weapons and/or to acquire the requisite special nuclear materials (SNM) 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 SNM which could assist NNWS 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.)

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

Operations security (OPSEC): Those measures designed to deny information concerning planned, ongoing, and completed operations to an enemy or potential enemy, and which might otherwise provide him with a tactical or strategic advantage.

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

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) (intelligence 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 successful and repeatable 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 (PI): 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 like 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) A finished 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.

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. (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. (See noncommunications emanations.)

Raw intelligence: A colloquial term meaning collected intelligence information which has not yet been converted into intelligence. (See intelligence information.)

Reconnaissance (RECCE): A mission 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 of his former habitual residence and who, because of fear of being persecuted in that country, is unwilling to return to it. (Also see 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 other 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 altering intelligence information or reports in order to protect sensitive intelligence sources, methods, capabilities, and analytical procedures in order to permit wider dissemination.

Scientific and technical (S&T) intelligence: Intelligence concerning foreign developments 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.

Scientific and Technical Intelligence Committee (STIC): See Director of Central Intelligence Committee.

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

Security classification: See classification.

Security Committee (SECOM): See Director of Central Intelligence Committee.

Sensitive: Requiring special protection from disclosure to avoid compromise or threat to the security of the sponsor.

Sensitive compartmented information (SCI): All information and material requiring special controls for restricted handling within compartmented intelligence systems. (Also see compartmentation.)

Sensitive intelligence sources or 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 Agency(ies) (SCA): See service cryptologic element(s).

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; Navy and Air Force elements are also known as Service Cryptologic Agency(ies) (SCA).

Sensor: (1) A technical device designed to detect and respond to one or more particular stimulæ 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.

SIGINT operational tasking authority (SOTA): That authority delegated by the Director, National Security Agency, to military commanders which enables them to task specified signals intelligence resources that have tactical applicability and the ability to respond to time-sensitive requirements.

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 (as opposed to intelligence) information and which is required in the further collection or analysis of signals intelligence.

Signal: Anything intentionally transmitted by visual, other electromagnetic, or acoustical methods intended to convey a meaning to the recipient.

Signals intelligence (SIGINT): A category of intelligence information comprising all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, either individually or in combination, including nonimagery infrared and coherent light signals.

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: 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 concerned.)

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

Special intelligence (SI): An unclassified term used to designate a category of sensitive compartmented information (SCI). (See sensitive compartmented information.)

Special intelligence communications (SPINTCOMM): 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 only to the extent that time permits.

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 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 aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means.

Tactical intelligence: Foreign intelligence collected with assets funded in DoD programs and evaluated by DoD elements for the use 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. (See combat intelligence.)

Tactical intelligence asset: An intelligence asset, the primary purpose of which is the collection, processing or production of tactical intelligence. (See tactical intelligence and intelligence asset.)

Target: A country, area, installation, organization, weapon system, military force, situation (political or economic), 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 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.

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.

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 emissions security.

Terrorist organization: A group that engages in terrorist activities. (See international terrorist activity.)

Traffic analysis (TA): The study of the external characteristics of communications.

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 multi-level security. (Also see multi-level security.)

United States Signals Intelligence System (USSIS): 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. (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.

Weapon and Space Systems Intelligence Committee (WSSIC):
See Director of Central Intelligence Committee.

ACRONYMS AND ABBREVIATIONS

ACINT	Acoustical Intelligence (Naval acronym; see definition.)
ACOUSTINT	Acoustical Intelligence
ACSI	Assistant Chief of Staff/Intelligence (Army or Air Force)
CAMS	COMIREX Automated Management System
CBR	Chemical, Biological, Radiological Warfare
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
CISR	Communications Intelligence Security Regulation
CIVISION	Enciphered Television
COINS	Community On-Line Intelligence Network 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
EEI	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
FCI	Foreign Counterintelligence
FI	Foreign Intelligence
FIS	Foreign Instrumentation Signals
FISINT	Foreign Instrumentation Signals Intelligence
FLIR	Forward Looking Infrared
FORMAT	Foreign Material
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	Information Handling Committee
II	Imagery Interpretation
IIM	Interagency Intelligence Memorandum
ILC	International Lines of Communications
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
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
NNWS	Non-Nuclear Weapon States
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
OB	Order of Battle
OPCON	Operational Control
OPINTEL	Operational Intelligence
OPSEC	Operations Security
OPTINT	Optical Intelligence
PHOTINT	Photographic Intelligence
PI	Photographic Interpretation or Photographic Interpreter
PRC(I)	Policy Review Committee (Intelligence)
RADINT	Radar Intelligence
RECCE	Reconnaissance
RINT	Radiation Intelligence

S&T SAFE	Scientific and Technical 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
SECOM	Security Committee
SI	Special Intelligence
SIGINT	Signals Intelligence
SIGINT Committee	Signals Intelligence Committee
SIRVES	SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee)
SLAR	Side-Looking Airborne Radar
SNIE	Special National Intelligence Estimate
SNM	Special Nuclear Materials
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
TELINT	Telemetry Intelligence
TRANSEC	Transmission Security
USSID	United States Signals Intelligence Directive
USSIS	United States Signals Intelligence System
WSSIC	Weapon and Space Systems Intelligence Committee

I. PREFACE

This publication is designed to provide definitions for words and terms used frequently in the daily conduct of business in the Intelligence Community. It is the product of an interagency working group formed by the National Foreign Intelligence Board in September 1977, in recognition of the need for an authoritative and comprehensive glossary of intelligence terms.

The definitions that appear in this publication have been carefully constructed to reflect as nearly as possible an accurate and modern sense of the meaning of each term, focusing on the potential utility of the definition in each case. No attempt has been made to include terms which have no special connotation within the Intelligence Community. Many technical intelligence terms have not been included for the reason that their use is restricted to a small specialized segment of the Community and would not have the broad applicability that this glossary aims to provide. Additionally, the limited number of classified terms that might otherwise be appropriately included in this glossary have been intentionally omitted to enable the broadest possible distribution and use of this publication. Those terms defined here in unclassified form, and which may also have classified definitions, have not been altered in meaning although form and content have been modified to protect classified information.

DRAFT

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

This glossary of intelligence terms will serve as a primary basis for interdepartmental communication and understanding within the Intelligence Community. It is not intended to restrict intelligence agencies from the use of identical terms in different contexts when good and sufficient reasons exist. It should be recognized, for example, that the definitions in this glossary may not coincide precisely with definitions used elsewhere for departmental or legal purposes. Neither should the list of terms in this glossary be considered to be completely exhaustive. Rather, the glossary should be treated as a living compendium designed to provide the principal meanings of intelligence terms as they are understood in the Intelligence Community. Unless otherwise specified the meanings provided will be used so that the full value of a standardized glossary may be realized. Thus, while the definitions found in this glossary will form the basis for a common Intelligence Community language, they will serve as well to unify the disparate elements of the Community as they communicate with other parts of the Executive Branch and with Congress and the Judiciary.

Authors of other special-use glossaries which contain intelligence terms should try to align definitions of terms with those found here as an important step toward language commonality. Where that is not possible--such as in legislation

Approved For Release 2004/03/23² : CIA-RDP80M00596A000500020018-1

DRAFT

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1
or in other public and/or legal documents--the special applicability of a definition will be recognized for that purpose but will not be considered to have replaced the "Community" definition contained here until authorized by the Director of Central Intelligence.

In addition to the glossary of definitions itself, other information is contained in this publication which is designed to enhance its usefulness and contribute to its instructional value. In the ensuing section, brief treatment is accorded both the methodology and the most cogent considerations involved in devising the definitions. Included in the several appendices are a list of acronyms and abbreviations related to the terms in the glossary, duplicate definitions of certain glossary terms where they appear in and for the special purpose of clarifying an executive order or statute, graphic displays of certain families of intelligence terms which portray word relationships, and a reference index of other glossaries which contain intelligence terms and their definitions.

II. 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 "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

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

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.

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

"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 functions in addition to those. It also embraces the activities--and their resultant products--which are known as "counterintelligence." For these reasons, one might be

DRAFT

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

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.

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 that is possible, and frequent cross-referencing is a technique employed intentionally to that end.

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

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.

DRAFT

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

III. MAINTENANCE OF THE GLOSSARY

This publication is intended to be a reference and guidance document for members of the Intelligence Community. As such it may be updated or amended at any time by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board. Proposed corrections, additions, deletions, or amendments may be forwarded by any member of the Community to the Executive Secretary, National Foreign Intelligence Board, who will be responsible for coordination of proposed changes and, when approved, for providing appropriate notification to the Intelligence Community.

An interagency definitions working group will be responsible for the general administration of the glossary. It will consider proposals for changing the glossary as they occur, will review the entire glossary for currency and adequacy at least annually, and will in each case pass its recommendations to the National Foreign Intelligence Board.

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

25X1

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1

Approved For Release 2004/03/23 : CIA-RDP80M00596A000500020018-1