

GLOSSARY (UNCLASSIFIED)

TERMS & DEFINITIONS OF INTEREST
FOR DoD COUNTERINTELLIGENCE PROFESSIONALS

Wisdom begins with the definition of terms
-- Socrates

2X The counterintelligence and human intelligence advisor to the C/J/G/S-2. Denotes the 2X positions at all echelons. The 2X staff conducts technical control and oversight for all counterintelligence and human intelligence entities with[in] their operational purview. It coordinates, de-conflicts, and synchronizes all counterintelligence and human intelligence activities at each level of command. (Army FM 2-22.2, Counterintelligence, Oct 2009) Also see *J2X*.

-- Also, the manager of the counterintelligence and human intelligence missions at various levels of DoD structure, including joint, command, service, and task force. The 2X structure includes the Counterintelligence Coordinating Authority (CICA) and the Human Intelligence Operations Center (HOC). (AR 381-20, Army CI Program (U), 25 May 2010)

811 Referral. See *Section 811 Referral*.

A-Space. An abbreviation for Analytical Space. A virtual work environment that provides analyst from across the Intelligence Community a common platform to do their research and analysis and to easily connect with colleagues working the same or similar issues to collaboratively achieve common mission objectives. (Intellipedia; accessed 22 Oct 2010) Also see *J-Space*.

Abort. To terminate a mission for any reason other than enemy action. It may occur at any point after the beginning of the mission and prior to its completion. (JP 1-02)*

This unclassified glossary is periodically updated. Recommended changes, corrections, and/or additions are encouraged. For recommended additions provide a source for the definition.

Editor: COL Mark L. Reagan (USA Ret), Special Advisor, Office of Counterintelligence (DXC), Defense Counterintelligence and Human Intelligence Center (DCHC), Defense Intelligence Agency.
Contact Information: mark.reagan@dodis.mil, 703-699-7661 or VoIP 982-8844.

* Joint Publication 1-02, DoD Dictionary of Military and Associated Terms (JP 1-02), as amended. Available online at: http://www.dtic.mil/doctrine/dod_dictionary/ -- Also online at: <https://jdeis.js.mil>

Abduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *deduction; induction; scientific method.*

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David T. Moore, JMIC Press (2006).

Access. In counterintelligence and intelligence use: 1) A way or means of approach to identify a target; 2) Exploitable proximity to or ability to approach an individual, facility, or information that enables target to carry out the intended mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge. (Counterintelligence Community Lexicon, June 2000, hereinafter referred to as CI Community Lexicon)

-- Also, the ability or opportunity to obtain knowledge of classified or sensitive information. (IC Standard 700-1, 4 Apr 2008)

-- Also, the ability and opportunity to obtain knowledge of classified information. (DoD 5200.1-R, Information Security Program, Jan 1997)

Access generally refers to the ability of a human source (either CI or HUMINT) or an operational asset to perform a specific operational task within the limits of acceptable risk.

Access Agent. An individual used to acquire information on an otherwise inaccessible target. (Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and Related Activities, April 2008, hereinafter referred to as HDI Lexicon) Also see *agent.*

-- Also, an agent whose relationship or potential relationship with a foreign intelligence personality allows him or her to serve as a channel for the introduction of another controlled agent for the purpose of recruitment of the target. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, a person who facilitates contact with a target individual or entry into a facility. (Spycraft: The Secret History of the CIA's Spyspechs from Communism to Al-Qaeda, 2008; hereinafter referred to as Spycraft)

Accommodation Address. An address for a person or organization that does not occupy the premises. (HDI Lexicon, April 2008)

-- Also, an address where regular posted mail, or sometimes another type of communication, is received and then held for pickup or forwarded, transmitted, or relayed to a member of an intelligence service who does not occupy the premises. Sometimes called a mail drop, live letterbox, or cutout. (AFOSI Manual 71-142, 9 Jun 2000 and Spy Book -- The Encyclopedia of Espionage, 2002, hereinafter referred to as Spy Book)

-- Also, an address with no obvious connection to an intelligence agency, used for receiving mail containing sensitive material or information (Spycraft)

Acknowledged SAP. A SAP [Special Access Program] whose existence is acknowledged but its specific details (technologies, materials, techniques, etc.) are classified as specified in the applicable security classification guide. (DoDD 5205.07, SAP Policy, 1 July 2010)

Acquisition Systems Protection (ASP). The safeguarding of defense systems anywhere in the acquisition process as defined in DoD Directive 5000.1, the defense technologies being developed that could lead to weapon or defense systems, and defense research data. ASP integrates all security disciplines, counter-intelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our force uncompromised combat effectiveness over the life expectancy of the system. (DoD 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

Actionable Intelligence. Intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process. (ICS Glossary and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Ad-Hoc Requirement (AHR). A HUMINT collection requirement with a limited emphasis, based on time or other requirements. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

-- Also, an intelligence need that was not addressed in [a] standing tasking. (National HUMINT Glossary)

Adaptive Planning (AP). The joint capability to create and revise plans rapidly and systematically, as circumstances require. (JP 5-0, Joint Operation Planning, 26 Dec 2006) See *APEX* below.

Adaptive Planning is the DoD initiative to change the overarching process, transforming the way we plan and execute joint operations. Also see *Intelligence Planning*.

Adaptive Planning and Execution (APEX). Department level system of joint policies, process, procedures and reporting structures, supported by communications and information technology that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment sustainment, redeployment, and demobilization activities associated with joint operations. Governs the planning and execution of Joint operations consistent with the AP [Adaptive Planning] vision. These departmental level policies and procedures will be documents in CJCSMs and will constitute the successor to the Joint Operations Planning and Execution CJCSMs currently in effect. (*Adaptive Planning Roadmap II*, 5 Mar 2008)

Administrative Control (ADCON). Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1-02)

Advanced Persistent Threat (APT). An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010)

-- Also, [in computer security usage] cyber attacks mounted by organizational teams that have deep resources, advanced penetration skills, specific target profiles and are remarkably persistent in their efforts. They tend to use sophisticated custom malware that can circumvent most defenses, stealthy tactics and demonstrate good situational awareness by evaluating defenders responses and escalating their attack techniques accordingly. (<www.hackingtheuniverse.com/infosec/isnews/advanced-persistent-threat>, accessed 5 Jan 2010)

The technological (cyber) APT has been used by actors in many nations as a means to gather intelligence on individuals, and groups of individuals of interest. Also see information at:
-- <http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm >
-- <<http://www.prometheus-group.com/blogs/36-web-security/152-anatomy-of-apt.html>>
-- <<http://en.wikipedia.org/wiki/GhostNet>>

Adverse Information. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. (DoD Manual 5220.22-M, 28 Feb 2006)

Adversary. Any individual, group, organization, or government that conducts or has the intent and capability to conduct activities detrimental to the US Government or its assets. Adversaries may include intelligence services, political or terrorist groups, criminals, and private interests. (CI Community Lexicon)

-- Also, an individual, group, organization, or government that must be denied essential information. (DoD Manual 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

-- Also, a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 1-02 & JP 3-0)

Advisory Tasking. A term used in collection management to refer to collection notices that are discretionary rather than directive in nature, with the receiving agency determining whether the requirement is relevant to the mission of the agency and whether the agency has the resources to collect against it. (AR 381-20, Army CI Program, 25 May 2010)

Agent. In intelligence usage, one who is authorized and trained to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (JP 1-02) Also see *agent of influence; agent of a foreign entity; asset; foreign intelligence agent.*

-- Also, a person who engages in clandestine intelligence activities under the direction of an intelligence organization, but is not an officer, employee, or co-opted worker of that organization. (National HUMINT Glossary)

-- Also, 1) 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; 2) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes; [and] 3) One who is authorized or instructed to obtain or assist in obtaining information for intelligence or counterintelligence purposes. (ICS Glossary)

*Typically, the aim of an espionage operation is to recruit an **agent** [emphasis added], usually a foreign person, to carry out the actual spying. The person who targets, recruits, trains, and runs the agent is, in American parlance, the 'case officer.'*

-- Arthur S. Hulnick, "Espionage: Does It Have a Future in the 21st Century?" *The Brown Journal of World Affairs*; v XI: n 1 (2004).

Espionage is one of the toughest games played. An agent in the right place is hard to find, but when he is found he should be regarded as a pearl beyond price.

-- David Nelligan, *The Spy in the Castle* (1968)

Agent of Influence. An agent of some stature who uses his or her position to influence public opinion or decision making to produce results beneficial to the country whose intelligence service operates the agent. (AFOSI Manual 71-142, 9 Jun 2000) [Originally a Soviet term]

-- Also, a person who is directed by an intelligence organization to use his position to influence public opinion or decision-making in a manner that will advance the objective of the country for which that organization operates. (ICS Glossary)

-- Also, an individual who acts in the interest of an adversary without open declaration of allegiance and attempts to exert influence covertly, but is not necessarily gathering intelligence or compromising classified material, is known as an agent of influence. (Historical Dictionary of Cold War Counterintelligence, 2007)

-- Also, an agent operating under intelligence instructions who uses his official or public position, and other means, to exert influence on policy, public opinion, the course of particular events, the activity of political organizations and state agencies in target countries. (KGB Lexicon: The Soviet Intelligence Officer's Handbook, edited by KGB archivist Vasiliy Mitrokhin, 2002).

Agent of a Foreign Entity. A person who engages in intelligence activities under the covert direction of a foreign intelligence or security entity, but is not an officer, employee, or co-opted worker of that entity. (ONCIX Analytic Chiefs Working Group Definition, Jan 2011) Also see *agent*; *asset*.

Agent Handler. An intelligence officer or co-opted worker directly responsible for the operational activities of an agent. Also see *case officer*.

-- Also, an officer or principal agent who directly manages an agent or agent network. (National HUMINT Glossary)

Agent Net. An intelligence gathering unit of agents supervised by a principal agent who is operating under the direction of an intelligence officer. An agent net can be operative in either the legal or illegal field. (ICS Glossary)

-- Also, an organization for clandestine purposes that operates under the direction of a principal agent. (JP 1-02) *Note: Pending removal from JP1-02 per JP 2-01.2, 16 Mar 2011.*

Air Force Office of Special Investigations (AFOSI). U.S. Air Force element responsible for providing professional investigative service to commanders of all Air Force activities. AFOSI identifies, investigates and neutralizes criminal, terrorist, and espionage threats to Air Force and Department of Defense personnel and resources. (www.osi.andrews.af.mil)

All-Source. Intelligence product or analysis that uses all the sources of intelligence available to come to a conclusion, instead of just relying on one primary source. May also be referred to as multi-INT reporting. (National Intelligence: A Consumer's Guide - 2009) See *all-source analysis*; *all-source intelligence*.

All-Source Analysis. An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement & signature intelligence, and open source intelligence. (DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007) Also see *analysis*; *analysis and production*; *counterintelligence analysis*.

All-source analysis can transform raw intelligence, data, and information into knowledge and understanding.

Integrated all-source analysis should also inform and shape strategies to collect more intelligence.... The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots."

-- Final Report of the National Commission on Terrorist Attacks Upon the United States (2004)

All-Source Intelligence. 1) Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2) In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 2-0, Joint Intelligence)

-- Also, intelligence product or analysis that uses all the sources of intelligence available to come to a conclusion, instead of just relying on one primary source. This may also be referred to as multi-INT reporting. (National Intelligence: A Consumer's Guide - 2009)

-- Also, the intelligence discipline concerned with all-source products and the processes used to produce them. (Army FM 2-0, Intelligence 23 Mar 2010)

Alliance. The relationship that results from a formal agreement (e.g., treaty) between two or more nations for broad, long-term objectives that further the common interests of the members. (JP 1-02 & JP 3-0)

Alias. An alternative name, used for cover purposes. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

-- Also, a false name. (National HUMINT Glossary)

-- Also, a false name assumed by an individual for a specific and often temporary purpose, i.e., to conceal a true identity from persons or organizations with whom he or she is in contact. Also called a pseudonym or cover name. (AFOSI Manual 71-142, 9 Jun 2000)

Alternative Compensatory Control Measures (ACCM). Measures designed to safeguard sensitive intelligence and operations when normal security measures are either not sufficient to achieve strict controls over access to information, but where strict SAP [Special Access Program] access controls are either not required or are too stringent. (AR 381-20, Army CI Program, 25 May 2010)

Ambassador. Diplomatic official of the highest rank who is accredited to a foreign sovereign or government, or to an international organization, as the resident representative of the sending government or appointed for a specific diplomatic assignment. (Department of State) Also see *Chief of Mission*.

A U.S. ambassador serving abroad symbolizes the sovereignty of the United States and serves as the personal representative of the President of the United States. Ambassadorial duties include negotiating agreements, reporting on political, economic and social conditions, advising on policy options, protecting American interests, and coordinating the activities of all U.S. Government agencies and personnel in the country.

Analysis. [In intelligence usage] a process in the production of intelligence in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions. (CIA, *A Consumer's Guide to Intelligence*, July 1995) Also see *analysis and production*; *all-source analysis*; *counterintelligence analysis*.

-- Also, the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat, terrain and weather, and civil considerations on operations. (Army FM 2-0, Intelligence, 23 Mar 2010)

Analysis is the thinking part of the intelligence process

-- James B. Bruce and Roger Z. George

Analysis is the process by which people transform information into intelligence. It includes integrating, evaluating, and analyzing all available data -- which is often fragmented and even contradictory -- and preparing intelligence products.

Former DCI Richard Helms noted that despite all the attention focused on the operational (collection) side of intelligence, *analysis* is the core of the process to inform decision makers.

***It is not enough, of course, simply to collect information.
Thoughtful analysis is vital to sound decisionmaking.***

-- President Ronald Reagan (4 Dec 1981)

It is of the highest importance in the art of detection to be able to recognize, out of a number of facts, which are incidental and which are vital.

-- Sherlock Holmes

From A. Conan Doyle's "The Reigate Squire" June 1893
(M. Hardwick, *The Complete Guide to Sherlock Holmes*, 1986, pp. 86-87)

"Intelligence analysts select and filter information; they interpret the resultant evidence, put it into context, and tailor it to meet... customers' needs. In short, analysts and analysts only, create intelligence."

-- David T. Moore, "Species of Competencies for Intelligence," *American Intelligence Journal* (2005)

Analysis must do more than just describe what is happening and why; it must identify a range of opportunities... Analysis is the key to making sense of the data and finding opportunities to take action.

-- DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

The primary purpose of analytic effort is "sensemaking" and understanding, not producing reports; the objective of analysis is to provide information in a meaningful context, not individual factoids.

-- Jeffrey R. Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 42

Intelligence analysis is inherently an intellectual activity that requires knowledge, judgment, and a degree of intuition.

Selected references for **intelligence analysis**:

Richard J. Heur, Jr, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999). Copy available online at: <http://www.archive.org/details/PsychologyOfIntelligenceAnalysis> Also at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html>

Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovation* (Washington, DC: Georgetown University Press, 2008)

Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, rev. ed. (Washington, DC: CQ Press, 2007)

David A. Schum, *Evidence and Inference for the Intelligence Analyst* (Lanham, MD: University Press of America, 1987)

Morgan Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, rev. ed. (New York: Three Rivers Press, 1998)

Robert S. Sinclair, *Thinking and Writing: Cognitive Science and Intelligence Analysis*, revised edition (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2010). Copy available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/thinking-and-writing.html>

A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis (Washington, DC: U.S. Government, 2009). Copy available online at: <https://www.cia.gov/library/publications/publications-rss-updates/tradecraft-primer-may-4-2009.html>

A Compendium of Analytic Tradecraft Notes, Volume I, Notes 1-10, reprinted (Washington, DC: Central Intelligence Agency, 1997). Copy available online at: http://www.au.af.mil/au/awc/awcgate/cia/tradecraft_notes/contents.htm

Also see *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, available online at: <https://www.cia.gov/library/kent-center-occasional-papers/index.html>

Analysts are the voice of the Intelligence Community

-- WMD Report (31 Mar 2005), p. 388

Analysts must absorb information with the thoroughness of historians, organize it with the skill of librarians, and disseminate it with the zeal of journalists.

--TRADOC Pam 525-2-1, *US Army Functional Concept for Intelligence 2016-2028*, 13 Oct 2010; p. 66

Analysis and Production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 1-02 and JP 2-01) Also see *analysis*; *all-source analysis*; *counterintelligence analysis*.

-- Also, the ability to integrate, evaluate, and interpret information from available sources and develop intelligence products that enable situational awareness. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Analysis of Competing Hypothesis (ACH). Identification of alternate explanations (hypothesis) and evaluation of all evidence that will disconfirm rather than confirm hypotheses. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

ACH a highly effective technique when there is a large amount of data to absorb and evaluate. It is particularly appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments.

Analysis Report. A type of DoD CI analytical product prepared IAW DoDI 5240.18; it may require in-depth study and research, but generally is not as involved as an assessment. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009). Also see *Counterintelligence Analytical Product*.

Analytic Tradecraft. The practiced skill of applying learned techniques and methodologies appropriate to an issue to mitigate, gain insight, and provide persuasive understanding of the issue to members of the U.S. Government and its allies. (DIA, *A Tradecraft Primer: Basic Structured Analytic Techniques*, March 2008).

Note: The source document (First Edition) cited above is no longer available online. The current version: *Tradecraft Primer: Structured Analytic Techniques*, 3rd Edition (3 March 2010) is now Defense Intelligence Reference Document, Analytic Methodologies, DIA-01-1003-001A, and is controlled as UNCLASSIFIED//FOR OFFICIAL USE ONLY.

Anomalies. Foreign power activity or knowledge, inconsistent with the expected norms that suggest prior foreign knowledge of US national security information, processes or capabilities. (DoDD O-5240.02, CI, 20 Dec 2007)

-- Also, irregular or unusual activities that may cue the analyst on the existence of FISS and ITO [international terrorist organizations] activity. (Army FM 2-22.2, CI, Oct 2009)

Anomalous Activity: Irregular or unusual deviations from what is usual, normal, or expected; activity inconsistent with the expected norm.

-- Also, [in DoD cyber usage] network activities that are inconsistent with the expected norms that may suggest FIE [Foreign Intelligence Entity] exploitation of cyber vulnerabilities or prior knowledge of U.S. national security information, processes, or capabilities. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010)

Anomaly-based Detection. The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (NIST Special Publication 800-94, Feb 2007)

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (JP 1-02)

Apportionment. In the general sense, distribution for planning of limited resources among competing requirements. (JP 1-02 and JP 3-0)

Apprehension. The taking of a person into custody or the military equivalent of “arrest.” Under Rule 304, Manual for Courts Martial (MCM), the restraint of a person by oral or written order directing him to remain within specified limits. (AR 381-20, Army CI Program, 25 May 2010)

Armed Forces Courier Service. A joint service of the Departments of the Army, the Navy, and the Air Force, with the Chief of Staff, US Army, as Executive Agent. The courier service provides one of the available methods for the secure and expeditious transmission of material requiring protected handling by military courier. (JP 1-02)

Assassination. The murder or attempted murder of DoD personnel for political or retaliatory reasons by international terrorists or agents of a foreign power. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, to murder (usually a prominent person) by a sudden and/or secret attack, often for political reasons. (Wikipedia, accessed 15 Feb 2010)

“[We] did everything from plotting ways to poison the capital’s water systems to drawing up assassination plans for US leaders.”

-- Oleg Kalugin, Former Major General in the KGB
as cited in Andrew & Mitrokhin, *The Mitrokhin Archive* (1999)

Unquestionably the most neglected aspect of U.S. counterintelligence. EO 12333 specifically provides that “*Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against... **assassinations** [emphasis added] conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.”

The word *assassin* is derived from the word Hashshashin (Arabic: *حشاشين*, *hashshāshīyīn*, also Hashishin, Hashashiyyin, or Assassins). It referred to the Nizari branch of the Ismā‘īlī Shia founded by the Persian Hassan as-Sabbah during the Middle Ages. They were active in Iran from the 8th to the 14th centuries, and also controlled the castle of Masyaf in Syria. The group killed members of the Muslim Abbasid, Seljuq, and Christian Crusader elite for political and religious reasons.

The important thing to know about any assassination or an attempted assassination is not who fired the shot, but who paid for the bullet.

-- Eric Ambler, *A Coffin for Dimitrios* (1939)

Assessment. A type of DoD CI analytical product prepared IAW DoDI 5240.18; it requires in-depth study and research. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009). Also see *Counterintelligence Analytical Product*.

-- Also, [in intelligence usage,] 1) analysis of the security, effectiveness, and potential of an existing or planned intelligence activity; or 2) judgment of the motive s, qualifications, and characteristics of present or prospective employees or “agents.” (JP 1-02)

-- Also, [in intelligence usage], appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinence, accuracy, or usefulness of information in terms of an intelligence need. (National HUMINT Glossary)

Assessment--within the human source environment...

“A process of getting to know and understand people and describing them.”

-- Robert R. Holt, *Assessing Personality* (1971)

Effective assessment of human beings is an art

Asset. [In intelligence usage,] any resource--person, group, relationship, instrument, installation, or supply--at the disposition of an intelligence organization for use in an operational or support role. Often used with a qualifying term such as agent asset or propaganda asset. (JP 1-02 and JP 2-0) Also see *agent; foreign intelligence agent; source*.

-- Also, [in human source operations] a recruited source. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, [in defense infrastructure usage] a distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned or operated by domestic, foreign, public, or private sector organization. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Asset Validation. In intelligence use, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *Source Validation*.

-- Also, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. This process continues through the life of the relationship. It may be more or less formal depending on the sensitivity of the relationship and the nature of the source. For clandestine sources, particularly foreign nationals, the process is usually formal and revalidation is required on a periodic basis. Whether or not it is conducted formally, it must be a well-planned and thought out activity. (DoD CI Collection IWG Handbook, TTP for CI Collection, Collection Management, and Collection Operations, 8 Aug 2006)

For any organization that collects human intelligence, having an independent system for asset validation is critical to producing reliable, well-vetted intelligence.

-- WMD Report (31 Mar 2005), p. 455

See DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U) and National HUMINT Manager Directive 001.008, HUMINT Source Validation.

Assign. 1) To place units or personnel in an organization when such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel; or 2) To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *attach*.

Assumption. A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 1-02)

Asymmetric Threat. An adversary strength that can be used against a friendly vulnerability. An adversary may pursue an asymmetric advantage on the tactical or strategic level by identifying key vulnerabilities and devising asymmetric concepts and capabilities to strike or exploit them. To complicate matters, our adversaries may pursue a combination of asymmetries. (USD/I Taking Stock of Defense Intelligence Report, 22 Jan 2004)

-- Also, a broad and unpredictable spectrum of military, paramilitary, and information operations, conducted by nations, organizations, or individuals or by indigenous or surrogate forces under their control, specifically targeting weaknesses and vulnerabilities within an enemy government or armed force. (Source: Michael L. Kolodzie, USA)

Attach. 1) The placement of units or personnel in an organization when such placement is relatively temporary; or 2) The detailing of individuals to specific duties or functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *assign*.

Attaché. A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity. Also see *Senior Defense Official / Defense Attaché (SDO/DATT)*.

Authenticate. A challenge given by voice or electrical means to attest to the authenticity of a message or transmission. (JP 1-02)

Authentication. 1) A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator; 2) A means of identifying individuals and verifying their eligibility to receive specific categories of information; 3) Evidence by proper signature or seal that a document is genuine and official; and 4) In personnel recovery missions, the process whereby the identity of an isolated person is confirmed. (JP 1-02 & JP 3-50)

Authenticator. A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (JP 1-02)

Background Investigation (BI). An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject. (IC Standard 700-1, 4 Apr 2008)

Backstop. The arrangement made by documentary or oral means to support a cover story so that inquiries about it will elicit responses indicating the story is true. (ICS Glossary & AFOSI Manual 71-142, 9 Jun 2000)

-- Also, to make arrangements made through documentary, oral, technical, fiscal, legal, or other means to support covers (both individual and organizational). A backstopped cover provides sufficient documentation to protect an identity in the immediate area or circumstance and in primary U.S. Government and commercial information systems. A backstopped cover is constructed to withstand routine scrutiny. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Backstopping. Arrangements made to support covers and activities. (HDI Lexicon, April 2008)

-- Also, verification and support of cover arrangements for an agent [case officer or intelligence operative] in anticipation of inquiries or other actions that might test credibility of his or her cover, (Spy Book)

Basic Intelligence. Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

Battlespace. The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. (JP 1-02)

Battlespace Awareness. Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission. (JP 1-02)

-- Also, the ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Beacon. A device typically fastened to an object or individual that transmits a radio signal in order to track its location. The technological discipline is called beaconry. (Spycraft)

Behavioral Science Consultant. A professional with extensive training in behavioral science, mental health, psychiatry, or psychology. (JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

Bilateral Collection. A collection activity run jointly with a foreign intelligence service. (DoDI S-5240.17, CI Collection, 12 Jan 2009)

Bilateral/BILAT Operation. An operation run jointly with a foreign intelligence service or between two US intelligence/CI services. (CI Community Lexicon)

Bigot Case. An investigation that due to the sensitivity of the subject or the nature of the investigation, requires that it be handled on a strict need to know basis. Access to these investigations is controlled by maintaining a list of personnel who have been approved for access, called a "bigot list." (AR 381-20, Army CI Program, 25 May 2010) Also see *bigot list*.

Bigot List. Tradecraft jargon for any list of names of cleared personnel having access (need-to-know) to a sensitive operation, investigation or to special access/compartimented intelligence. Also see *bigot case*, *compartmentation*.

The term dates back to World War II when Allied orders for officers were stamped "TO GIB" for those being sent to Gibraltar for preparations for the invasion of North Africa; later their orders were stamped "BIG OT" (TO GIB backwards) when they were sent back to begin planning Operation OVERLORD, the invasion of Normandy. In WWII, it was convenient, in trying to find out if someone had access to highly restricted NEPTUNE and OVERLORD planning information, to ask "are you bigoted?" An indignant answer of "no" ended that part of classified discussion.

Biometric. Measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual. (JP 1-02 and JP 2-0)

Biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 1-02 and JP 2-0)

-- Also, a general term used alternatively to describe a characteristic or a process. *As a characteristic:* A measurable biological (anatomical & physiological) and behavioral characteristic that can be used for automated recognition. *As a process:* Automated methods of recognizing an individual based on measurable biological (anatomical & physiological) and behavioral characteristics. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008)

-- Also, the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition. (NSPD 59 / HSPD 24, 5 Jun 2008)

-- Also, measurable biological (anatomical and physiological) and behavioral characteristic that may be used for automated recognition of the identity of a person or to verify his claimed identity. Includes fingerprints, iris/retina, voice, facial, DNA, fingernail, and thermal signature. (AR 381-20, Army CI Program, 25 May 2010)

The Secretary of the Army is the DoD Executive Agent for DoD Biometrics.

Biometrics-enabled Intelligence. Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist / insurgent network and related pattern analysis, facilitates high value individual targeting, reveals movement patterns, and confirms claimed identity. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008)

Black: 1) tradecraft jargon for inconspicuousness in the sense of being free of hostile surveillance [*going black*: become free of surveillance before conducting an operational act]; and 2) CIA tradecraft jargon for clandestine or covert. (Leo D. Carl, *The CIA's Insider Dictionary*, 1996)

Black Bag Job: Tradecraft jargon for clandestine breaking and entering.

Black List. [A list that] contains the identities and locations of individuals whose capture and detention are of prime importance, or individuals who have been determined to be intelligence fabricators. (CI Community Lexicon) Also see *Gray List*; *White List*.

Previous DoD definition in JP 1-02 (rescinded by JP 2-01.02, 11 Mar 2011): an official counterintelligence listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces.

Bona Fides. The lack of fraud or deceit: a determination that a person is who he/she says he/she is. (National HUMINT Glossary)

Tradecraft jargon for credentials, that which establishes the credibility of a human source.

-- Also, 1) Good faith. In personnel recovery, the use of verbal or visual communication by individuals who are unknown to one another, to establish their authenticity, sincerity, honesty, and truthfulness (JP 1-02 and JP 3-50); and 2) The lack of fraud or deceit: a determination that a person is who he/she says he/she is (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, physical and/or oral exchanges employed by an unknown individual to prove identity and foster trust. (HDI Lexicon, April 2008)

-- Also, documents, information, action, codes, etc., offered by an unknown or otherwise suspected individual to establish his or her good faith, identification, dependability, truthfulness, or motivation. (ICS Glossary & AFOSI Manual 71-142, 9 Jun 2000)

Border Crosser. An individual, living close to a frontier, who normally has to cross the frontier frequently for legitimate purposes. (JP 1-02)

Botnet. A collection of zombie PCs [personal computers]. Botnet is short for robot network. A botnet can consist of tens or even hundreds of thousands of zombie computers. A single PC in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers. (McAfee Labs - Threat Glossary) Also see *zombie*.

-- Also, Botnets, or Bot Networks, are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. (CRS Report PL32114, 29 Jan 2008)

Botnets have been described as the "Swiss Army knives of the underground economy" because they are so versatile.

Brevity Code. A code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content. (JP 1-02 & JP 3-04)

Brief Encounter. A short and discreet operational contact. (HDI Lexicon, April 2008) Also see *brush contact*; *brush pass*.

-- Also, any brief physical contact between a case officer and an agent under threat of surveillance. (CI Centre Glossary)

Brush Contact. A discreet momentary contact, usually prearranged between intelligence personnel, during which material or oral information is passed. (ICS Glossary & AFOSI Manual 71-142, 9 Jun 2000) Also see *brush pass*; *brief encounter*.

“Such a contact is extremely brief as well as surreptitious, and usually it is quite secure if well executed.” -- Victor Marchetti & John D. Marks, *The CIA and the Cult of Intelligence*, 2nd edition (1980), p 230

-- Also, a technique used by case officers to receive [or] exchange information from an agent clandestinely without betraying any signs of recognition between participants. The objective is to complete the transaction without detection by any hostile surveillance. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Brush Pass. A brief operational encounter (seconds or less) in which the case officer passes something (verbally or physically) to or receives something from the agent, or a two-way exchange takes place. (National HUMINT Glossary) Also see *brief encounter*; *brush contact*, *car toss*.

-- Also, a discreet, monetary contact during which something is exchanged. (HDI Lexicon, April 2008)

-- Also, a brief encounter where something is passed between a case officer and an agent. (CI Centre Glossary)

-- Also, the clandestine, hand-to-hand delivery of items or payments – made as one person walks past another in a public place [The Russian Foreign Intelligence Service (SVR) refers to a brush pass as a “flash meeting”]. (FBI Court Affidavit re: Russian Illegals, 25 June 2010)

Bug. [Tradecraft jargon] 1) Concealed listening device or other equipment used in audio surveillance; 2) To install such a device; the term “bugged” refers to a room or object that contains a concealed listening device. (Spy Book)

Bugging is a term in common use that refers to the various forms of clandestine electronic surveillance, or eavesdropping. See *Spycraft*, pp. 405-416, for details.

Bugged. Room or object that contains a concealed listening device. (JP 1-02)

Burned. [Tradecraft jargon] When a case officer or agent is compromised, or a surveillant has been made by a target, usually because they make eye contact. (CI Centre Glossary)

Burn Notice. An official statement by one intelligence agency to other agencies, domestic or foreign, that an individual or group is unreliable for any of a variety of reasons. (JP 1-02)

Campaign. A series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02) Also see *DoD Strategic CI Campaign*.

Campaign Plan. A joint operations plan for a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02) Also see *Campaign*; *Campaign Planning*; *DoD Strategic CI Campaign*.

Campaign Planning. The process whereby combatant commanders and subordinate joint force commanders translate national or theater strategy into operational concepts through the development of an operation plan for a campaign. Campaign planning may begin during contingency planning when the actual threat, national guidance, and available resources become evident, but is normally not completed until after the President or Secretary of Defense selects the course of action during crisis action planning. Campaign planning is conducted when contemplated military operations exceed the scope of a single major joint operation. (JP 1-02) Also see *campaign*; *campaign plan*.

Capability Gap. The inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability or lack of proficiency or sufficiency in existing capability.

Car Pick-Up. A personal meeting wherein the handler picks up the source. (HDI Lexicon, April 2008)

Car Toss. A form of dead drop using a concealment device thrown to a preselected site from a vehicle traveling along a designated route. (HDI Lexicon, April 2008) Also see *brief encounter*; *brush contact*, *brush pass*.

-- Also, the method of conveying information clandestinely by throwing a package into, or out of, a vehicle is known as the "car toss." (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Carbons. Paper that produces secret writing [SW] through the use of chemicals. (Spy Book) Also see *secret writing*.

Carve-Out. A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS [Defense Security Service] of its National Industrial Security Program obligation to perform industrial security oversight functions for a DoD SAP [Special Access Program]. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

Case. 1) An intelligence operation in its entirety; or 2) Record of the development of an intelligence operation, including personnel, modus operandi, and objectives. (JP 1-02)

--Also, the framework which not only acts as the repository for all logically/physically related facts, issues, allegations and products (outputs) associated with the investigative process, but also serves to document, in a case file, the approvals, authorities, waivers, plans, notes and other artifacts relevant to that particular instance of the process. (ONCIX Insider Threat Detection – Glossary)

Can also be used as a verb, to case, meaning to surreptitiously observe a physical location to determine its suitability for possible future operational use.

Case Officer (C/O). A professional employee of an intelligence or counterintelligence organization who is responsible for providing directions for an agent operation and/or handling intelligence assets. (JP 1-02; JP 2-01.2; CI Community Lexicon and ICS Glossary) Also see *Agent Handler*.

"...the case officer's job is to handle operational cases and assets; this is to say the case officer recruits and directs foreign indigenous spies who are known as "agents."
-- Fred Rustmann, Jr., "Debunking the CIA Case Officer Myth," *AFIO Newsletter*, 25: 1&2 (2002)

Casing. Reconnaissance of an operating area, whether for surveillance or for personal or impersonal communications. (CI Community Lexicon)

-- Also, a study of a site to determine operational suitability. (HDI Lexicon, April 2008)

-- Also, covert or clandestine inspection or surveillance of an area, place, or building to determine its suitability for operational use or its vulnerability to an intelligence operation. (AFOSI Manual 71-142, 9 Jun 2000)

Catastrophic Event. Any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (JP 1-02 & JP 3-28)

Caveat. A designator used with or without a security classification to further limit the dissemination of restricted information, e.g., FOUO and NOFORN. (IC Standard 700-1, 4 Apr 2008)

Cell. [In intelligence usage,] a small group of individuals who work together for clandestine or subversive purposes.

Center [British spelling: *Centre*]. The headquarters site in the home country where control of intelligence and espionage operations in foreign countries is maintained. (AFOSI Manual 71-142, 9 Jun 2000)

Center of Gravity (COG). The source of power that provides moral or physical strength, freedom of action, or will to act. (JP 3-0, Joint Operations)

Central Intelligence Agency (CIA). An independent US Government agency responsible for providing national security intelligence to senior US policymakers. Primary mission: collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security. Major components: National Clandestine Service (NCS), Directorate of Intelligence, Directorate of Science & Technology and Directorate of Support. (cia.gov)

Director CIA coordinates the clandestine collection of foreign intelligence through human sources or through human-enabled means and counterintelligence activities outside the United States (EO 12333). The Director CIA is designated the Functional Manager for human intelligence IAW EO 12333; and is also the National HUMINT Manager IAW ICD 304.

The CIA may engage in covert action at the President's direction and in accordance with applicable law; see *covert action*.

We do espionage. That is the nature of what we do. We steal secrets.

-- DCI George Tenet (23 Jun 1998)

Interview in *Studies in Intelligence*, 42:1 (1998)

Chain of Custody. A chronological written record reflecting the release and receipt of evidence from initial acquisition until final disposition. (AR 195-5, Evidence Procedures, 25 Jun 2007) Also see *evidence*.

Chairman's Guidance (CG). Provides a common set of assumptions, priorities, intent, and critical planning factors required to develop future strategies and plans. It is an integral part of the strategy development process. CG may be established pursuant to conducting a Joint Strategy Review, to preparing a Joint Vision, or to Drafting a new National Military Strategy; or it may be provided separately if deemed appropriate. (CJCSI 3100.01A, Joint Strategic Planning System, 1 Sep 1999)

Chancery. The building upon a diplomatic or consular compound which houses the offices of the chief of mission or principal officer. (JP 1-02)

Chief of Mission (CoM). The principal officer in charge of U.S. Diplomatic Missions and U.S. offices abroad, which the Secretary of State has designated as diplomatic in nature. The CoM reports to the President through the Secretary of State. Also see *Ambassador*.

-- Also, the principal officer (the ambassador) in charge of a diplomatic facility of the United States, including any individual assigned to be temporarily in charge of such a facility. The CoM is the personal representative of the President to the country of accreditation and is responsible for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). The security of the diplomatic post is the CoM's direct responsibility. (JP 1-02 and JP 3-08)

The U.S. Ambassador to a foreign country, for example, is the Chief of the U.S. Mission (CoM) in that country. Other CoMs include the Chiefs of permanent U.S. Missions to international organizations (e.g., the U.S. Mission to International Organizations in Vienna), the Principal Officers of Consulates General, and the U.S. Interest Section in the Swiss Embassy in Havana.

The CoM has full responsibility and authority for the direction, coordination, and supervision of all USG executive branch employees in country and at international organizations, regardless of their employment categories or location, except those under command of a U.S. area military commander or on the staff of an international organization.

Chief of Station (CoS). Senior US intelligence officer in a foreign country, and is the direct representative of the Director National Intelligence (DNI), to whom the officer reports through the Director Central Intelligence Agency (CIA). Usually the senior representative of the CIA assigned to a US Mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Choke Point. A narrow passage--such as a bridge, tunnel, or Metro station--used as a surveillance or countersurveillance tool for channeling the opposing force or monitoring their passage. (CI Centre Glossary)

CI. See *counterintelligence*.

CI Campaign. See *DoD Counterintelligence Campaign*.

CI Mission Tasking Authority. See *Counterintelligence Mission Tasking Authority*.

Cipher. Any cryptographic system in which arbitrary symbols (or groups of symbols) represent units of plain text of regular length, usually single letters; units of plain text are rearranged; or both, in accordance with certain predetermined rules. (JP 1-02) Also see *code*; *cipher pad*.

Cipher Pad. A small thin pad of paper sheets having nonrepetitive key, usually machine printed. A sheet is used once for enciphering and another sheet used once for deciphering a communication. Occasionally called a one-time pad (OTP). (AFOSI Manual 71-142, 9 Jun 2000)

CISO. Also see *Counterintelligence Staff Officer*.

Note: in the revision to DoDI 5240.10, this term will be replaced by "Command CI Coordinating Authority" or CCICA and will also be updated in JP 1-02.

Civil Authorities. Those elected and appointed officers and employees who constitute the government of the United States, the governments of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States possessions and territories, and political subdivisions thereof. (JP 1-02)

Civil Disturbance. Group acts of violence and disorder prejudicial to public law and order. (JP 3-28)

Civilian Internee. A civilian who is interned during armed conflict, occupation, or other military operation for security reasons, for protection, or because he or she committed an offense against the detaining power. (JP 3-63, Detainee Operations, 6 Feb 2008)

Clandestine. Any activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, any HUMINT [Human Intelligence] or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (ICD 304, HUMINT, 1 Mar 2007 and DoDD S-5200.37, 9 Feb 2009)

-- Also, any illicit/illegal activity that is designed not to be detected by anyone, including a local security service. Concealed, hidden, secret, or surreptitious operation conducted without the knowledge of anyone but the organization conducting the operation or investigation. (CI Community Lexicon)

-- Also, method of conducting operations with secrecy by design. Differs from covert in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary)

-- Also, secret or hidden activity conducted with secrecy by design. (ICS Glossary, 1978)

Clandestine Collection. The acquisition of protected intelligence information in a way designed to protect the source, and conceal the operation, identity of operators and sources, and actual methodologies employed. (DoDI S-5240.17, CI collection, 12 Jan 2009)

Clandestine Intelligence Collection. The acquisition of protected intelligence information in a way designed to conceal the nature of the operation and protect the source. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

--Also, the acquisition of protected intelligence information in a way designed to protect the source. (National HUMINT Glossary)

Clandestine Operation. An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. (JP 1-02 and JP 3-05.1)

-- Also, activities to accomplish intelligence, CI, or similar activities in such a way as to maintain secrecy or concealment especially for the purpose of deception or subversion. (CI Community Lexicon)

-- Also, a pre-planned secret intelligence information collection activity, technical operation, or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses clandestine collection, counterintelligence, and covert action. (National HUMINT Glossary)

-- Also, any HUMINT or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (DHE-M 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See *covert operation*.

Classification. The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (JP 1-02)

Classified Information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 1-02)

-- Also, information or material designated and clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security. (50 USC § 426[1])

Classified Information Procedures Act (CIPA). The tool with which the proper protection of classified information may be ensured in indicted cases. After a criminal indictment becomes public, the prosecutor remains responsible for taking reasonable precautions against the unauthorized disclosure of classified information during the case. This responsibility applies both when the government intends to use classified information in its case-in-chief as well as when the defendant seeks to use classified information in his/her defense. (18 USC, App III, Sec 1-16) Also see *graymail*.

Congress enacted CIPA (Public Law 96-456) in 1980. The procedural protections of CIPA protect unnecessary disclosure of classified information. The primary purpose was to limit the practice of "graymail" by criminal defendants in possession of sensitive government secrets. "Gray mail" refers to the threat by a criminal defendant to disclose classified information during the course of a trial.

The gray mailing defendant essentially presented the government with a "Hobson's choice": either allow disclosure of the classified information or dismiss the indictment.

CIPA is a procedural statute that balances the right of a criminal defendant with the right of the sovereign to know in advance of a potential threat from a criminal prosecution to its national security. CIPA's provisions are designed to prevent unnecessary or inadvertent disclosures of classified information and to advise the government of the national security "cost" of going forward.

See: <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm>

Clean Phone. Tradecraft jargon which typically refers to a disposable, pre-paid cellular telephone that cannot be traced back to the original retail purchaser or subsequent user(s).

Clearance. Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL). (National Information Assurance Glossary, CNSS Instruction No. 4009, Revised June 2006, hereinafter referred to as CNSS Instruction No. 4009)

Coalition. An ad hoc arrangement between two or more nations for common action. (JP 1-02) Also see *alliance*; *multinational*.

Code. 1) Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or for security; 2) a cryptosystem 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 which are primarily words, phrases, or sentences. (JP 1-02) Also see *cipher*.

"There is no sharp theoretical line between codes and ciphers; [a] useful distinction is that code operates on linguistic entities, dividing its raw material into meaningful elements and cipher does not." -- David Kahn, *The Code Breakers* (1967)

Code Word. 1) A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation; and 2) A cryptonym used to identify sensitive intelligence data. (JP 1-02)

-- Also, a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher. (DoD 5200.1-R, Information Security Program, Jan 1997)

-- Also, a single classified word assigned to represent a specific SAP or portions thereof. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, a prearranged word used in communication or conversation to disguise the identity of someone or something or to convey a meaning other than its conventional meaning. (AFOSI Manual 71-142, 9 Jun 2000) Also see *nickname*.

Cold Pitch. Recruitment approach without prior development or, in some cases, contact. (National HUMINT Glossary)

COLISEUM. See *Community On-Line Intelligence System for End-Users and Managers*.

Collaborating Analytical Center (CAC). An intelligence organization that has responsibility to support and assist a Responsible Analytical Center (RAC) produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. CACs may provide all-source analysis, application of analysis, or single-source analysis, exploitation, or reporting. DoD organizations that may serve as CACs include: Combat Support Agencies (DIA, NSA, NGA), the COCOM JIOCs, and the Service Intelligence Centers (NGIC, ONI, NASIC & MCIA). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Collateral. All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive Order for which special systems of compartmentation (such as SCI or SAPs) are not formally required. (DoDI 5200.01, 9 Oct 2008)

Collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 1-02 and JP 2-0) Also see *counterintelligence collection*; *clandestine intelligence collection*; *intelligence collection*; *military counterintelligence collection*.

-- Also, the acquisition of information to meet an intelligence requirement. (ICD 300, 3 Oct 2006)

-- Also, the ability to obtain required information to satisfy intelligence needs. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, the exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for the use in the production of intelligence; obtaining information or intelligence information in any manner, including direct observations, liaison with official agencies, or solicitation from official, unofficial, or public sources, or quantitative data from test or operation of foreign systems. (CIA, *A Consumer's Guide to Intelligence*, July 1995)

-- Also, the exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (National HUMINT Glossary)

The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect... turns analysis into guesswork. -- WMD Report (2005); p. 351

EO 12333, US Intelligence Activities, directs that IC elements use the least intrusive collection techniques feasible within the United States or directed against US persons abroad (para 2.4 - Collection Techniques).

Collection Asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

Collection Emphasis. Identifies new short- to intermediate-term information needs in response to unforeseen situations, emerging crises, or contingencies. It can be used to register additional or refined requirements in connection with a unique collection opportunity. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Collection Management (CM). In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking, as required. (JP 1-02 and JP 2-0)

CM has two distinct functions: collection requirements management and collection operations management. See *collection requirements management* and *collection operations management*.

Collection Management Authority (CMA). Within DoD, CMA constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Collection Manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02 & JP 2-01)

Collection Operations Management (COM). The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. (JP 1-02 & JP 2-0) Also see *collection management*, *collection requirements management*.

-- Also, COM specifies how to satisfy the [intelligence] requirement. It focuses on the selection of the specific intelligence disciplines(s) and specific systems within a discipline to collect information addressing the customer's requirement. COM is conducted by organizations to determine which collection assets can best satisfy the customers' product requests. (JP 2-01, Joint and National Intelligence Support to Military Operations, 7 Oct 2004)

COM is the process by which it is determined "how" a requirement will be answered within an intelligence discipline and "who" will execute the collection activity.

Collection Plan. A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02 & JP 2-01)

The collection plan determines how a collection requirement will be satisfied.

Collection Planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. (JP 1-02 & JP 2-0)

Collection Requirement. 1) An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency; or 2) An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *intelligence requirement; information requirements*.

Collection Requirements Management (CRM). The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. (JP 1-02 and JP 2-0) Also see *collection management; collection operations management*.

CRM is the process by which it is determined "what" will be collected and by "which" intelligence discipline. CRM defines "what" intelligence systems must collect and focuses on the requirements of the customer; it is all-source oriented and advocates "what" information is necessary for collection.

Collection Resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02 & JP 2-01)

Collection Support Brief (CSB). A supplement to a collection requirement on key country topics, technical subjects, and other complex issues. It provides more detailed tutorial information for HUMINT collectors regarding technical developments, organizations, facilities, and personalities associated with the collection topic. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Collector. A person who acquires information or services from a source. (HDI Lexicon, Apr 2008)

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 5-0, Joint Planning, 26 Dec 2006)

Combatant Command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02 & JP 5-0) Also see *Unified Command Plan*.

-- Also, combatant command (command authority): Nontransferable command authority established by Title 10 ("Armed Forces"), United States Code, Section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). (JP 1-02 & JP 1)

Combatant Commander. A commander of one of the unified or specified combatant commands established by the President. (JP 1-02) Also see *Unified Command Plan*.

Combating Terrorism (CbT). Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (JP 1-02 & JP 3-26)

Combat Intelligence. That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (JP 1-02 & JP 2-0)

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 1-02 & JP 5-0)

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02 & JP 1)

Command Counterintelligence Coordinating Authority (CCICA). The Combatant Commander's senior representative for CI. The CCICA serves as the authoritative point of contact for the Combatant Command on CI issues and activities and assists in exercising the command's CI activities. JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *Counterintelligence Coordinating Authority* (CICA).

For additional information see JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011 (para 2a)

Note: in the revision to DoDI 5240.10, the term "Counterintelligence Staff Officer" or "CISO" will be replaced by Command CI Coordinating Authority or CCICA; to be updated in JP 1-02.

Commander's Critical Information Requirement (CCIR). An information requirement identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements. (JP 1-02 & JP 3-0)

Committee of Foreign Investment in the United States (CFIUS). An interagency committee that serves the President in overseeing the national security implications of foreign investments. CFIUS has 12 members under the chairmanship of the Secretary of Treasury consisting of: the Secretaries of State, Defense, Commerce, and Homeland Security, the Attorney General, Director OMB, Director of the Office of Science and Technology Policy, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, US Trade Representative, and Chairman of the Council of Economic Advisers. (Department of Treasury website <<http://www.treas.gov/offices/international-affairs/exon-florio/>>)

Originally established in 1975 by EO 11858 mainly to monitor and evaluate the impact of foreign investment in the United States. In 1988, EO 12661 designated CFIUS to receive notices of foreign acquisitions of U.S. companies, to determine whether a particular acquisition has national security issues sufficient to warrant an investigation and to undertake an investigation, if necessary, and to submit a report and recommendation to the President at the conclusion of an investigation.

On 26 July 2007, *the Foreign Investment and National Security Act of 2007* (PL 110-49) was enacted. The act was implemented by EO 13456 and addresses many issues, e.g., Congressional notification requirements; more stringent rules for the review and formal investigation of transactions, especially those involving foreign governments or critical infrastructure assets; requires senior-level involvement in various required certifications and reports, limiting the agencies' delegation authority; established the membership of CFIUS by statute; and created a defined role for the Director of National Intelligence as an ex-officio member who must evaluate the transaction's national security implications.

Common Operational Picture (COP). A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02 & JP 3-0)

Communications Intelligence (COMINT). Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 1-02 & JP 2-0) Also see signals intelligence.

Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 1-02 & JP 6-0)

-- Also, protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security, and jamming resistance) to telecommunications and to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials. (DoDD 4640.6 Communications Security Telephone Monitoring and Recording, 26 Jun 1981)

-- Also, measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (DoDD 5100.20, NSA, 26 Jan 2010)

Communications Security Monitoring. The act of listening to, copying, or recording transmissions of one's own circuits (or when specially agreed, e.g., in allied exercises, those of friendly forces) to provide material for communications security analysis in order to determine the degree of security being provided to those transmissions. In particular, the purposes include providing a basis for advising commanders on the security risks resulting from their transmissions, improving the security of communications, and planning and conducting manipulative communications deception operations. (JP 1-02)

Community Acquisition Risk Center (CARC). The CARC conducts multi-source threat analysis of commercial entities doing business with any component of the Intelligence Community. (ODNI News Release 2-06, 11 Jan 2006) [now known as the Community Acquisition Risk Section (CARS)]

-- Also, the CARC evaluates the risk to the Intelligence Community posed by commercial entities conducting business with the individual components of the Intelligence Community. Common acquisition-risk methodologies, tools, and training that are now under development will significantly enhance the program. The Center is a joint enterprise composed of staff from all members of the Intelligence Community. (<<http://www.ncix.gov/sections/carc/index.html>>)

See DCID 7/6, Community Acquisition Risk Center, 2 Mar 2005 (Unclassified//FOUO).

Community Acquisition Risk Section (CARS). See *Community Acquisition Risk Center* above.

Community On-Line Intelligence System for End-Users and Managers (COLISEUM). The management system for production requirements and requests for information. CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

-- Also, the primary production requirements management system for the Defense Intelligence Analysis Program (DIAP). It supports the DIAP mission to consolidate and gain synergism of DoD intelligence production resources by automating the basic production requirement process defined in the DIAP and its key operational concepts. (DIA DIAP)

-- Also, an analysis requirement management tool used throughout the Defense Intelligence Community to register and track requests for information/analytical requirements, search for existing intelligence, and manage/account for analytical resources. It is a web-based application available through Intelink. (Joint Military Intelligence Training Center, *Fundamentals of COLISEUM 5.0*, JMITC, Jun 2008)

Defense CI Components shall use the CI-approved electronic archiving system to validate, task, and disseminate production requirements for CI analysis. The approved system is the primary method to communicate analysis and production requirements within the DoD CI enterprise. Defense CI Components without access to the approved system may use COLISEUM.
-- IAW DoDI 5140.18, CI Analysis & Production, 17 Nov 2009

Compartmentation. The principle of controlling access to sensitive information so that it is available only to those individuals or organizational components with an official "need-to-know" and only to the extent required for the performance of assigned responsibilities. (National HUMINT Glossary)

-- Also, establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (JP 1-02 & 3-05.1)

-- Also, the process of strictly limiting the number of people who are aware of a given intelligence operations.... Only personnel with an absolute "need to know" should be admitted into the compartment. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

The primary purpose of compartmentation is security, to protect extremely sensitive information from compromise.

An intelligence service that is carless about compartmentation pays the price.

-- James M. Olson (CIA Retired)

Compartmented Intelligence. National intelligence placed in a DNI-approved control system to ensure handling by specifically identified and access approved individuals. (IC Standard 700-1, 4 Apr 2008)

-- Also, national intelligence information under a control system and only available to designated individuals. (National Intelligence: A Consumer's Guide - 2009).

Compartmented intelligence became institutionalized during World War II [SIGINT, e.g., ULTRA, MAGIC, etc.]... Compartmentalizing information is the way they restrict what is known.
-- William E. Burrows, *Deep Black* (1986)

In the secret operations canon it is axiomatic that the probability of leaks escalates exponentially each time a classified document is exposed to another person.... Effective compartmentation is fundamental to all secret activity.
-- Richard Helms (Former DCI), *A Look Over My Shoulder* (2003)

Complaint-type Investigation. A counterintelligence investigation in which sabotage, espionage, treason, sedition, subversive activity, or disaffection is suspected. (JP 1-02)

Compromise. The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (JP 1-02)

-- Also, a communication or physical transfer of classified information to an unauthorized recipient. (DoDD 5200.1, DoD Information Security Program, 13 Dec 1996)

-- Also, an unauthorized disclosure of classified information. (DoD 5200.1R, Information Security Program, Jan 1997 and DoD 5220.22-M, NISPOM, 28 Feb 2006)

-- Also, the disclosure or release of classified information to unauthorized person(s). (IC Standard 700-1, 4 Apr 2008)

-- Also, type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (CNSS Instruction No. 4009)

Compromised. A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (JP 1-02)

-- Also, when an operation, asset, or agent is uncovered and cannot remain secret. (CI Centre Glossary)

Compromising Emanations. Unintentional emissions that could disclose information being transmitted, received, or handled by any information-processing equipment. (ICS Glossary) Also see *TEMPEST*.

Computer Forensics. The scientific, systematic inspection and analysis of digital media and its contents to gather information on the facts and circumstances which may connect an incident to a threat to national security or other computer use that is contrary to security of information systems or may indicative of espionage. The objectives are to perform a structured investigation, maintain the proper chain of evidence, reconstruct the activities of a computer user, and preserve the integrity of the data. (AR 381-20, Army CI Program, 25 May 2010)

Computer Intrusion. An incident of unauthorized access to data or an automated information system. (JP 1-02)

Computer Intrusion Detection. The process of identifying that a computer intrusion has been attempted, is occurring, or has occurred. (JP 1-02)

Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02 & JP 3-13)

-- Also, operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

Computer Network Defense (CND). Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 1-02 & JP 6-0)

-- Also, efforts to defend against the computer network operations of others, especially that directed against U.S. and allied computers and networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 1-02 & JP 6-0)

-- Also, intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

Computer Network Operations (CNO). Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. (JP 1-02 & JP 3-13)

Computer Security (COMUSEC). The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02 & JP 6-0) Also see *Information Security (INFOSEC)*; *Cybersecurity*.

Computer Trespasser. A person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; see 18 USC 2510 (21)(a). (AR 381-20, Army CI Program, 25 May 2010)

Computer Virus. A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, a computer program that can copy itself and infect a computer without permission or knowledge of the user. (Wikipedia, accessed 2 Oct 2007)

Concealed Monitoring. Targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time. (DoD 5240.1-R, Dec 1982)

Concealed monitoring includes, but is not limited to the use of microphones, video cameras, beepers, beacons, transponders, and GPS locators.

Concealment Device (CD). A container designed to hide materials. (HDI Lexicon, April 2008)

-- Also, innocuous object designed or adapted as a container for secreting and selected material or equipment. Also called containers. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, any one of a variety of innocuous devices used to secretly store and transport materials relating to an operation. (CI Centre Glossary)

-- Also, an object modified or fabricated to contain either a device or intelligence materials for the purpose of covert storage, transport, placement within a target, or dead-dropping. (Spycraft)

Concept of Intelligence Operations. A verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. The concept of intelligence operations, which supports the commander's concept of operations, is contained in the intelligence annex of operation plans. The concept of intelligence operations is designed to give an overall picture of intelligence support for joint operations. It is included primarily for additional clarity of purpose. (JP 2.0)

Concept of Operations (CONOPS). A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. The concept is designed to give an overall picture of the operation. (JP 5-0)

Concept Plan (CONPLAN). In the context of joint operation planning level 3 planning detail, an operation plan in an abbreviated format that may require considerable expansion or alteration to convert it into a complete operation plan or operation order. (JP 1-02 & JP 5-0)

Confidential Source. Any individual or organization that provides information to the U.S. Government on matters pertaining to national security and expects, in return, that the information or relationship, or both, will be held in confidence. This definition is not to be confused with "intelligence source" as used in the Human Intelligence Community. (IC Standard 700-1, 4 Apr 2008)

-- Also, any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence. (DoD 5200.1-R, Information Security Program, Jan 1997 and EO 13526, 31 Dec 2009)

Confusion Agent. Within DoD, none.

This term was previously in JP 1-02 (rescinded 11 Mar 2011): an individual who is dispatched by the sponsor for the primary purpose of confounding the intelligence or counterintelligence apparatus of another country rather than for the purpose of collecting and transmitting information.

Congressional Intelligence Committees. The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). Also see *SSCI*; *HPSCI*.

The 1980 Intelligence Oversight Act charged the SSCI and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.
-- SSCI website at <http://intelligence.senate.gov/> and HPSCI at <http://intelligence.house.gov/>

Consensual Monitoring. Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication. (Attorney General's Guidelines for Domestic FBI Operations, 29 Sep 2008)

Consequence Management (CM). Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, man-made, or terrorist incidents. (JP 1-02 & JP 3-28)

Constraint. In the context of joint operation, a requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action. (JP 5-0, Joint Planning, 26 Dec 2006)

Contact Report (CR). A report of an operational event; a format providing the officer the ability to document routine aspects of operational activities not otherwise covered by other intelligence or operational reporting. (National HUMINT Glossary)

-- Also, a report used during the conduct of source operations to document the circumstances of, and establish a historical report of the operation. (Army FM 2.22-2, CI, Oct 2009)

Continental United States (CONUS). United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. (JP 1-02)

Contingency. A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (JP 5-0, Joint Planning, 26 Dec 2006)

Contingency Planning. The Joint Operation Planning and Execution System [JOPES] planning activities that occur in noncrisis situations. The Joint Planning and Execution Community uses contingency planning to develop operation plans for a broad range of contingencies based on requirements identified in the Contingency Planning Guidance, Joint Strategic Capabilities Plan, or other planning directive. Contingency planning underpins and facilitates the transition to crisis action planning. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *crisis action planning*.

Contingency Planning Guidance (CPG). The CPG fulfills the statutory duty of the Secretary of Defense to furnish written policy guidance annually to the Chairman of the Joint Chiefs of Staff for contingency planning. The SECDEF issues this guidance with the approval of the President after consultation with the Chairman of the Joint Chiefs of Staff. The CPG focuses the guidance given in the National Security Strategy and Defense Planning Guidance, and is the principal source document for the Joint Strategic Capabilities Plan [see CJCSI 3110.01]. (JP 1-02)

Control. [In intelligence human source operations], the capacity of a case officer (and his service) to generate, alter, or halt agent behavior by using or indicating his capacity to use physical or psychological means of leverage. (Source: John P. Dimmer, Jr., "Observations on the Double Agent," *Studies in Intelligence*, vol. 6, no. 1 (Winter 1962), pp 57-72. Declassified, originally classified SECRET.)

-- Also, [in intelligence usage,] physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. (JP 1-02)

-- Also, physical or psychological pressure exerted on an agent to ensure that he or she responds to directions from an intelligence agency or service. (Spy Book)

"A case officer does not control an agent the way he controls an automobile [or] the way a policeman controls an informer. The intelligence officer who thinks of control in absolutes of black and white does his operations a disservice; the areas of gray predominate."

-- John P. Dimmer, Jr. (1962)

Controlled Counterintelligence Activities. CI activities managed or monitored through a centralized control system, involving direct or indirect engagement with FIS [Foreign Intelligence Service] through human source or technical efforts. They include offensive CI operations, CI investigations, CE projects... intelligence polygraphs, and use of specialized techniques. (AR 381-20, Army CI Program, 15 Nov 1993)

Controlled Information. 1) Information conveyed to an adversary in a deception operation to evoke desired appreciations; or 2) Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to US interests and objectives. (JP 1-02)

Controlled Source. In counterintelligence use, a person employed by or under the control of an intelligence activity and responding to intelligence tasking. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *source; control; controlled source operation*.

Controlled Source Operation (CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008.

Controlled Technical Services (CTS). The controlled use of technology to enhance counterintelligence and human intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

CTS include asset communications, validation tools, tailored form factors, and technology or tools used with sources or CI and HUMINT officers to enhance their collection efforts. CTS are a support function of CI and HUMINT and are not independent operations.
-- JP 2.01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 (p. II-15)

Controlled Unclassified Information (CUI). Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (White House Memo, subj: Designation and Sharing of Controlled Unclassified Information, dated 7 May 2008)

All federal agencies routinely generate, use, store, and share information that, while not appropriate for "classification" under EO 12958 or other authority, nevertheless requires some level of protection from unauthorized access and release. Currently this information is identified by over 100 unique markings and handling regimes, such as "Law Enforcement Sensitive," "FOUO," etc.
An Interagency Task Force reviewed the CUI framework and recommended that the definition of CUI should be simplified to: *All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls.*
See *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*, 25 August 2009, at <http://www.dhs.gov/xlibrary/assets/cui_task_force_rpt.pdf>

Cooperative Contact. An asset validation term referring to an individual who wittingly responds to tasking in certain areas, but is unwilling to enter into a controlled clandestine relationship. (National HUMINT Glossary)

Co-Opted Worker or Co-Optee. A national of a country, but not an officer or employee of that country's intelligence service, who assists that service on a temporary or opportunity basis. (ICS Glossary & CI Community Lexicon)

Coordination. The process of sharing information regarding planned activity, affording potentially affected parties the opportunity to comment, prior to undertaking action. The process of coordination does not infer seeking authorization for action. (DoDD S-5200.37, 9 Feb 2009)

EO 12333 directs that the Director FBI coordinates CI activities inside the U.S. and that Director CIA coordinates CI activities outside the U.S. For coordination of DoD CI activities see:
-- Attorney General/SECDEF "Agreement Governing the Conduct of Defense Department CI in Conjunction with the Federal Bureau of Investigation," 9 Feb 1979 and supplement entitled "DoD/FBI MOU Regarding Coordination of Counterintelligence Matters (U)," 1 Apr 1996.
-- DCID 5/1 and USD(I) Memo, subj: Procedures for Coordination of CI Activities Outside the US, 4 Jan 2009
For coordination regarding HUMINT see ICD 304, *Human Intelligence*, 6 Mar 2008

Coordinating Authority. A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments, two or more joint force components, or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (JP 1-02)

Counter surveillance (also countersurveillance). Measures or actions taken when under verified or suspected surveillance. (DoDI S-5240.15, 20 Oct 2010) Also see *surveillance*.

-- Also, all measures, active or passive, taken to counteract hostile surveillance. (JP 1-02 & JP 3-07.2)

-- Also, activities undertaken by intelligence professionals to determine whether US forces are being surveyed [under surveillance] by potential adversaries. (Cole Commission Report, 8 Jan 2001)

-- Also ...security techniques designed to detect, prevent, or deceive hostile observation of friendly operations or activities. (CI Community Lexicon)

-- Also, countersurveillance, term for the tradecraft technique of detecting hostile surveillance of a person, rendezvous, safehouse, dead drop, et al. (Leo D Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, the practice of avoiding surveillance or making surveillance difficult. (Wikipedia)

Counter Threat Finance (CTF). Efforts to stop money that funds terrorism, proliferation, narcotics networks, espionage, WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, and other activities that generate revenue through illicit trafficking networks. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *threat finance*.

See DTM 08-034, *DoD Counterthreat Finance (CTF) Policy*, 2 Dec 2008

A DoD strategy for Counter Threat Finance is under development. The draft strategy offers a baseline definition for CTF: the means to detect, counter, contain, disrupt, deter, or dismantle the transnational financing of state and non-state adversaries threatening U.S. national security.

-- CTF Activities and Capabilities [within DoD]. DoD activities and capabilities, apart from those included under CTF intelligence, to deny, disrupt, destroy, or defeat financial systems and networks that negatively affect U.S. interests. This includes those activities and capabilities undertaken by other Government agencies and/or partner nations. CTF activities include, WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, terrorist revenue and logistics, and other such activities that generate revenue through illicit trafficking networks.

-- CTF Intelligence [within DoD]. DoD intelligence actions, including those undertaken with other U.S. Government agencies and/or coalition partners, that involves the collection, processing, integration, evaluation, analysis, interpretation, production, and dissemination of intelligence products in support of CTF activities and capabilities. CTF intelligence includes, but is not limited to, counternarcotics, Counterproliferation, counterterrorism, **counterintelligence**, and information operations.

Counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. *Counterdeception* does not include the intelligence function of identifying foreign deception operations. (JP 1-02) Also see *deception*; *military deception*.

Counterespionage. That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, actions undertaken to investigate specific allegations or circumstances and to acquire information concerning a person or persons involved in the violation of US espionage laws. (National HUMINT Glossary)

It is essential to seek out enemy agents who have come to conduct espionage against you...

-- Sun Tzu, *Art of War* (circa 500 B.C.)

Counterespionage... is a widely misunderstood branch of secret operations.... CE is an offensive operation, a means of obtaining intelligence about the opposition by using—or, more usually, attempting to use—the opposition’s operations. CE is a form of secret intelligence operation, but it is a form so esoteric, so complex and important as to stand by itself.

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and a knowledge of the specific operation he is conducting. Counterespionage personnel must then attempt to counter these operations by infiltrating the hostile service (called penetration) and through various forms of manipulation. Ideally, the thrust of the hostile operation is turned back against the enemy.

-- Senate Report # 94-755, aka Church Committee Report, 26 April 1976, p. 166

Counterquerrilla Operations. Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. (JP 1-02 & JP 3-24)

Counterinsurgency (COIN). Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency. (JP 1-02 & JP 3-24)

Counterintelligence (CI). Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended 30 July 2008 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Counterintelligence... countering adversarial intelligence threat

For DoD CI policy, see DoDD O-5240.02, *Counterintelligence*.

-- Also, information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Note: In update to JP 1-02, definition will be revised to reflect current definition in EO 12333 (cited above).

-- Also, encompasses actions taken to detect and counteract foreign intelligence activity that adversely affects U.S. national security interest. (WMD Report, 31 Mar 2005)

-- Also, intelligence activity, with its resultant product, devoted to destroying the effectiveness of inimical foreign intelligence activities and undertaken to protect the security of the nation and its personnel, information, and installations against espionage, sabotage, and subversion. Includes the process of procuring, developing, recording, and disseminating information concerning hostile clandestine activity and of penetrating, manipulating, or repressing individuals, groups, or organizations conducting such activity. (National Security Council Intelligence Directive [NSCID] No. 5, 17 Feb 1972)

-- Also, counters or neutralizes foreign intelligence and security services (FISS) and international terrorist organizations (ITO) intelligence collection efforts. It does this through collection, CI investigations, operations, analysis, production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to the protection of U.S. interests and equities. CI helps identify EEfIs [essential elements of friendly information] by identifying vulnerabilities to threat collection and actions taken to counter collection and operations against U.S. forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

Counterintelligence: [noun] intelligence activities concerned with identifying and countering the threat to security posed by hostile intelligence organizations or by individuals engaged in espionage or sabotage or subversion or terrorism.



CI “embraces all activities, human and technical, whether at home or abroad, that are undertaken to identify, assess, neutralize and exploit foreign intelligence threats... counterintelligence is inherently a strategic, national security instrument.”

-- Hon. Michelle Van Cleave, NCIX, 18 Nov 2004

Counterintelligence's core mission can be simply stated as countering adversarial intelligence threats. It is the business of identifying and combating foreign intelligence threats through **knowledge and action** -- knowledge of and action in countering global adversarial intelligence threats posed by a variety of intelligence entities directed by foreign states, as well as non-state actors, such as transnational terrorist groups.

CI “is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. ...But the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals.”

-- Roy Godson (1995)

CI is an integral component of U.S. Intelligence—historically and doctrinally, as well as by statute, executive order and policy. CI is an “intelligence activity” in accordance with the National Security Act of 1947 and EO 12333, which both specifically define “intelligence” as including counterintelligence and foreign intelligence. CI is *intelligence activity* focused on undermining the effectiveness of -- as well as exploiting -- adversary intelligence activities directed against US national security interests. Counterintelligence is one word in the United States (it is not counter intelligence or counter-intelligence).

Counterintelligence an instrument of national security...

“A ‘special form’ of intelligence activity, separate and distinct from other disciplines.”

-- U.S. Senate Report 94-755, 26 April 1976

CI is often confused with the foreign intelligence (FI) collection discipline referred to as human intelligence or HUMINT. Although CI and HUMINT are both intelligence activities that operate in the human domain, they are distinctly different. Both use human sources but is each focused on distinctly different content, as well as outcomes. The need for CI knowledge and action is much different from the need for FI collection.

CI wages “nothing less than a secret war against antagonist intelligence services.”

-- U.S. Senate Report 94-755, 26 April 1976

-- Also, CI encompasses information collections, analysis, investigations and operations conducted to identify and neutralize espionage and foreign intelligence activities, the intelligence-related activities of terrorists, and adversary efforts to degrade, manipulate or covertly influence U.S. intelligence, political processes, policy or public opinion. (NIPF [U], Jul 2006)

-- Also, CI may also be thought of as **knowledge** needed for the protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs against or from espionage, sabotage, and all other similar clandestine activities designed to weaken or destroy the United States. (Report of the Commission on Government Security - 1957, as cited in Church Committee Report, 26 April 1976, p. 163, footnote 1)

CI works closely with intelligence, security, infrastructure protections and law enforcement to ensure an integrated approach to the protection of U.S. forces, our intelligence and national assets, U.S. research, development and technology, and the U.S. economy.

CI is composed of both offensive and defensive elements. Offensive CI includes the penetration and deception of adversary groups. Defensive CI involves protecting vital U.S. national security related information from being obtained or manipulated by an adversary's intelligence organizations, activities and operations. This two-pronged approach forms a comprehensive CI strategy that is informed by collection results and feeds more effective CI operations.

Counterintelligence is a universal constant that should be factored in whenever U.S. intelligence or national security capabilities are deployed or when we are targeted by our adversaries. 'Every' U.S. intelligence capability and requirement needs to be protected and 'every' intelligence threat deployed against us should be countered by effective offensive and defensive CI.

-- NIPF - Intelligence Topic Definitions and Information Needs (U), July 2006

Counterintelligence Activities. [An alternate term for] One or more of the five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (JP 1-02 and DoDD O-5240.02, Counterintelligence, 20 Dec 2007) Also see *counterintelligence functions*.

Counterintelligence Activities in Cyberspace. CI activities in cyberspace include those forensics examinations of DoD affiliated information systems and other approved virtual or on-line activities to identify, disrupt, neutralize, penetrate, or exploit FIEs [Foreign Intelligence Entities]. DoD CI activities in cyberspace do not include Offensive Computer Operations as defined in NSPD-38 or the collection and processing of technical and intelligence information derived from foreign communications by other than an intended recipient. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010)

Counterintelligence Analysis. The methodical process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of foreign powers, international terrorists, and other entities. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007)

Astute analysis is [a] critical enabler... Strategic analysis allows DoD CI to understand today's risk environment. ...[it] allows the Department to learn and use an adversary's pressure points to influence its actions. -- DoD Counterintelligence Strategy - FY 2004

CI analysis informs decision makers, drives collections, shapes operations, and enables mission execution

"Effective counterintelligence analysis is a tall order. Good macro-analysis is not synonymous with journalism, or narrative description, or even investigations. Macro-counterintelligence analysis is meant to be explanatory, systematic, empirical, cumulative, reliable, comprehensive, integrated, and policy relevant. Analysis should discover and connect the seemingly disconnected, illuminate hidden relationships, identify unseen linkages, reveal patterns of activity and behavior heretofore unobserved. Good counterintelligence analysis should provide reliable knowledge and authoritative judgments to policymakers and operators. The product of counterintelligence and security analysis is understanding and explanation, and if possible, to answer the questions how and why."

-- Kenneth E. deGraffenreid, *Countering Hostile Intelligence Activities as a Strategic Threat* (1989)

-- Also, the process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of state and non-state actors and other entities and activities of CI interest. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, a step in the process of producing timely, accurate, and relevant assessments regarding the actual and potential foreign intelligence and international terrorist threat to Department of Defense in which the collected information is subjected to review to identify significant facts for subsequent interpretation. (AR 381-20, Army CI Program, 25 May 2010)

I can't possibly overstate the importance of good research. Everyone goes through life dropping crumbs. If you can recognize the crumbs, you can trace a path all the way back from your death certificate to the dinner and a movie that resulted in you in the first place. But research is an art, not a science, because anyone who knows what they're doing can find the crumbs, the wheres, whats, and whos. The art is in the whys: the ability to read between the crumbs, not to mix metaphors. For every event, there is a cause and effect. For every crime, a motive. And for every motive, a passion. The art of research is the ability to look at the details, and see the passion.

-- Daryl Zero, *The Zero Effect* (1998)

CI analysis... look at the details and see the passion

For a "snap shot" of CI analysis see Irvin D. Sugg, Jr., *Basic Counterintelligence Analysis in a Nutshell: Quick Reference Guide*, n.d., Joint Counterintelligence Academy (JCITA).

Copy available at: <<http://www.ntis.gov/search/product.aspx?ABBR=PB2010105593>>

Counterintelligence Analysis and Production Council (CIAPC). The principal forum for coordinating CI analysis and production requirements, discussing CI analysis and production priorities within the enterprise, and discussing other IC issues. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

CIAPC Membership: The Director, Defense CI & HUMINT Center (DCHC), appoints the Chair. Core membership includes the DCHC analysis and production enterprise manager and the managers of the Defense CI Component analysis and production elements. The Chair may expand membership, to include other full-time or permanent part-time Federal employees.

Counterintelligence Analysis and Production Element. The element within a Defense CI Component that performs CI analysis in any form; produces a CI analytical product in any of the categories of CI analysis; or responds to requests for CI analysis from an internal organization and/or from organizations external to the Defense CI Component. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analysis Report. A document produced by a CI analysis and production element stating the results of analysis regarding a relevant CI topic, event, situation, or development, and containing the characteristics outlined in [DoDI 5240.18] Appendix 2 to Enclosure 3. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analytical Product. Any document that contains the work of, is supported by, collaborated on, or produced by a CI analyst at any echelon within a Defense CI Component. It may or may not include CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Objectives of CI analytical products are to: 1) Outline, describe, or illustrate the threat posed by an Foreign Intelligence Entity (FIE) to installations, personnel, assets, operations, or resources; 2) Identify opportunities to conduct offensive CI operations (OFCO) targeting a FIE; and 3) Identify CI investigative opportunities.

CI analytical products seek to satisfy a core CI production requirement to identify people, organizations, locations, activities, and resources associated with a FIE or a target of a FIE.

Within DoD, CI analytical products are categorized based on the purpose of the product, analytical effort, the production timeline, and other distinguishing characteristics. The primary categories of CI analytical products are: 1) Assessment, 2) Analysis Report, 3) Threat Advisory, and 4) Functional Support. Associated analytical products with CI collections, investigations and operations are summarized below.

-- *Analytical products associated with CI collections are:*

Collection Support Brief. Provides near-comprehensive background detail on a collection issue to guide and enhance collection efforts. (DoDI 5240.18, 17 Nov 2009)

Collection Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Collection Emphasis. Supplements a standing collection requirement and identifies areas of emphasis or information gaps to the CI collector. (DoDI 5240.18, 17 Nov 2009)

Source-Directed Requirement. Established by a CI analysts based on knowledge of a source's access and placement to necessary information. (DoDI 5240.18, 17 Nov 2009)

IIR Evaluation. An analyst's evaluation of how well an IIR satisfied the intelligence requirement for which it was collected. (DoDI 5240.18, 17 Nov 2009)

-- *Analytical products associated with CI investigations are:*

Investigative Analysis Report. An evaluation of all available information obtained during a CI inquiry to determine if an investigation is warranted; an evaluation of an on-going CI investigation to develop leads, identify trends, patterns, or anomalies in furtherance of the investigative effort; or produced at the conclusion of a CI investigation to identify previously unknown methods of operation, describe lessons learned, and to support damage assessments when initiated. (DoDI 5240.18, 17 Nov 2009)

Investigative Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible, and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Investigative Support Package. An evaluation of all available information pertaining to an unknown subject CI inquiry or investigation in an effort to identify a person, place, or thing of CI interest based on analysis of the information. (DoDI 5240.18, 17 Nov 2009)

-- *Analytical products associated with CI operations are:*

Operational Analysis Report. An evaluation of information from a variety of sources to determine if favorable conditions are present for initiation of a CI operation and the report may offer suggestions as to the type of asset and/or the access and placement required to meet the foreign essential elements of information requirements. (DoDI 5240.18, 17 Nov 2009)

Operational Asset Evaluation. Evaluates an asset's reliability and veracity in a CI operation. (DoDI 5240.18, 17 Nov 2009)

Operational Support Package. Comprehensive analysis of all available intelligence on a target of interest to a Defense CI Component or determined to be of interest to DoD CI. It details the significance of the target, relates it to strategic objectives, identifies desired effects, and suggests methods of engagement to achieve desired results. (DoDI 5240.18, 17 Nov 2009)

Counterintelligence Assessment. A document produced by a CI analysis and production element stating the in-depth and comprehensive results of analysis regarding a relevant CI topic, event, situation, or development, and contains the characteristics outlined in [DoDI 5140.18] Appendix 2 to Enclosure 3. (DoDI 5140.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Awareness. A state of being aware of the sensitivity of classified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the United States while being able to recognize attempts to compromise one's information, and the actions one should take, when one suspects he has been approached, to impart the necessary facts to trained counterintelligence personnel. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Counterintelligence Awareness Products. A DoD Component's analysis of a CI topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate. The Defense Security Service "*Technology Collection Trends in Defense Industry*" and the Office of the National Counterintelligence Executive "*Annual Report to Congress on Foreign Economic Espionage*" are examples of products meeting this objective. (DoDI 5200.39, 16 Jul 2008)

Counterintelligence Campaign (CI Campaign). See *DoD Counterintelligence Campaign*.

Counterintelligence Collection. The systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons that are directed against or threaten DoD interests. (JP 1-02)

-- Also, the systematic acquisition of intelligence information to answer CI collection requirements. (DoDI S-5140.17, CI Collection, 12 Jan 2009) Also see *Military Counterintelligence Collection*.

-- Also, the systematic acquisition of information to answer CI collection requirements. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

CI Collection feeds analysis... analysis in turn informs decision makers, drives collections, shapes operations, and enables mission execution

CI collection activities are designed to collect specific information or develop leads concerning adversary intelligence collection requirements, capabilities, efforts, operations, structure, personalities, and methods of operations targeting US interests. CI collection can result from ongoing CI investigations or operations or serve to initiate CI investigations and/or operations.

Types of CI collection within DoD include: Military Counterintelligence Collection (MCC); CI debriefing of enemy prisoners of war, displaced persons, and refugees; CI debriefings & interviews; liaison; open source & media exploitation; and CI collection in the cyberspace domain.

See DoDI S-5240.17, *CI Collection (U)*, 12 Jan 2009 for DoD policy and additional information.

Counterintelligence Collection in Cyberspace. The use of cyber means as the primary tradecraft methodology to engage in targeting and collecting cyber based FIE [Foreign Intelligence Entity] activities. CI Collection in cyberspace may include the use of authorized non-attributable Internet connections, development and use of national cyber personas, use of authorized obfuscation techniques, as well as appropriate digital tradecraft and cover. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010)

Counterintelligence Collection Operations. Intelligence collection operations that use human sources and CI resources to answer validated CI requirements. CI collection operations are deliberate, planned activities primarily using human sources to satisfy one or more validated CI information requirements. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Counterintelligence Controlled Source Operation (CI CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008.

Counterintelligence Coordinating Authority (CICA). A designated CI representative in country, the CICA coordinates, deconflicts, and/or synchronizes all joint CI issues in the country with the Service CI elements assigned to or operating within that country, and with the US embassy or consulate. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *Command Counterintelligence Coordinating Authority* (CCICA).

Counterintelligence Cyber Investigation. An investigation using techniques that identify and interdict the misuse of DoD information systems by a trusted insider or an external intruder. These investigations may involve computer intrusions, exceeding authorized network access, denial of service attacks, or the introduction of a virus or a malicious code. (DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 27 Aug 2007)

Counterintelligence Effects-Based Operations (CI EBO). As applied to counterintelligence, effects-based operations is a process for obtaining a desired strategic outcome of effect on adversary intelligence activities through the synergistic, multiplicative, and cumulative application of the full range of CI capabilities at the tactical, operational and strategic levels, to include leveraging non-CI capabilities. Successful CI effects-based operations rest on an explicit linking of CI actions to desired strategic outcomes. CI effects-based operations proactively shape the battlespace in our war against adversary intelligence activities and terrorist networks through the robust execution of *full-spectrum* CI capabilities across the entire spectrum of conflict in an orchestrated and synchronized manner to achieve national, departmental, and combatant commander objectives.

Counterintelligence Enhancement Act of 2002. The act facilitates enhancement of US counterintelligence activities by: (1) enabling the counterintelligence community of the US Government to fulfill better its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the United States; (2) ensuring that the counterintelligence community of the US Government acts in an efficient and effective manner; and (3) providing for the integration of all the US CI activities. The act also established the National Counterintelligence Executive (NCIX), the National CI Policy Board and the Office of the National CI Executive (ONCIX) which replaced the National Counterintelligence Center (NACIC). (§§ 901-904 PL 107-306) Link to the act available at <<http://www.ncix.gov/publications/law/index.html>>

Counterintelligence Flags. Indicators that should alert a source handler to suspicious action that may bring the source's bona fides into question. DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009.

Counterintelligence Force Protection Detachment. See Force Protection Detachment (FPD).

Counterintelligence Functions. The five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (JP 1-02) Also see *CI Activities*.

CI functions are interrelated, mutually supporting, and can be derived from one another.

Functions vs. Missions: "Functions differ from CI missions in that missions focus on end results to be accomplished, rather than on the means for accomplishment. "

-- Mission Area Analysis of DoD Counterintelligence, Institute for Defense Analyses, May 1999, p.7

***Functions are useful terms of reference to describe "what is done"
Missions focus on the "objectives" for the CI efforts***

Counterintelligence Functional Services. CI activities that support other intelligence or DoD operations by providing specialized defensive CI services to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against US national security. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007)

-- Also, CI activities that support other intelligence or DoD operational activities, providing specialized defensive CI services to identify and counter terrorism, espionage, sabotage and related activities of foreign intelligence services. (DoDI 5240.16, DoD CI Functional Services, 21 May 2005)

-- Also, CI activities countering foreign intelligence service and terrorist threats to personnel, facilities, operations, research, critical technology, and critical infrastructure. These may include CI staff support to operational planning, military exercises, treaty-mandated inspections; Red Team activities; CI awareness briefing and/or debriefing programs; and physical and electronic surveillances and/or counter-surveillances. (DoDI 5240.10, CI Support to COCOMs and Defense Agencies, 14 May 2004)

-- Also, CI activities that support other intelligence or DoD operational activities, providing specialized defensive CI services to identify and counter terrorism, espionage, sabotage, and related activities of Foreign Intelligence Entities. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

For more in-depth information regarding CI functional services see Department of Defense, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services*, 19 Feb 2009. This handbook further defines CI functional services as: those activities that are not unique to other CI functions and that support other CI functions and missions; specialized services, which are not inherently CI but support the CI mission and functions.

Within DoD, CI functional services consist of basic CI activities (including espionage detection and CI support to military operations) and specialized services (e.g., polygraph/credibility assessments, TSCM, behavioral science support, cyber services).

Counterintelligence Functional Support Plan (CI FSP). Director Defense CI and HUMINT Center is responsible for preparation of CI FSPs as part of the Intelligence Planning process (CJCSM 3314.01). Format for CI FSPS is provided at enclosure E to CJCSM 3314.01, Intelligence Planning, 28 Feb 2008.

Counterintelligence Inquiry. An examination of the facts surrounding an incident of potential CI interest, to determine if a CI investigation is necessary. (DoDD 5240.02, CI, 20 Dec 2007 with Change 1, 30 Dec 2010)

For information regarding CI inquiries within DoD see: 1) DoDI O-5240.21, CI Inquires, 14 May 2009, which provides DoD policy and outlines the procedures for initiating and conducting CI Inquires; and 2) DoD, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services (U)*, 19 Feb 2009.

According to the DoD handbook on CI functional services, “[w]ithin DoD a CI inquiry does not require “investigative authority” as it is not a CI investigation.” A **CI inquiry** is designed to gather information, identify and/or verify the credibility of potential sources and subjects(s) of CI interest, and to recommend appropriate action if the inquiry does not resolve the matter. The goal is to establish or refute a **reasonable belief** that a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying, or committing espionage, sabotage, or other national security crimes (e.g., treason), or international terrorist activities. Establishment of *reasonable belief* provides the basis for opening a CI investigation. Once a *reasonable belief* is established the matter must be refer to the appropriate Military Department CI organization and/or the FBI [see Section 811 referral]. Refer to the definition of *reasonable belief*.

The DoD handbook stresses that “[w]ithin DoD, only Military Department CI organizations have CI investigative authority and may, accordingly, use the intrusive techniques provided for in Procedures 5 through 13 of DoD 5240.1-R.... It is absolutely vital that CI personnel obtain guidance from their own organization’s legal counsel as to what specific investigative techniques and activities are allowable in their organization and approval from their organization’s leadership to employ those techniques in the course of CI activity.”

A CI Inquiry is not a CI investigation, but it can provide the basis for a CI investigation.

Counterintelligence Insider Threat. A known or suspected person who uses their authorized access to DoD facilities, systems, equipment, or infrastructure to cause damage, disrupt operations, or commit espionage on behalf of a FIE [Foreign Intelligence Entity]. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010) Also see *Insider Threat*.

Counterintelligence Investigation. An official, systematic search for facts to determine whether a person(s) is engaged in activities which may be injurious to U.S. national security or advantageous to a foreign power. (JP 1-02) Also see *counterintelligence inquiry, investigation*.

The agencies responsible for the investigation and ultimate referral for prosecution of violations of US espionage law (primarily Sections 792-798, Chap 37 of Title 18) are the FBI and the CI components of the military services that participate in the DoD Foreign CI Program (FCIP).

Within DoD, all significant CI activities must be reported promptly to the Director, Defense CI & HUMINT Center IAW DoDD O-5240.02 (see encl 4 for significant CI reporting criteria).

The Secretaries of the Military Departments exercise authority, direction, and control over CI investigations and attendant matters (para 5.10.3, DoDD O-5240.02).

-- Also, formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts. (DoDI 5240.04, CI Investigations, 4 February 2009)

-- Also, inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007)

-- Also, includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for the purposes of conducting espionage and other intelligence activities, sabotage, assassinations, treason, international terrorist activities, and actions to neutralize such acts. (DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 Dec 1982)

-- Also, formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize or exploit such acts. (JP 2.01.2, 11 Mar 2011)

-- Also, the systematic collection of information regarding a person or group which is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, or international terrorist activities conducted for, or on behalf of, foreign powers, organizations, or persons. (CI Community Lexicon)

The first priority for all CI investigative situations is to assess for possible exploitation.

-- Army FM 2-22.2, *Counterintelligence*, October 2009

CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or Uniform Code of Military Justice (UCMJ). Investigative actions must preserve the potential for legal action and when appropriate exploit threatening intelligence collection directed against DoD. In simple terms, CI investigations seek to *identify spies and put them out of business*. CI investigations are about discovering the facts and conveying them to decision makers, while maintaining a full range of options, including apprehension, prosecution, expulsion, as well as exploitation.

Credentialed CI Special Agents use specialized investigative techniques and methodologies to gather intelligence (facts/evidence) about known and/or suspected acts that may constitute National Security crimes, e.g., espionage, treason, spying, etc. All investigative activities are conducted within guidelines established in applicable departmental policy/directives, Attorney General Guidelines, and U.S. federal statutes. DoD CI investigations are conducted in a manner to "preserve" the potential for prosecution of all culpable parties identified.

CI investigative results also contribute to the identification and elimination of security vulnerabilities; identification of current foreign intelligence tradecraft, agent handlers/operatives and their support networks; assessment of damage to DoD and National Security; and improvement of the overall DoD security posture, as well as assisting decision makers in risk management decisions.

DoD CI investigations are conducted in accordance with DoDI 5240.04, *CI Investigations*. The DoD agencies responsible for CI investigations and the ultimate referral for prosecution of violations of US espionage law (primarily §§ 792-798, Chap 37, Title 18 USC) are the CI components of the military departments, i.e., NCIS, AFOSI, and Army CI.

See Stuart A. Herrington, *Traitors among Us: Inside the Spy Catcher's World* (2000), for an excellent overview of two Army CI investigations concerning Clyde Conrad and James Hall.

Spy catching... the surgery of counterintelligence

***“The thankless and exhausting task of tracking down
a traitor always seems much easier in retrospect than in prospect.
The clues always seem so obvious—but only after the hunt has caught its prey.”***

— Markus Wolf, Former Director HVA, East German Intelligence Service (1958-1987)

Counterintelligence Mission. Exploit and defeat adversarial intelligence activities directed against US interests; protect the integrity of the US intelligence system; provide incisive, actionable intelligence to decision makers at all levels; protect vital national assets from adversarial intelligence activities; and neutralize and exploit adversarial intelligence activities targeting the armed forces. (ONCIX website: <<http://www.ncix.gov/about/mission.html>>)

Counterintelligence Missions (aka CI Mission Areas). DoD CI responsibilities to support force protection, DoD research and technology protection, infrastructure protection, and information & capabilities protection [counterespionage]. (DoDD 5240.16, DoD CI Functional Services, 21 May 2005)

Counterintelligence Mission Manager. The National Counterintelligence Executive (NCIX) serves as the Mission Manager for Counterintelligence IAW Intelligence Community Directive (ICD) 900. Also see *mission managers*.

Counterintelligence Mission Tasking Authority (CI MTA). The authority to task a Military Service CI organizations' headquarters or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's CI charter. (DoDD O-5240.02, CI, 20 Dec 2007)

Director, Defense CI & HUMINT Center, exercises CI MTA to ensure the effective integration and synchronization of the DoD CI community (para 5.2.3, DoDD O-5240.02).

Counterintelligence Operational Concept/Proposal. The document used to propose an offensive counterintelligence operation (OFCO) which serves as the basis for the planning, review, and approval process. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Operational Lead (CIOL). Counterintelligence referral from CIA operations; generally produced and disseminated by the Counterespionage Group (CEG), Counterintelligence Center (CIC) at CIA headquarters. (902d MI Group Investigative Handbook, Feb 2007)

Counterintelligence Operational Tasking Authority (CIOTA). The levying of CI requirements specific to joint military activities and operations. Counterintelligence operational tasking authority is exercised through supporting components. (JP 1-02 and DoDI 5240.10, 14 May 2004)

Counterintelligence Operations. Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the United States. (JP 1-02) Also see *Offensive Counterintelligence Operation (OFCO)*; *recruitment-in-place (RIP)*; *penetration*; *penetration operation*.

-- Also, operations/efforts intended to negate, confuse, deceive, subvert, monitor, or control the clandestine collection operations of foreign governments or agencies. (CI Community Lexicon)

-- Also, activities taken to hinder the multidisciplinary activities of foreign intelligence and security services, and to cause FIS to doubt the validity of its own analysis. (AR 381-20, Army CI, 15 Nov 1993)

Counterintelligence Operations—one of five CI functions—are conducted to:

- manipulate, disrupt, neutralize and or destroy the effectiveness of foreign intelligence activities;
- recruit or induce defection of foreign intelligence officers and personnel;
- collect threat information on foreign intelligence operations, modus operandi, intelligence requirements, targeting, objectives, personalities, communications, capabilities, limitations, and vulnerabilities;
- provide information and operations databases to support decision makers;
- provide CI support to clandestine human intelligence operations;
- identify past, ongoing or planned espionage;
- support force protection, operations other than war and peacekeeping;
- acquire foreign intelligence espionage equipment for analysis and countermeasures development;
- develop operational data, threat data and espionage leads for future CI operations, investigations, and projects and develop the potential of these leads to enhance DoD security overall; and
- support specific [Service], Chairman Joint Chiefs of Staff, DoD and national plans.

-- JP 1-02 and SEVNAVINST 3850.2C, *Department of Navy Counterintelligence*, 20 Jul 2005

Counterintelligence Production. The process of analyzing all-source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the DoD, and the US Intelligence Community and developing it into a final product that is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the creation of finished intelligence products incorporating CI analysis in to known or anticipated CI concerns. (DoDD 5240.02, CI, 20 Dec 2007)

-- Also, the creation of finished intelligence products incorporating CI analysis in response to known or anticipated customer CI concerns. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the conversion of analyzed CI information into intelligence products in support of known or anticipated user requirements. (DIA Instruction 5240.002, 15 Jun 2005)

Counterintelligence Recruitment Lead (CIRL). An individual being assessed for possible use in a counterintelligence operation, investigation, or project as a controlled source. (AR 381-47, OFCO, 17 Mar 2006)

Counterintelligence Scope Polygraph (CI Scope Poly). A polygraph examination, consisting of questions regarding espionage, sabotage, terrorism, unauthorized disclosure, secret contacts with foreign entities, and damage of U.S. Government information systems.

Counterintelligence Special Agent. Within DoD, US Government personnel (military and civilian employees) who have successfully completed an approved CI Special Agent Course of Instruction and who are authorized to be issued Badge and Credential (B&Cs).

Within the US Army: military personnel holding the MOS 35L, 351L, and 35E as a primary or additional specialty, and selective civilian employees in the GS-0132 career field; see AR 381-20 (Army CI Program).

Counterintelligence Staff Officer (CISO). An experienced senior CI officer (military grade O-5 or above, or civilian grade GS/GM/GG-14 or above) assigned or attached to a Combatant Command or JTF J2 or Special Staff as the senior authoritative command representative for CI. The CISO develops and implements the command's CI strategy and plans, serves as the focal point for all CI issues impacting the command, identifies and tasks command CI requirements, and coordinates CI support to the command. (DoDI 5240.10, 14 May 2004)

Note: in the revision to DoDI 5240.10, this term will be replaced by "Command CI Coordinating Authority" or CCICA; it will also be updated in JP 1-02.

Counterintelligence Support. Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons. (JP 1-02 & JP 2-01.2) Also see *counterintelligence*.

Counterintelligence Support Plan (CISP). A formal plan that outlines and describes the CI support to be provided to research and development facilities, RDA [Research, Development and Acquisition] programs with CPI [critical program information], and CPI resident at cleared Defense contractor facilities. CISPs are coordinated with and approved by the RDA Director, Program Executive Office, or Program Manager, as appropriate, and are an appendix to the PPP. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008)

Counterintelligence Support to HUMINT. [CI activities which] prevents the detection, neutralization or manipulation of strategic U.S. DoD HUMINT collection activities by foreign intelligence or security services. (DIA Instruction 5240.002, *DIA Counterintelligence Activities*, 15 Jun 2005)

For additional information see Appendix D, *Counterintelligence Support to Human Intelligence (U)*, JP 2-01.2, *CI & HUMINT in Joint Operations (U)*, 11 Mar 2011

Counterintelligence Technical Services (CITS). Encompasses Technical Surveillance Countermeasures (TSCM) and Technical Support to Counterintelligence (TSCI). TSCM is used to detect the presence of technical surveillance devices and hazards and to identify technical security vulnerabilities that put the surveyed facility at risk. TSCI provides technical surveillance and countersurveillance in support of CI functions. Also see *Technical Surveillance Countermeasures*.

Counterintelligence Training. Institutional training in knowledge, skills, abilities, and core competencies unique to CI missions and functions. (DoDI 3305.11, DoD CI Training, 19 Mar 2007)

-- Also, instructions and applies exercises offered through various media and methods for the acquisition, retention, and enhancement of skills, knowledge, and abilities required to counter or neutralize: intelligence collection efforts; other intelligence activities; sabotage; and terrorist activities and assassination efforts on behalf of foreign powers. (DoDI 3305.12, Intelligence and Counterintelligence Training of Non-US Persons, 25 Oct 2007)

Counterproliferation (CP). Those actions (e.g., detect and monitor, prepare to conduct counter-proliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies. (JP 1-02 & JP 3-40)

-- Also, the activity by United States government intended to prevent the proliferation of nuclear, chemical and biological capabilities to other nations. (HPSCI Report, 27 Jul 2006)

Countermeasure. Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

Countersurveillance. See *counter surveillance*.

Counterterrorism (CT). Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. (JP 1-02 and JP 3-26) Also see *terrorism; combating terrorism*.

Country Clearance. Clearance for official U.S. Government representative travel to a foreign country granted through the cognizant U.S. Embassy or U.S. Mission. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Country Team. The senior, in-country, US coordinating and supervising body, headed by the chief of the US diplomatic mission, and composed of the senior member of each represented US department or agency, as desired by the chief of the US diplomatic mission. (JP 1-02 and JP 3-07.4)

Courier. Person who carries an item or information from one person or place to another. The courier may or may not be aware of the nature of the item or information being transported. (AFOSI Manual 71-142, 9 Jun 2000)

Cover. In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from enemy intelligence effort and leakage of information. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *cover for action; cover for status*.

-- Also, actions to conceal actual friendly intentions, capabilities, operations, and other activities by providing a plausible yet erroneous explanation of the observable. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a protective guise used by a person, organization, or installation to conceal true affiliation with clandestine or other sensitive activities. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010)

-- Also, a verifiable and documented protective guise used by a person, organization, or installation to conceal true identity or affiliation. (HDI Lexicon, April 2008)

-- Also, a protective guise used by an individual, organization, or installation to prevent identification with intelligence activities. To hide, conceal, obscure, or otherwise protect the exact identity of an individual, unit, or activity. Supported with or without documentation and backstopping depending on the sensitivity and scope of the operation. *Cover* can be anything that masks the true nature of an activity. (CI Community Lexicon)

DoD cover may be used to protect the Department of Defense, its intelligence sources and methods, and its clandestine tactics, techniques, and procedures from exposure to the enemy and overt association with sensitive activities. The fact that DoD uses cover to protect its activities is unclassified. -- See DoDD S-5105.61, *DoD Cover and Cover Support Activities (U)*, 6 May 2010)

Cover shields secret activities from the opposition

Good cover ...reaches into the mind of the opponent, thinks as he would think, and then creates a combination of fact and fancy, of actual arrangements and contrived impressions, which the opposing mind is prepared to believe.... Cover takes an infinite variety of forms.

*The best cover is that which contains the least notional and the maximum possible legitimate material.... **Perfect cover is an ideal, rarely achieved in practice***

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Cover for Action. A logical reason for doing the specific action involved. (CI Community Lexicon)

-- Also, a verifiable and documented protective guise used to disguise the true intent of an individual, organization, or activity and to provide a credible explanation as to participation in a particular activity. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *cover for status*.

Cover for Action. This cover, combined with the use of appropriate clandestine tradecraft techniques (e.g. alias, disguise, darkness, surveillance detection routes to and from meetings, etc.) is what provides cover and security for clandestine meetings.

-- F.W. Rustmann, Jr. (Fall 2003), <http://ctcintl.com/Debunk.htm>, accessed 7 Mar 2011

Cover for Status. A logical and backstopped reason for being in an area or processing a particular item at a particular time. (CI Community Lexicon) Also see *cover for action*.

-- Also, a verifiable and documented protective guise used to legitimize an individual's, organization's, or activity's extended presence in a particular area. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Cover for Status. This is the cover that permits [a case officer] to live and work in a particular country. If the case officer is under official cover, this means he must blend into the environment of an embassy or other official US installation abroad.

-- F.W. Rustmann, Jr. (Fall 2003), <http://ctcintl.com/Debunk.htm>, accessed 7 Mar 2011

Cover Legend. A contrived scenario, designed to explain an organizational or personal background and past or present activities, in terms intended to protect and/or conceal involvement in a clandestine or otherwise sensitive activity. It incorporates as much truth as possible. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Cover Stop. A stop made while under surveillance that provides an ostensibly innocent reason for a trip. (CI Centre Glossary)

Cover Story. Coherent and plausible account of background, residence, employment, activities, access, etc., furnished to an individual to substantiate whatever claims are necessary to successfully carry out an operation. The difference between a cover story and a legend is that a legend is furnished to an illegal or agent by FIS. (AFOSI Manual 71-142, 9 Jun 2000)

The cover story is most frequently used to explain the visible evidences of a clandestine operation or to provide an explanation when an operations encounters difficulties.

...cover stories in general: they should not be too precise or too detailed, and they should not be forthcoming too quickly or all at once. ...To be too precise in a cover story qualitatively increases the chances of repudiation of the story; to be too detailed increases those chances quantitatively.

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Cover Support Activities. All measures taken to develop, coordinate, approve, activate, operate, and terminate cover. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010)

Covert. A method of conducting operations that hides the true intent, affiliation or relationship of its participants. Differs from clandestine in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary)

Covert Action. An activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. Covert action **does not include** activities the primary purpose of which is to acquire intelligence, **traditional counterintelligence activities** [*emphasis added*], traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities. (Section 503e, National Security Act of 1947 [50 USC §413b]) Also see *special activities; covert operation; finding*.

**...the overt foreign activities of the US Government
must be supplemented by covert operations**

NSC Directive 10/2 (dated 18 Jun 1948)
as cited in Warner, *CIA Under Truman* (1994)

"Typically, covert actions are carried out by the CIA with such assistance as may be necessary by other elements of the intelligence Community as directed by the President. U.S. law requires that all covert actions be approved prior to their execution by the President in a written 'finding' and that notification be provided to the two intelligence committees in Congress. Covert actions may involve political, economic, propaganda, or paramilitary activities." -- WMD Report, 31 Mar 2005

"Covert action is often called the "dirty tricks" side of spying. It consists of sabotage, subversion, paramilitary operations, political action, psychological operations, and black propaganda. It is not always pretty. Covert action has historically been a relatively small part of the CIA's overall activity, but it is certainly the aspect of U.S. spying that has been the most controversial."

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

Covert actions are designed to avoid revealing the role of the United States in their planning or execution. EO 12333 (as amended 30 Jul 2008) directs that no agency except CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective. No covert action may be conducted which is intended to influence US political processes, public opinion, policies, or media.

Covert action by DoD must be directed by the President, subsequently approved by the Secretary of Defense, and executed in accordance with applicable law.

"The three basic types of covert action are perception management (historically known as propaganda), political action (influencing the actions of a foreign leader or government), and paramilitary operations (support to insurgents)."

-- Duane R. Clarridge, *A Spy For All Season: My Life in the CIA* (1997), p. 410

**Covert action can serve as a more subtle and surgical tool
than forms of acknowledge employment of U.S. power and influence.**

-- WMD Report, 31 Mar 2005 (p. 33)

-- Also, clandestine activity designed to influence **foreign** [*emphasis added*] governments, events, organizations or persons in support of U.S. foreign policy conducted in such a way that involvement of the U.S. Government is not apparent. In its attempts directly to influence events it is distinguishable from clandestine intelligence gathering—often referred to as espionage. (Senate Report # 94-755, aka Church Committee Report, 26 April 1976, p. 131)

Covert Communication (COVCOM). Clandestine, hidden communication that protects both the information being shared and the relationship between the sending and receiving parties. (National HUMINT Glossary)

-- Also, any technique or device used to relay data clandestinely from case officer to agent or agent to case officer. (Spycraft)

Covert Operation. An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation. (JP 1-02 and JP 3-60) Also see *covert*; *covert action*, *clandestine operation*.

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See *clandestine operation*.

Avowal of a covert operation, however implicit, is a hostile act, and it is wise never to indulge in hostile acts unless one is able and prepared to back them up.

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Credible Information. Information disclosed or obtained by an investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained investigator to presume that the fact or facts in question are true. (DoDI 5505.7, 7 Jan 2003)

Credibility Assessment. The multi-disciplinary field of existing as well as potential techniques and procedures to assess truthfulness that relies on physiological reactions and behavioral measures to test the agreement between an individual's memories and statements. (DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007)

Credentials. Official documents which identify the bearer as a representative of a specific agency or department of the U.S. Government.

Criminal Intelligence (CRIMINT). Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

Criminal Investigation. The process of searching, collecting, preparing, identifying, and presenting evidence to prove the truth or falsity of an issue of law. (US Army, FM 3-19.13, Law Enforcement Investigations, Jan 2005)

-- Also, investigation into alleged or apparent violations of law undertaken for purposes which include the collection of evidence in support of potential criminal prosecution. (DoDI 5505.7, 7 Jan 2003)

Criminal investigation is both an art and a science. In science, the absolute truth is often achieved. Experience has shown that in criminal investigations a less decisive hypothesis may sometimes be all that is possible to achieve.

Objectives of Criminal investigations: 1) *Determine if a crime was committed*; 2) *Collect information and evidence legally to identify who was responsible*; 3) *Apprehend the person responsible*; 4) *Recover stolen property*; 5) *Present the best possible case to the prosecutor*; and 6) *Provide clear, concise testimony*. -- US Army, FM 3-19.13, *Law Enforcement Investigations*, Jan 2005

Criminal Investigation Task Force (CITF). The DoD CITF is a strategic-level organization with a mission to develop and fuse police intelligence with MI [military intelligence] for the purpose of building criminal cases against terrorist criminals that have attacked U.S. interests. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

The CITF conducts complicated criminal investigations targeting terrorists and complex criminal organizations. These cases typically cross international borders and involve criminals captured as a result of military operations, requiring coordination with international police and intelligence agencies. The CITF combines USACIDC special agents (and criminal investigators from other Services), police and intelligence analysts, and attorneys into teams. These teams synchronize and fuse information and intelligence from all available sources to conduct criminal investigations that enable criminal prosecution in U.S. or host nation legal systems.

-- ATTP 3-39.20 (FM 3-19.50), *Police Intelligence Operations*, July 2010

Crisis. An incident or situation involving a threat to the United States, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of US military forces and resources is contemplated in order to achieve national objectives. (JP 1-02 & JP 3-0)

Crisis Action Planning (CAP). One of the two types of joint operation planning. The Joint Operation Planning and Execution System process involving the time-sensitive development of joint operation plans and operation orders for the deployment, employment, and sustainment of assigned and allocated forces and resources in response to an imminent crisis. Crisis action planning is based on the actual circumstances that exist at the time planning occurs. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *contingency planning*.

Critical Asset. A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 1-02 & JP 3-07.2)

-- Also, any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and its timely restoration. Critical assets may be DoD assets or other Government or private assets, (e.g., industrial or infrastructure critical assets), domestic or foreign, the disruption or loss of which would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations. Critical assets include traditional "physical" facilities and equipment, non-physical assets (such as software systems), or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks). (DoDD 5200.12, 18 Aug 2003)

-- Also, *Defense Critical Asset*: an asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

CRITIC. Critical information messages sent over the CRITICOMM System that must be delivered to the President within 10 minutes upon recognition. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02 & JP 2-0)

-- Also, decisions, intentions, or actions of foreign governments, organizations, or individuals that could imminently and materially jeopardize vital U.S. policy, economic, informational, or military interests to such an extent that the immediate attention of the President and the National Security Council may be required. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, national public health or safety, or may combination if those matters. (Critical Infrastructures Protection Act of 2002 and USA Patriot Act §1016)

-- Also, [within DoD] infrastructure deemed essential to DoD operations or the functioning of a critical asset.

Nation's critical infrastructure and key resources, as set forth in the 2006 National Infrastructure Protection Plan (NIPP) includes the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

-- Cited in the *National Strategy for Homeland Security*

Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc. (JP 1-02 & JP 3-28) Also see *Defense Critical Infrastructure*.

PDD-63 set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber).

Critical Intelligence. Intelligence that is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential or actual enemy. It includes but is not limited to the following: 1) strong indications of the imminent outbreak of hostilities of any type (warning of attack); 2) aggression of any nature against a friendly country; 3) indications or use of nuclear, biological, and chemical weapons; or 4) significant events within potential enemy countries that may lead to modification of nuclear strike plans. (JP 1-02 & JP 2-0)

Critical Program Information (CPI). Elements or components of an RDA [research, development & acquisition] program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. CPI includes information about applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness; and technology that would reduce the US technological advantage if it came under foreign control. (DoDD 5200.39, CPI Protection within DoD, 16 Jul 2008)

Critical Technology. Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service which makes or could make a significant contribution to the military potential of any country, including the United States. This includes, but is not limited to, design and manufacturing know-how, technical data, keystone equipment, and inspection and test equipment. (DoDI 2040.02, International Transfers of Technology, Articles, and Services 10 Jul 2008)

Cross-cuing. The use of one intelligence source to initiate the collection against a particular target with another intelligence collector. Also see *cueing*.

CI and HUMINT provide unique opportunities for enabling and cross-cuing other intelligence disciplines or capabilities. CI and HUMINT sources can enable other intelligence collection disciplines or provide time sensitive "tip off" information to cue other collection capabilities.

-- JP 2-01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 (p. V-2)

Cryptanalysis. The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption. (DoD 5200.1-R, Information Security Program, Jan 1997)

-- Also, the steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption. (JP 1-02)

Cryptography. The art and science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (DoDD 5100.20, NSA, 26 Jan 2010)

-- Also, the branch of cryptology that treats the principles, means, and methods of designing and using cryptosystems. (DoD 5200.1-R, Information Security Program, Jan 1997)

Cryptology. The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (JP 1-02)

-- Also, the branch of knowledge that treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC). (DoDD 5100.20, NSA, 26 Jan 2010)

Cueing. The use of one or more sensor systems to provide data that directs collection by other systems. (term previously defined in FM 2-0, Intelligence, May 2004) Also see *cross-cueing*.

Cultural Intelligence. Knowledge resulting from all-source analysis of cultural factors, which assists in anticipating the actions of people or groups of people. (National Intelligence: A Consumer's Guide - 2009).

Current Intelligence. One of two categories of descriptive intelligence that is concerned with describing the existing situation. (JP 1-02 & JP 2-0)

Custodial Interview. Interview conducted of a subject following formal arrest or detention. Subjects are made fully aware of their deprivation of freedom or their "in custody" status. (Army FM 2.22-2, CI, Oct 2009).

Cutout. An intermediary or device used to obviate direct contact between members of a clandestine organization. (JP 1-02)

-- Also, an individual whose services are used to prevent contact and recognition between specific members of an intelligence service with the purpose of providing compartmentation and security. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, a mechanism or person that acts as a compartment between the members of an operation but which allows them to pass material or messages securely. (CI Centre Glossary)

-- Also, an intermediary used to obviate direct linkage between either the origin or destination of an intelligence operation or action. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Cyber. 1) Any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and 2) any matter relating to, or involving the use of, computers or computer networks. (Cybersecurity Act of 2009)

Cyber Counterintelligence. Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. (JP 1-02)

-- Also, counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon. (The United States Government-Wide Cyber Counterintelligence Plan - 2008 (U))

Cyber Espionage. The act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on internet, networks or individual computers...
(http://en.wikipedia.org/wiki/Cyber_espionage, accessed 5 Jan 2010)

Cyber Incident. Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority. (NSPD-54 / HSPD-23)

Cyber Intrusion Damage Assessment. A managed, coordinated, and standardized process conducted to determine the impact on future defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from an intrusion into a DIB unclassified computer system or network. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center [DC3], 1 Mar 2010)

Cyber Persona. An identity used in cyberspace to obtain information or influence others, while dissociating the actor's true identity or affiliation. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec10)

Cyber Power. The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. (Daniel T. Kuehl, "from Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, Washington, D.C.: National Defense University, 2009)

Cyber power can be used to produce preferred outcomes within cyberspace or it can be use cyber instruments to produce preferred outcomes in other domains outside cyberspace. See "Cyber Power" by Joseph S. Nye, Harvard Kennedy School, May 2010; available online at: belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Cyber Security (or Cybersecurity). Measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010) Also see *computer security*; *information security (INFOSEC)*.

-- Also, includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Cyberattacks are possible only because systems have flaws.

As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk.

-- Rand Report, "Cyberdeterrence and Cyberwar," by Martin C. Libicki (2009)

U.S. military networks "are constantly under attack. They are probed thousands of times a day. They are scanned millions of times a day. And the frequency and sophistication of attacks are increasing exponentially."

"The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime, from hacker activists to teenage hackers, from industrial spies to foreign intelligence services."

-- William Lynn, Deputy Secretary of Defense

(as quoted in "In Cyber War, Most of U.S. Must Defend Itself," by William Matthews, *DefenseNews*, 1 Feb 2010, p. 29)

Cyber Threat Investigation. Any actions taken within the United States, consistent with applicable law and presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals. (NSPD-54 / HSPD-23)

-- Also, actions taken, consistent with applicable law and Presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more FIEs [Foreign Intelligence Entities], that has attempted to penetrate or has, in fact, penetrated a DoD, IC, or DIB [defense industrial base] information system. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010)

Attribution is a major problem in the cyber realm

"The damage caused by malicious activity in cyberspace is enormous and unrelenting. Every year, cyber attacks inflict vast damage on our Nation's consumers, businesses, and government agencies. This constant cyber assault has resulted in the theft of millions of Americans' identities; exfiltration of billions of dollars of intellectual property; loss of countless American jobs; vulnerability of critical infrastructure to sabotage; and intrusions into sensitive government networks."

-- Senator Sheldon Whitehouse, 14 April 2011

Cyber-Terrorism. A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda. (FBI)

Cyberspace. A global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02 & CJCS CM-0363-08) Also see *cyberspace domain*.

-- Also, the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded possessors and controllers in critical industries. (NSPD-54 / HSPD-23, 8 Jan 2008)

-- Also, the range of information and resources available through computer networks -- especially the Internet. (ODNI Cyberspace Initiative)

In cyberspace, the war has begun...

Cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, inexpensively, and anonymously. This environment presents enormous challenges and unprecedented opportunities...

Cyberspace is a domain that requires man-made technology to enter and exploit. Effects of cyberspace operations can occur simultaneously in many places and they can be precise, broad, enduring and transitory.

Challenges -- Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. Cyberspace crosses geographic and jurisdictional boundaries. The expanding use of cyberspace places United States' interests at greater risk from cyber threats and vulnerabilities. Cyber actors can operate globally, within our own borders, and within the borders of our allies and adversaries. The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities.

Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. On the flip side -- cyberspace offers DoD unprecedented opportunities to shape and control the battlespace to achieve national objectives.

Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

-- The Joint Operating Environment 2010, USJFCOM

[I]n cyberspace some malicious actors consider that no boundaries exist between military and civilian targets.

-- Congressional Research Service, Report RL32114 (29 Jan 2008)

For additional information see *The United States Government-Wide Cyber Counterintelligence Plan - 2008* (classified) and *The DoD Strategy for Counterintelligence in Cyberspace* (28 Aug 2009)

Cyberspace Domain. A domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (DoDI S-5240.17, CI Collection, 12 Jan 2009)

Cyberspace Operations. The employment of cyber capabilities where the primary purpose is to achieve military objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (JP 1-02; JP 3-0; and CM-0856-09)

Damage Assessment. [In intelligence usage,] a determination of the effect of a compromise of classified information on national security. (JP 1-02)

-- Also, the analysis of the impact on national security of a disclosure of classified information to an unauthorized person. (IC Standard 700-1, 4 Apr 2008)

-- Also, systematic analysis that determines the impact of a compromise of classified information on the national security of the United States. (CI Community Lexicon)

-- Also, systematic, comprehensive examination of an intentional and/or inadvertent compromise of classified or sensitive information. (ONCIX, Damage Assessment Guide (U), 21 Mar 2008)

See ONCIX *Damage Assessment Guide* - October 2009 (U) for a standardized framework and outline of the processes and procedures involved in national-level damage assessment activity.

Damage to the National Security. Harm to the national defense or foreign relations of the United States from unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information. (EO 13526, National Security Information, 29 Dec 2009)

Danger Signals. Prearranged signals or marks on walls, posts, etc., [used] as a communication system between agents or [case] officers to indicate that the opposition or active enemy is nearby, has been tipped off, or has the area under surveillance. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Dangle. A person controlled by one intelligence service who is made to appear as a lucrative and exploitable target to an opposing intelligence service. (HDI Lexicon, April 2008) Also see *penetration*.

-- Also, an asset placed within the professional or personal view of a FIS [Foreign Intelligence Service] officer or agent with the intention of observing the actions of and possibly being recruited by the FIS. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, counterespionage terminology for the process of presenting an individual to a foreign intelligence service in a manner as to encourage his recruitment as an agent; as "to dangle" or a dangle operation. (CIA in D&D Lexicon, 1 May 2002)

If you wait for the enemy to come to you, you may not know when he does.

...If the fish do not swim into your net, you have to give them a lure, a provocation, something that looks like a juicy worm but that has a hook in it.

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Database. Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 2-0, Joint Intelligence)

Data Mining. A program involving pattern-based queries, searches or other analyses of 1 or more electronic databases, where -- (a) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely- (i) the detection of fraud, waste, or abuse in a Government agency or program; or (ii) the security of a Government computer system. (Data Mining Reporting Act, §804(b)(1)(A))

This definition limits covered activities to predictive, *pattern-based* data mining, which is significant because analysis performed within the ODNI and its constituent elements for counterterrorism and similar purposes is often performed using various types of "link analysis" tools.

Unlike "pattern-based" tools, these link analysis tools start with a known or suspected terrorist or other subject of foreign intelligence interest and use various methods to uncover links between that known subject and potential associates or other persons with whom that subject is or has been in contact. The Data Mining Reporting Act does not include such analyses within its definition of "data mining" because such analyses are not "pattern-based."

-- ODNI 2009 Data Mining Report

DCII. See *Defense Central Index of Investigations*.

Dead Drop. A clandestine location for transferring material to or from an agent or asset. (National HUMINT Glossary)

-- Also, a place, unattended by witting individuals, to which communications, materials, or equipment can be left by one individual and from which they can be taken by another individual without either meeting or, ordinarily, seeing one another. Also called a dead letter box, or simply drop. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, a secret location where materials can be left in concealment for another party to retrieve. This eliminates the need for direct contact in hostile situations. (CI Centre Glossary)

-- Also, a clandestine communications technique, the dead drop allows agents to exchange messages and other items without the need for a meeting that might attract the attention of hostile surveillance. The dead drop is usually an innocuous, prearranged site where a package or film canister can be secreted temporarily so it can be recovered by the addressee. Ideally, the location is sufficiently innocent to enable both parties to visit it, at different times, without compromising themselves. The use of dead drops is standard tradecraft for espionage professionals, and is usually associated with a remote signaling arrangement so both sides can indicate to the other when a particular drop is ready for servicing. The objective is to obviate the need for personal contact that in denied areas is high risk. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, a preferred means of covert communications in denied areas, separates the agent and handler [case officer] by time, but carries the risk of leaving the package unattended in an environment that could change without warning. (Spycraft, pg 61)

-- Also, pre-cased hiding places used by intelligence services to conduct [clandestine] exchanges with agents. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

In intelligence usage, dead drops are used as a clandestine cut-out to avoid personal meetings which can draw attention to the connection between an intelligence officer/agent handler and an agent/asset. As a rule, dead drops are not used more than once.

For a detailed description of dead drops and concealment devices, see *Spycraft*, pp. 388-400.

Debriefing. The process of using direct questions to elicit intelligence information from a cooperative detainee to satisfy intelligence requirements. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 9 Oct 2008) Also see *strategic debriefing; educing information; elicitation; intelligence interrogation; interrogation; interview.*

-- Also, the systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

-- Also, systematically covering topics and areas with a voluntary source who consents to a formal interview. (*Educing Information - Interrogation: Science and Art*, Dec 2006)

Debriefing Operations. Operations conducted to debrief cooperating sources may include refugees, émigrés, displaced persons (DPs), local populace, friendly forces, members of U.S. and foreign governmental and non-governmental organizations, as well as U.S. and foreign personnel employed within the academic, business, or scientific communities. The source may or may not be in custody, and their willingness to cooperate need not be immediate or constant. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Decentralized Execution. Delegation of execution authority to subordinate commanders. (JP 1-02)

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. (JP 1-02 and JP 3-13.4) Also see *counterdeception; deception means; denial, military deception.*

-- Also, deliberately manipulating information and perceptions in order to mislead. (Foreign Denial & deception Committee, 30 Mar 2006)

-- Also, an action intended by an actor to influence the perceptions, decisions, and actions of another. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

***O, what a tangled web we weave,
When first we practise to deceive!***
-- Sir Walter Scott, *Marmion* (1808)

Deception is a fundamental ingredient of military art.

"Deception is an instrument of policy.... [It] must be orchestrated to succeed."
-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Analysts should routinely consider that their information base is susceptible to deception.

Richard Heuer (author *Psychology of Intelligence Analysis*) notes that analysts often reject the possibility of deception because they see no evidence of it. He then argues that rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.

-- See *Deception 101 –A Primer on Deception* (2004) by Joseph W. Caddell; available online at: <<http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>>

All warfare is based on deception.

-- Sun Tzu (400-320 B.C.)

Deception Channel. A means by which controlled information can be reliably transmitted to the target. (CIA in D&D Lexicon, 1 May 2002)

Deception Means. Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: 1) physical means -- activities and resources used to convey or deny selected information to a foreign power; 2) technical means -- military material resources and their associated operating techniques used to convey or deny selected information to a foreign power; and 3) administrative means -- resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02)

-- Also, the vehicles or resources for conveying the deception story or deception-related information directly or indirectly to the target. These generally consist of sources accepted by the target as reliable or believable. Deception means have been subdivided into: physical, technical, administrative, and special means. (CIA in D&D Lexicon, 1 May 2002)

Deception Target. The adversary decisionmaker with the authority to make the decision that will achieve the deception objective. (JP 1-02 & JP 3-13.4)

Declared. An individual or action whose intelligence affiliation is disclosed. (HDI Lexicon, April 2008)

-- Also, an officer, asset, agent, or action whose Agency affiliation is formally identified to a foreign intelligence or security service, government or organization, or other USG entity. (National HUMINT Glossary)

Declassification. The authorized change in the status of information from classified information to unclassified information. (EO 13526, National Security Information, 29 Dec 2009)

Deconfliction. The process of sharing information regarding collection between multiple agencies to eliminate potential duplication of effort, multiple unintended use of the same source, or circular reporting. (DoDI S-5240.17, CI Collection, 12 Jan 2009)

Decoy. An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. (JP 1-02).

Deduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion. (Cited in (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; induction; scientific method*.

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Deep Cover. A cover for status designed to withstand close scrutiny by the opposition or through due diligence. (National HUMINT Glossary)

Defection. Conscious abandonment of loyalty, duty, and principle to one's country. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, conscious (mental and/or physical) abandonment of loyalty, allegiance, duty, and principle to one's country. (ICS Glossary)

Defector. A person who has consciously abandoned loyalty to his country and who possess intelligence information of value to another country or countries. (CI Community Lexicon)

-- Also, a person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the US Government. (ICS Glossary)

-- Also, a person of any nationality, usually from a country whose interests are hostile or inimical to the U.S., who has escaped from the control of his or her country, is unwilling to return to that country, and is of special value to the U.S. Government because: he or she is able to add valuable new or confirmatory information to existing U.S. intelligence knowledge; he or she is, or has been, of operational or political value to a U.S. department or agency; or the defection can be psychologically exploited to the advantage of the U.S. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

“Next to penetrations (moles), defectors are your best weapon against alien intelligence services.”

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

An act of treason -- “[D]efector is an individual who has committed treason, a person who first accepted identification with a regime and then betrayed his allegiance to cooperate with a hostile foreign intelligence service.”

-- Wilhelm Marbes, “Psychology of Treason,” in *Studies of Intelligence*, vol. 30, no. 2 (Summer 1986), pp. 1-11. Originally classified “Secret” [declassified].

Defense Attaché. See *Senior Defense Official / Defense Attaché (SDO/DATT)*.

Defense Attaché Office (DAO). An organizational element of the U.S. diplomatic mission through which the Defense Attaché System conducts its mission and to which may be attached or assigned such other military detachments or elements as the Secretary of Defense may direct. (DoDI C-5105.32, Defense Attaché System, 18 Mar 2009) Also see *Senior Defense Official / Defense Attaché (SDO/DATT)*.

Defense Central Index of Investigations (DCII). An automated central index that identifies investigations conducted by Department of Defense investigative agencies. (<http://www.dss.mil/diss/dcii-newacct.html>)

Effective 26 July 2010, DCII is operated and maintained by the Defense Manpower Data Center (DMDC) on behalf of the DoD components and USD(I). See website at: <<https://dcii.dmdc.osd.mil>>

Access to DCII is normally limited to DoD and other federal agencies that have adjudicative, investigative and/or counterintelligence missions. Although the DCII database is physically maintained by the DMDC the data it contains is the responsibility of the contributing agencies.

-- Also, a centralized database, organized in a searchable format, of selected unique identifying information and security clearance data utilized by security and investigative agencies in the Department of Defense, as well as selected other Federal agencies, to determine security clearance status and the existence/physical location of criminal and personnel security investigative files. (DoDI 5505.7, Titling and Indexing Subjects of Criminal Investigative Organizations, 7 Jul 2003)

-- Also, an automated DoD repository that identifies investigations conducted by DoD investigative agencies. DCII does not contain eligibility information. (IC Standard 700-1, 4 Apr 2008)

Defense Counterintelligence and Human Intelligence Center (DCHC). A center within the Defense Intelligence Agency (DIA) for counterintelligence (CI) and human intelligence (HUMINT); established on 3 August 2008. See DoDI O-5100.93, Defense Counterintelligence and Human Intelligence Center (DCHC), 13 Aug 2010.

Defense Counterintelligence and Human Intelligence Enterprise (DCHE). The DoD components that conduct CI, HUMINT, and enabling activities. (DoDI O-5100.93, Defense CI & HUMINT Center, 13 Aug 2010)

Defense Counterintelligence Components. DoD organizations that perform national and DoD counterintelligence and counterintelligence-related functions, including the DoD Counterintelligence Field Activity and the counterintelligence elements of the Military Departments, the Defense Agencies with organic counterintelligence, the Joint Staff, the Office of the Secretary of Defense, and the Combatant Commands. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Counterintelligence Knowledge Base (DCIKB). Serves the Defense CI enterprise as the web-enabled system for collecting observations of CI best practices and lessons learned, disseminating these across DoD CI, conducting triage for further action and facilitating change.

DCIKB collects, analyzes, manages, and disseminates knowledge gained through operational experience, exercises, and supporting activities in order to achieve higher levels of performance and to provide information and analysis on emerging issues and trends.

-- NIPRNet website at: <https://sss.mccl.usmc/dcikb>

-- SPIRNet website at: www.mccl.usmc.smil.mil/dcikb

Defense Counterintelligence Manager. The official responsible who provides the centralized management of Defense CI Enterprise-wide activities. (DoDD O-5240.02, CI, 20 Dec 2007 with Change 1, 30 Dec 2010)

Director DIA serves as the Defense CI Manager, with responsibility to provided for central management of Defense CI Enterprise-wide activities. This role is a corollary to the Director DIA's role as the Defense HUMINT Manager; see *Defense HUMINT Manager*.

Defense Criminal Investigative Service (DCIS). The criminal investigative arm of the Inspector General (IG) of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cyber crime; substandard/defective products; and fraud, bribery & corruption. (DCIS – see website at <http://www.dodig.mil/INV/DCIS/index.html>)

Defense Criminal Investigative Organizations (DCIOs). The Naval Criminal Investigation Service (NCIS), the Air Force Office of Special Investigations (AFOSI), the US Army Criminal Investigation Command (USACIDC), and the Defense Criminal Investigative Service (DCIS), and any successor organizations. (DoDD 5210.56, 1 Nov 2001)

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Defense Critical Infrastructure (DCI). DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. (DoD Strategy for Homeland Defense & Civil Support)

-- Also, the composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of task critical assets and defense critical assets. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, Department of Defense and non-Department of Defense networked assets and essential to project, support, and sustain military forces and operations worldwide. (JP 1-02 & JP 3-27)

Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of DCI [Defense Critical Infrastructure]. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Defense HUMINT Enterprise. The collective of DoD organizations authorized to conduct HUMINT and related activities. (DoDD S-5200.37, Management & Execution of Defense HUMINT (U), 9 Feb 2009)

Defense HUMINT Executor. The senior DoD intelligence official as designated by the head of each of the DoD components who are authorized to conduct human intelligence and related intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Defense HUMINT Manager. The Director DIA, as designated by the USD(I), is the official responsible for the centralized management of the DoD-wide HUMINT Enterprise. (DoDD S-5200.37, 9 Feb 2009)

-- Also, [Dir DIA] serve as the Defense HUMINT Manager (DHM) responsible for centralized management of the DoD-wide HUMINT enterprise, which is based on decentralized execution of HUMINT operations and related activities. (DoDD 5105.21, DIA, 18 Mar 2008)

Defense Industrial Base (DIB). The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (JP 1-02 & JP 3-27)

DoD is responsible for critical infrastructure protection within the defense industrial base per HSPD-7.

Defense Industrial Security Clearance Office (DISCO). An office of the Defense Security Service (DSS) located in Columbus, Ohio, which processes requests for personnel security clearances for industry personnel under the National Industrial Security Program (NISP).

Defense Intelligence. Integrated departmental intelligence that covers the broad aspects of national policy and national security and that intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, including any foreign military or military-related situation or activity which is significant to Defense policy-making or the planning and conduct of military operations and activities. Defense intelligence includes Active and Reserve military, strategic, operational, and tactical intelligence. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Agency (DIA). A Department of Defense combat support agency and a member of the United States Intelligence Community responsible for providing timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. DIA is a major producer and manager of foreign military intelligence.

DIA is the nation's premier all-source military intelligence organization, providing the most authoritative assessments of foreign military intentions and capabilities to U.S. military commanders and civilian policymakers. As combat support agency,

DIA performs five core intelligence functions: all-source analysis; counterintelligence; human intelligence collection; technical intelligence collections; and document and media exploitation.

Defense Intelligence Analysis Program (DIAP). The DoD intelligence analysis community's resource allocation and prioritization program. The DIAP establishes the policies, procedures, responsibilities, and levels of analytic effort required to provide timely, objective, and cogent intelligence to warfighters, defense planners, and policymakers. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

-- Also, a DIA developed intelligence analysis production plan to enhance the ability of defense intelligence to focus on critical areas of national security interest, while maintaining a perspective on potential emerging threats. (DIA)

GDIP Directive No. 006, Subject: *Defense Intelligence Analysis Program*, 31 Oct 2005, establishes the policies, procedures, responsibilities, and levels of analytical effort required for Defense intelligence to provide timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. Program guidance and roles and responsibilities posted on INTELINK at: <<http://www.dia.ic.gov/admin/diap/index.htm>>.

DIAP organizations are responsible for proactively producing intelligence on topics for which they are assigned responsibility IAW *Defense Intelligence Analysis Program Management Guidance*, 24 Feb 2010. The Defense CI & HUMINT Center is responsible for analyzing foreign intelligence activities and threats to US Defense and Service interests.

Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; the National Security Agency/Central Security Service; and the intelligence elements of the Active and Reserve component of the Military Departments, including the United States Coast Guard when operating as a service in the United States Navy. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Operations Coordination Center (DIOCC). [Defense-level entity that] integrates and synchronizes military and National Intelligence capabilities. The DIOCC plans, prepares, integrates, directs, manages and synchronizes continuous full-spectrum Defense intelligence operations in support of Combatant Commands. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Joint Intelligence Operations Center (JIOC)*.

To be disestablished -- see SECDEF memo, subj: Track Four Efficient Initiatives Decision, 14 Mar 2011 (p.43): disestablish the DIOCC and transfer functions to the Joint Staff.

Defense Personnel Security Research Center (PERSEREC). A Department of Defense entity dedicated to improving the effectiveness, efficiency and fairness of the DoD personnel security system.

PERSEREC was established in response to a recommendation by the DoD Security Review Commission (known as the Stilwell Commission), set up in the wake of the very damaging Walker espionage case, to improve DoD's personnel security system. In its 1985 report, the commission called for a personnel security research center to provide policymakers with an objective basis for policies and processes related to the security clearance system.

PERSEREC report entitled, *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (11 Aug 2009), provides summaries of 141 publicly reported espionage related cases. These cases demonstrate that loyal and conscientious employees continue to be the target of attempts by agents of foreign intelligence services to recruit them as sources of sensitive defense and intelligence information. Copy of this report is available for download from PERSEREC web site at: <<http://www.dhra.mil/perserec/index.html>>

Defense Planning Guidance (DPG). Issued by the Secretary of Defense, the DPG provides firm guidance in the form of goals, priorities, and objectives, including fiscal constraints, for the development of the Program Objective Memorandums by the Military Departments and Defense agencies. (JP 1-02)

Defense Sectors. An identified grouping of DoD functions that perform essential services required for military operations and the ability to project and support forces worldwide. (JP 1-02 & JP 3-26)

Defense Security Service (DSS). A DoD agency headquartered located in Alexandria, Virginia with field offices throughout the United States which provides the military services, Defense Agencies, 23 federal agencies and approximately 12,000 cleared contractor facilities with security support services. DSS administers and implements the defense portion of the National Industrial Security Program (NISP) pursuant to EO 12829. DSS Industrial Security personnel provide oversight and assistance to cleared contractor facilities and assist management and Facility Security Officers in ensuring the protection of

U.S. and foreign classified information. DSS facilitates classified shipments between the U.S. and 60 foreign countries and implements foreign ownership, control and influence countermeasures. (DSS Fact Sheet, Jan 2008) Also see *industrial security*; *National Industrial Security Program (NISP)*.

DSS is the DoD Cognizant Security Office for industrial security, responsible for the DoD portion of the National Industrial Security Program (NISP) and, by mutual agreement, other U.S. Government departments and agencies; provides security education & training products and services; administers the industrial portion of the DoD Personnel Security Program (PSP); provides authorized counterintelligence services; and also supports DoD efforts to improve security programs and processes.

– DoDD 5105.42, *Defense Security Service*, 3 Aug 2010 (w/ chg 1 dated 31 Mar 2011)

Deliberate Compromise. The act, attempt, or contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including public disclosure, or the intentional misuse or mishandling of classified information, (AR 381-20, Army CI Program, 25 May 2010)

Delimitations Agreement. Common term for the DoD/Department of Justice Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation. (AR 381-20, Army CI Program, 25 May 2010)

Denial. Measures taken to block, prevent, or impair US intelligence collection. (Foreign Denial & Deception Committee, 30 Mar 2006)

-- Also, the attempt to block information that could be used by an opponent to learn some truth. (Roy Godson and James J. Wirtz, "Strategic Denial and Deception," in *Strategic Denial and Deception: The 21st Century Challenge*, eds. Roy Godson and James J. Wirtz, 2002) Also see *deception*.

-- Also, methods used to conceal state and military secrets particularly from foreign intelligence collections. (Joseph W. Caddell; *Deception 101 – A Primer on Deception*, Strategic Studies Institute, US Army War College, 2004)

-- Also, activities and programs designed to eliminate, impair, degrade, or neutralize the effectiveness of intelligence collection within and across any or all collection disciplines, human and technical. (Dr. James B. Bruce, "Denial and Deception in the 21st Century: Adaptation Implications for Western Intelligence," in *Defense Intelligence Journal*, Vol 15, No 2, 2006; pp 13-27)

Denial and Deception – equal parts art and science

Keeping secrets and negating access conceals the truth from an opponent's acquisition. *Denial* hides the real and *deception* portrays the fake.

For additional information see Joint Pub 3-13.4, *Military Deception*, 13 Jul 2006

Denial of intelligence collection is a significant impediment to successful analysis

Denied Area. An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 1-02 & JP 3-05)

-- Also, a country with which the US has no official or formal diplomatic relations, or a country in which the capabilities and focus of the local CI services create an operating environment so hostile as to require non-traditional tradecraft of the highest order. (National HUMINT Glossary)

Denied Area Tradecraft. The specialized clandestine methodology used in handling agents in particularly difficult and hostile environments. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Departmental Intelligence. Intelligence that any department or agency of the Federal Government requires to execute its own mission. (JP 1-02)

Department of Defense Intelligence Information System (DoDIIS). The combination of DoD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. (JP 2-0, Joint Intelligence)

-- Also, a DIA-led enterprise that manages the intelligence information technology activities of and provides intelligence technology to the Department of Defense, the combatant commands, and other national security entities. (National Intelligence: A Consumer's Guide - 2009)

Department of Defense Intelligence Production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (JP 2-0, Joint Intelligence)

Department of State / Bureau of Diplomatic Security (DS). The security and law enforcement arm of the U.S. Department of State. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy; it is involved in international investigations, threat analysis, cyber security, counterterrorism, security technology, and protection of people, property, and information. (www.state.gov) Also see *Regional Security Officer*.

Every diplomatic mission in the world operates under a security program designed and maintained by DS. In the United States, diplomatic security personnel protect the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States, investigate passport and visa fraud, and conduct personnel security investigations. Operating from a global platform in 25 U.S. cities and 159 foreign countries, diplomatic security ensures that America can conduct diplomacy safely and securely. DS plays a vital role in protecting U.S. embassies and personnel overseas, securing critical information systems, investigating passport and visa fraud, and fighting the war on terror.

-- Department of State website: <<http://state.gov/m/ds/index.htm>>

Department of State / Bureau of Intelligence and Research (INR). State's intelligence component that provides analysis of global developments to the State Department and contributes its unique perspectives to the community's National Intelligence Estimates. (WMD Report, 31 Mar 2005)

For additional information: <<http://www.state.gov/s/inr/>>

Department of Homeland Security (DHS) / Directorate of Information Analysis and Infrastructure Protection. Monitors, assesses, and integrates terrorist-related information; and assesses and addresses the vulnerabilities of the nation's critical infrastructure. (WMD Report, 31 Mar 2005)

Department of Treasury / Office of Terrorism and Financial Intelligence. Treasury's intelligence component that collects and processes information that bears on U.S. fiscal and monetary policy and threats to U.S. financial intuitions. (WMD Report, 31 Mar 2005)

Derogatory Information. Issue information that adversely reflects on a person's loyalty, reliability and trustworthiness. (IC Standard 700-1, 4 Apr 2008)

Desired Perception. In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 1-02)

Detainee. A term used for any person captured or otherwise detained by an armed force. (JP 1-02)

Within DoD, detainee includes any person captured, detained, or otherwise under the control of DoD personnel (military, civilian, or contract employee). It does not include persons being held primarily for law enforcement purposes except where the United States is the occupying power. As a matter of policy, all detainees will be treated as EPWs until some other legal status is determined by competent authority.

For additional information see JP 3-63, *Detainee Operations*, 6 Feb 2008.

Detection. 1) In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition; 2) In surveillance, the determination and transmission by a surveillance system that an event has occurred; 3) In arms control, the first step in the process of ascertaining the occurrence of a violation of an arms control agreement; and 4) In chemical, biological, radiological, and nuclear environments, the act of locating chemical, biological, radiological, and nuclear hazards by use of chemical, biological, radiological, and nuclear detectors or monitoring and/or survey teams. (JP 1-02)

Deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (JP 1-02)

Devil's Advocacy. Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

Devil's Advocacy is most effective when used to challenge an analytical consensus or key assumption regarding a critically important intelligence question.

DIAP. Also see *Defense Intelligence Analysis Program (DIAP)*.

Digital Evidence. Information of probative value stored or transmitted in binary form. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010)

-- Also, information stored or transmitted in binary form that may be introduced and relied upon in court. (DoJ, *Electronic Crime Scene Investigation, 2nd Edition: A Guide for First Responders*, Apr 2008)

Electronic Crime Scene Investigation, 2nd Edition online at: <www.ncjrs.gov/pdffiles1/nij/219941.pdf>

Digital Forensics. In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision now support the range of military operations and courses of action, e.g., computer network operations as well as CI objectives. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010)

Digital Tradecraft. The conduct, topics, or techniques of modern espionage or CI that employ digital or cyber means. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010)

Disguise. Concealment or misrepresentation of the physical characteristics or true nature or identity of a person or object. (CIA in D&D Lexicon, 1 May 2002)

Digraph and/or Trigraph. A two and/or three-letter acronym for the assigned Codeword or nickname. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Diplomatic and/or Consular Facility. Any Foreign Service establishment maintained by the US Department of State abroad. It may be designated a "mission" or "consular office," or given a special designation for particular purposes, such as "United States Liaison Office." A "mission" is designated as an embassy and is maintained in order to conduct normal continuing diplomatic relations between the US Government and other governments. A "consular office" is any consulate general or consulate that may participate in most foreign affairs activities, and varies in size and scope. (JP 1-02)

Diplomatic Security. See *Department of State / Bureau of Diplomatic Security*.

Direct Access. Descriptor used for sources with firsthand access to the information provided. (DoDI S-5200.42, Defense HUMINT and Related Intelligence Activities (U), 8 Dec 2009) Also see *indirect access*.

Direct Liaison Authorized (DIRLAUTH). That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. Direct liaison authorized is more applicable to planning than operations and always carries with it the requirement of keeping the commander granting direct liaison authorized informed. Direct liaison authorized is a coordination relationship, not an authority through which command may be exercised. (JP 1-02)

Direct Support (DS). A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. (JP 1-02 & JP3-09.3)

Director Defense Intelligence Agency. Advises the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders on all matters concerning all-source Defense Intelligence. Serves as the Defense Counterintelligence Manager, the Defense HUMINT Manager, the Defense Collection Manager, the Director of the Defense Intelligence Operations Coordination Center (DIOCC), and the Commander of the Joint Functional Component Command-Intelligence, Surveillance, and Reconnaissance (JFCC-ISR). (DoDD 5105.21, DIA, 18 Mar 2002)

Director of National Intelligence (DNI). Serves as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; oversees the 16 federal organizations that make up the intelligence community (IC); and manages the implementation of the National Intelligence Program (NIP). (IRTPA 2004)

Office of the Director of National Intelligence (ODNI) is charged with: 1) integrating the domestic and foreign dimensions of US intelligence so that there are no gaps in our understanding of threats to our national security; 2) bringing more depth and accuracy to intelligence analysis; and 3) ensuring that US intelligence resources generate future capabilities as well as present results.

DNI created by Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) in December 2004. The Office of the Director of National Intelligence (ODNI) began operations in April 2005. It was created to drive strategic integration, ensure better coordination, and provide oversight & governance of the Intelligence Community (IC).

-- See ODNI Fact Sheet (July 2010) at: <http://www.dni.gov/press_releases/20100716_Fact%20Sheet.pdf>

Disaffected Person. A person who is alienated or estranged from those in authority or lacks loyalty to the government; a state of mind. (JP 1-02)

Discards. [S]pies supposedly deliberately sacrificed to distract a counterintelligence investigation away from a better target. This is a controversial strategy about which there remains much debate within the intelligence community... (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Disinformation. Carefully contrived misinformation prepared by an intelligence or CI service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments. (CI Community Lexicon)

Dissemination. The timely distribution of intelligence products (oral, written, or graphic form) to departmental and agency intelligence Consumer's in a suitable format. (CI Community Glossary)

-- Also, the timely conveyance of intelligence in suitable form to customers. (ICS Glossary)

Dissemination and Integration. In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. Also see *intelligence process*. (JP 1-02 & JP 2-01)

Document and Media Exploitation (DOMEX). The processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under U.S. Government's physical control and are not publicly available; excludes: handling of documents and media during collection, initial review, and inventory process; and documents and media withheld from the IC DOMEX dissemination system in accordance with DNI-sanctioned agreements and policies to protect sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007) Also see Document Exploitation (*DOCEX*), *Harmony*, and *National Media Exploitation Center (NMEC)*.

-- Also, the processing, translation, analysis, and dissemination of collected hard-copy documents and electronic media that are under U.S. Government physical control and are not publicly available. In the Department of Defense this includes the handling of documents and media during their collection, initial review, inventory, and input to a database. (DoDD 3300.03, DoD DOMEX, 11 Jan 2011)

-- Also, the handling and exploitation of documents and/or media for intelligence purposes. (HDI Lexicon, April 2008)

The National Media Exploitation Center (NMEC) is responsible for ensuring the rapid collection, processing, exploitation, dissemination and sharing of all acquired and seized media throughout the intelligence, counterintelligence, military and law enforcement communities. See ICD 302, copy available online at <<http://www.fas.org/irp/dni/icd/icd-302.pdf>>

Director DIA is the IC Executive Agent for NMEC (DoDD 3300.03, *DoD DOMEX*, 11 Jan 2011)

Document Exploitation (DOCEX). The systematic extraction of information from all media formats in response to collection requirements. (Term previously defined in Army FM 2-0, Intelligence, May 2004) Also see *Document and Media Exploitation (DOMEX)*; *Harmony*; and *NMEC*.

-- Also, the process of deriving intelligence information from captured documents, which includes all media capable of storing fixed information, including but not limited to paper, video/audio tapes, computer storage material (e.g., floppy discs, CD ROMs, thumb drives, hard drives), navigation devices capable of storing waypoints & other data, and other forms of stored textual and graphic information. DOCEX involves receiving, collecting, inventorying, cataloging, selectively translating and disseminating capture enemy documents. (CIFA DOCEX, working definition - 2007)

Doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)

"Doctrine evolves from theory and concepts based on values, beliefs, historical perspective, experience, and research."

-- AR 600-100, *Army Leadership*, 8 Mar 2007

-- Also, *Joint Doctrine*: fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

DoD CI Campaign (previously referred to as "*DoD CI Strategic Campaign*"). See the FOUO definition in O-DoDD 5240.02, Counterintelligence, 20 Dec 2007, with Change 1, 30 Dec 2010; available on SIPRNet at <<http://www.dtic.smil.mil/whs/directives/corres/pdf/524002p.pdf>>

DoD CI Campaigns drive and shape Defense CI engagement against critical foreign intelligence threats globally to achieve strategic outcomes; these CI Campaigns are managed by the Office of Counterintelligence (DXC), Defense Counterintelligence & HUMINT Center (DCHC), DIA.

DoD Criminal Investigative Organizations. The term refers collectively to the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, U.S. Air Force Office of Special Investigations, and Defense Criminal Investigative Service, Office of the IG DoD. (DoDD 5525.07)

DoD Components with Organic CI. DoD Components that have internal CI organizations or elements; currently includes: the Army, Air Force, Navy, USMC, Combatant Commands, Defense Intelligence Agency, National Security Agency, Defense Security Service, Defense Threat Reduction Agency, National Reconnaissance Office, Defense Security Service, National Geospatial-Intelligence Agency, Missile Defense Agency, Pentagon Force Protection Agency, and the Joint Staff.

DoD Installation. A facility subject to the custody, jurisdiction, or administration of any DoD component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, vessel/ships, or laboratories where a DoD component has operational responsibility for facility security and defense. (JP 3-26, Homeland Security, 2 Aug 2005)

DoD Personnel Travel Clearance. Travel clearance for DoD and DoD-sponsored personnel performing official temporary travel abroad. The three types of clearance are country clearance, theater clearance, and special area clearance. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

DoD Strategic CI Campaign. See FOUO definition in O-DoDD 5240.02, CI, 20 Dec 2007.

DoD Unknown Subject. The subject of a DoD CI investigation whose identity has not been determined. (DoDI 5240.04, CI Investigations, 2 February 2009)

An "unknown subject" is also commonly referred to as an "UNSUB."

Domestic Activities. Activities within the United States that do not involve a significant connection with a foreign power, organization, or person. (AR 381-20, Army CI Program. 25 May 2010)

Domestic Intelligence. Intelligence relating to activities or conditions within the United States that threaten internal security and that might require the employment of troops; and intelligence relating to activities of individuals or agencies potentially or actually dangerous to the security of the Department of Defense. (JP 1-02)

Domestic Terrorism. Terrorism perpetrated by the citizens of one country against persons in that country. This includes acts against citizens of a second country when they are in the host country, and not the principal or intended target. (DoDD 2000.12, DoD AT Program, 18 Aug 2003)

Dossier. A file consisting of information concerning an individual. (National HUMINT Glossary)

Double Agent. Agent in contact with two opposing intelligence services, only one of which is aware of the double contact or quasi-intelligence services. (JP 1-02)

No term is more misused by amateurs and greenhorns than "double agent."

The first purpose of any double agent program is to engage the enemy. ...The basic use of double agents is to keep contact with the enemy. What you use that contact for depends on the state of your CI program at any moment. But without contact, there isn't much you can do.

A double agent operation is a channel in which information moves in both directions. On each end of the channel is an intelligence or counterintelligence service. The intelligence service seeks to ensure that the flow of material through the channel is beneficial to itself. The CI service seeks to ensure that the flow of material is detrimental to its opponent.

-- William R. Johnson (Former CIA Officer)

-- Also, a person pretending to work as a spy for one government while actually working as [an asset] for another government. (WMD Report, 31 Mar 2005)

-- Also, 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. (Glossary of Intelligence Terms and Definitions, IC Staff, 1978)

-- Also, an agent working for two opposing agencies; he is loyal to one while betraying the other. (TOP SECRET: The Dictionary of Espionage and Intelligence, 2005)

-- Also, a person who engages in clandestine activity for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary. (John P. Dimmer - 1962; see below)

A World of Stratagems

*"To tackle enemy espionage (whoever the enemy may turn out to be) it is therefore of paramount importance to keep a firm hold on the enemy's own system of agents and informers. Knowledge of his methods, knowledge of his intentions, and knowledge of the personnel of his organization are all vitally necessary. Surely all these objects are the best attained by the maintenance of double agents! The confession of faith is consequently a simple one. It amounts to this: that **in peace as well as in war a carefully cultivated double agent system is the safest and surest weapon of counterespionage** [emphasis added], and the one most easily adaptable to changing conditions, changing problems, and even changing enemies."*

-- J.C. Masterman, *The Double-Cross System* (1972)

The term "double agents" as used during OSS operations in WWII: "...captured agents who would be persuaded to continue their activities for the enemy, ostensibly in good faith but acting at the direction of X-2 [OSS Counterintelligence]..." Also "the case of an agent recruited by X-2 [OSS CI] and infiltrated into enemy territory to induce the enemy to employ him as an agent and return him to Allied territory."

-- Kermit Roosevelt, *War Report of the OSS* (1976)

"The fact that doubles have an agent relationship with both sides distinguishes them from penetrations, who normally are placed with the target service in a staff or officer capacity.... The double agent is one of the most demanding and complex counterintelligence activities in which an intelligence service can engage. Directing even one double agent is a time-consuming and tricky undertaking that should be attempted only by a service having both competence and sophistication."

-- John P. Dimmer (1962)

Double Agents "can serve as excellent channels through which misleading information can flow to the enemy. So double agents serve both as collectors of positive intelligence and channels for deception."

-- Senate Report 94-755 (26 April 1976)

A condoned channel of communication with the enemy

For additional open source information see the following:

William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer* (2009); pp. 91-153.

Federal Government Security Clearance Programs, Report # 99-166, Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, April 1985, specifically testimony on pp. 63-103 regarding two Army CI controlled double agent operations: 1) Chief Warrant Officer Jamos Szmolka against the Hungarian Intelligence Service in 1977-1981; and 2) Sergeant "Smith" against the KGB for over 10 years starting in the early 1970's.

"Double Agent Operations," *Espionage*, Naval Investigative Service Command (nd, circa 1989); pp. 24-33.

John P. Dimmer (aka F.M. Begum), "Observations on the Double Agent," *Studies in Intelligence*, V6: 11, pp 57-72 (1962); declassified, originally classified Secret. Available online at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm

Dry Clean. [Tradecraft jargon] Actions taken to determine if one is under surveillance. (Spy Book)

Dry Cleaning. [Tradecraft jargon] Any technique used to elude surveillance. A usual precaution used by intelligence personnel when actively engaged in an operation. (AFOSI Manual 71-142, 9 Jun 2000)

Dynamic Threat Assessment (DTA). An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Contingency Planning Guidance (CPG). (JP 1-02 & JP 2-0, Joint Intelligence)

The DTA is used by the Combatant Commanders and COCOM planning staffs to conduct Mission Analysis for Step 1 - Strategic Guidance under Adaptive Planning and Execution (APEX).

Dual Agent. Within DoD, none.

Previously defined in JP 1-02 (*rescinded by JP 2-01.2, 11 Mar 2011*): one who is simultaneously and independently employed by two or more intelligence agencies, covering targets for both.

Educing Information (EI). The full range of approaches to obtain useful information from sources. EI includes elicitation, debriefing, and interrogation. (*Educing Information – Interrogation: Science and Art*, Dec 2006) Also see *debriefing; elicitation; interrogation; interview*.

The 2006 Intelligence Science Board report *Educing Information – Interrogation: Science and Art* is available online at <<http://www.ndic.edu/press/3866.htm>>

Effect. 1) The physical or behavioral state of a system that results from an action, a set of actions, or another effect; 2) The result, outcome, or consequence of an action; or 3) A change to a condition, behavior, or degree of freedom. (JP 1-02 & JP 3-0, Joint Operations)

Effects-Based Operations (EBO). [Non-doctrinal term] A process for obtaining a desired strategic outcome of effect on the enemy, through the synergetic, multiplicative, and cumulative application of a full range of military and non-military capabilities at the tactical, operational, and strategic levels. (USJFCOM Glossary)

eGuardian. The FBI's unclassified, law enforcement-centric threat reporting system. It provides a means to disseminate SARs dealing with information regarding a potential threat or suspicious activity rapidly throughout the national law enforcement community. (DTM 10-018, Law Enforcement Reporting of Suspicious Activity, 1 Oct 2010)

All reports in the eGuardian system Shared Data Repository are viewable through Guardian, the FBI's classified threat reporting system. DoD personnel assigned to Joint Terrorism Task Forces (JTTFs) and the National Joint Terrorism Task Force (NJTTF) have access to Guardian. For additional information see: http://foia.fbi.gov/eguardian_threat.htm

Electronic Surveillance. The acquisition of a nonpublic communication by electronic means without the consent of a person who is party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication. (DoD 5240.1-R, Dec 1982) Also see *surveillance; foreign intelligence surveillance act (FISA)*.

Governed by the Foreign Intelligence Surveillance Act (FISA) of 1978 (50 USC §1805).

-- Also, the use of electronic devices to monitor or record conversations, activities, sound, or electronic impulses. (Army FM 2-22.2, Counterintelligence, Oct 2009)

-- Also, the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Electronic Tracking Device. Direction finder including electronic tracking devices, such as, radio frequency beacons and transmitters, vehicle locator units, and the various devices that use a Global Positioning System [GPS] or other satellite system for monitoring non-communication activity. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Elements of Espionage. The fundamentals components in which an intelligence service conducts espionage... some or all of the following elements are present in every espionage operation: 1) contact & communication; 2) collection; 3) motive / reward; 4) travel; and 5) tradecraft. (*Espionage 101: Elements of Espionage*, AFCITC Course Handout, 3 Dec 1996, authored by CW4 Constance Y. Huff) Also see *Espionage; Espionage against the United States*.

Espionage *investigative elements* are different than the *prosecutorial elements* (which are addressed in Title 18 USC, §§ 792-798 and Article 106, UCMJ).

Elicitation (Intelligence). Acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. A technique of human source intelligence collection, generally overt, unless the collector is other than he or she purports to be. (JP 1-02 and JP 2-0) Also see *educing information; debriefing; interrogation; interview*.

-- Also, engaging with a source in such a manner that he or she reveals information without being aware of giving away anything of value. (Educing Information – Interrogation: Science and Art, Dec 2006)

“Elicitation, that is to say, like a lot of other tradecraft techniques, has its Scylla and Charybdis. On one hand, the cautious seeker risks concealing his purpose in such general questions or remarks that he evokes nothing of value. On the other hand, if the questions are excessively direct, the contact may quickly suspect he is being interrogated for intelligence purposes and bring the interview to an abrupt and unpleasant end.”

-- George G. Bull, “The Elicitation Interview,” *Studies in Intelligence*, vol. 14 no. 2 (Fall 1970), pp. 115-22. Originally classified “Secret” [declassified].

Émigré. A person who lawfully departed his or her country with the intention of resettlement elsewhere. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (ICS Glossary)

Equipment Exploitation Operations. Intelligence exploitation operations of all types foreign and non-foreign material which may have military application or answer a collection requirement. This material includes material found on a detainee or on the battlefield (Captured Enemy Equipment (CEE)), or purchased through either open or clandestine means (Foreign Military Acquisition). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Enabling Activities. [In CI and HUMINT usage] Any activity that supports Defense CI and HUMINT operations, functions, and missions, including source validation, collection management, collection requirements management, cover, cover support, information systems, production management, source communications, targeting, and training. (DoDI O-5100.93, Defense CI & HUMINT Center, 13 Aug 2010)

Encipher. To convert plain text into unintelligible form by means of a cipher system. (JP 1-02)

End State. Set of required conditions that defines achievement of the commander's objectives. (JP 1-02)

Enemy Combatant (EC). In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. (JP 3-56, Detainee Operations, 6 Feb 2008)

Espionage. Intelligence activity directed towards the acquisition of information through clandestine means. (NSCID 5 and DCID 5/1) Also see *Elements of Espionage*; *Espionage Against the United States*.

“The object of secret intelligence activity [espionage] is to obtain by secret means information which cannot otherwise be secured and which is not elsewhere available.”
-- Kermit Roosevelt, *War Report of the OSS* (1976)

-- Also, 1) Intelligence activity directed toward the acquisition [of] information through clandestine means and proscribed by the laws of the country against which it is committed; 2) Overt, cover, or clandestine activity designed to obtain information relating to the national defense with an intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. (CI Community Lexicon)

-- Also, 1) The art of spying; 2) The act of seeking information for one government that the other government wishes to keep secret. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

“Espionage—the use of spies or secret agents to steal information from enemies, adversaries, or competitors—is one of the oldest forms of intelligence gathering.”

-- Arthur S. Hulnick, “Espionage: Does It Have a Future in the 21st Century?”
The Brown Journal of World Affairs; XI: 1(2004)

Espionage is the clandestine collection of information by people either in a position of trust for the targeted entity, or with access to people with such access. The process of recruiting such individuals and supporting their operations is the HUMINT discipline of *agent handling*.

“Espionage is distinguished from other forms of intelligence gathering by its clandestinity and its ‘illegal means’ of acquisition.” -- Frederick P. Hitz, Former Inspector General of the CIA (1990-1998)

“Espionage is the theft of information in contravention of another nation’s laws by a person known as an ‘agent.’ This act of theft may be direct, as in the secret copying of a classified document, or the indirect, as in hiding of an eavesdropping device, or merely oral, but is done by an agent and it breaks either a foreign law or the internal regulation of an alien organization. Espionage is not the confidential purchase of information where mere embarrassment, rather than illegality, is risked. It is not the flattery, bribery, or coercion of a person to influence his actions within legal limits. It is not ‘a scuttling, violence-prone business. . . incompatible with democracy.’ But rather a silent, surreptitious, violence-shunning business serving the nation.”

-- William R. Johnson, “Clandestinity and Current Intelligence,” *Studies in Intelligence*, vol. 20, no. 3 (Fall 1976), pp. 15-69. Originally classified “Secret / No Foreign Dissem” [declassified].

Espionage, since it is based on human vulnerability, can penetrate even the most heavily guarded repositories of national secrets.

-- Also, the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. (JP 1-02)

Espionage is a national security crime, specifically a violation of Title 18 USC, §§ 792-798 and Article 106, Uniform Code of Military Justice (UCMJ).

“Espionage is a crime almost devoid of evidence...”

-- Peter Wright (Former Asst Director MI5), *Spycatcher* (1987)

Espionage Act. The Espionage Act of 1917 (18 USC § 792 et seq.) is a U.S. federal law passed in June 1917, shortly after the U.S. entry into World War I. It prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment. The law was further strengthened by the *Espionage and Sabotage Act of 1954*, which authorized the death penalty or life imprisonment for espionage or sabotage in peacetime as well as during wartime. The Act requires agents of foreign governments to register with the U.S. Government. It also suspended the statute of limitations for treason. In 1958, the scope of the act was broadened to cover Americans engaged in espionage against the U.S. while overseas. Also see *espionage*.

Essential Elements of Information (EEI). The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. (JP 1-02)

Essential Secrecy. The condition achieved from the denial of critical information to adversaries. (JP 1-02)
Note: to be removed from JP 1-02 per JP 2-01.2, 16 Mar 2011.

Essential Task. In the context of joint operation planning, a specified or implied task that an organization must perform to accomplish the mission. An essential task is typically included in the mission statement. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *implied task*; *specified task*.

Estimative Intelligence. Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations. (JP 1-02 & JP 2-0)

Evaluating. In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (Term previously defined in Army FM 2-0, Intelligence, May 2004)

Evaluation and Feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (JP 2-01)

Evidence. Testimony, writings, material object, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact. In legal proceedings there are several different types: 1) in terms of their relationship to the crime, they are known as "direct" or "circumstantial," and 2) in terms of their relationship to the world at large, they are known as "physical" or "testimonial."

-- Also, anything that helps to ascertain the truth of a matter, or gives proof of a fact. Evidence may be physical or testimonial. (AR 195-5, Evidence Procedures, 25 Jun 2007)

-- Also, the legal data that conclusions or judgments may be based on. It is the documentary or verbal statements and material objects admissible as testimony in a court of law. Evidence is the means by which any alleged matter of fact is proven or disproved. Evidence includes all matters, except comment or argument, legally submitted to a court. Evidence is the source from which a court-martial or jury must form its conclusions as to the guilt or innocence of an accused. *Testimonial evidence*, e.g., sworn statements of eyewitness accounts and admissions of guilt, is obtained through communication with people. *Physical evidence*, e.g., identified weapons and fingerprints, is obtained by searching crime scenes, tracing leads, and developing technical data. Investigators must always be evidence conscious. Both physical and testimonial evidence are vital to the successful prosecution of an investigation. (Army FM 3-19.13, Law Enforcement Investigations, Jan 2005)

-- Also, evidence in its broadest sense, refers to anything that is used to determine or demonstrate the truth of an assertion; the term has specialized meanings when used with respect to specific fields, such as criminal investigations and legal discourse. ...Legal evidence concerns the tight rules governing the presentation of facts that tend to prove or disprove the point at issue. ...Testimony (which tells) and exhibits (which show) are the two main categories of evidence presented at a trial or hearing. (Wikipedia, accessed 1 Aug 2007)

The law of evidence governs the use of testimony (e.g., oral or written statements, such as an affidavit) and exhibits (e.g., physical objects) or other documentary material which is admissible (i.e., allowed to be considered by the trier of fact, such as a jury) in a judicial or administrative proceeding (e.g., a court of law). Evidence must be acquired/received, processed, safeguarded and disposed of properly.

"Espionage is a crime almost devoid of evidence..."

-- Peter Wright, *Spycatcher* (1987)

"While espionage may be ALMOST devoid of evidence, it is NOT VOID of evidence."

-- ESPIONAGE 101: Elements of Espionage by CW4 Connie Huff (USA), 3 Dec 1996

Execute Order (EXORD). 1) An order issued by the Chairman of the Joint Chiefs of Staff, by the authority and at the direction of the Secretary of the Defense, to implement a decision by the President or SECDEF to initiate military operations; 2) An order to initiate military operations as directed. (JP 1-02 & JP 5-0)

Executive Agent. A term used to indicate a delegation of authority by the Secretary of Defense to a subordinate to act on the Secretary's behalf. Designation as executive agent, in and of itself, confers no authority. The exact nature and scope of the authority delegated must be stated in the document designating the executive agent. An executive agent may be limited to providing only administration and support or coordinating common functions, or it may be delegated authority, direction, and control over specified resources for specified purposes. (JP 1-02)

Exfiltration. The removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means. (JP 1-02)

-- Also, a clandestine rescue operation designed to get a defector, refugee, or operative and his or her family out of harm's way. (CI Centre Glossary)

-- Also, a clandestine operation undertaken to remove an individual from a denied area. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, an operation to get an individual secretly and illegally [in violation of a foreign country's law] out of a hostile area. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Examples include the escapes of KGB officer Oleg Gordievsky from the Soviet Union in 1985, orchestrated by MI6, and KGB officer Victor Sheymov, his wife, and daughter from the Soviet Union in 1980, carried out by the CIA.

Expeditionary Intelligence. Intelligence in support of an armed force organized to accomplish a specific objective in a foreign country. (National Intelligence: A Consumer's Guide - 2009).

Eyewash. [Tradecraft jargon] False entries made in files, usually to protect the security of a source, often indicating that a particular target has rejected a pitch, when in fact the offer was accepted. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Fabricator. An individual or group who, usually without genuine resources, invents or inflates information for personal or political gain or political purposes. (JP 1-02)

False Flag. Development or execution of any imitative or operation under false national sponsorship or credentials (aka “false colors”). The Russian term is foreign flag. (CIA in D&D Lexicon, 1 May 2002) Also see *false-flag approach* and *false-flag recruitment*

-- Also, the technique for misrepresenting an individual’s country of origin is a risky but well-established tactic adopted by all counterintelligence agencies in the absence of other, safer alternatives. Invariably, the strategy is one of last resort when a suspect is known to have engaged in espionage, but is thought to be currently inactive. The offer to be reengaged as a spy may be accepted and result in sufficient evidence to secure a conviction, or may prompt an incriminating action. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, approach by a hostile intelligence officer who misrepresents himself or herself as a citizen of a friendly country or organization. The person who is approached may give up sensitive information believing that it is going to an ally, not a hostile power. (Spy Book)

False-Flag Approach. An intelligence officer or agent who represents themselves as a person of another nationality in order to foster trust and lessen suspicion about the contact. (AR 381-12, Threat Awareness and reporting Program, 4 Oct 2010) Also see *false flag*; *false-flag recruitment*.

False-Flag Recruitment. A situation that occurs when an individual is recruited believing that he/she is cooperating with an intelligence eservice of a specific country, when in actually he/she has been deceived and is cooperating with an intelligence service of another country. (CI Community Lexicon) Also see *false-flag*; *false-flag approach*.

“...‘false flag’ recruitment—when an intelligence service recruits a target while pretending to represent another nation—a common piece of tradecraft. When you finally recruit the target, he believes he is providing information to some other nation. The Israelis have often used this technique by impersonating CIA officers when trying to recruit Arabs.”

-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 97

-- Also, an individual recruited believing he/she is cooperating with an intelligence service of a specific country when, in reality, the individual has been deceived and is working on behalf of an intelligence service of another country. (ICS Glossary & AR 381-47)

-- Also, recruitment of an individual under the guise of working for one entity when actually working for another entity. (HDI Lexicon, April 2008)

Can also be used as a CI investigative technique to determine whether a suspected spy intends to or has committed espionage or other national security crimes against the United States; in this type of false flag a U.S. CI or law enforcement officer poses as an intelligence operative of a foreign power in an undercover operation. The FBI has successfully used this type of false flag operation in several espionage cases, e.g., see *United States of America v. Stewart Davis Nozette* (U.S. District Court for the District of Columbia, case number: 09-0565M)

Federal Bureau of Investigation (FBI). The primary investigative arm of the US Department of Justice (DoJ) with jurisdiction over violations of more than 200 categories of federal law and also a statutory member of the US Intelligence Community. The FBI’s mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. (www.fbi.gov)

The FBI is unique in having a dual responsibility—to prevent harm to national security as a member of the U.S. Intelligence Community and to enforce federal laws as part of the Department of Justice. The Bureau reports to both the Attorney General and the Director of National Intelligence.

-- Today’s FBI – Facts and Figures 2010-2011

The FBI has authority to investigate threats to the national security pursuant to Presidential Executive Orders, Attorney General authorities, and various statutory sources. Per EO 12333 (US Intelligence Activities) the FBI coordinates the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States.

"We always thought of the FBI highly. We viewed it, this organization, as a formidable one. In the intelligence business, it's better to overestimate than underestimate, we never just thought of the FBI as incompetent or weak organization. It was an adversary, a formidable adversary, truly."
-- Oleg Kalugin, Retired KGB General (served in Washington DC and Former Chief of Line KR)

Federal Polygraph Examiner. Military, civilian, or contractor personnel authorized to conduct polygraph examinations on behalf of a Federal agency. (DoD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007)

Feedback. Information or intelligence provided to deception planners as to the progress of a deception operation and, ultimately, its success or failure. (CIA in D&D Lexicon, 1 May 2002)

Financial Crimes Enforcement Network (FINCEN). An element of the Department of Treasury with the mission to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity. FINCEN administers the Bank Secrecy Act; supports law enforcement, intelligence, and regulatory agencies through sharing and analysis of financial intelligence; builds global cooperation with counterpart financial intelligence units; and networks people, ideas, and information. (website: <<http://www.fincen.gov>>)

Finding. A written legal determination made by the President of the United States authorizing a particular covert action important to US national security, in compliance with the Foreign Assistance Act of 1961, as amended by the 1971 Hughes-Ryan Amendment. (National HUMINT Glossary) Also see *covert action*.

According to the Congressional Research Service, the reference to a "**presidential finding**" took on its current popular meaning when Congress adopted the Hughes-Ryan amendment to the Foreign Assistance Act in 1974. Section 662 of the statute prohibits the expenditure of appropriated funds by or on behalf of the CIA for covert actions "unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of Congress."

The requirements of this provision subsequently went through a series of transformations, the vestiges of which were recently codified in the Intelligence Authorization Act, FY1991, which still requires a written presidential finding satisfying certain conditions set forth in the statute for covert actions to occur. Such presidential findings, which are classified, are to be "reported to the intelligence committees as soon as possible" after being approved "and before the initiation of the covert action authorized by the finding." These findings are not published in the Federal Register or reproduced in CFR Title 3 compilations.

FIVE EYES (FVEY). Australia, Canada, New Zealand, United Kingdom and the United States. (CAPCO)

Five Ws (also known as the Five Ws and one H). The formula for getting the "full" story on something. The maxim of the Five Ws (and one H) is that in order for a report to be considered complete it must answer a checklist of six questions, each of which comprises an interrogative word: Who, What, When, Where, Why, and How? (Wikipedia, accessed 20 Feb 2009)

Flag Officer. A term applied to an officer holding the rank of general, lieutenant general, major general, or brigadier general in the US Army, Air Force or Marine Corps or admiral, vice admiral, or rear admiral in the US Navy or Coast Guard. (JP 1-02)

Flaps and Seals. [Intelligence parlance for] the clandestine opening, reading, and resealing of either envelopes or packages without the recipient's knowledge. (Spycraft)

Force Multiplier. A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. (JP 1-02 & JP 3-05.1)

Force Protection (FP). Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JP 1-02 & JP 3-0)

Force Protection Detachment (FPD). A CI element that provides CI support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007; also JP 1-02 and JP 2-01.2)

The FPD primary mission is to detect and warn of threats to DoD personnel and resources in-transit at overseas locations without a permanent DoD CI presences.
-- DoDI 5240.22, *CI Support to Force Protection*

Force Protection Response Group (FPRG). For specifics see DoDI S-5240.15, FPRG, 20 Aug 2010.

Foreign Agents Registration Act (FARA). A disclosure statute, enacted in 1938, that requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities. Disclosure of the required information facilitates evaluation by the government and the American people of the statements and activities of such persons in light of their function as foreign agents. (22 USC §611)

The FARA Registration Unit of the Counterespionage Section in the National Security Division (NSD), Department of Justice (DoJ) is responsible for the administration and enforcement of the Act. See DoJ website at <<http://www.usdoj.gov/criminal/fara/index.html>>

Foreign Computer Intrusion. The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers. (AG Guidelines for Domestic FBI Operations, 29 Sep 2008)

Foreign Contact. Contact with any person or entity that is not a U.S. Person. (IC Standard 700-1, 4 Apr 2008)

Foreign Denial & Deception. Foreign capabilities and techniques designed to conceal, manipulate, deny, deceive, influence, induct uncertainty, and generate gaps in U.S. intelligence capabilities and/or conceal intentions. Also see *denial; deception, military deception*.

Aggressive foreign D&D efforts erode our intelligence advantage

Foreign knowledge and understanding of US intelligence capabilities are significant and growing problems across all intelligence disciplines and represent serious challenges to US national Security.

“America’s toughest adversaries know a great deal about our intelligence system and are becoming better at hiding their intentions and capabilities.”

-- The National Intelligence Strategy, October 2005, p.9

Foreign Denial & Deception Committee (FDDC). An interagency intelligence committee that operates under the auspices of the National Intelligence Council (see ICD 204).

Foreign Instrumentation Signals Intelligence (FISINT). Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. (JP 1-02 & JP 2-01) Also see *signals intelligence (SIGINT)*.

Foreign Intelligence (FI). Information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities. (National Security Act §3(2), 50 USC §401a; also JP 1-02 & JP 2-0, Joint Intelligence) Also see *positive intelligence*.

FI collection disciplines include: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); and measurement & signatures intelligence (MASINT). FI does not include counterintelligence.

FI is one of the two components of intelligence, the other is counterintelligence (CI) per Executive Order 12333 *US Intelligence Activities* as amended and the National Security Act of 1947 as amended.

Foreign Intelligence Agent. A person other than a foreign intelligence officer, who is engaged in intelligence activities or sabotage for on the behalf of a foreign power, or international terrorist activity, or who knowingly conspires with or aids and abets such a person in these activities. (CI Community Lexicon) Also see *agent*; and *agent net*.

Foreign Intelligence and Security Service (FISS). An organization of a foreign country capable of executing all or part of the intelligence cycle. Note: sometimes referred to as FIS (Foreign Intelligence Service) Also see *foreign intelligence entity*.

Foreign Intelligence Collection Threat. The potential of a foreign power, organization, or person to overtly or covertly collect information about U.S. acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations. (DoD 5200.1-M, Acquisition Systems Protection Program, March 1994)

Foreign Intelligence Entity (FIE). Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire US information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service [FISS] and international terrorists. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011; to be included in update to JP 1-02)

FIE is a more encompassing term, which includes but not limited to Foreign Intelligence and Security Services (FISS).

-- Also, any known or suspected foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs US intelligence collection, influence US policy, or disrupts US systems and programs. This term includes foreign intelligence and security services and international terrorists. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010) *Note: this definition is slightly different than the one above from JP 2-01.2.*

-- Also, any foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service as defined in Joint Publication 1-02. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Foreign Intelligence Liaison. Activities or relationships between elements of the United States Government and elements of foreign governments or international organizations on matters involving foreign intelligence, counterintelligence, or clandestine intelligence activity.

Foreign Intelligence Officer. A member of a foreign intelligence service. (CI Community Lexicon) [Also referred to as an IO (intelligence officer)]. Also see *agent handler*.

Foreign Intelligence Service (FIS). An organization of a foreign country capable of executing all or part of the intelligence cycle. (CI Community Lexicon) Also see *Foreign Intelligence and Security Service*, *Foreign Intelligence Entity*.

Foreign Intelligence Surveillance Act (FISA). [Public Law 95-111] ...the legal authority authorizing and regulating electronic surveillance within the United States for foreign intelligence or counterintelligence purposes and physical searches within the United States for foreign intelligence purposes. The act sets out the application, order, and report process to be followed. (CI Community Lexicon)

FISA prescribes procedures for the physical & electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers". Subchapters of FISA provide for: electronic surveillance; physical searches; pen registers and trap & trace devices for Foreign Intelligence (FI) purposes; and access to certain business records for FI purposes. FISA does not apply to U.S. counterintelligence activities overseas.

-- FISA, codified in 50 U.S.C. §§ 1801, et seq was amended by the FISA Amendments Act of 2008.

Foreign Liaison Officer (FLO). A foreign government military member or civilian employee who is authorized by his or her government to act as an official representative of that government in its dealings with the DoD and Military Services in connection with programs, projects, or agreements of mutual interest to DoD and the foreign government. (adapted from AR 380-10, 22 Jun 2005)

Three types of FLOs: 1) A *Security Assistance FLO* is a foreign government representative who is assigned to a DoD element or contractor facility pursuant to a requirement that is described in an FMS LOA; 2) An *Operational FLO* is a foreign government representative who is assigned to a DoD element pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education; and 3) A *National Representative FLO* is a foreign government representative who is assigned to his or her national embassy or legation in Washington, DC (for example, an attaché), to conduct liaison activities with DoD / Military Services.

Foreign Material Acquisition (FMA). Foreign Material Program (FMP) activities that include gaining physical possession, or access to, an item of foreign material or technology. (DoDD C-3325.01E, Foreign Material Program (U), 10 Oct 2006)

Foreign Material Exploitation (FME). Foreign Material Program (FMP) activities that include analysis, testing, evaluation, and documentation of the scientific and technical intelligence (S&TI) characteristics of an item of foreign material. (DoDD C-3325.01E, Foreign Material Program (U), 10 Oct 2006)

Foreign Military Intelligence Collection Activities (FORMICA). Entails the overt debriefing, by trained HUMINT personnel, of all U.S. persons employed by the Department of Defense who have access to information of potential national security value. (DoDI C-5205.01, FORMICA (U), 22 Jan 2009; also JP 1-02 and JP 2-01.2)

Foreign National. Any person other than a US citizen, US permanent or temporary legal resident alien, or person in US custody. (JP 1-02)

-- Also, any person who is not a citizen of the U.S. (IC Standard 700-1, 4 Apr 2008)

Foreign Ownership, Control or Influence (FOCI). A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified matters. (ISC 20008-700-1, 4 Apr 2008)

Within DoD, see DTM 09-019, *Policy for FOCI*, 2 Sep 2009

Foreign Power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities. (DoD 5240.1-R, Dec 1982)

Foreign Service National (FSN). Foreign nationals who provide clerical, administrative, technical, fiscal, and other support at foreign service posts abroad and are not citizens of the United States. The term includes third country nationals who are individuals employed by a US mission abroad and are neither a citizen of the US nor of the country to which assigned for duty. (JP 1-02 & JP 3-68)

Foreign Terrorist Tracking Task Force (FTTTF). A specialized task force that was created pursuant to Homeland Security Presidential Directive No. 2 and was consolidated into the FBI pursuant to the Attorney General's directive in August 2002. The FTTTF uses innovative analytical techniques and technologies that help keep foreign terrorists and their supporters out of the United States or lead to their location, detention, prosecution, or removal. The participants include DoD, Department of Homeland Security's bureaus of Immigration and Customs Enforcement (ICE) and Customs and Border Protection, State Department, Social Security Administration, Office of Personnel Management, Department of Energy, and CIA. (FBI website: <<http://www.fbi.gov/congress/congress06/mueller120606.htm>>)

Foreign Visits System (FVS). Automated system operated by the Office of the Under Secretary of Defense (Policy) that provides staffing and database support for processing requests for visits by foreign nationals to DOD activities and defense contractors. FVS consists of an unclassified segment that allows the online submission of visit requests from embassies in Washington, DC, and, in some cases, directly from foreign governments overseas. FVS also has a classified segment that provides staffing, decision-making support, and database capabilities to the military departments and DIA.

FORMICA. See *Foreign Military Intelligence Collection Activities*.

FOUR EYES (ACGU). Australia, Canada, United Kingdom, and the United States. (CAPCO)

Full-Spectrum Counterintelligence Activities. Full array of CI activities – both offensive & defensive – that can be applied in executing CI effects-based operations to achieve strategic outcomes in peacetime, crisis, war and post conflict activities (e.g., stabilization operations/reconstruction efforts). These activities support national security objectives, as well as defense decision-makers and the Combatant Commanders.

Functional Managers. EO 12333 designates three Functional Managers: Director CIA for human intelligence (HUMINT), Director NSA for signals intelligence (SIGINT), and Director NGA for geospatial intelligence (GEOINT), (EO 12333, para 1.3 (b)(12)(A)(i-iii)) See ICD 113, *Functional Managers*.

Pursuant to EO 12333, Functional Managers report to the DNI concerning the extent of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; setting training and tradecraft standards; and ensuring coordination within and across intelligence disciplines and IC elements and with related non-intelligence activities.

Functional Managers may also advise on resource management; policies and procedures; collection capabilities and gaps; intelligence processing and dissemination; technical architectures; and other issues or activities, as applicable.

Note: The National Counterintelligence Executive (NCIX) is the Mission Manager for CI.

Functional Support [Analytical Product]. A type of CI analytical product that supports the specific needs of a Defense CI Component. A functional support product is related to the CI functions of collection, investigation, OFCO [Offensive Counterintelligence Operation], and functional services as described in DoDI 5240.16. The depth and comprehensiveness varies depending on the requestor's requirements. An investment in analytical effort may be significant. The production timeline ranges from hours to weeks, but can vary widely depending on the function the analysis supports. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009) Also see *Counterintelligence Analytical Product*.

Functional Support Plan (FSP). Annexes to the National Intelligence Support Plan (NISP) [that] describe how service intelligence centers and Combat Support Agencies support COCOM plans. (Adaptive Planning Roadmap II, 5 Mar 2008) Also see *Counterintelligence Functional Support Plan (CI FSP)*.

Director Defense CI & HUMINT Center will "conduct CI and HUMINT planning in support of the Joint Chiefs of Staff adaptive planning process."

-- Para 3a(19), DoDI O-5100.93, DCHC, 13 Aug 2010

Director DoD Counterintelligence Field Activity (CIFA) will "fully integrate CI into the intelligence campaign planning process by developing and updating the CI functional support plans."

-- DUSD (CI&S) memo, subj: Counterintelligence Support to COCOMs, 29 Dec 2006

Note: CIFA's mission and functions transitioned into the Defense CI & HUMINT Center effective 3 August 2008.

Fusion. In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02 & JP 2-0)

General Defense Intelligence Program (GDIP). An integrated Defense Intelligence capability that includes DIA, the Service technical production centers, and special collection activities. The GDIP integrates and produces National Intelligence for Defense and national Consumer's. It represents the national Defense Intelligence priorities for operational customers, national and Defense-wide collection management, All-Source Analysis, HUMINT, MASINT, IT, and Special Activities. The GDIP is an integrated capability, and the Director, DIA, serves as the Program Manager. The GDIP is part of the NIP, as defined in EO 12333. The GDIP may include other NIP activities as agreed between the Secretary of Defense and the DNI. (DoDI 5105.21, DIA, 18 Mar 2008)

General Support (GS). That support which is given to the supported force as a whole and not to any particular subdivision thereof. (JP 1-02) Also see *direct support*.

Geospatial Information. Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

Geospatial Information and Services (GI&S). The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the Earth's surface. Geospatial services include tools that enable users to access and manipulate data, and also include instruction, training, laboratory support, and guidance for the use of geospatial data. (DoDD 5105.60, NGA, 29 Jul 2009 & JP 2-03)

Geospatial Intelligence (GEOINT). The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (JP 1-02, JP 2-03 and ICD 1, 1 May 2006)

-- Also, information describing, visually depicting, and accurately locating physical features and human activities on the Earth. Examples of GEOINT products include imagery, analyses, maps, and navigation charts. Imagery intelligence (IMINT) is a subset of GEOINT. (National Intelligence: A Consumer's Guide - 2009)

The Intelligence Community refers to the use and analysis of geospatial information to assess geographically referenced activities on Earth as *geospatial intelligence* (GEOINT). It is everything you can see or know about the earth. GEOINT consists of: Imagery - a likeness of any natural or man-made feature, as well as its location; Imagery Intelligence (IMINT) - information derived through interpreting imagery; and Geospatial Information - information that identifies a natural or constructed feature on Earth by its geographic location and other characteristics.

-- www.cia.gov (accessed 30 Nov 2010)

GEOINT collection encompasses all aspects of: literal, infrared (IR), and synthetic aperture radar (SAR) imagery; overhead persistent infrared capabilities; and geospatial information and services. GEOINT includes the exploitation and analysis of electro-optical, IR, and radar imagery; and of geospatial, spectral, laser, IR, radiometric, SAR phase history, polarimetric, spatial, and temporal data. It employs all ancillary data, signature information, and fused data products, as necessary. Integrated GEOINT products may also include data and information from collateral sources.

-- DoDD 5105.60, NGA, 29 Jul 2009

Ghost Surveillance. Extremely discreet and seemingly omnipresent surveillance, working mostly out of the view of the target. (CI Centre Glossary) Also see *surveillance*.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02 & JP 6-0)

Global Force Management (GFM). The ability to align force apportionment, assignment, and allocation methodologies in support of the National Defense Strategy and joint force availability requirements; present comprehensive insights into global availability and operational readiness of U.S. military forces; globally source joint force requirements; and provide senior decision-makers a vehicle to quickly and accurately assess the impact and risk of proposed allocation, assignment, and apportionment changes. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Global Positioning System (GPS). A satellite-based radio navigation system operated by the Department of Defense to provide all military, civil, and commercial users with precise positioning, navigation, and timing. Also called GPS. (JP 1-02 & JP 3-14)

Goldwater-Nichols Act (GNA). The Goldwater-Nichols Department of Defense Reorganization Act of 1986 (PL 99-433), sponsored by Sen. Barry Goldwater and Rep. Bill Nichols, was a major reorganization of U.S. defense institutions and processes. Operational authority was centralized through the Chairman of the Joint Chiefs of Staff as opposed to the service chiefs. The Chairman was designated as the principal military advisor to the President, National Security Council, and Secretary of Defense. The act established the position of vice-chairman and streamlined the operational chain of command from the President to the Secretary of Defense to the Unified Commanders.

For additional information see <<http://www.ndu.edu/library/goldnich/goldnich.html>>
Copy of PL 99-443 at <http://www.au.af.mil/au/awc/awcgate/congress/title_10.htm>

Graymail. Threat by a defendant in a trial to expose intelligence activities or other classified information if prosecuted. (Spy Book) Also see *Classified Information Procedures Act (CIPA)*.

“Graymail” colloquially refers to situations where a defendant may seek to introduce tangentially related classified information solely to force the prosecution to dismiss the charges against him.

A criminal prosecution involving classified information may cause tension between the government’s interest in protecting classified information and the criminal defendant’s right to a constitutionally valid trial. In some cases, a defendant may threaten to disclose classified information in an effort to gain leverage. Concerns about this practice, referred to as “graymail,” led the 96th Congress to enact the *Classified Information Procedures Act (CIPA)* to provide uniform procedures for prosecutions involving classified information.

Gray List. Contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States are obscure. Regardless of their political inclinations or attitudes, personalities may be listed on gray lists when they are known to possess information or particular skills required by US forces. They may be individuals whose political motivations require further exploration before they can be utilized effectively by US forces. (CI Community Lexicon) Also see *White List; Black List*.

-- Also, a list of those foreign personalities of operational interest whose inclinations and attitudes toward the political and military objectives of the United States are unknown. (HDI Lexicon, April 2008)

GRU. *Glavnoye Razvedyvatel’noye Upravlenie* (Chief Intelligence Directorate of the General Staff); aka Russian Military Intelligence.

Hacker. Unauthorized user who attempts to or gains access to an Information System. (CNSS Instruction No. 4009)

-- Also, a person who creates and modifies computer software and hardware, including computer programming, administration, and security-related items. This can be done for either negative or positive reasons. Criminal hackers create malware in order to commit crimes. (McAfee.com, accessed 15 Nov 2010)

In computer security usage, a term used for a person who accesses a computer system by circumventing its security system.

Hactivism. The nonviolent use of ambiguous digital tools in pursuit of political ends; these tools include website defacements, redirects, denial-of-service attacks, information theft, website parodies, virtual sit-ins, virtual sabotage, and software development. (en.wikipedia.org/wiki/Hactivists - accessed 2 Apr 2009)

Hactivism is a controversial term. Some argue it was coined to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform.

For additional information see McAfee White Paper, “Cybercrime and Hactivism” (undated), available online at: <www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf>

Handler. An intelligence officer or co-opted worker directly responsible for the operational activities of an agent; also agent handler or case officer. (CI Community Lexicon) Also see *agent handler; case officer*.

-- Also, an intelligence collector directly responsible for the operational activities of an agent, source, or asset. (HDI Lexicon, April 2008)

Hard Target. A person, nation, group, or technical system often hostile to the US or heavily protected, with a well-honed counterintelligence capability that presents a potential threat to the US or its interests, and provides significant difficulty for agent infiltration or penetration. (National HUMINT Glossary)

Harmony. The Intelligence Community's centralized database for foreign military, technical and open-source documents and their translations. Harmony is managed by the US Army's National Ground Intelligence Center (NGIC). Also see *DOMEX*; *DOCEX*.

Hello Number.. Tradecraft jargon for a cutout telephone where the speaker does not identify himself or his/her location. This procedure is used by proprietaries, devised facilities or cover offices of clandestine intelligence agencies for certain types of contacts with agents or affiliated personnel, usually in an emergency, and only information given by the caller over the phone is a codeword or danger signal to be relayed to the appropriate case officer for immediate call-back or other pre-arranged action. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Heuristics. Normal, intuitive mental shortcuts for processing information. They can be effective aids for problem-solving, but can lead to biases and thus to analytic errors.

High-Payoff Target (HPT). A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02 & JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-value target*; *target*.

High-Value Detainee Interrogation Group (HIG). The interagency body under the administrative control of the Federal Bureau of Investigation that was established to assemble and dispatch mobile interrogation teams to interrogate high-value detainees. (DoDD 3115.13, DoD Support to the High-Value Detainee Interrogation Group, 9 Dec 2010)

High-Value Target (HVT). A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02 & JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-payoff target* and *target*.

HOCNet. HUMINT Operational Communication Network (HOCNet) provides information technology, communications, and desktop services for DoD HUMINT needs. (National Intelligence: A Consumer's Guide - 2009)

Homeland. The physical region that includes the continental United States, Alaska, Hawaii, US territories and possessions, and surrounding territorial waters and airspace. (JP 1-02 & JP 3-28)

Homeland Defense (HD). The protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President. (JP 1-02 & JP 3-27)

DoD is responsible for homeland defense and is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions. -- JP 3-26, *Homeland Security*, 2 Aug 2005

Homeland Security. A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security, Oct 2007).

-- Also, a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. (JP 1-02 & JP 3-28)

-- Also, describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration. (Quadrennial Homeland Security Review Report, Feb 2010)

In the years since 9/11, homeland security has become commonly and broadly known as both a term and as a Federal department.

Department of Homeland Security (DHS) is the lead federal agency for homeland security. DoD contributes to homeland security through its missions overseas, homeland defense, and support to civil authorities. -- JP 3-26, *Homeland Security*, 2 Aug 2005

Homeland security is a concerted effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive. Ultimately, homeland security is about effectively managing risks to the Nation's security. -- Quadrennial Homeland Security Review Report, Feb 2010

The *Quadrennial Homeland Security Review Report* (Feb 2010) is available online at: http://www.dhs.gov/xabout/gc_1208534155450.shtm

Homeland Security Information. Any information possessed by a Federal, State, or local agency that: a) relates to the threat of terrorist activity; b) relates to the ability to prevent, interdict, or disrupt terrorist activity; c) would improve the identification or investigation of a suspected terrorist organization; or d) would improve the response to a terrorist act. (Homeland Security Act, § 891)

Honey Pot. In computer terminology, a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers. (Wikipedia, accessed 18 Jan 2011)

Honey Trap. The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail that might result in espionage. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, slang for use of men or women in sexual situations to intimidate or snare others... use of sex to trap or blackmail an individual.... (Spy Book)

Horizontal Integration. Processes and capabilities to acquire, synchronize, correlate, and deliver National Security Community data with responsiveness to ensure success across all policy and operational missions. (CJCSI 3340.02, Horizontal Integration of Warfighter Intelligence, 23 Dec 2005)

Horizontal Protection Analysis. The process that determines if critical Defense technologies, to include CPI [critical program information], associated with more than one RDA [research, development & acquisition] program are protected to the same degree by all involved DoD activities. (DoDI 5200.39, 16 Jul 2008)

Horizontal protection within DoD is focused on ensuring that research, development and acquisition (RDA) information associated with more than one research and technology activity or acquisition program is protected to the same degree by all DoD activities, or is adequately protected based on the impact of an aggregation of the correlated information.

Host Country. A nation which permits, either by written agreement or official invitation, government representatives and/or agencies of another nation to operate, under specified conditions, within its borders. (JP 1-02)

Host Nation (HN). A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 1-02)

Host-Nation Support (HNS). Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. (JP 1-02)

Hostile. In combat and combat support operations, an identity applied to a track declared to belong to any opposing nation, party, group, or entity, which by virtue of its behavior or information collected on it such as characteristics, origin, or nationality contributes to the threat to friendly forces. (JP 1-02)

Hostile Act. An attack or other use of force against the US, US forces, or other designated persons or property. It also includes force used directly to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel or vital US Government property. (JP 1-02 & JP 3-28)

Hostile Environment. Operational environment in which hostile forces have control as well as the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (JP 1-02)

Hostile Intent. The threat of imminent use of force by a foreign force, terrorist(s), or organization against the United States and US national interests, US forces and, in certain circumstances, US nationals, their property, US commercial assets, and other designated non-US forces, foreign nationals, and their property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. A determination that hostile intent exists and requires the use of proportional force in self-defense must be based on evidence that an attack is imminent. Evidence necessary to determine hostile intent will vary depending on the state of international and regional political tension, military preparations, intelligence, and indications and warning information. (JP 1-02)

House Permanent Select Committee on Intelligence (HPSCI). A committee of the US House of Representatives, established by House Resolution 658 on July 14, 1977. It is the primary committee in the U.S. House of Representatives charged with the oversight of the US Intelligence Community and intelligence-related activities of all other government organizations.

The 1980 Intelligence Oversight Act charged the Senate Select Committee on Intelligence and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.

Human Derived Information (HDI). Activities related to the conduct of the collection of intelligence information by or through humans. It includes the following forms of information: FI, CI, Force Protection, Research and Technology Protection, and Law Enforcement. (SECNAVINST S3821.1, 19 Nov 2008)

Human Enabled Information (HEI). Activities designed to spot, assess and develop platforms which facilitate information collection and other assigned operations. (SECNAVINST S3821.1, 19 Nov 2008)

Human Factors. The psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups. (JP 1-02 & JP 2-0)

Human Intelligence (HUMINT). A category of intelligence derived from information collected and provided by human sources [includes HUMINT enabling]. (JP 1-02, JP 2-0, and ICD 1, 1 May 2006)

-- Also, a category of intelligence derived from information collected by USG civilian employees or military personnel. Who are trained and certified HUMINT collectors, and assigned to an organization with the mission and authority to collect foreign intelligence from human sources in response to validated intelligence requirements. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, intelligence derived from information collected and provided by human sources. This intelligence includes overt data collected by personnel in diplomatic and consular posts, as well as otherwise unobtainable information collected via clandestine sources of information, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation. (National Intelligence: A Consumer's Guide - 2009)

-- Also, [from CIA perspective] vital information from human sources acquired by Core Collectors of the National Clandestine Service in response to national intelligence requirements. (www.cia.gov, posted 23 Mar 2009) Also see *national clandestine service*.

-- Also, the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (Army FM 2-0, Intelligence 23 Mar 2010 and FM 2-22.2, CI, Oct 2009)

-- Also, consists of information obtained from individuals who know or have access to sensitive foreign information that has implications for U.S. security interests. (WMD Report, 31 Mar 2005)

--Also, a category of intelligence, that which is reported by a government information collector, who has obtained it either directly or indirectly from a human source. (IC21, HPSCI Staff Study, 9 Apr 1996)

HUMINT collection is a science and an art.

-- Army FM 2-22.3, *HUMINT Collector Operations*

Core Mission: Collect foreign intelligence through human sources to fill critical intelligence gaps.

HUMINT is intelligence derived from human beings who may act as both sources and collectors, and where the human is the primary collection instrument. It is a foreign intelligence (FI) collection discipline. HUMINT collectors focus on acquiring information from individuals with access to vital intelligence on the full range of national security issues.

There are two basic types of HUMINT: overt and clandestine. Overt HUMINT methods include, but are not limited to, debriefing, interrogation, elicitation, and observation. Clandestine HUMINT, sometimes referred to as Clan HUMINT, involves intelligence activity using human sources directed towards the acquisition of information through clandestine means, i.e., *espionage*.

The Director CIA serves as the **National HUMINT Manager** for the Intelligence Community (IC) with the authority to coordinate, deconflict, and evaluate HUMINT operations across the IC; authorities for clandestine HUMINT delegated to the Director of the National Clandestine Service (NCS); see ICD 300 and ICD 304.

The Director DIA serves as the **Defense HUMINT Manager**. Director, DIA is responsible for providing centralized management of DoD HUMINT, which is accomplished through the Defense CI & HUMINT Center (JP 2-01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011)

U.S. FI collection priorities are driven by the National Intelligence Priorities Framework (NIPF); see NSPD 26 and ICD 204. For DoD HUMINT policy see DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (HUMINT) (U)*, 9 Feb 2009.

Foreign intelligence entities worldwide, as well as a variety of non-state actors, commercial enterprises, and regional organizations) use clandestine human intelligence collection to "acquire information" (aka conduct espionage). Typically intelligence entities rely upon specially trained or designated employees, often referred to as "agent handlers" or "case officers" (aka operations officers within CIA) to spot, access, develop, and recruit agents who can provide information that is not publicly available.

Within CIA, Operations Officers (OOs) are certified *Core Collectors* who collect human intelligence of concern to the U.S. President, policymakers, and military by recruiting and handling clandestine human sources in a secure manner. OOs clandestinely spot, assess, develop, recruit and handle human sources with access to vital intelligence.

-- See <<https://www.cia.gov/offices-of-cia/clandestine-service/careers/careers-operations-officer.html>>

Counterintelligence is often mistaken as part of or a subset of HUMINT. Although HUMINT and CI are both intelligence activities that operate in the human domain, they are distinctly different – *each focused on different content, as well as outcomes*. FI collection values the information above all, whereas CI insists on acting on that information – *a totally different operational dynamic*. See *counterintelligence*.

HUMINT – espionage – is the heart of the spy business

The U.S. will continue to need the capabilities to collect HUMINT, especially as a major insight into intentions and plans of hostile states or groups, and to carry out covert action.

-- IC 21: HPSCI Staff Study, 9 Apr 1996 (Finding, pg 18)

Human Source. A person who wittingly or unwittingly conveys by any means information of potential intelligence value. (ICS Glossary) Also see *HUMINT Source*; *Source*.

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

"[H]uman sources collect the smallest volume of intelligence but generally it is the most difficult to obtain and the most useful when we do get it. It is in this area that the best information is acquired on the all-important subject of intentions."

-- General Veron Walters (Former DCI), *Silent Missions* (1978)

Human Source Contact Operations (SCO). HUMINT collection activity directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

SCO sources include: one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. The basic goal of all levels of contact is to collect information in response to collection tasking.

-- Army FM 2-22.3, *HUMINT Collector Operations* (2006)

HUMINT Collection Activities. There are two HUMINT collection methods authorized for use within DoD: overt and clandestine. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, categories include: tactical questioning; screening, interrogation; debriefing; liaison; human source contact operations (SCOs), documents exploitation (DOCEX); and captured enemy equipment (CEE) operations. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Collection Requirement (HCR). A long-term DoD-wide HUMINT collection requirement which supports DoD operational planning, policy- and decision-making, intelligence production, and intelligence databases. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Collection Team (HCT). Element that collects information from human sources. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Collector. A person who is specifically trained and certified for, tasked with, and engages in the collection of information from HUMINT sources for the purposes of answering intelligence information requirements. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person who is specifically trained and certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

HUMINT Enabling. An operational support function in which non-HUMINT intelligence collection operations are facilitated by HUMINT collection platforms.

HUMINT Operations Cell (HOC). Assigned under the J/G2X to track all HUMINT activities in the area of intelligence responsibility. It provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the AO. (Term previously defined in Army FM 2-0, Intelligence, May 2004)

For additional information on the HOC see: JP 2-01.2, *CI & HUMINT in Joint Operations (U)*, 11 Mar 2010, p. II-8 (para 3c).

HUMINT Source. A person from which services or intelligence information are obtained. The source may possess either first or second-hand knowledge normally obtained through sight or hearing and may be witting or unwitting. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *human source*; *source*.

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Support Element (HSE). A DIA representative or staff element assigned to support a COCOM. An HSE provides liaison and assists the COCOM with HUMINT planning, coordination, collection management, training, and operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Targeting. The integration of all-source intelligence and systemic analytic methodologies to identify and develop relevant HUMINT leads in direct support of HUMINT collection operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Tasks. Include but not limited to: conducting source operations; liaising with host nation officials and allied counterparts; eliciting information from select sources; debriefing US and allied forces and civilian personnel including refugees, displaced persons, third-country nationals, and local inhabitants; interrogating enemy prisoners of war and other detainees; and initially exploiting documents, media, and material. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

Hybrid Threats. Hybrid threats refer to the ability of adversaries—lone attackers, criminal, transnational terrorist organizations, even nation-states—to employ combinations of tactics, technologies, and capabilities to gain an asymmetric advantage. (Quadrennial Homeland Security Review Report, Feb 2010)

-- Also, a hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects. (Army FM 3-0, Operations, Feb 2008)

IC E-mail. Email between organizations over JWICS network. Also referred to as ICE-mail or JWICS email. (National Intelligence: A Consumer's Guide - 2009)

IDSRS. See *Integrated Defense Source Registry System*.

Illegal. An officer, employee, or agent of an intelligence organization who is dispatched abroad and who has no overt relationship with the intelligence service with which he/she is connected or with the government operations that intelligence service. Term is derived from the fact that the individual is in the host country illegally. (CI Community Lexicon)

-- Also, *Illegal Agent* – an officer or employee of an intelligence service dispatched abroad who has no overt connection with the intelligence service with which he or she is connected or with the government operating the service. An illegal, before dispatch, is trained to assume supervisory control over agents or to operate alone. Generally an illegal will be a national of the country operating the intelligence service. An illegal is operated through the center or illegal residency, but not by legal residency. (AFOSI Manual 71-142, 9 Jun 2000)

Illegal agents have no “easily” detectable contacts with their intelligence service. They pose as legitimate residents of the target country and operate without benefits of diplomatic cover.

“The illegal is a highly trained specialist in espionage tradecraft. He may be a [foreign] national and/or a professional intelligence officer dispatched to the United States under a false identity.”

-- FBI as cited in Senate Report # 94-755 (aka Church Committee Report), 26 April 1976, p.164

“Illegal agents—that is, operatives for whom an alias identity has been systemically developed which enables them to live in the United States as America citizens or resident aliens without our knowledge of their true origins.”

-- Rockefeller Committee Report, June 1975, p. 8

Illegal Net. An intelligence gathering unit operating under the control of an illegal residency. (AFOSI Manual 71-142, 9 Jun 2000)

Illegal Residency. An intelligence apparatus established in a foreign country and composed of one or more intelligence officers, which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (ICS Glossary)

Illegal Support Officer. An intelligence officer assigned to a legal residency whose primary function is to support illegal agents by supplying anything needed. A secondary function is the gathering of information and documents that will serve as guidance and models for documentation of future illegal agents. (AFOSI Manual 71-142, 9 Jun 2000)

Imagery. A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 1-02 & JP 2-03)

Imagery Exploitation. The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (JP 1-02)

Imagery Intelligence (IMINT). The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 1-02 and JP 2-03) Also see *geospatial intelligence*.

-- Also, IMINT is derived from the exploitation of imagery collected by visual photography, infrared sensors, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. (Army FM 2-0, Intelligence, 23 Mar 2010)

There are two general types of imagery collection platforms:

- + Satellites—comprised of national technical means [NTM] and commercial platforms.
- + Airborne Systems—comprised of national, commercial, theater, and tactical.

There are two general types of imagery sensors:

- + Electro-optical: panchromatic (visible); infrared; special (multispectral & hyperspectral); and polarimetric.
- + Radar: synthetic aperture radar systems that collect and display data either as representations of fixed targets or as moving target indicators.

-- Army FM 2-0, *Intelligence*, 23 Mar 2010, pp. 9-2 & 9-3

Impersonal Communication. Communications between a handler and asset which do not involve direct contact. (HDI Lexicon, April 2008)

-- Also, secret communication techniques used between a case officer and a human intelligence asset when no physical contact is possible or desired. (CI Centre Glossary)

Implied Task. In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *essential task*; *specified task*.

Improvised Explosive Device (IED). A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. (JP 1-02)

Inadvertent Disclosure. Type of incident involving accidental exposure of information to an individual not authorized access. (CNSS Instruction No. 4009)

-- Also, a set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Indications. In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 2-0, Joint Intelligence)

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 the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied and/or coalition nations. (JP 2-0, Joint Intelligence)

Indicator. In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (JP 1-02 & JP 2-0)

-- Also, data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Indirect Access. Descriptor used for sources who do not have firsthand access to the information provided and who have come upon it through one or more sub-sources. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009) Also see *direct access*.

Indoctrination (or read-on). An initial indoctrination and/or instruction provided each individual approved to a SAP prior to his exposure concerning the unique nature of program information and the policies, procedures, and practices for its handling. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Induced Defection. Tradecraft jargon for developing and encouraging a foreign official's defection from his country. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

"Inducement" is the jargon used for persuading somebody to defect to you.
-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Induced Operation. An operation in which a source or agent is established in such a manner as to induce the opposition to recruit him as its agent. (CI Community Lexicon)

Induction. [One of the four basic types of reasoning applied to intelligence analysis, it is the process] of discovering relationships among the phenomena under study. ...[it draws] generalizations on the basis of observations or other evidence. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; scientific method*.

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Industrial Security. That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry. (DoD 5220.22-M, NISPOM, 28 Feb 2006) Also see *Defense Security Service (DSS); National Industrial Security Program (NISIP)*.

-- Also, a multi-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry. (IC Standard 700-1, 4 Apr 2008)

In Extremis. A situation of such exceptional urgency that immediate action must be taken to minimize imminent loss of life or catastrophic degradation of the political or military situation. (JP 1-02 & JP 3-05)

Infiltrate. Tradecraft jargon for the act of penetrating a country or organization. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Infiltration. In intelligence usage, placing an agent or other person in a target area in hostile territory. Usually involves crossing a frontier or other guarded line. Methods of infiltration are: black (clandestine); grey (through legal crossing point but under false documentation); and white (legal). (JP 1-02)

Informant. A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. (ICS Glossary)

Information. Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1)

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 1-02 and DoDD 8500.01E, Information Assurance)

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009).

-- Also, the protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA is a security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST). (AR 25-2, Information Assurance, 3 Aug 2007)

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02 and JP 3-13)

Information Operations (IO). The integrated employment... of information-related capabilities in concert with other lines of operations to influence, corrupt, disrupt, or usurp the decision-making of adversaries and potential adversaries, while protecting our own. (SECDEF memo, subj: Strategic Communication and Information Operations in the DoD, 25 Jan 2011)

-- Also, the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02 and JP 3-13)

Core IO Capabilities: IO employs five core capabilities to achieve desired effects or prevent enemy from achieving his desired effects: EW, CNO, PSYOP, MILDEC, and OPSEC. Supporting capabilities include: Counterintelligence investigations, operations, collection, analysis, production, and dynamic functional CI services will be employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.

-- DoDD 3600.01, *Information Operations*, 14 Aug 2006

Information Requirements. In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 2-0, Joint Intelligence) Also see *intelligence requirement*; *collection requirement*.

The requirements process has traditionally been one of the most vexing aspects of intelligence management.

-- IC 21: HPSCI Staff Study, 6 Apr 1996

Information Security (INFOSEC). The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of computer security and communications security. (JP 1-02 & JP 3-13) Also see *computer security*; *cyber security*.

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009)

INFOSEC plays a vital role in national security and in the Critical Infrastructure

The goal of INFOSEC is to ensure that the National Security Community has reliable and secure networks to originate, store, manipulate, and make information available to those who need it and are authorized to have it.

-- Joint Security Commission II Report, 24 Aug 1999, p. 18

Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02 & JP 3-13) Also see *information operations*.

Initial Contact Point (ICP). A physical location where an intelligence officer makes an initial contact or brush pass with his source or asset. (AFOSI Manual 71-142, 9 Jun 2000)

Insider. Any person with authorized access to any U.S. Government (USG) resource, to include personnel, facilities, information, equipment, networks, or systems. (National Insider Threat Working Group, Dec 2010)

-- Also, anyone with access, privilege, or knowledge of information systems or services. Malicious insider is [a person] motivated to intentionally adversely impact an organization's mission (e.g., deny, damage, degrade, destroy). (Rand Study, *Understanding the Insider Threat*, March 2004)

Insider Threat. A person, known or suspected, who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt, operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the threat that an insider will use their authorized access to cause harm to the security of the United States. This threat can include damage to the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities. (National Insider Threat Working Group, Dec 2010) Also see *Counterintelligence Insider Threat*.

-- Also, acts of commission or omission, by an individual working for or on behalf of DoD, that intentionally or unintentionally compromise DoD's ability to accomplish its mission. Insider threats include, but are not limited to espionage, other criminal activity, unauthorized disclosure of information, and loss or degradation of DoD resources or capabilities. (*Draft DoDI 5240.n*, Countering Espionage)

-- Also, acts of commission or omission, by an insider, that intentionally or unintentionally compromise the DoD's ability to accomplish its mission. Insider Threats include, but are not limited to, espionage, other criminal activity, unauthorized disclosure of information, and loss or degradation of departmental resources or capabilities. (DoD CI Strategy FY 2008-2013)

-- Also, activities conducted by a person with placement and access that intentionally or unintentionally compromise an agency's ability to accomplish its mission, including but not limited to espionage, other criminal activity, unauthorized disclosure of information and loss or degradation of departmental resources or capabilities. (National CI Strategy Operating Plan 2008-2010, 9 Aug 2007)

-- Also, the ability of a trusted insider to bypass or defeat security safeguards or otherwise adversely affect the national security. (IC Standard 700-1, 4 Apr 2008)

-- Also, a person with placement and access who intentionally or unintentionally causes loss or degradation of resources or capabilities and compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, other criminal activity, or unauthorized release or disclosure of information. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, any insider with legitimate access to government information, personnel, and facilities may intentionally or unintentionally pose a threat. (NSA CI Awareness Pamphlet on Insider Threat, undated)

Trusted insiders with means, motive, and opportunity pose a major threat

"[H]istory teaches us to expect spies among us and to anticipate that some of those spies will be us.... [W]e cannot eliminate espionage... [but we must] minimize the harm that those who betray us can do to our national security and minimize the time between their defection and detection."

-- Webster Commission Report (A Review of FBI Security Programs), March 2002, pp. 17-18.

"The Insider Threat is the single-most pervasive and damaging security risk facing global organizations and governments today." -- www.intrusic.com

"...the threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals cover a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate."

-- T. Noonan and E. Archuleta, *The Insider Threat to Critical Infrastructures*, The National Infrastructure Advisory Council, April 6, 2008, p. 32.

Additional open source information on insider threat issues at http://www.cert.org/insider_threat/

***"A nation can survive its fools and even the ambitious.
But it cannot survive treason from within."***

-- Cicero (106-43 B.C.)

Insurgency. An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. (JP 1-02 & JP 3-24)

Insurgent. See *insurgency*.

Integrated Defense Source Registration System (IDSRS). A DoD-level system to enable the sharing of HUMINT source information, meant to ensure Deconfliction of DoD-wide HUMINT sources. (Defense HUMINT Enterprise Manual, Vol II, 23 Nov 2010)

See classified USD(I) Memorandum, dated 13 August 2005 and the IDSRS website on SIPRNet at: <http://dh.dia.smil/idsr/>

Intelligence. The product resulting from the collection, analysis, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 1-02 and JP 2-0, Joint Intelligence) Also see *foreign intelligence*; *counterintelligence*.

"Timely intelligence is a critical component of preserving our national security."

-- Ambassador John D. Negroponte (12 April 2005)

A plethora of definitions for intelligence

Sherman Kent, former Chairman of CIA's Office of National Estimates asserted that intelligence can be thought of as a process, a product, as well as an organization. His point is valid, as organizations that make up the US Intelligence Community use the term "intelligence" in three different ways:

- 1) Intelligence is a **product** that consists of information that has been refined to meet the needs of policymakers/decision makers;
- 2) Intelligence is also a **process** through which that information is identified, collected, Analyzed, and disseminated; and
- 3) Intelligence refers to both the individual **organizations** that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations collected referred to as the Intelligence Community or IC.

"Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities."

-- Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. 4th Edition (2009), p. 8

"By definition, intelligence deals with the unclear, the unknown the deliberately hidden.... In the intelligence business, you are almost never completely wrong or completely right."

-- George J. Tenet, Director CIA (5 Feb 2004)

"The truth is that there is never enough good intelligence."

-- R. Jack Smith (Former DDI CIA), *The Unknown CIA* (1989)

-- Also, the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 10)

-- Also, a body of evidence and the conclusions drawn there from that is acquired and furnished in response to the known or perceived requirements of Consumer's. It is often derived from information that is concealed or not intended to be available for use by the acquirer. (ODNI website www.dni.gov)

-- Also, information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security. (FBI at <http://www.fbi.gov/about-us/intelligence/defined>)

-- Also, secret, state activity to understand or influence foreign entities. (Michael Warner, "Wanted: A definition of Intelligence," *Studies in Intelligence*, 46: 3 (2002), pp.15-22)

The term "intelligence" includes foreign intelligence and counterintelligence.

-- National Security Act of 1947 (as amended), 50 USC §401a, and EO 12333 (as amended 30 Jul 2008)

The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).

Intelligence Activities. The collection, production and dissemination of foreign intelligence and counterintelligence pursuant to DoDD 5143.01 and EO 12333. (DoDD 5240.01, 27 Aug 2007)

-- Also, all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (DoD 5240.1-R, Dec 1982)

-- Also, all activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (EO 12333, as amended 30 Jul 2008)

EO 12333 specifically defines *intelligence* as foreign intelligence and counterintelligence.

Intelligence Collection. The acquisition of information or intelligence information and the provision of it to processing and/or production elements. (CI Community Lexicon) Also see *counterintelligence collection*; *clandestine intelligence collection*; *intelligence collection*.

The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).

Intelligence Collection Activities. The collection of foreign intelligence and counterintelligence information. (Title 10 USC §431)

Intelligence Collection Plan. A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit. (JP 1-02)

Intelligence Collector. A phrase sometimes used to refer to an individual, system, organization or agency that engages in the collection step of the intelligence cycle. (ICS Glossary)

Intelligence Community (IC). All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 1-02)

-- Also, the federal agencies and departments that have a legal mandate to collect, analyze, and disseminate intelligence. Executive Order 12333 specifically identifies members of the IC. (CI Community Lexicon)

-- Also, a group of executive branch agencies and organizations that work separately and together to engage in intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. (National Intelligence: A Consumer's Guide - 2009)

U.S. Intelligence Community (50 USC §401a and EO 12333):

- Office of the Director of National Intelligence
- Central Intelligence Agency
- National Security Agency
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- Intelligence & CI components of the U.S. Army, Navy, Marines, and Air Force
- Federal Bureau of Investigation (National Security Branch)
- Department of Energy (Office of Intelligence & Counterintelligence)
- Drug Enforcement Administration (Office of National Security Intelligence)
- Department of Homeland Security (Office of Intelligence & Analysis)
- Department of State (Bureau of Intelligence & Research)
- Department of Treasury (Office of Intelligence & Analysis)
- Intelligence & CI components of the Coast Guard

For additional information see "An Overview of the United States Intelligence Community" at <http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf>

Intelligence Community Directives (ICDs). Principal issuances through which the Director of National Intelligence (DNI) provides policy direction to the Intelligence Community (IC). (ICD 1, 1 May 2006)

ICDs are overarching policy documents of the Intelligence Community signed by the DNI and are replacing the legacy Director of Central Intelligence Directives (DCIDs).

Intelligence Contingency Funds (ICF). Appropriated funds to be used for intelligence activities when the use of other funds is not applicable or would either jeopardize or impede the mission of the intelligence unit. (JP 1-02 and JP 2-01)

Intelligence Cycle. The process by which information is acquired, converted into intelligence, and made available to policymakers and Consumer's. (National HUMINT Glossary) Also see *intelligence process*.

-- Also, the process of developing raw information into finished intelligence for Consumer's to use in decision making and action. (National Intelligence: A Consumer's Guide - 2009)



INTELLIGENCE CYCLE

Source: CIA. Also see *National Intelligence: A Consumer's Guide – 2009*, pp 16-19.

The Intelligence Cycle is customarily illustrated as a repeating process consisting of five steps [see graphic above].

- [1] **Planning and direction** encompasses the management of the entire effort and involves, in particular, determining collection requirements based on customer requests.
- [2] **Collection** refers to the gathering of raw data to meet the collection requirements. These data can be derived from any number and type of open and secret sources.
- [3] **Processing** refers to the conversion of raw data into a format analysts can use.
- [4] **Analysis and production** describes the process of evaluating data for reliability, validity, and relevance; integrating and analyzing it; and converting the product of this effort into a meaningful whole, which includes assessments of events and implications of the information collected.
- [5] [**Dissemination**] the product is disseminated to its intended audience.

-- Judith Meister Johnston and Rob Johnston., Chapter Four – "Testing the Intelligence Cycle Through Systems Modeling and Simulation," in *Analytic Culture in the U.S. Intelligence Community*, The Center for the Study of Intelligence, CIA, 2005, pp 45-46.

-- Also, the process of developing unrefined data into polished intelligence for the use of policymakers. The graphic below shows the circular nature of this process, although movement between the steps is fluid. Intelligence uncovered at one step may require going back to an earlier step before moving forward. (FBI at <<http://www.fbi.gov/about-us/intelligence/intelligence-cycle>>)



INTELLIGENCE CYCLE

Source: FBI

-- Also, an iterative process [see graphic below] in which collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of customers. Consumers sometimes provide feedback on finished intelligence products, which can be used to refine any part of the intelligence cycle to ensure consumers are getting the intelligence they need to make informed decisions and/or take appropriate actions. (Congressional Research Report (CRS) Report RL33616, 14 Jan 2009)



The Intelligence Cycle – An Iterative Process

Note. The Army refers to the intelligence cycle as the “intelligence process” [see intelligence process].

Intelligence drives national security policies

The successful intelligence process converts acquired information into clear, comprehensible intelligence and delivers it to the President, policymakers, and military commanders in a form they can utilize to make educated policy decisions. Generating reliable, accurate intelligence is an active, never-ending process commonly referred to as the intelligence cycle.

The process begins with identifying the issues in which policy makers are interested and defining the answers they need to make educated decisions regarding those issues. We then lay out a plan for acquiring that information and go about collecting it. Once we have the proper intelligence, we sort through it, analyze what it means, and prepare summary reports and recommendations, which we deliver to national security policy makers. The answers our reports supply often reveal other areas of concern, which lead to more questions. In this way, the end of one cycle effectively leads to the start of the next.

-- Intelligence.Gov -- How Intelligence Works (accessed 28 April 2011)
<<http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/>>

Dynamic Process Fueling Dynamic Solutions

Intelligence Discipline. A well defined area of intelligence planning, collection, processing, exploitation, analysis and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, imagery geospatial intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), open-source intelligence, technical intelligence, and counterintelligence. (JP 1-02 & JP 2-0) Also see *human intelligence (HUMINT)*; *geospatial intelligence (GEOINT)*; *measurement and signature intelligence MASINT*; *signals intelligence (SIGINT)*; *open-source intelligence (OSINT)*; *technical intelligence (TECHINT)*; *counterintelligence (CI)*.

Intelligence Estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 1-02 & JP 2-0)

Intelligence Federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations. (JP 1-02 & JP 2-01)

Intelligence Gap. Information that is needed to inform intelligence analysis but is absent from reporting—*what we know we don't know*.

Intelligence Information Need. A need, expressed by users of intelligence, for information necessary to support their mission. (Intellipedia)

Intelligence Information Report (IIR). The primary vehicle used to provide HUMINT information to the consumer. It utilizes a message format structure that supports automated data entry into the Intelligence Community databases. (JP 1-02 & JP 2-01.2)

IIRs contain *raw intelligence*—unevaluated intelligence information, generally from a single source, that has not been fully evaluated, integrated with other information, or interpreted and analyzed.

-- Also, a report used to provide information of intelligence value collected generally via human sources to DoD and IC customers. The IIR utilizes a message format to support automated data entry into IC databases. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Intelligence Interrogation. The systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. (JP 1-02 & JP 2-01.2) Also see *educing information; elicitation; debriefing; interrogation; intelligence interviewing; interview.*

DoD Policy: No person in the custody or physical control of DoD or detained in a DoD facility shall be subject to cruel, inhuman, or degrading treatment or punishment as defined in title XIV of Public Law 109-163, also known as, "The Detainee Treatment Act of 2005." Acts of physical or mental torture are prohibited.

All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted humanely, in accordance with applicable law and policy, including Army FM 2-22.3 (Human Intelligence Collector Operations, 6 Sep 2006).

Intelligence interrogations and tactical questioning will be conducted only by personnel trained and certified IAW DoDD 3115.09. All DoD interrogations will operate using US Army Field Manual 2-22.3, *Human Intelligence Collection Operations.*

-- JP 2-01.2, *CI & HUMINT in Joint Operations (U)*, 16 Mar 2011, p. IV-9

For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 9 Oct 2008.

Also see *Interrogation: World War II, Vietnam, and Iraq* (Washington, DC: National Intelligence College, Sep 2008); available online at <<http://www.ndic.edu/press/12010.htm>>

Intelligence Interviewing. The [non-coercive] gathering of useful and accurate information by professionals questioning detainees. (Intelligence Science Board, *Intelligence Interviewing: Teaching Papers and Case Studies*, April 2009) Also see *educing information; elicitation; debriefing; interrogation; interview.*

See the 2009 Intelligence Science Board report, *Intelligence Interviewing: Teaching Papers and Case Studies*, available online at <www.fas.org/irp/dni/isb/interview.pdf> -- the emphasis of this report is on non-coercive intelligence interviewing.

This report may be of interest to the full range of intelligence professionals involved with interrogation and intelligence interviewing. In particular to those who focus on strategic interrogation and/or "high-value" detainees.

Intelligence Liaison. [Activity which] includes official contacts between a component of the US Intelligence Community and a foreign intelligence or security service which are directly related to espionage or counterintelligence, or other intelligence activities. (DCID 5/1P) Also see *liaison.*

Intelligence Officer (IO). A professionally trained member of an intelligence service. He or she may be serving in the home country or abroad as a member of a legal or illegal residency. (AFOSI Manual 71-142, 9 Jun 2000)

Intelligence Operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. Intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 & JP 2-01)

Note: Intelligence consists of two components: foreign intelligence (FI) and counterintelligence (CI). *Intelligence operations* is a broad term with broad application, whereas "CI operations" is a specific term with a precise application.

Intelligence Planning. The intelligence portion of Adaptive Planning and Execution (APEX). Intelligence planning provides a process that effectively integrates, synchronizes, prioritizes and focuses Defense intelligence (both Theater and National) on achieving the supported commander's operational objectives and desired effects during all phases of the plan. Additionally, the process identifies knowledge gaps and capability shortcomings within the DoD intelligence community (IC). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2008) Also see *Counterintelligence Functional Support Plan (CI FSP)*.

Note: the term "Intelligence Campaign Planning" or "ICP" is no longer in use; now referred to just as "intelligence planning."

Intelligence Planning Process. The intelligence component of Adaptive Planning. It is a process that integrates, synchronizes, prioritizes, and focuses DoD Intelligence (both theater and national) on achieving the supported commander's operational objectives and desired effects during all phases of an OPLAN or concept plan. Additionally, the process identifies knowledge gaps and capability shortfalls within DoD Intelligence. (DoDI 5105.21, DIA, 18 Mar 2008)

Intelligence Preparation of the Battlespace (IPB). The analytical methodologies employed by the Services or joint force component commands to reduce uncertainties concerning the enemy, environment, time, and terrain. Intelligence preparation of the battlespace supports the individual operations of the joint force component commands. (JP 2-01.3)

Intelligence Process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 & JP 2-01) Also see *intelligence cycle*.

-- Also, the Army refers to the intelligence cycle as the "intelligence process," which it defines as: intelligence operations are conducted by performing four steps that constitute the intelligence process: Plan, Prepare, Collect, and Produce. Additionally, there are four continuing activities that occur across the four intelligence process steps: Generate intelligence knowledge, Analyze, Assess, and Disseminate. (See Chapter 4, "Intelligence Process in Full Spectrum Operations," Army FM 2-0, Intelligence, Mar 2010)

Intelligence Processing. Conversion of collected information and/or intelligence into a form more suitable for the production of intelligence. (CI Community Glossary and ICS Glossary)

Intelligence Product. An intelligence report disseminated to customers by an intelligence agency or element. The report contains information and/or analysis of potential intelligence value to meet the intelligence needs of users within and outside the Intelligence Community. It may involve current or future developments or capabilities, intentions, and activities of entities of interest. (ICD 208, 17 Dec 2008)

Intelligence Production. Conversion of material into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements. (CI Community Glossary and ICS Glossary) Also see *production*.

Intelligence Reach. A process by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command. (Army FM 2-0, Intelligence, 23 Mar 2010)

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). An act to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes. IRTPA established both the position of Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC). (PL 108-458, 17 Dec 2004)

Link to the IRTPA: <<http://www.ncix.gov/publications/law/index.html>>

Intelligence-Related Activities. Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02 and JP 2-01)

Intelligence Report (INTREP). A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. (JP 1-02)

-- Also, a product of the production step of the intelligence cycle. (ICS Glossary)

Intelligence Reporting. The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. (JP 1-02)

Intelligence Requirement. 1) Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence; or 2) A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace operational environment or threat forces. (JP 1-02 & JP 2-0, Joint Intelligence) Also see *information requirements; collection requirement*.

The articulation of the requirement is the most important part of the process, and it seldom is as simple as it might seem.

– DIA, *Intelligence Essentials for Everyone*, June 1999

-- Also, [intelligence] requirement: a general or specific validated request for intelligence information made by a user. (National HUMINT Glossary)

-- Also, a type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. (Army FM 2-0, Intelligence, 23 Mar 2010)

Intelligence Source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors. (JP 1-02)

Intelligence Sources and Methods. 1) *Sources*: Persons, images, signals, documents, data bases, and communications media capable of providing intelligence information through collection and analysis programs, e.g., HUMINT, IMINT, SIGINT, and MASINT; and 2) *Methods*: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources and methods are disclosed without authorization their effectiveness may be substantially negated or impaired. (IC Standard 700-1, 4 Apr 2008)

The terms "intelligence sources and methods" are used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence (DNI).

Intelligence, Surveillance, and Reconnaissance (ISR). An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations; this is an integrated intelligence and operations function. (JP 1-02, JP 2-01 & DoDD 5143.01)

Intelligence Task List (ITL). A compilation of the specified and implied intelligence tasks required to satisfy the information needs to support the successful achievement of the Combatant Command's operational objectives. The ITL is developed by the Combatant Command J2 and Defense Intelligence Operations Coordination Center (DIOCC). Assignment of roles and responsibilities for the specific collection, analysis and production is accomplished during the development of the [COCOM's IPLAN] and the NISP. The end state is a synchronized collection, analysis and production effort, from tactical to national level that will support the successful achievement of the Combat Command's operational objectives. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Intelligence Threat. The intention and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S program, operations, or industrial activity. (IOSS Intelligence Threat Handbook - Jun 2004) Also see *threat; threat to national security; transnational threat; foreign intelligence collection threat*.

INTELINK. INTELINK is the classified, worldwide intranet for the U.S. Intelligence Community. At its most secure level, INTELINK utilizes the Joint Worldwide Intelligence Communications System (JWICS) as its communication vehicle. JWICS is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide up to the Top Secret/SCI level.

INTELINK-S. INTELINK-S is similar to INTELINK except that it is accessed through the Secret Internet Protocol Router Network (SIPRNet). It is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide at the Secret level and below.

Interagency. United States Government agencies and departments, including the Department of Defense. (JP 1-02 & JP 3-08) Also see interagency coordination.

Interagency Coordination. Within the context of DoD involvement, the coordination that occurs between elements of DoD, and engaged US Government agencies, nongovernmental organizations, and regional and international organizations for the purpose of accomplishing an objective. (JP 1-02 & JP 3-0)

Interdiction. An action to divert, disrupt, delay, or destroy the enemy's military potential before it can be used effectively against friendly forces, or to otherwise achieve objectives. (JP 1-02)

Interdiction. 1) An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives; and 2) In support of law enforcement, activities conducted to divert, disrupt, delay, intercept, board, detain, or destroy, as appropriate, vessels, vehicles, aircraft, people, and cargo. See also air interdiction. (JP 1-02 & JP 3-03)

Intergovernmental Organization (IGO). An organization created by a formal agreement (e.g., a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. Formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. (JP 1-02 & JP 3-08)

-- Also, an organization comprised primarily of sovereign states (referred to as member states), or of other IGOs. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Internal Security. The state of law and order prevailing within a nation. (JP 1-02)

International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum. (DoD 5240.1-R, 7 Dec 1982)

International Terrorism. Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state. Local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national borders in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

INTERPOL. The world's largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. (www.interpol.int/)

INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits 'any intervention or activities of a political, military, religious or racial character.'

Interpretation. A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. (JP 2-0, Joint Intelligence)

Interrogation. Systematic effort to procure information by direct questioning of a person under the control of the questioner. (JP 1-02) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interview.*

An overt human intelligence (HUMINT) collection method.

-- Also, interaction and conversation with a source who appears initially unwilling to provide information. (Educing Information – Interrogation: Science and Art, Dec 2006)

-- Also, systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006 and FM 2-0, Intelligence, 23 Mar 2010)

-- Also, a methodology employed during the interview of a person to obtain information that the source would not otherwise willingly disclose. A typical purpose is not necessarily to force a confession, but rather to develop, playing on the source's character, sufficient rapport as to prompt the source to disclose information valuable to the interrogator. (Wikipedia, accessed 1 Aug 2007)

Within DoD: Intelligence interrogation is the systematic process of using approved techniques, consistent with applicable law, to question a captured or detained person to obtain reliable information responsive to intelligence requirements. Interrogation is considered an overt HUMINT collection method but is regulated separately from other DoD HUMINT activities.

For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogation, Detainee Debriefings, and Tactical Questioning*, 9 Oct 2008. Army FM 2-22-3 available online at: <<http://www.fas.org/irp/doddir/army/fm2-22-3.pdf>>

Interview. [In intelligence usage,] to gather information from a person who is aware that information is being given although there is ignorance of the true connection and purposes of the interviewer. Generally overt unless the collector is other than purported to be. (JP 1-02) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interrogation.*

-- Also, a dynamic human interaction to collect facts to be used for decision-making and/or action-taking. Interviewing is the gathering of facts/information; it is non-accusatory and less structured than an interrogation.

-- Also, a conversation between two or more people (the interviewer and the interviewee) where questions are asked by the interviewer to obtain information from the interviewee. Interviews can be divided into two rough types, interviews of assessment and interviews for information. (Wikipedia)

Intrusion. [In cyber usage], unauthorized access to a DoD, DIB [defense industrial base], or critical infrastructure network, information system, or application. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010)

Investigation. Investigation is the process of inquiring into a matter through research, follow-up, study, or formal procedure of discovery. (Wikipedia, accessed 1 Aug 2007) Also see *counterintelligence investigation.*

-- Also, the systematic inquiry into an allegation of unfamiliar or questionable activities, wherein evidence is gathered to substantiate or refute the allegation or questionable activity. An investigation is initiated when there are articulable facts that indicate a possible violation of law or policy. Some investigations may be conducted unilaterally by an agency (depending on their authorities), jointly with an external investigate body, or referred to an external investigate body for unilateral investigation. (ONCIX Insider Threat Detection – Glossary)

Investigative Jurisdiction. Term for the jurisdiction of an investigative agency over a particular crime or over the locus of where the crime was committed. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Investigative Lead. A person who possesses information about or was a witness to an incident under investigation or a record which contains information of value to the investigation. (AR 381-20, Army CI Program, 25 May 2010) Also see *lead.*

Investigative Plan (IP). Detailed plan for the conduct of a counterintelligence investigation to ensure that all investigative activity is conducted in a properly sequenced, coordinated, coherent, timely and efficient manner; it also serves as the primary means for the technical oversight and command chain to monitor and influence the investigation. The lead special agent uses the IP to plan and integrate the activities of all elements conducting the investigative activity in furtherance of a CI investigation.

-- Also, a document used to plan proposed investigative activities, including special investigative techniques, to support counterintelligence investigation. (Army FM 2-22.2, CI, Oct 2009)

CI investigations will vary in scope, objective, and resources to successfully resolve the incident under investigation. The IP is the document that provides a detailed road map on the conduct of CI investigations including all investigative participants, all investigative activities required, all resources and external support required, and all interagency or legal coordination required to successfully resolve the incident. IPs are living documents and may require revision due to information development and case direction. – Army FM 2-22.2, *Counterintelligence* (2009)

Irregular Warfare. A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. (DoD 3000.07, Irregular Warfare, 1 Dec 2008)

-- Also, (Army) A violent struggle among state and nonstate actors for legitimacy and influence over a population. (Army FM 3-0, Operations, Feb 2008)

J-2X. The staff element of the intelligence directorate of a joint staff that combines and represents the principal authority for counterintelligence and human intelligence support. (JP 1-02) Also see 2X.

-- Also, a J-2 staff element normally associated with a deployed joint force, consisting basically of the HUMINT operations cell (HOC) and the task force counterintelligence coordinating authority (TFCICA), and the Operational Support Element (OSE). The J-2X is responsible for coordination and deconfliction of all human source-related activity. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

J-Space. An abbreviation for Joint Space. A virtual work environment that equips National and Strategic Intelligence producers and Consumer's with tools that speed discovery and exploitation of data and expertise, techniques that enhance collaboration, and technologies and business processes that optimize the community's collective strengths. It provides mission focused collaboration groups from across the Intelligence Community a common platform to work common problem sets. (Intellipedia, accessed 22 Oct 2010) Also see *A-Space*.

Jack-in-the-Box (JIB). A dummy—sometimes inflatable—placed in a car to deceive [surveillance] about the number of persons in the vehicle. (Spy Book)

“A three-dimensional human torso sitting atop a spring-activated scissor-lift mechanism fitted with a rotating head, which collapse[s] into a small portable briefcase or duffel bag. “ Can be used to effectively elude surveillance by “controlling the location of the event (an empty street...), the lighting (an unlit area), the audience (the trailing surveillance car), the timing (when the cars were a sufficient distance apart), and the sight line (visible only from the rear).”

-- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)

“It is used in an automobile to evade surveillance, by deceiving (a) surveillant(s) that a person being tailed is still in the automobile, when, in fact, the jib has replaced him or her. The FBI was allegedly thus deceived while staking out Edward Lee Howard, the former CIA case officer who escaped and subsequently defected to the former USSR. “

-- Leo D. Carl, *The CIA Insider's Dictionary* (1996), p. 319

Jihad. Arabic word derived from a verb that means “to struggle, strive, or exert oneself.” Violent Islamists’ understand the concept *jihad* as a “religious call to arms.” Also see *jihadist*.

Historically, key Sunni and Shia religious texts most often referred to *jihad* in terms of religious approved fighting on behalf of Islam and Muslims. Most Al Qaeda-produced ideological material reflects Al Qaeda supporters’ shared view of *jihad* as an individual duty to fight on behalf of Islam and Muslims, and, in some case, to offensively attack Muslims and non-Muslims who are deemed insufficiently pious or who oppose enforcement of Islamic principles and religious law.

The terms *jihadist*, *violent Islamist*, and *militant Islamist* refer to groups and individuals whose statements indicate that they share such an understanding of *jihad* and who advocate or use violence against the United States or in support of transnational Islamist agendas.

-- Congressional Research Service (CRS) Report R41674, 8 Mar 2011 (www.crs.gov)

Jihadist. Term describes radicalized individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph. (CRS Report R41416, 7 Dec 2010)

Jihadists draw on Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and following the model of the immediate followers and companions of the Prophet Muhammad.

The CRS Report points out there is an important distinction between the terms “radicalization” and “violent extremism” as it relates to the threshold of U.S. law enforcement interest and action. This is because Americans have the right under the First Amendment to adopt, express, or disseminate

ideas, even hateful and extremist ones. But when radicalized individuals mobilize their views, i.e., they move from a radicalized viewpoint to membership in a terrorist group, or to planning, materially supporting, or executing terrorist activity, then the nation's public safety and security interests are activated. Thus, the terms may be differentiated as follows:

- "Radicalization" describes the process of acquiring and holding radical, extremist, or jihadist beliefs.
- "Violent extremism" describes violent action taken on the basis of radical or extremist beliefs. For many, this term is synonymous with "violent jihadist" and "jihadist terrorist."

The term "violent jihadist" characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity.

See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*. For more on Salafi Islam, see CRS Report RS21695, *The Islamic Traditions of Wahhabism and Salafiyya*.

For more on Al Qaeda's global network, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*.

JITF-CT. See *Joint Intelligence Task Force-Combating Terrorism*.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP 1-02)

Joint Captured Materiel Exploitation Center (JCMEC). A physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the Joint Force/J-2. (JP 1-02)

Joint Counterintelligence Unit (JCIU). An organization composed of Service and Department of Defense agency counterintelligence personnel, formed under the authority of the Secretary of Defense and assigned to a combatant commander, which focuses on the combatant command strategic and operational counterintelligence missions. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, an organization composed of Service and Defense agency CI personnel, formed under the authority of a Secretary of Defense-approved operation order, which focuses on combatant command strategic and operational CI missions within an area of conflict. This unit is under the combatant command authority of the Combatant Commander, or his or her duly designated subordinate joint force commander, for the duration of the operation, or as otherwise specified in the operation plan or order. (DoDI S-5240.09, OFCO, 29 Oct 2008)

For more detailed discussion of the JCIU see Appendix B, Joint Counterintelligence Unit (U), JP 2-01.2, CI & HUMINT in Joint Operations (U), 11 Mar 2011.

Joint Doctrine. Fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

Joint Document Exploitation Center (JDEC). A physical location for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force intelligence directorate. (JP 1-02 and JP 2-01.2, CI and HUMINT in Joint Operations, 11 Mar 2011)

-- Also, a joint center established to receive, inventory, catalogue, selectively translate, and disseminate captured or acquired documents and media. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Joint Intelligence. Intelligence produced by elements of more than one Service of the same nation. (JP 1-02 & JP 2-0)

Joint Intelligence Operations Center (JIOC). An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. (JP 1-02 & JP 2-0, Joint Intelligence)

-- Also, those centers, below the Defense-level (COCOM and specified Unified Commands) established by the Secretary of Defense on 3 April 2006, to plan, prepare, integrate, direct, synchronize, and manage continuous, full-spectrum defense intelligence operations within their respective AORs. The J2 of each command is designated as the respective JIOC Director. (DIA HUMINT Manual, Vol I, DHE-M 3301.001, 30 Jan 2009)

Joint Intelligence Preparation of the Operational Environment (JIPOE). The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action. (JP 1-02 & JP 2-01.3)

Joint Intelligence Support Element (JISE). A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. (JP 1-02 & JP 2-01)

Joint Intelligence Task Force-Combating Terrorism (JITF-CT). A consolidated all-source intelligence fusion center focused on warning, threat assessment, options development, and operational intelligence support to the DoD campaign against international terrorism. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

-- Also, DIA's office of primary responsibility for intelligence production on terrorist groups posing a threat to U.S. and DoD interests around the world, and on host-nation counterterrorist (CT) forces. (DIA Instruction 5240.002, 15 Jun 2005)

JITF-CT is DoD's all-source national-level intelligence fusion center responsible for enabling DoD counterterrorism and force protection operations. JITF-CT analytical assessments address terrorist capabilities, activities and intentions, including terrorist finance activity.

The Office of Counterintelligence (DXC), Defense Counterintelligence & HUMINT Center (DCHC) focuses on the intelligence apparatus and intelligence activities of international terrorists. In instances where the two missions intersect, JITF-CT and DXC / DCHC collaborate and coordinate to ensure that DIA presents a timely, accurate, and consistent picture of the threat to U.S. forces and interests around the world.

Joint Intelligence Training (JIT). Fundamental training that guides the development and utilization of intelligence professionals and organizations designed to support two or more Services employed in coordinated action. (DoDI 3305.14, JIT, 28 Dec 2007)

Joint Inter-Agency Cyber Task Force (JIACTF). Joint inter-agency task force created by the Director of National Intelligence (DNI) to execute DNI responsibilities in monitoring and coordinating the CNCI and to report to the President on Comprehensive National Cybersecurity Initiative (CNCI) implementation, together with recommendations as deemed appropriate. (Securing Cyberspace for the 44th Presidency, Dec 2008)

Joint Interrogation and Debriefing Center (JIDC). Physical location for the exploitation of intelligence information from detainees and other sources. (JP 1-02 & JP 2-01.2)

JIDCs are established under the direction of the joint force commander within the joint operations area and are normally collocated with detainee holding facilities. The mission of the JIDC is to conduct screening and interrogation of detainees, questioning of walk-in sources, and translation and exploitation of documents associated with detainees. The JIDC coordinates exploitation of captured equipment with the joint captured material exploitation center, captured documents with the joint document exploitation center, and high-value human sources with the joint strategic exploitation center.

-- For additional information see JP 3-63, *Detainee Operations*, 6 Feb 2008

Joint Interrogation Operations (JIO). 1) Activities conducted by a joint or interagency organization to extract information for intelligence purposes from enemy prisoners of war, dislocated civilians, enemy combatants, or other uncategorized detainees; or 2) Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against US persons or property. (JP 1-02 & JP 2-01)

Joint Investigation. An investigation in which more than one investigative agency has established investigative authority over an offense and/or subject of the investigation, and the agencies involved agree to pursue the investigation in concert, with agreements reached detailing investigative responsibilities, procedures, and methods. (CI Community Lexicon)

Joint Force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (JP 1-02)

Joint Operational Planning. Planning activities [of] associated joint military operations by combatant commanders and their subordinate joint force commanders in response to contingencies and crises. Joint operations planning includes planning for the mobilization, deployment, employment, sustainment, redeployment, and demobilization of joint forces. (JP 5-0, Joint Planning, 26 Dec 2006)

Joint Operation Planning and Execution System (JOPES). A system of joint policies, procedures, and reporting structures, supported by communication and computer systems, that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. (JP 5-0, Joint Planning, 26 Dec 2006)

Joint Operation Planning Process (JOPP). An orderly, analytical process that consists of a logical set of steps to analyze a mission; develop, analyze, and compare alternative courses of action against criteria of success and each other; select the best course of action; and produce a joint operation plan or order. (JP 5-0, Joint Planning, 26 Dec 2006)

Joint Operations. A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not establish joint forces. (JP 1-02 & JP 3-0)

Joint Personnel Adjudication System (JPAS). The centralized database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations. (IC Standard 700-1, 4 Apr 2008)

-- Also, JPAS is DoD's automated system of record for recording and providing personnel security eligibility and access information for DoD government, military and contractor personnel. JPAS consists of two systems: the Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS). JAMS provides Central Adjudication Facilities (CAFs) with a single, integrated information system to record individual security clearance eligibility information; it assists the adjudication process by consolidating and disseminating timely and accurate personnel security

information. JCAVS provides DoD security personnel the ability to access and update personnel security clearance and access information in order to ensure the reciprocal acceptance of clearances throughout DoD and among the National Industrial Security Program members. (JPAS Fact Sheet, DSS, Jan 2008)

Joint Personnel Recovery Center (JPRC). The primary joint force organization responsible for planning and coordinating personnel recovery for military operations within the assigned operational area. (JP 1-02)

Joint Strategic Capabilities Plan (JSCP). The JSCP provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. It apportions resources to combatant commanders, based on military capabilities resulting from completed program and budget actions and intelligence assessments. The JSCP provides a coherent framework for capabilities-based military advice provided to the President and Secretary of Defense. (JP 1-02 & JP 5-0)

-- Also, the JSCP provides strategic guidance, establishes requirements, and apportions resources to the Combatant Commanders and Service Chiefs to accomplish tasks and missions based on near-term military capabilities. (CJCSI 3100.01A, Joint Strategic Planning System, 1 Sep 1999)

Joint Strategic Exploitation Center (JSEC). Theater-level physical location for an exploitation facility that functions under the direction of the joint force commander and is used to hold detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the United States, its citizens or interest, or US allies. (JP 1-02)

The JSEC is a theater-level exploitation facility and is normally collocated with a rear area collection and holding center for detainees. The JSEC's mission is the conduct of interrogations and debriefings to generate intelligence information responsive to theater and national requirements, and to identify detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the United States, its citizens or interests, or US allies.

Joint Task Force (JTF). A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. (JP 1-02)

Joint Task Force Counterintelligence Coordinating Authority. See *Task Force Counterintelligence Coordinating Authority (TFCICA)*.

Joint Terrorism Task Forces (JTTFs). Small cells of highly trained, locally based, investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. (DoJ website: <<http://www.usdoj.gov/jtff/>>) Also see *National Joint Terrorism Task Force*.

-- Also, FBI-led multi-organization task forces composed of local, state, and federal entities. They were established by the FBI to conduct operations to predict and disrupt terrorist plots. JTTFs are in over 100 cities nationwide; in addition, there is at least one in each of the FBI's 56 field offices. The National Joint Terrorism Task Force (NJTTF), in Washington, D.C., coordinates all the JTTFs. (National Intelligence: A Consumer's Guide - 2009)

Joint Worldwide Intelligence Communications System (JWICS). The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (JP 1-02 & JP 2-0)

-- Also, the Intelligence Community's TS-SCI global network; a communications network that delivers secure information services to national and defense intelligence components around the world. All U.S. Government TS-SCI networks run off of JWICS. (National Intelligence: A Consumer's Guide - 2009)

Judgment. [As used in intelligence analysis] Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known into the uncertain. Judgment is an integral part of all intelligence analysis. (*Psychology of Analysis* by Richard J. Heur, Jr, 1999)

Key Enabler. That crucial element that supplies the means, knowledge, or opportunity that allows for the success of an assigned task or mission. (USJFCOM Glossary)

Knowledge. In the context of the cognitive hierarchy, information analyzed to provide meaning and value or evaluated as to implications for the operation. (FM 6-0, Mission Command).

Knowledge Management. The art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decisionmaking. (Army FM 3-0, Operations, Feb 2008)

Knowledgeability Brief (KB). A document used to notify consumers of the availability and background of an overt source for debriefing. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Laser Intelligence (LASINT). Technical and geo-location intelligence derived from laser systems; a subcategory of electro-optical intelligence. (JP 1-02 & JP 2-0) Also see *electro-optical intelligence*.

Laundering. In counterdrug operations, the process of transforming drug money into a more manageable form while concealing its illicit origin. Foreign bank accounts and dummy corporations are used as shelters. (JP 1-02 & JP 3-07.4)

Law Enforcement. Activities to protect people, places and things from criminal activity resulting from non-compliance with laws, includes patrols, emergency responses, undercover operations, arrests, raids, etc.

-- Also, agency of a community or government that is responsible for maintaining public order and preventing and detecting crime; preserving order by enforcing rules of conduct or laws. (encarta.msn.com)

Counterintelligence is part art, part science, a discipline aimed at identifying and exploiting or stopping foreign spies. Law enforcement is easier: You identify the bad guys and arrest them.

-- Bill Gertz, "Enemies," *The Washington Times*, 18 Sep 2006

Law Enforcement is police work waging a war against crime—it's *evidence-prosecution centric*. Whereas counterintelligence is national security work waging a war against foreign intelligence threats—it's *information-exploitation centric*.

Each operates in fundamentally dissimilar manners... *different legal authorities, oversight structures, governing paradigms, cultures, etc.* These two disciplines merge or intersect when hidden intelligence activity is also criminal, i.e., national security crimes (espionage, treason, spying, etc.).

"Effective enforcement of U.S. espionage statutes and Articles 104 and 106 of the Uniform Code of Military Justice is essential to national security.... Services have different approaches to counterintelligence due to their unique missions.... NCIS and AFOSI counterintelligence doctrine holds that counterintelligence primarily is a law enforcement issue. ...under Army counterintelligence doctrine, counterintelligence is, first and foremost, an intelligence mission.... Considerable intersection exists between law enforcement, counterintelligence, and intelligence in the areas of espionage, terrorism, and low-intensity conflict.... The law enforcement, counterintelligence, and intelligence collection disciplines must complement one another."

-- "Report of the Advisory Board on the Investigative Capability in the Department of Defense - Vol. I," Department of Defense, January 1995, pp. 67-75.
Copy available online at: <http://handle.dtic.mil/100.2/ADA299523>

The goals of law enforcement and intelligence collection conflict...

"Law enforcement agencies collect information solely to put criminals in prison—a onetime, short-term goal; pay the informant, make a bust, go to trial with the informer as witness. Espionage is conducted for long-term production of intelligence: recruit the agent, collect the information, hopefully for years or decades."

-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 409

Law Enforcement Agency (LEA). Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the following jurisdictions: The United States, a state (or political subdivision) of the United States, a territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation. (JP 1-02 & JP 3-28)

Law Enforcement Officer. An employee, the duties of whose position are primarily the prevention, investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws, including an employee engaged in this activity who is transferred to a supervisory or administrative position; or serving as a probation or pretrial services officer. (Cited as 18 USC at <<http://www.lectlaw.com/def/I008.htm>>)

Law of War. That part of international law that regulates the conduct of armed hostilities. Also called the law of armed conflict. (JP 1-02)

Lead. In intelligence usage, a person with potential for exploitation, warranting additional assessment, contact, and/or development. (JP 1-02 & JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *Counterintelligence Operational Lead (CIOL)*.

-- Also, an identified potential source. (HDI Lexicon, April 2008 and Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, [for investigative purposes,] single investigative element of a case requiring action. (IC Standard 2008-700-01, 4 Apr 2008)

-- Also, any source of information that, if exploited, may reveal information of value in the conduct of a counterintelligence investigation. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, for CI collection purposes, any person who has the potential to provide information of value to the supported command. (DoD, CI Functional Services IWG Handbook, 19 Feb 2009)

Lead Agency. The head of a DoD Component or designee who is responsible for providing CI support for another DoD Component or group of DoD Components. (DoDI 5240.10, 14 May 2004)

-- Also, in CI usage concerning an investigation, the agency in a joint investigation that has primary authority concerning the offense committed or is designated as such by agreement of the investigative agencies involved. The lead agency is ultimately responsible for determination of investigative responsibilities, procedures, and methods. Also see *joint investigation*.

-- Also, designated among US Government agencies to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. The lead agency is to chair the interagency working group established to coordinate policy related to a particular operation. The lead agency determines the agenda, ensures cohesion among the agencies, and is responsible for implementing decisions. (JP 1-02)

Lead Federal Agency (LFA). The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority. (JP 1-02 & JP 3-41)

Leaks. See *unauthorized disclosure*.

Legal Attaché (LEGAT). The FBI has offices around the globe. These offices—called legal attachés or legats—are located in U.S. embassies. (fbi.gov) -- See <<http://www.fbi.gov/contact-us/legat>>

-- Also, the title of FBI special agents deployed abroad to liaison posts in overseas diplomatic missions... (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Legal Residency. An intelligence apparatus in a foreign country composed of intelligence officers assigned as overt representatives of their government, but not necessarily identified as intelligence officers. (ICS Glossary)

Legal Traveler. Any individual traveling with legitimate documentation to perform a specific collection or support mission. (National HUMINT Glossary)

-- Also, any individual traveling with legal documentation to perform specified intelligence collection or support missions, or any individual who may be selected for debriefing on legal travel to or through geographical areas of interest. (AR 381-20, Army CI Program, 25 May 2010)

Legend. The complete cover story developed for an operative. (CI Centre Glossary)

-- Also, false identify that an agent builds up through forged documents and other means such as living under the name of the person whose identify he assumes. (Spy Book)

-- Also, a carefully constructed cover for an intelligence officer. (Spycraft)

Liaison. That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 1-02 & JP 3-08) Also see *intelligence liaison*.

-- Also, [activity] conducted to obtain information and assistance, to coordinate or procure material, and to develop views necessary to understand counterparts. Liaison contacts are normally members of the government, military, law enforcement, or other member of the local or coalition infrastructure. The basic tenet of liaison is *quid pro quo*. An exchange of information, services, material, or other assistance is usually a part of the transaction. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

"A crucial but often overlooked part of U.S. intelligence efforts is liaison with foreign intelligence services.... A productive liaison relationship does not necessarily preclude spying on each other—but it does mean both sides try to be especially careful not to get caught at it."

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

"Liaison is not explicitly spelled out in the theoretical approaches [regarding] intelligence. If one looks to the intelligence cycle paradigm, one will even discover that liaison has no fixed location in the cycle... it is actually a mode of activity in every point in the intelligence cycle [and] shares this quality with counter-intelligence."

-- Dutch Analysts Bob De Graaf and Cees Wiebes in Jeffreys-Jones, *External Vigilance* (1997)

Liaison Operations. Operations to coordinate activities and exchange information with foreign military, governmental, and non-governmental civilian agencies. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2011)

According to Army FM 2-22.3 (HUMINT Collector Operations), "liaison operations" are programs to coordinate activities and exchange information with host country and allied military and civilian agencies and NGOs. CI liaison activities are designed to ensure a cooperative operating environment for CI elements and/or to obtain information, gain assistance, develop CI leads for further exploitation, procure material, etc.

Light Cover [aka shallow cover]. A type of cover that will not withstand close scrutiny or due diligence. (National HUMINT Glossary)

Line of Operations. A line that defines the directional orientation of a force in time and space in relation to the enemy and links the force with its base of operations and objectives. (Army FM 3-0, Operations, Feb 2008)

Link. A behavioral, physical, or functional relationship between nodes.

Link Analysis. Subset of network analysis, exploring associations between objects.

Listening Post. A secure site at which signals from an audio operation are monitored and/or received. (Spycraft)

Load. Tradecraft jargon... to put something in a dead drop; to service a dead drop. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Load Signal. A visual signal to indicate the presence of an individual or object at a given location. (HDI Lexicon, April 2008)

-- Also, a visual signal displayed in a covert manner to indicate the presence of an individual or object at a given location. (JP 1-02 & JP 3-50)

Local Agency Check (LAC). A review of the appropriate criminal history and court records in jurisdictions over areas where the Subject has resided, attended school, or been employed during a specific period of time. (IC Standard 700-1, 4 Apr 2008)

-- Also, a records or files check of official or publicly available information conducted at any local office of government agencies within the operational area of the [CI] field element conducting the check. These records may include holdings and databases maintained by local and state law agencies, local courts, and local offices of federal agencies. (902d MI Group Investigations Handbook, Feb 2007)

Logic Bomb. Computer jargon for programmed instructions clandestinely inserted into software, where they remain inactive and undetected until the computer reached a certain point in its operations, at which time the instructions take over. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, [in cyber usage] also known as a "time bomb," a program that allows a Trojan to lie dormant and then attack when the conditions are just right. Triggers for logic bombs include a change in a file, a particular series of keystrokes, or a specific time or date. (McAfee Labs - Threat Glossary)

Low Visibility Operations. Sensitive operations wherein the political-military restrictions inherent in covert and clandestine operations are either not necessary or not feasible; actions are taken as required to limit exposure of those involved and/or their activities. Execution of these operations is undertaken with the knowledge that the action and/or sponsorship of the operation may preclude plausible denial by the initiating power. (JP 1-02 & JP 3-05.1)

Mail Cover. The process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service. (DoD 5240.1-R, Dec 1982)

-- A record of information on the outside (cover) of any mail piece. It is kept to locate a fugitive, protect national security, or obtain evidence of a crime punishable by a prison term exceeding 1 year. This record is one of the few ways information on mail may be disclosed outside the USPS, and its use is lawful only if authorized by postal regulations. (USPS Pub 32, *Glossary of Postal Terms*, May 1997)

-- Also, an investigative tool used to record information on the outside container, envelope, or wrapper of mail, including the name and address of the sender and the place and date of postmarking. (USPS Publication 146, *A Law Enforcement Guide to the U.S. Postal Service*, Sep 2008)

See USPS Pub 146, *A Law Enforcement Guide to the U.S. Postal Service* (Sep 2008)* and USPS Pub 55, *USPS Procedures: Mail Cover Requests*, available from the US Postal Service by request to authorized users.

* USPS Pub 146 also available at: <www.hSDL.org/?view&doc=112575&coll=limited>

Make (aka made). Tradecraft jargon... surveillance term for the surveillant being detected by the subject of a surveillance. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Malicious Code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS [information system]. (CNSS Instruction No. 4009) Also see *Trojan Horse*.

Malware. A generic term used to describe malicious software such as viruses, Trojan horses, spyware, and malicious active content. (McAfee.com, accessed 15 Nov 2010)

-- Also, [malicious] software such as viruses or Trojans designed to cause damage or disruption to a computer system. (AFDD 3-13)

-- Also, malicious software that secretly accesses a computer system without the owner's informed consent. A general term to mean a variety of forms of hostile, intrusive, or annoying software or program code, including computer viruses, worms, trojan horses, spyware, most rootkits, and other malicious software or program. (Wikipedia)

Manipulation. The mixing of factual and fictitious or exaggerated evidence (one of the four deception means for conveying deception information to a target). (CIA, D&D Lexicon, 1 May 2002)

Maritime Domain. All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. (NSPD-41/HSPD-13, Maritime Security Policy, 21 Dec 2004)

-- Also, the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

Measurement and Signature Intelligence (MASINT). Information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, and identify them. (ICD 1, 1 May 2006 and National Intelligence: A Consumer's Guide - 2009)

-- Also, information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, locate, and identify them. MASINT exploits a variety of phenomenologies to support signature development and analysis, to perform technical analysis, and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized, technically-derived measurements of physical phenomenon intrinsic to an object or event and it includes the use of quantitative signatures to interpret the data. (DoDI 5105.58, MASINT, 22 Apr 2009)

-- Also, intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. (JP 2-0, Joint Intelligence)

-- Also, describes a category of technically derived information that provides distinctive characteristics of a specific event such as a nuclear explosion, or locates, identifies, and describes distinctive characteristics of targets through such means as optical, acoustic, or seismic sensors. (WMD Report, 31 Mar 2005)

MASINT will become increasingly important in providing unique scientific or highly technical information contributions to the IC. It can provide specific weapon identifications, chemical compositions and material content, and a potential adversary's capability to employ weapons.
-- IC21: HPSCI Staff Study, 6 Apr 1996 (p. 40)

Measures of Effectiveness (MOE). A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02 and JP 3-0)

Media Exploitation. The receipt, cataloging, duplication, screening/prioritizing, gisting, initial evaluation, translating key pieces of media, uploading data into appropriate data bases, identifying the need for further detailed exploitation of pieces of media, tracking the requested detailed exploitation efforts, and disseminating selected media for further use/analysis by the Intelligence Community. (National Media Exploitation Center CONOPS, Jan 2004)

MI5. British Security Service is responsible for "protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means." (www.mi5.gov.uk/)

MI6. British Secret Intelligence Service (SIS) is responsible for foreign intelligence. MI6 collects secret intelligence and mounts covert operations overseas in support of British Government objectives IAW the UK's Intelligence Services Act of 1994. (www.sis.gov.uk/)

MICE. The commonly used acronym to explain the motivation of traitors. MICE stands for "money, ideology, coercion, and ego," a combination of which may prompt an individual to betray his/her country. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Microdot. The photographic reduction of writing or other material to facilitate transfer from one location to another without detection. (Spy Book)

-- Also, an optical reduction of a photographic negative to a size that is illegible without magnification, usually 1mm or smaller in area. (Spycraft)

Mikrat. The product of microphotography, as used in microdots. (Spt Book)

Militarily Critical Technology. See *critical technology; militarily critical technologies list*.

Militarily Critical Technologies List (MCTL). A technical reference for the development and implementation of DoD technology security policies on international transfers of defense related goods, services, and technologies as administered by the Director, Defense Technology Security Administration (DTSA). (DoDI 3020.46, MCTL, 24 Oct 2008)

-- MCTL website at <<http://www.dtic.mil/mctl/>>
-- Also see <<http://www.dhra.mil/perserec/csg/t1threat/mctl.htm>>

Military Counterintelligence Collection (MCC). An activity for the collection of information responsive to operational, tactical, and Service CI requirements. MCC entails the use of recruited or non-recruited sources, including U.S. and non-U.S. persons, to collect information in support of efforts to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *counterintelligence collection*; *collection*.

Military Deception (MILDEC). Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02 & JP 3-13.4)

-- Also, those actions executed to deliberately mislead adversary decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (Army FM 3-0, Operations, with Chg 1 2011)

In war-time, truth is so precious that she should always be attended by a bodyguard of lies

-- Winston Churchill (November 1943)

as cited in Anthony Cave Brown, *Bodyguard of Lies: The Extraordinary True Story Behind D-Day* (1975)

According to JP 3-13.4, Counterintelligence provides the following for MILDEC planners:

- 1) Identification and analysis of adversary intelligence systems to determine the best deception conduits;
- 2) Establishment and control of deception conduits within the adversary intelligence system, also known as offensive CI operations;
- 3) Participation in counterdeception operations;
- 4) Identification and analysis of the adversary's intelligence system and its susceptibility to deception and surprise; and
- 5) Feedback regarding adversary intelligence system responses to deception operations.

-- For additional information see Joint Pub 3-13.4, Military Deception, 13 Jul 2006

It was Desert Storm that I became convinced of the power of deception in warfare, it truly is a force multiplier.

-- Tommy Franks (General, USA Ret), *American Solider* (2004)

Military Department (MILDEP). One of the departments within the Department of Defense created by the National Security Act of 1947, as amended. (JP 1-02)

Military Information Support Operations (MISO). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02 and JP 3-13.2)

Previously known as Psychological Operations or PSYOP. This change directed by SECDEF Memo, subject: Changing the Term Psychological Operations (PSYOP) to Military Information Support Operations (MISO), dated 3 Dec 2010.

Military Intelligence (MI). Intelligence on any foreign military or military-related situation or activity which is significant to military policymaking or the planning and conduct of military operations and activities. (JP 1-02 & JP 2-01)

-- Also, the collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities. (DoDD 5143.01, USD/I, 23 Nov 2005)

Military intelligence appears in three basic forms: strategic, operational, and tactical.

- **Strategic Intelligence:** intelligence that is required for the formulation of strategy, policy, and military plans and operations at the national and theater levels.
- **Operational Intelligence:** intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. It focuses on narrower, but significant theater-oriented military responsibilities.
- **Tactical Intelligence:** intelligence that is required for planning and conducting tactical military operations at the local level. It concerns information about the enemy that is designed to help locate the enemy and decide which tactics, units, and weapons will most likely contribute to victory in an assigned area, and when properly applied, it can be a significant force multiplier.

Military Intelligence Board (MIB). A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. (JP 2-0, Joint Intelligence)

Military Intelligence Program (MIP). The MIP consists of programs, projects, or activities that support the Secretary of Defense's intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters' operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence. The term "MIP" replaces the terms "Joint Military Intelligence Program (JMIP)" and "Tactical Intelligence and Related Activities (TIARA)." (DoDD 5205.12, MIP, 14 Nov 2008)

The MIP was established to improve management of Defense Intelligence capabilities and resources. USD/I is the Program Executive for the MIP.

-- USD/I Memo, subj: Establishment of the MIP, 1 Sep 2005

The Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA) were combined in 2005 to form the MIP.

-- National Intelligence: A Consumer's Guide – 2009, p. 68

Military Service. A branch of the Armed Forces of the United States, established by act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a military or executive department. The Military Services are: the United States Army, the United States Navy, the United States Air Force, the United States Marine Corps, and the United States Coast Guard. (JP 1-02)

Military Source Operations. The collection, from, by and/or via humans, of foreign, military and military-related intelligence. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011)

-- Also, the collection from, by, and/or via humans, of foreign military and military-related intelligence conducted under SecDef authorities to satisfy DoD needs. (HDI Lexicon, April 2008)

-- Also, DoD HUMINT activity or operation which is conducted to specifically respond to, and satisfy, DoD intelligence collection requirements. These operations directly support the execution of the Secretary's responsibilities, commanders in the field, military operational planners, and the specialized requirements of the military departments (e.g., research and development process, the acquisition of military equipment, and training and doctrine) and span the entire HUMINT operational continuum, utilizing varying degrees of tradecraft to ensure the safety and security of the operation. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Military Source Operations are conducted by trained personnel under the control of Defense HUMINT Executors. See DoDD S-5200.37, *Management and Execution of Defense HUMINT (U)*, 9 Feb 2009 for specifics.

Misdirection. A classic conjurer's trick, misdirection is the term applied in the counterintelligence community for the tactic of supplying an ostensibly plausible explanation for an event actually caused by something quite different, probably by an individual or an operation, deemed sufficiently valuable to require protection. Invariably a human asset may produce some information which requires action that could compromise him or her, so misdirection is intended to divert attention elsewhere. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Misperception. The formation of an incomplete or inaccurate image or perception of some aspect of reality. The faulty image may be formed due to a lack of information or intentionally erroneous information provided to the perceiver. (CIA, D&D Lexicon, 1 May 2002)

Mission. 1) The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore; 2) in common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 1-02 & JP 3-0)

Mission Assurance. A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Mission Manager. A position with the [Intelligence] Community for an individual, operating with the Director's [DNI] authorities, who coordinates all intelligence activities against a specific country or topic [e.g., counterterrorism counterproliferation, counterintelligence]. (HPSCI Report 27 Jul 2006)

-- Also, *Mission Managers* are the principal Intelligence Community officials overseeing all aspects of national intelligence related to their respective mission areas. Mission Managers are designated for counterintelligence, counterterrorism, Counterproliferation, Iran, North Korea, and Cuba & Venezuela. (ICD 900, Mission Management, 21 Dec 2006)

The NCIX serves as the Mission Manger for Counterintelligence.
Director NCTC serves as the Mission Manager for Counterterrorism.

Mission Need. A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Mission needs are determined by the mission and functions of an IC element or the roles and responsibilities of particular IC personnel in the course of their official duties. (ICD 501, 21 Jan 2009)

Mission Statement. A short sentence or paragraph that describes the organization's essential task (or tasks) and purpose—a clear statement of the action to be taken and the reason for doing so. The mission statement contains the elements of who, what, when, where, and why, but seldom specifies how. (JP 5-0, Joint Planning, 26 Dec 2006) Also see *mission*.

Mission Tasking Authority (MTA). See *Counterintelligence Mission Tasking Authority*.

Mitigation. Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Modus Operandi (MO). A distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or an organization involved in criminal or intelligence activity. (AR 381-20, Army CI Program, 25 May 2010)

Modus Operandi, a Latin phrase, approximately translated as "method of operating" -- the term is used to describe someone's habits or manner of working, their method of operating or functioning. In English, it is frequently shortened to M.O.

Mole. A member of an organization who is spying and reporting on his/her own organization on behalf of a foreign country; also called a penetration. (National HUMINT Glossary) Also see *mole hunt*, *penetration*.

-- Also, a human penetration into an intelligence service or other highly sensitive organization. Quite often a mole is a defector who agrees to work in place. (CI Centre Glossary)

-- Also, literary and media term for penetration agent infiltrated into an opposition government agency. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, the opposing faction's insert, or penetration, into an intelligence apparatus. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

In 1622, Sir Francis Bacon used the term "mole" in the *History of the Reign of King Henry VII*:

He was careful and liberal to obtain good Intelligence from all parts abroad.... As for his secret spials, which he did employ both at home and abroad, by them to discover what practices and conspiracies were against him, surely his care required it; he had such moles [emphasis added] perpetually working and casting to undermine him. (p. 216)

In modern times, the term was popularized by John le Carré (penname for David Cornwell, a British author of espionage novels) who used "mole" to mean a "penetration" of a hostile intelligence service. In le Carré's 1974 novel, *Tinker, Tailor, Soldier, Spy*, Smiley is recalled to hunt down a Soviet "mole" in the Circus (British Secret Intelligence Service, aka MI6).

Also a title of a book by William Hood, *Mole: The True Story of the First Russian Spy to Become an American Counterspy* about Pyotr Semyonovich Popov, a Major in Soviet Military Intelligence (the GRU); see http://en.wikipedia.org/wiki/Pyotr_Semyonovich_Popov.

Hood's book, *Mole*, is one of the best publicly available descriptions of a penetration of an intelligence service and provides a detailed and highly personal account of how intelligence tradecraft is practiced, the mental and psychological toll this takes, and the risks involved (for both agent and case officer).

Mole Hunt. The term popularized by John le Carré for a counterintelligence investigation conducted into hostile penetration. (*Historical Dictionary of Cold War Counterintelligence*, 2007) Also see *mole*.

Also the title of a book by David Wise, *Molehunt: The Secret Search for Traitors That Shattered the CIA*.

Motivation. Tradecraft jargon for bases for agent recruitment that are usually (1) ideological; (2) financial; (3) coercion or blackmail; (4) sexual; (5) ego satisfaction; (6) familial; (7) love of adventure or excitement; (8) a combination of two or more of the preceding. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Multilateral Collection. A collection activity conducted with two or more cooperating foreign intelligence services against a mutually targeted foreign intelligence, security service, or international terrorist entity. (DoDI S-5240.17, CI Collection, 12 Jan 2009)

Multilateral OFCO. An OFCO [Offensive Counterintelligence Operation] conducted by a U.S. CI agency with two or more cooperating foreign intelligence services against a mutually targeted FISS, foreign entity, or terrorist element. (DoDI S-5240.09, 29 Oct 2008)

Multilevel Security (MLS). Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (CNSS Instruction No. 4009)

Multinational. Between two or more forces or agencies of two or more nations or coalition partners. Also see also *alliance*; *coalition*. (JP 1-02)

Multinational Force (MNF). A force composed of military elements of nations who have formed an alliance or coalition for some specific purpose. (JP 1-02) Also see multinational operations.

Multinational Operations. A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 1-02 and JP 3-16) Also see *alliance*; *coalition*; *coalition action*

Narco-terrorism. Terrorism that is linked to illicit drug trafficking. (JP 1-02 & JP 3-07.4)

Name Trace. A search of available recoded data to find information about a person, normally conducted to determine the presence or absence of derogatory information about the person, as a first step in judging his suitability or intelligence value. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a search of data for information about an individual, organization, or subject. (National HUMINT Glossary)

National Agency Check (NAC). An in-depth name trace consisting of Federal Bureau of Investigation Name and Criminal History Fingerprint Checks, Defense Clearance Investigation Index (DCII) search, and can include checks on military personnel records, citizenship, selective service, Central Intelligence Agency records, State Department records, and other US Government agencies.

-- Also, [part of a] personnel security investigation consisting of a review of: investigative and criminal history files of the Federal Bureau of Investigation, including a technical fingerprint check; Office of Personnel Management Security/Suitability Investigations Index; DoD Central Index of Investigations (DCII) and Joint Personnel Adjudication System (JPAS); and such other national agencies (e.g., CIA, DNI) as appropriate to the individual's background. (IC Standard 700-1, 4 Apr 2008)

-- Also, a formal request to federal agencies for searches of their indices and supporting databases and files for information of investigative interest. (902d MI Group Investigations Handbook, Feb 2007)

National Capital Region (NCR). A geographic area encompassing the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia. (JP 1-02 & JP 3-28)

National Clandestine Service (NCS). The NCS operates as the clandestine arm of the CIA, and serves as the national authority for the coordination, deconfliction, and evaluation of clandestine human intelligence operations across the Intelligence Community. The NCS supports our country's security and foreign policy interests by conducting clandestine activities to collect information that is not obtainable through other means. The NCS also conducts counterintelligence and special activities as authorized by the President. (CIA at <<https://www.cia.gov/offices-of-cia/clandestine-service/index.html>>)

-- Also, the NCS serves as the national authority for the integration, coordination, deconfliction, and evaluation of human intelligence operations across the entire Intelligence Community, under authorities delegated to the Director of the CIA who serves as the National HUMINT Manager. The Director of the NCS reports directly to the Director of the CIA and will work with the Office of the Director of National Intelligence to implement all of the DNI's statutory authorities. (ODNI News release 3-05, 13 Oct 2005)

Formerly known as CIA Directorate of Operations or DO. The NCS was established in response to recommendations made in March 2005 by the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

National Counterintelligence Executive (NCIX). Performs duties provided in the CI Enhancement Act of 2002 and such other duties as may be prescribed by the Director of National Intelligence or specified by law. NCIX serves as Mission Manager of Counterintelligence and the Chairperson of the National CI Policy Board. Resides within the Office of the Director of National Intelligence (ODNI). (CI Enhancement Act of 2002) Also see *Office of the National Counterintelligence Executive*.

-- Also, the NCIX serves as the head of national counterintelligence for the U.S. Government, per the CI Enhancement Act of 2002. (National Intelligence: A Consumer's Guide - 2009)

Additional information on NCIX at <<http://www.ncix.gov/about/index.html>>

National Counterproliferation Center (NCPC). Coordinates strategic planning within the Intelligence Community (IC) to enhance intelligence support to United States efforts to stem the proliferation of weapons of mass destruction and related delivery systems. It works with the IC to identify critical intelligence gaps or shortfalls in collection, analysis or exploitation, and develop solutions to ameliorate or close these gaps. It also works with the IC to identify long-term proliferation threats and requirements and develop strategies to ensure the IC is positioned to address these threats and issues. NCPC will reach out to elements both inside the IC and outside the IC and the U.S. Government to identify new methods or technologies that can enhance the capabilities of the IC to detect and defeat future proliferation threats. (ODNI News release 9-05, 21 Dec 2005)

-- Also, the NCPC, which resides in the ODNI, is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). (National Intelligence: A Consumer's Guide - 2009)

National Counterterrorism Center (NCTC). The primary center for US government analysis of terrorism. It falls under the Office of the Director of National Intelligence (ODNI). One of its primary missions is "to serve as the central and shared knowledge bank on known and suspected terrorists and international terrorist groups, as well as their goals, strategies, capabilities, and networks of contacts and support." (EO 13354, National Counterterrorism Center, 27 Aug 2004)

In August 2004, the President established the NCTC to serve as the primary USG organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism and to conduct strategic operational planning by integrating all instruments of national power. In December 2004, Congress codified the NCTC in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and placed the NCTC in the Office of the Director of National Intelligence (ODNI). NCTC is a multi-agency organization dedicated to eliminating the terrorist threat to US interests at home and abroad. -- NCTC website: <http://www.nctc.gov/about_us/about_nctc.html>

NCTC was established in 2004 to ensure that information from any source about potential terrorist acts against the U.S. could be made available to analysts and that appropriate responses could be planned. NCTC is composed of analysts with backgrounds in many government agencies and currently operates with a staff of some 600 analysts from a headquarters in northern Virginia. It prepares studies ranging from strategic assessment of the future terrorist threats to daily briefings and situation reports. It is also responsible, directly to the President, for planning (but not directing) counterterrorism efforts. -- CRS Report, 15 Jan 2010

National Critical Infrastructure and Key Assets. The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations. (JP 1-02 & JP 3-28)

National Defense Strategy (NDS). A document approved by the Secretary of Defense for applying the Armed Forces of the United States in coordination with Department of Defense agencies and other instruments of national power to achieve national security strategy objectives. (JP 1-02 & JP 3-0)

-- Also, the guidance that the Secretary of Defense provides the Department on how to and on what the Department has to do to implement the President's National Security Strategy; it serves as the foundation for the QDR process. (Special Defense Department Briefing, 18 Mar 2005)

National Detainee Reporting Center (NDRC). National-level center that obtains and stores information concerning enemy prisoners of war, civilian internees, and retained personnel and their confiscated personal property. May be established upon the outbreak of an armed conflict or when persons are captured or detained by U.S. military forces in the course of the full range of military operations. Accounts for all persons who pass through the care, custody, and control of the U.S. Department of Defense. (JP 1-02 & JP 3-63)

National Disclosure Policy (NDP-1). A document that promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to disclose classified information to foreign governments and international organizations. NDP-1 establishes and provides for management of interagency mechanisms and procedures required for effective implementation of the national policy.

National Disclosure Policy Committee. Central authority for formulation, promulgation, administration, and monitoring of the NDP-1.

National Emergency. A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. Action to be taken may include partial, full, or total mobilization of national resources. (JP 3-28).

National Foreign Intelligence Program. All programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (50 USC §401a)

National Geospatial-Intelligence Agency (NGA). A member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense, that provides timely, relevant and accurate geospatial intelligence in support of national security objectives.

The term "geospatial intelligence" or "GEOINT" means the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial (e.g., mapping, charting and geodesy) information.

-- See NGA website at <https://www1.nga.mil/>

National HUMINT Collection Directive (NHCD). An integrated inter-agency mechanism for tasking human intelligence requirements to members of the Intelligence Community that have the best capability and probability of acquiring that information at the least cost and least risk. A standing / enduring intelligence requirement. (National HUMINT Glossary)

National HUMINT Requirements Tasking Center (NHRTC). Congressionally mandated to integrate all HUMINT collection and reporting capabilities within the US Government. [Staffed by] senior officers from the Department of State, Department of Defense, and CIA; the center produces National HUMINT Collection Directives (NHCDs) and Collection Support Briefs (CSBs). (National HUMINT Glossary)

The NHRTC reports to the the National HUMINT Manager. See DCID 3/7, *National HUMINT Requirements Center*, 1 Jun 1992 (classified CONFIDENTIAL).

National Industrial Security Program (NISP). National program established by EO 12829 for the protection of information classified under EO 12958 as amended, or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense is the Executive Agent for the NISP. The Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. (DoD 5220.22-M, NISPOM, 26 Feb 2006) Also see the *Defense Security Service (DSS)*; *industrial security*.

National Intelligence. All intelligence, regardless of the source from which derived and including information gathered within or outside of the United States, which pertains, as determined consistent with any guidelines issued by the President, to the interests of more than one department or agency of the Government; and that involves (a) threats to the United States, its people, property, or interests; (b) the development, proliferation, or use of weapons of mass destruction; or (c) any other matter bearing on United States national or homeland security. (JP 1-02, JP 2-01, and Intelligence Reform and Terrorism Prevention Act of 2004, §1012)

-- Also, intelligence which pertains to the interest of more than one department or agency of the US Government. (50 USC §401a)

The US Government uses intelligence to improve and understand the consequences of its national security decisions.

National Intelligence Board. Serves as the senior Intelligence Community advisory body to the Director of National Intelligence (DNI) on the analytic judgments and issues related to analysis of national intelligence; functions include: production, review, and coordination of national intelligence; interagency exchanges of national intelligence information; sharing of IC intelligence products with foreign governments; protection of intelligence sources and methods; activities of common concern and other matters as may be referred to it by the DNI. (ICD 202, National Intelligence Board, 16 Jul 2007)

National Intelligence Council (NIC). The Intelligence Community's center for mid-term and long-term strategic thinking. Its primary functions are to: 1) Support the DNI in his role as head of the Intelligence Community; 2) Provide a focal point for policymakers to task the Intelligence Community to answer their questions; 3) Reach out to nongovernmental experts in academia and the private sector to broaden the Intelligence Community's perspective; 4) Contribute to the Intelligence Community's effort to allocate its resources in response to policymakers' changing needs; and 5) Lead the Intelligence Community's effort to produce National Intelligence Estimates (NIEs) and other NIC products. (ODNI website)

The NIC is responsible for the US Intelligence Community's most authoritative assessments of major issues affecting the national security. By law [50 USC §403-3b(b)(1)], the NIC is to consist of "senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure" of the DNI. The senior analysts are known as National Intelligence Officers (NIOs).

NIC responsibilities are set forth in ICD 207, *National Intelligence Council*, 9 June 2008.

National Intelligence Coordination Center (NIC-C). Provides a mechanism to strategically manage and direct collection across defense, foreign and domestic realms. [Interfaces with the Defense Intelligence Coordination Center (DIOCC)]. (National Intelligence: A Consumer's Guide - 2009)

National Intelligence Estimate (NIE). The DNI's most authoritative written judgment concerning national security issues. NIEs contain the coordinated judgments of the Intelligence Community regarding the likely course of future events. (ODNI website)

National Intelligence Priorities Framework (NIPF). The Director of National Intelligence's guidance to the IC on the national intelligence priorities approved by the President. (National Intelligence: A Consumer's Guide - 2009)

-- Also, the DNI's sole mechanism for establishing national intelligence priorities. The NIPF consists of: intelligence topics approved by the President; a process for assigning priorities to countries and non-state actors relevant to the approved intelligence topics; and a matrix showing those priorities. It is updated semi-annually. The NIPF is used by the ODNI and IC elements in allocating collection and analytical resources. (ICD 204, 13 Sep 2007)

A key instrument for keeping the IC attentive to both policymaker concerns and potential shocks... The NIPF process gathers the needs of senior decision makers across the US government on a semi-annual basis to support prudent allocation of both collection and analytical resources for the following 6-to-12 months.

– DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

National Intelligence Program (NIP). All programs, projects, and activities of the IC, as well as any other programs of the IC designated jointly by the DNI and the head of a US department or agency or by the President. It does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (National Security Act §3(6) and ICD 1, 1 May 2006)

Formerly known as the National Foreign Intelligence Program (NFIP), the NIP provides the resources needed to develop and maintain intelligence capabilities that support national priorities.

National Intelligence Strategy. A strategy document prepared by the ODNI in consultation with the relevant departments that establishes the strategic objectives for the Intelligence Community (IC); it sets forth the framework for a more unified, coordinated and effective IC [and] guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. (ODNI News release 4-05)

The National Intelligence Strategy (NIS) sets forth the framework for a more unified, coordinated, and effective US Intelligence Community (IC) and guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. The strategy outlines strategic objectives that are referred to as either mission or enterprise objectives. The unclassified *National Intelligence Strategy* (Aug 2009) is available at <http://www.dni.gov/reports/2009_NIS.pdf>

CI is one of six mission objectives of the NIS (Mission Objective 4 is *Integrate Counterintelligence*). This is the first time that CI was identified as a mission objective within the NIS; see NIS pp 8-9.

National Intelligence Support Plan (NISP). The NISP, in conjunction with the Combatant Command's Annex B: [Intelligence Plan or IPLAN] supports COCOM operational plans directed by the President and the Secretary of Defense. The NISP defines the national Intelligence Community (IC) agencies' and related organizations' intelligence collection, and analysis & production support roles and responsibilities within the COCOM area of responsibility and the national IC to ensure integrated intelligence operations, synchronized with the COCOM operational plan. The NISP supports the COCOM's operational objectives during all phases of the operation and contributes to the achievement of the COCOM's desired operational effects. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Counterintelligence Functional Support Plan (CI FSP)*.

National Joint Terrorism Task Force (NJTTF). The NJTTF was established in July 2002 to serve as a coordinating mechanism with the FBI's partners on terrorism issues. Over 40 agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners. Also see *Joint Terrorism Task Force (JTTF)*. (DoJ website: <<http://www.usdoj.gov/jtff/>>)

-- Also, the NJTTF was created to act as a liaison and conduit for information on threats and leads from FBI Headquarters to the local JTTFs and to 40 participating agencies including representatives from members of the Intelligence Community; components of the departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior; NYPD; Nuclear Regulatory Commission; Railroad Police; U.S. Capitol Police; and others. (FBI)

See FBI website at: <<http://www.fbi.gov/congress/congress06/mueller120606.htm>>

National Media Exploitation Center (NMEC). A Director of National Intelligence (DNI) Center composed of DIA, CIA, FBI, NSA, and Defense Cyber Crime Center (DCCC) as partner organizations; DIA is the Executive Agent. NMEC acts as a DOMEX [document and media exploitation] service of common concern and ensures prompt and responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other US Government Consumer's, to include provision of timely and accurate collection, processing, exploitation, and dissemination consistent with the protection of intelligence sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007)

Director DIA is the IC Executive Agent for the NMEC (para 2d, DoDD 3300.03).

National Military Strategy (NMS). A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain national security strategy and national defense strategy objectives. (JP 1-02 & JP 3-0) Also see *national security strategy*.

The NMS defines the national military objectives, establishes the strategy to accomplish these objectives, and addresses the military capabilities required to execute the strategy. The Chairman develops the NMS by deriving overall security policy guidance from the President's NSS, and through consulting with the other JCS members and combatant commanders. The NMS describes the strategic landscape and includes a discussion of the potential threats and risks.

-- CJCSI 3100.01A, *Joint Strategic Planning System*, 1 Sep 1999

National Policy. A broad course of action or statements of guidance adopted by the government at the national level in pursuit of national objectives. (JP 1-02)

National Reconnaissance Office (NRO). A DoD agency tasked to ensure that the United States has the technology and spaceborne and airborne assets needed to acquire intelligence worldwide, including support to such functions as monitoring of arms control agreements, indications and warning, and the planning and conducting of military operations. (JP 1-02 & JP 2-0)

The NRO designs, builds and operates the nation's reconnaissance satellites. In recent years, the NRO has implemented a series of actions declassifying some of its operations. The existence of the organization was declassified in September 1992. See NRO website at <www.nro.gov/>

Throughout the 1960s, U.S. operation of reconnaissance satellites was officially classified. It was not until Jan 1971 that the NRO's existence was first disclosed by the media, when it was briefly mentioned in a New York Times article. A more extensive discussion of the NRO appeared in the Washington Post (9 Dec 1973) as a result of the inadvertent disclosure in a Congressional report.

For additional information see Jeffrey T. Richelson, "Undercover in Outer Space: The Creation and Evolution of the NRO," *International Journal of Intelligence and Counterintelligence*, 13, 3 (Fall 2000): pp. 301-344.

National Security. A collective term encompassing both national defense and foreign relations of the United States. Specifically, the condition provided by: 1) a military or defense advantage over any foreign nation or group of nations; 2) a favorable foreign relations position; or 3) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. (JP 1-02)

-- Also, the national defense or foreign relations of the United States. (EO 13526, National Security Information, 29 Dec 2009)

National Security Act. The National Security Act of 1947 realigned and reorganized the United States' armed forces, foreign policy, and Intelligence Community apparatus in the aftermath of World War II. The Act merged the Department of War and the Department of the Navy into the National Military Establishment (NME) headed by the Secretary of Defense. It was also responsible for the creation of a separate Department of the Air Force from the existing United States Army Air Forces. Initially, each of the three service secretaries maintained quasi-cabinet status, but the act was amended in 1949 to assure their subordination to the Secretary of Defense. At the same time, the NME was renamed as the Department of Defense. Aside from the military reorganization, the act established the National Security Council, a central place of coordination for national security policy in the Executive Branch, and the Central Intelligence Agency, the United States' first peacetime intelligence agency. (Public Law No. 235, 80 Cong., 61 Stat. 496)

The National Security Act has been amended numerous times since its enactment. Reference to the "*National Security Act of 1947, as amended*" indicates the legal authority cited is legislation passed after 1947 that replaced one or more provisions of the original act.
-- See <http://www.intelligence.gov/0-natsecact_1947.shtml>

National Security Agency (NSA). The U.S.'s cryptologic organization, with responsibility for protecting U.S. National Security information systems and collecting and disseminating foreign signals intelligence. Areas of expertise include cryptanalysis, mathematics, computer science, and foreign language analysis. (National Intelligence: A Consumer's Guide - 2009)

-- Also, a member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense. NSA/Central Security Service leads the community in delivering responsive, reliable, effective, and expert Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Network Warfare operations to gain a decisive information advantage for the Nation and our allies under all circumstances. (www.nsa.gov)

NSA is the U.S. Government lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS. NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers.
-- DoDD 5100.20, NSA/CSS, 26 Jan 2010

The Central Security Service (CSS) oversees the function of the military cryptologic system, develops policy and guidance on contributions of military cryptology to the Signals Intelligence / Information Security (SIGINT/INFOSEC) enterprise, and manages the partnership of NSA and the Service Cryptologic Components. NSA as a whole is known as "NSA/CSS."
-- National Intelligence: A Consumer's Guide - 2009. P. 43

National Security Branch (NSB). Major element of the FBI that executes the FBI's national security mission to lead and coordinate intelligence efforts that drive actions to protect the United States. The NSB is composed of the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, Weapons of Mass Destruction Directorate, and Terrorist Screening Center. (www.fbi.gov)

The FBI's national security and intelligence missions are unified under the authority of the Executive Assistant Director (EAD) who reports to the Deputy Director FBI. The EAD-NSB has full operational and management authority over all FBI Headquarters and field national security programs, including the authority to initiate, terminate, or reallocate any of the investigations or other activities within the NSB.

The EAD-NSB is also responsible for the continued development of a specialized national security workforce and is the lead FBI official responsible for coordination and liaison with the Director of National Intelligence (DNI) and the Intelligence Community (IC).

-- See <http://www.fbi.gov/hq/nsb/nsb_brochure.pdf>

National Security Council (NSC). A governmental body specifically designed to assist the President in integrating all spheres of national security policy. The President, Vice President, Secretary of State, and Secretary of Defense are statutory members. The Chairman of the Joint Chiefs of Staff; Director, Central Intelligence Agency; and the Assistant to the President for National Security Affairs serve as advisers. (JP 1-02)

The NSC was established by the National Security Act of 1947 as the principal forum to consider national security issues that require presidential decision. Congress envisioned that the NSC would allow military and civilian government departments and agencies to work more effectively together on national security matters.

-- AFSC Pub 1

The NSC system is the principal forum for deliberation of national security policy issues requiring Presidential decision. The NSC system provides the framework for establishing national strategy and policy objectives. The NSC develops policy options, considers implications, coordinates operational problems that require interdepartmental consideration, develops recommendations for the President, and monitors policy implementation. The NSC prepares national security guidance that, with Presidential approval, implements national security policy. These policy decisions provide the basis for military planning and programming.

-- JP 5-0, *Joint Planning* (26 Dec 2006)

National Security Council Intelligence Directive (NSCID). A formal statement of policy by the National Security Council, binding upon those US Government agencies within the purview of NSC authority. (National HUMINT Glossary)

Regarding counterintelligence, see NSCID 5, *US Espionage and Counterintelligence Activities Abroad*, 17 Feb 1972 – copy available at: <www.fas.org/irp/offdocs/nsCID05.htm>

National Security Crimes. Crimes likely to impact upon the national security, defense, or foreign relations of the United States, including but not limited to espionage, sabotage, treason, and sedition.

National Security Division (NSD). Element of the Department of Justice (DoJ) created by the reauthorization of the USA PATRIOT Act in March 2006, the Division merges the primary national security elements of DoJ, fulfilling a key recommendation of the March 2005 report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). The Division consists of the Counterterrorism and Counterespionage Sections; the Office of Intelligence Policy and Review; and a Law & Policy Office. (DoJ website at <<http://www.usdoj.gov/nsd/>>)

The Counterespionage Section (CES), NSD, DoJ, supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology.

CES has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. It provides legal advice to U.S.

Attorney's Offices and investigative agencies on all matters within its area of responsibility, which includes 88 federal statutes affecting national security. It also coordinates criminal cases involving the application of the Classified Information Procedures Act (CIPA). In addition, the Section administers and enforces the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.

The Office of Intelligence Policy and Review (OIPR), NSD, DoJ, prepares and files all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978 (FISA). The Office also advises the National Security Division and various client agencies, including the CIA, FBI, and the Defense and State Departments, on questions of law, regulation, and guidelines, as well as on the legality of domestic and overseas intelligence operations.

National Security Emergency. Any occurrence, including natural disaster, military attack, technological, or other emergency, that seriously degrades or threatens the national security of the United States. (DoDD 5111.13, ASD(HD&ASA), 16 Jan 2009)

National Security Information (NSI). Any information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated. (IC Standard 700-1, 4 Apr 2008)

National Security Letter (NSL). A letter request for information from a third party that is issued by the FBI or by other government agencies with authority to conduct national security investigations. (FBI)

-- Also, a NSL seeks customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies. Five statutory provisions vest government agencies responsible for foreign intelligence investigations with authority to issue written commands comparable to administrative subpoenas. (CRS Report RS22406, 21 Mar 2006)

NSLs are only available for authorized national security investigations (international terrorism or foreign intelligence/CI investigations), not general criminal investigations or domestic terrorism investigations. NSLs can only be used to seek certain transactional information permitted under the five NSL provisions, and cannot be used to acquire the content of any communications.

Statutory provisions at 18 USC §2709, 12 USC §3414, 15 USC §1681u, 15 USC §1681v and 50 USC §436; as amended by PL 109-177 and PL 109-178.

For additional information see <http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm>

National Security Strategy (NSS). A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. (JP 1-02 & JP 3-0)

National Special Security Event (NSSE). A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. (JP 1-02 & JP 3-28)

-- Also, major event considered to be nationally significant as designated by the President or his designated representative, the Secretary of the Department of Homeland Security. Some events categorized as NSSE include presidential inaugurations, major international summits held in the United States, major sporting events, and presidential nominating. NSSE designation factors include: anticipated attendance by U.S. officials and foreign dignitaries; size of the event; and significance of the event. (CRS Report RS22752, updated 19 Mar 2008)

The US Secret Service is the lead federal agency responsible for coordinating, planning, exercising, and implementing security for NSSEs, and was designated as the lead agency in PL 106-544.

National Threat Identification and Prioritization Assessment (NTIPA). An annual strategic planning assessment of the counterintelligence requirements of the United States produced by the Office of the National Counterintelligence Executive (ONCIX); required by the Counterintelligence Enhancement Act of 2002. The NTIPA assess and priorities threats to the US posed by traditional and emerging foreign intelligence activities. It is a strategic planning tool to be used by intelligence community and national security decision makers. (ONCIX)

The NTIPA informs the President and the national security leadership of foreign intelligence threats to the United States. The NTIPA does not go into effect until approved by the President. The NCIX submits each approved NTIPA or modification thereof to the congressional intelligence committees.

NTIPA *versus* NIPF – CI action is driven by the approved NTIPA and foreign intelligence (FI) collection is driven by the NIPF (National Intelligence Priorities Framework). Each has different focus and priorities, as well as a totally different operational dynamic.

Need for CI action is much different from the need for FI collection.

National Virtual Translation Center (NVTC). Provides timely and accurate translations of foreign intelligence for all elements of the IC. Its mission includes acting as a clearinghouse for facilitating interagency use of translators; partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services; building a nationwide team of highly qualified, motivated linguists and translators, connected virtually to the program office in Washington, D.C.; and applying state-of-the-art technology to maximize translator efficiency. (National Intelligence: A Consumer's Guide - 2009)

The NVTC is a DNI Center and the FBI the IC Executive Agent.

Naval Criminal Investigative Service (NCIS). The primary law enforcement and counterintelligence arm of the United States Department of the Navy. It works closely with other local, state, federal, and foreign agencies to counter and investigate the most serious crimes, including terrorism, espionage, computer intrusion, homicide, rape, child abuse, arson, procurement fraud, etc. (www.ncis.navy.mil)

Mission: NCIS is a federal law enforcement agency that protects and defends the DON [Department of Navy] against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the UCMJ, assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis.
-- SECNAVINST 540.107, NCIS, 28 Dec 2005

Near Real Time. Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02 & TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 2010) Also see *real time*.

Need-to-know. A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 1-02)

-- Also, a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (DoD 5200.1-R, Jan 1997)

-- Also, a determination within the executive branch in accordance with directives issued pursuant to this order [EO 13526] that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (EO13526, Classified National Security Information, 29 Dec 2009)

“The need-to-know principle is fundamental to the intelligence business.”

-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 310

The “need-to-know” principle, simply put, is that a person in authorized possession of classified information must determine that another person requires access to that information in order to perform a specific and authorized function and that such person has appropriate clearances and access approvals.

...A major tightening up of the “need-to-know” practice is in order. It is particularly disturbing to see the proliferation of detailed knowledge about intelligence sources and methods.

-- HPSCI Report (#100-5), “United States Counterintelligence and Security Concerns - 1986” (p. 9)

Net-Centric. The ability to provide a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Network Operations (NetOps). Activities conducted to operate and defend the Global Information Grid. (JP 1-02 & JP 6-0)

Nickname. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes. (JP 1-02 and DoD 5200.1-R, Information Security Program, Jan 1997) Also see *codeword*.

Non Attributable Internet Access. Use of a commercial internet service provider to access publicly available information on the internet while protecting the unit’s U.S. government affiliation, disclosing essential elements of friendly information, or exposing U.S. government information systems to intrusion or manipulation. (AR 381-20, Army CI Program, 25 May 2010)

Noncustodial Interview. Interview conducted when subjects are interviewed without depriving them of their freedom in any significant manner (e.g., arrest or detention). Subjects voluntarily consent to the interview and are advised that they may depart at any time. (Army FM 2-22.2, CI, Oct 2009)

Nongovernmental Organization (NGO). A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02 and JP 3-08)

-- Also, a legally-constituted organization created by persons having the legal authority to do so with no participation or representation of any government. (DoDD 3240.40, Critical Infrastructure, 14 Jan 10)

Non-Official Cover (NOC). Term used by case officers who operate overseas outside the usual diplomatic cover. (Spy Book)

-- Also, NOC, pronounced as “knock,” an acronym for “nonofficial cover.” Primarily a CIA term used where one is operating without cover of diplomatic protection or US government employment. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Case officers that have no visible affiliation with the U.S. government. NOCs, as they are called, might typically operate as business executives, students, writers, or in some other nongovernmental capacity. They perform those jobs in addition to doing their espionage. If they are caught in the act of spying, they do not have diplomatic immunity and are subject to the full force of the local law, including prosecution for espionage and imprisonment. NOCs usually receive less scrutiny and surveillance from the local authorities than their official colleagues.

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

According a Congressional Research Service report, placing U.S. intelligence officials in foreign countries under “nonofficial cover” (NOC) in businesses or other private capacities is possible, but it presents significant challenges to U.S. agencies. Administrative mechanisms are vastly more complicated [than those] for officials formally attached to the embassy; special arrangements have to be made... The responsibilities of operatives under nonofficial cover to the parent intelligence agency have to be reconciled with those to private employers, and there is an unavoidable potential for conflicts of interest...

-- CRS Report RL33539, *Intelligence Issues for Congress*, 20 Jan 2011, p. 6

Non-permissive Environment. An operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have effective control of the territory and population in the intended operational area (Uncertain Environment); or an operational environment in which hostile forces have control as well as the intent and capability to oppose or react effectively to the operations a unit intends to conduct (Hostile Environment). (National Military Strategy to Combat Weapons of Mass Destruction, Feb 2006)

Non-State Sponsored Terrorism. Terrorist groups that operate autonomously receiving no significant support from any government. (DoDD 2000.12)

Non-Title 50 (NT50). Refers to those federal departments and organizations whose authorities derive from portions of United States Code other than Title 50, which addresses U.S. intelligence activities. NT50s are involved in many activities that affect national security, such as conducting foreign affairs; combating pandemic diseases; halting illicit trafficking; conducting scientific and medical research; regulating finance, commerce, and transportation; and protecting food, water and nuclear infrastructures.

Notice of Intelligence Potential (NIP). A document alerting consumers of a potential collection opportunity involving sources, It is often associated with travel by the source or attendance at some event. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Notional. Fictitious, imaginary, existing only in the perception of the target. Antonym of real, true, genuine, or legitimate. (CIA, D&D Lexicon, 1 May 2008)

Notorious Individual. Someone who is widely known and has an unfavorable public reputation. (DoDD S-5200.37, 9 Feb 2009)

Nuclear Intelligence (NUCINT). Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources. (JP 1-02 & JP 2-0)

Offensive Counterintelligence Operation (OFCO). A clandestine CI activity conducted for military, strategic, DoD, or national CI and security purposes against a target having suspected or known affiliation with FISS [Foreign Intelligence & Security Service], international terrorism, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department or the United States. The two types of OFCO are double agent operations and Counterintelligence Controlled Source Operations (CSO). (DoDI S-5240.09, OFCO, 29 Oct 2008)

If defensive counterintelligence is checkers, then offensive counterintelligence is chess.

-- Steven Aftergood, "DIA Takes on Offensive Counterintelligence," *Secrecy News* (12 Aug 2008)

An ideal counterintelligence system anticipates the enemy's move, notionally satisfies his needs, and indeed operates a notional intelligence service for him

-- Eric W. Timm, "Countersabotage--A CI Function" *Studies in Intelligence*, V7:2 (Spring 1963), p. 67

Offensive CI operations – CI folks call OFCO – are clandestine CI activities run in support of DoD military national security objectives and programs against individuals known or suspected to be foreign intelligence officers with connections to foreign intelligence or international terrorist activities. And they're run to counter the foreign intelligence operations, espionage, against DoD national activities and, of course, terrorist operations against DOD or national. These are very tightly controlled departmental activities run by a small group of specially selected people within DoD. There are only four organizations in the department that can run these operations – Army Counterintelligence, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and now DIA with the center [Defense CI & HUMINT Center].

-- Toby Sullivan, Director of Counterintelligence for USD/I, 5 Aug 2008;
see Federal News Service transcript at <<http://www.fas.org/irp/news/2008/08/dia-dchc.pdf>>

For detailed information concerning DoD OFCO see DoDI S-5240.09, *OFCO (U)*, 29 Oct 2008

Many of these offensive operations have changed history, but remain a misunderstood, and even unappreciated, CI penetration methodology.

-- CI Centre

-- Also, previously defined in DoDD O-5240.02, dated 20 Dec 2007, as an approved CI operation involving a formally recruited human source conducted for DoD or national purposes against a target having suspected or known foreign intelligence and security services affiliation, international terrorist affiliation, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department and/or the United States.

Note: this definition deleted from DoDD O-5240.02 with Change 1, dated 30 Dec 2010.

Offensive Cyber Operations. Includes all US Government programs and activities that, through the use of cyberspace, 1) actively gather information from computers, information systems or networks or 2) manipulate, disrupt, deny, degrade, or destroy targeted adversary computers, information systems, or networks. (NSPD-38)

Official Information. Information that is owned by, produced for or by, or is subject to the control of the United States Government. (JP 1-02 & JP 3-61)

Office of the National Counterintelligence Executive (ONCIX). [The U.S. Government agency] charged with integrating the activities of all CI programs to make them coherent and efficient, coordinating CI policy and budgets to the same end, and evaluating the performance of the CI community against the [National CI] strategy. (National Intelligence: A Consumer's Guide - 2009) Also see *National Counterintelligence Executive*.

-- Also, the ONCIX is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces: annual foreign intelligence threat assessments and other analytic CI products; an annual national CI strategy for the US Government; priorities for CI collection, investigations, and operations; CI program budgets and evaluations that reflect strategic priorities; in-depth espionage damage assessments; and CI awareness, outreach, and training standards policies. (www.ncix.gov)

Additional information on ONCIX at <<http://www.ncix.gov/about/index.html>>

One-Time Pad (OTP). Sheets of paper or silk printed with random five-number group ciphers to be used to encode and decode enciphered messages. (CI Centre Glossary)

-- Also, groups of random numbers or letters arranged in columns, used for encoding and decoding messages. Since the codes are only used once, a properly employed OTP is theoretically unbreakable. (Spycraft)

-- Also, sheets of randomly generated numbers, usually formatted into four- or five-digit groups. Each party to the secret communication... uses the same one-time pad. By a simple process of alphabetic substitution, along with "false subtraction" and "false addition," the two sides can securely communicate with each other. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

One-Time Source. A source who, may not reasonably be expected to provide information on a regular or continuing basis by reason of limited knowledgeability or circumstances of contact. (HDI Lexicon, April 2008)

-- Also, a source of information of value that was, and will be, encountered only once. (US Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

A one-time source **cannot be tasked** to collect information, but can be sensitized to information in which the collector is interested.

One-Way Radio Link (OWRL). The method of transmitting over radio (by voice, key, or impulses) messages to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, 9 Jun 2000)

One-Way Voice Link (OWVL). One-way radio link that transmits a coded voice message to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, 9 Jun 2000)

-- Also, shortwave radio link used to transmit prerecorded enciphered messages to an operative, who is usually working in place in a hostile area. (CI Centre Glossary)

Open. Not classified or concealed. (CIA, D&D Lexicon, 1 May 2002)

Open Source Acquisition. The act of gaining possession of, or access to open source information synonymous with "open source collection." The preferred term is acquisition because by definition, open sources are collected and disseminated by others[,] open source exploiters acquire previously collected and publicly available information second-hand. (ICD 301, National Open Source Enterprise, 11 Jul 2006)

Open Source Center (OSC). Advances the Intelligence Community's exploitation of openly available information to include the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery; functions include collection, analysis and research, training and information technology management to facilitate government-wide access and use. The Director CIA will administer the Center on behalf of the DNI. (ODNI News Release 6-05, 8 Nov 2005)

-- Also, the OSC acts as a service of common concern to advance the IC's exploitation of open source material and nurtures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the USG; established at CIA and builds on the former Foreign Broadcast Information Service and will include personnel from across the IC and other USG organizations; Dir CIA serves as the DNI's Executive Agent for the Center. (ICD 310, National Open Source Enterprise, 11 Jul 2006)

Open Source Information. Publicly available information which anyone can lawfully obtain by request or observation. (ICD 301, National Open Source Enterprise, 11 Jul 2006)

We have no need for spies. We have the Times.

-- Tsar Nicholas I cited in Haswell, *Spies and Spymasters* (1977)

Open-Source Intelligence (OSINT). Information of potential intelligence value that is available to the general public. (JP 1-02 & JP 2-0)

"Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond. "

-- Lieutenant General Samuel V. Wilson, USA (Ret.), Former Director, Defense Intelligence Agency

-- Also, intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (PL109-163 § 931 and ICD 1, 1 May 2006)

-- Also, relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements. (Army FM 2-22.9, Open Source Intelligence, Dec 2006)

-- Also, the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Army FM 2-0, Intelligence, 23 Mar 2010)

OSINT generally falls into four categories: 1) widely available data and information; 2) targeted commercial data; 3) individual experts; and 4) "gray" literature, which consists of written information produced by the private sector, government, and academe that has limited availability, either because few copies are produced, existence of the material is largely unknown, or access to information is constrained.

OSINT can include: media such as newspaper, magazines, radio, television, and computer-based information; public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches; information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts; commercial data such as commercial imagery; *gray literature* such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys; and information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging, as well as information derived from Internet blogs.

-- CRS Report RL34270 (5 Dec 2007)

Operation Order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5-0, Joint Planning, 26 Dec 2006)

Operation Plan (OPLAN). 1) Any plan for the conduct of military operations prepared in response to actual and potential contingencies; or 2) In the context of joint operation planning level 4 planning detail, a complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data. It identifies the specific forces, functional support, and resources required to execute the plan and provide closure estimates for their flow into theater. (JP 5-0, Joint Planning, 26 Dec 2006)

Operational Control (OPCON). Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP 1-02)

Operational Environment. A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02)

Operational Intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. (JP 1-02 & JP 2-0) Also see *strategic intelligence*; *tactical intelligence*.

Operational Interest (OI). [Within HUMINT usage] exclusive contact with a source, as established by a HUMINT organization. Within DoD, established for all sources upon IDSRS Deconfliction and assignment of a NFN. Between DoD and other national agencies, granted for clandestine leads and sources by the Interagency Source Registry (ISR). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Operational Level of War. The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. Activities at this level link tactics and strategy by establishing operational objectives needed to achieve the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. (JP 1-02 & JP 3-0) Also see *tactical level of war*; *strategic level of war*.

Operational Proposal. A formal document prepared by DoD collection elements to outline a proposed activity or operation. (HDI Lexicon, April 2008)

Operations Support Element (OSE). An element that is responsible for all administrative, operations support and services support functions within the counterintelligence and human intelligence staff element of a joint force intelligence directorate. (JP 1-02) [Normally in the J2X]

Operational Testing. A continuing process of evaluation that may be applied to either operational personnel or situations to determine their validity or reliability. (JP 1-02)

-- Also, any means or process employed to establish authenticity, reliability, or control. (HDI Lexicon, April 2008)

Operations Officer (CIA). A career track within the *Core Collector* profession of the National Clandestine Service (NCS), Central Intelligence Agency (CIA). Operations Officers (OO's) are focused full time on clandestinely spotting, assessing, developing, recruiting, and handling individuals with access to vital foreign intelligence on the full range of national security issues. OO's use their sound judgment, high integrity, strong interpersonal skills, and ability to assess the character and motivations of others to establish strong human relationships and trust that provides the foundation needed to acquire high-value intelligence from foreign sources. An OO's career can include assignments in the NCS's three key areas of activity—human intelligence collection, counterintelligence, and covert action—on issues of highest interest to US national security, such as international terrorism, weapons proliferation, international crime and narcotics trafficking, and capabilities and intentions of rogue nations. Operations Officers serve the bulk of their time in overseas assignments that range typically from 2-3 years. (CIA; see <<https://www.cia.gov/careers/jobs/view-all-jobs/core-collector.html>>, accessed 19 Mar 2009)

Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02 & JP 3-13.3)

Operations Security Vulnerability. A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking. (JP 1-02 & JP 3-13.3)

OPSEC Process. A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements: 1) critical information identification; threat analysis; 3) vulnerability analysis; 4) risk assessment; and 5) OPSEC countermeasures. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Organized Cyber Intruders/Attackers. Those individuals, groups or organizations who violate international law or conventions relating to computer networks or who otherwise use the cyberspace domain to interfere with, disrupt, or deny computer network services. (OSD, *Guidance for Employment of the Force*)

Other Government Agency (OGA). Within the context of interagency coordination, a non Department of Defense agency of the United States Government. (JP 1 & JP 1-02)

Overt. Activities that are openly acknowledged by or readily attributable to the US Government, and include activities designed to acquire information through legal and open means without concealment. Overt information may be collected by observation, elicitation, or from knowledgeable human sources. (ICD 304, HUMINT, 6 Mar 2008; DoDD S-5200.37, 9 Feb 2009; JP 1-02; and JP 2-01.2)

-- Also, refers to being in the open, without any attempt to deceive or mislead, with full knowledge of coordinating units or agencies; activity done without attempt to conceal it. (CI Community Lexicon)

-- Also, methods of conducting DoD activities that may be acknowledged by or attributable to the U.S. Government. (HDI Lexicon, April 2008)

Overt Collection. Intelligence activities with the ultimate goal of intelligence information collection which are not designed or executed to conceal sponsorship, collection activity, identity of operators, or methodologies employed. (DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *open source intelligence*.

-- Also, the acquisition of intelligence information in the public domain. (CI Community Lexicon)

“While the importance of clandestine collection should not be underestimated, many of the pieces of the jigsaw puzzle which is ‘finished foreign intelligence’ can be overtly collected by a well-organized information gathering system.”

-- Rockefeller Commission Report (June 1975), p. 209

Overt Operation. An operation conducted openly, without concealment. (JP 1-02 & JP 3-05.1)

Overt [HUMINT] Operations. Openly acknowledged by, or are readily attributable to, the US Government. Overt HUMINT methods include: debriefing, interrogation, elicitation, and observation. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Paramilitary Forces. Forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02 & JP 3-24)

Parole. A prearranged verbal exchange used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, 9 Jun 2000)

Patterns, [In CI usage,] ...repeated incidents that may be similar in nature or dissimilar events that occur in a specific location or time span that may indicate potential FISS and ITO [international terrorist organization] targeting or information exploitation. (Army FM 2-22.2, CI, Oct 2009)

Patriot Act. The official title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." An act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. (PL 107-56, 26 Oct 2001)

The Patriot Act substantially expanded the authority of U.S. law enforcement agencies for the stated purpose of fighting terrorism in the United States and abroad. Among its provisions, the Act:

- increased the ability of law enforcement agencies to search telephone and e-mail communications and medical, financial and other records;
- eased restrictions on foreign intelligence gathering within the United States;
- expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and
- enhanced the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts.

The act also expanded the definition of terrorism to include "domestic terrorism," thus enlarging the number of activities to which the Patriot Act's expanded law enforcement powers can be applied.

The Patriot Act made a number of changes to U.S. law. Key acts changed were the Foreign Intelligence Surveillance Act of 1978 (FISA), the Electronic Communications Privacy Act of 1968 (ECPA), the Money Laundering Control Act of 1986, and Bank Secrecy Act (BSA), as well as the Immigration and Nationality Act.

Link to the Patriot Act available at: <<http://www.ncix.gov/publications/law/index.html>>

Peace Building (PB). Stability actions, predominately diplomatic and economic, that strengthen and rebuild governmental infrastructure and institutions in order to avoid a relapse into conflict. (JP 3-0, Joint Operations)

Peace Enforcement. Application of military force or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order. (JP 3-0, Joint Operations)

Peacekeeping. Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peacemaking. The process of diplomacy, mediation, negotiation, or other forms of peaceful settlements that arranges an end to a dispute and resolves issues that led to it. (JP 3-0, Joint Operations)

Peace Operations (PO). A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts. (JP 3-07.3 Peace Operations, 17 Oct 2007)

Pen Register. A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider, or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider, or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; see 18 USC §3127(3). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *trap and trace*.

A pen register shows all outgoing phone numbers to a particular telephone has called.

-- Also, [a device that] records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Penetration. [In intelligence usage,] the recruitment of agents within or the infiltration of agents or technical monitoring devices in an organization or group for the purpose of acquiring information or of influencing its activities. (ICS Glossary)

Note: This term was previously in JP 1-02, however rescinded by JP 2-01.2, 11 Mar 2011.

-- Also, a principal counterintelligence objective is penetration of an adversary, and this can be achieved by the recruitment of a key source within an opponent's organization. Ideally, the penetration will be the recruitment of a senior figure with sufficient access to compromise all the service's operations, but lower-level penetrations, such as the management of a double agent, may be sufficient to reveal the identities of case officers and their operational premises. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

**Penetration – a time-honored espionage practice
...oh what a tangled web we weave**

"The key to CI success is penetration. For every American spy, there are several members of the opposition service who know who he or she is. No matter what it takes, we have to have penetrations."

-- James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, Vol. 54 No. 5; see <<https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol45no5/html/v45i5a08p.htm>>

"Almost every spy that we have found, both in the CIA and FBI, has been found with the aid of recruited sources of our own on other hostile intelligence services."

-- William Webster, Former FBI Director and DCI, in Senate testimony (9 Apr 2002)

If the purpose of counterespionage is to manipulate enemy intelligence, as it is, then to have controlled agents in the staff of an enemy service is the most important objective of counterintelligence. -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

...[C]ounterespionage has one purpose which transcends all others in importance: **penetration**. The only way to be sure that an enemy has been contained is to know his plans in advance and in detail. Moreover, only a high-level penetration of the opposition can tell you whether your own service is penetrated.

...**Conducting CE without the aid of penetrations is like fighting in the dark**. Conducting CE with penetrations can be like shooting fish in a barrel. The famous case of Col. Oleg Penkovskiy... illustrates the great value of penetrations. There can never be enough of them.

-- Austin B. Matschulat, "Coordination and Cooperation in Counterintelligence," *Studies in Intelligence*, V13: 2 (Spring 1969), pp. 29-30.

Penetrations - selected examples:

- Colonel L Oleg V. Penkovsky was a British-US penetration of Soviet military intelligence (GRU).
- Harold A.R. "Kim" Philby was a Soviet penetration of British intelligence.
- Aldrich "Rick" Ames was a Soviet/Russian penetration of the CIA.
- Robert (Bob) Hanssen was a Soviet/Russian penetration of the FBI.

Penetration Operation. The recruitment of agents within, the infiltration of agents, or the introduction of technical monitoring devices into an organization or physical facility to acquire information or influence the organization's activities. (AR 381-47, OFCO, 17 Mar 2006)

Perception Management. None within DoD; *term approved for removal from JP 1-02*.

Permissive Environment. Operational environment in which host country military and law enforcement agencies have control as well as the intent and capability to assist operations that a unit intends to conduct. (JP 1-02 & JP 3-0)

Persistent Conflict. The protracted confrontation among state, nonstate, and individual actors that are increasingly willing to use violence to achieve their political and ideological ends. (Army FM 3-0, Operations, Feb 2008)

Persistent Surveillance. A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time. Persistent surveillance facilitates the prediction of an adversary's behavior and the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action. (JP 1-02 & JP 2-0)

Persona Non Grata (PNG). An international diplomatic term meaning "person who is not acceptable or not welcome." It is a legal status applied to diplomats who have been caught by the host country in espionage or other unlawful activities and are expelled and thereafter denied access to the host country. (CI Community Lexicon)

Latin for "unwelcome person." The provision for declaring a person *persona non grata* is codified in international law; see Article 9 of the Vienna Convention on Diplomatic Relations of 1961.

-- Also, in diplomatic usage and under international law, the official act of declaring a foreign national, usually an official of a foreign government, as no longer welcome and forcing his/her expulsion. In tradecraft terminology, the undesirable individual in *PNG'd*. The most common use of *PNG* is for foreign diplomatic or official personnel caught in the act of engaging in illegal espionage activities. (*The CIA Insider's Dictionary*, 1996)

-- Also, a diplomatic expulsion by flag accrediting country. (AFOSI Manual 71-142, 9 Jun 2000)

Personal Meeting (PM). Face-to-face contact between a handler and a lead or asset. (HDI Lexicon, April 2008)

-- Also, a clandestine meeting between two operatives, always the most desirable but a more risky form of communication. (CI Centre Glossary)

Personnel Security. A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information. (IC Standard 700-1, 4 Apr 2008)

Personnel Security Investigation (PSI). An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. (JP 1-02)

A PSI is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he/she is eligible to access classified information, or for an appointment to a sensitive position or position of trust. DoD uses PSIs to determine an individual's eligibility for a security clearance.

The types of PSIs vary based on the level of security clearance necessary for a given sensitive position. DoD Regulation 5200.2-R, "Personnel Security Program," outlines criteria for sensitive positions and the corresponding clearance levels. Each clearance level requires a different type of PSI.

Phishing. A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. (McAfee.com, accessed 15 Nov 2010)

Physical Search. Any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. (DoD 5240.1-R, Dec 1982)

Types include consented physical search, plain view search, search incident to a lawful apprehension, and nonconsensual physical search. See USC 1821(5).

Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02 and JP 3-0)

-- Also, the security discipline concerned with physical measures designed to: protect personnel; prevent unauthorized access to facilities, equipment, material, and documents; and defend against espionage, terrorism, sabotage, damage, and theft. (IC Standard 700-1, 4 Apr 2008)

Physical Security Investigation. All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property. (JP 1-02)

Physical Surveillance. A systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. (DoD 5240.1-R, Dec 1982) Also see *surveillance*.

Surveillance, the job of following and observing designated persons without being noticed, is intrinsic to counterintelligence. -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

-- Also, the deliberate observation... of persons, places, or events, on either a limited or continuous basis, in a public or a semi-public (e.g., commercial business open to the public) setting. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Piracy. An illegal act of violence, depredation (e.g., plundering, robbing, or pillaging), or detention in or over international waters committed for private ends by the crew or passengers of a private ship or aircraft against another ship or aircraft or against persons or property on board such ship or aircraft. (JP 1-02)

Pitch. [In intelligence usage] the effort made to recruit a source. (HDI Lexicon, April 2008)

Placement. An individual's proximity to information of intelligence interest. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the rationale for a HUMINT source or operational asset's presence in an operational area. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Placement and Access. An individual's proximity to and ability to collect information of intelligence interest. (HDI Lexicon, April 2008)

Planned Target. Target that is known to exist in the operational environment, upon which actions are planned using deliberate targeting, creating effects which support commander's objectives. (JP 3-60)

Planning. The ability to establish a framework to employ resources to achieve a desired outcome or effect. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, the process by which commanders (and the staff, if available) translate the commander's visualization into a specific course of action for preparation and execution, focusing on the expected results. (Army FM 3-0, Operations, Feb 2008)

Planning and Direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (JP 1-02 & JP 2-01)

Planning Order (PLANORD). A planning directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action. (JP 5-0) Also see *execute order (EXORD)*.

Plant. [In intelligence usage,] 1) to insert information into a target's intelligence channel; 2) an individual infiltrated into a foreign organization (a penetration); 3) a forged document provided to a foreign organization. (CIA in D&D Lexicon, 1 May 2002)

Planted Information. False or misleading information that the target has been permitted or helped to collect. (CIA in D&D Lexicon, 1 May 2002)

Platform. In collection parlance, the conveyance for collection sensors.

Plausible Denial. Official disclaimer supported by a believable cover story. (CIA in D&D Lexicon, 1 May 2002) Also see *plausible deniability*.

Plausible Deniability. The concept that allows the United States government, specifically the U.S. president himself, to claim no knowledge of or involvement in a covert action that goes public, particularly if it has gone badly. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Pocket Litter. The usual litter found in pockets: coins, tickets, keys, etc. In this case, pocket litter is planted so that if the agent is caught, incidental-looking items will reinforce his cover story. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Political Intelligence. Intelligence concerning foreign and domestic policies of governments and the activities of political movements. (JP 1-02)

Polygraph Examination. A process that encompasses all activities that take place between a polygraph examiner and examinee during a specific series of interactions. (DoDD 5210.48, PCA Program, 25 Jan 2007) Also see *credibility assessment*.

-- Also, a highly structure technique conducted by specialty trained CI personnel certified by proper authority as polygraph examiners. (Army FM 2-22.2, CI, Oct 2009)

The most significant contribution of the polygraph is its success in eliciting information and its value as a deterrent; however, the polygraph should be one of several investigative tools.

-- Webster Commission Report (A review of FBI Security Programs), March 2002 (p. 68)

PORTICO. The nickname for the DoD Counterintelligence Community's enterprise information capability that promotes information sharing and provides standardized CI activity reporting across the Department. PORTICO operates in a secure network environment and facilitates standardization of DoD CI business processes by providing a common interface for shared results of core CI functions (i.e., collection, investigations, analysis & production, operations, and functional services).

Port Security. The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. (JP 1-02 & JP 3-10)

Positive Intelligence. A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence. (ICS Glossary, 1978)

-- Also, information gathered concerning a foreign power that is significant to national security, foreign relations, economic interest, and other plans and policies of a government. (CI Community Lexicon)

In the early 1900's military intelligence consisted of two separate fields of endeavor: positive intelligence and negative intelligence. Positive intelligence focused on "seeking information on our enemies or potential enemies" and negative intelligence focused on "preventing enemies or potential enemies from acquiring information of value about the United States." Following World War I, the term *negative intelligence* was replaced by *counterintelligence*.

-- Source: Bruce W. Bidwell, *History of the MI Division... Army General Staff: 1775 - 1941* (1986)

Posse Comitatus Act. Prohibits search, seizure, or arrest powers [by] US military personnel [in civilian law enforcement matters in the US unless authorized by legislation]. Amended in 1981 under Public Law 97-86 to permit increased DoD support of drug interdiction and other law enforcement activities. [Title 18, USC § 1385] (JP 1-02)

Posse Comitatus Act (PCA) places strict limits on the use of federal military personnel for law enforcement. Enacted in 1878, PCA prohibits the willful use of the US Army (and later, the US Air Force) to enforce laws, except as authorized by the Congress or the US Constitution. Although the PCA, by its terms, refers only to the Army and Air Force, DoD policy extends the prohibitions of the Act to the US Navy and Marine Corps, as well.

Specifically prohibited activities include: interdiction of a vehicle, vessel, aircraft, or similar activity; search and/or seizure; arrest, apprehension, "stop-and-frisk" detentions, and similar activities; and use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. Additionally, federal courts have recognized exceptions to the PCA. These common law exceptions are known as the "military purpose doctrine" and the "indirect assistance" exceptions.

Exceptions and/or circumstances not falling under PCA include:

- 1) Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States;
- 2) Federal troops acting pursuant to the President's Constitutional and statutory authority to respond to civil disorder;

- 3) Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations; and
- 4) Civil Disturbance operations authorized by statute.

The PCA does not apply to National Guard forces operating in state active duty or Title 32 USC status, nor to the USCG, which operates under Title 14 USC authority.

For an overview of the Posse Comitatus Act, see CRS Report 95-964, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, by Charles Doyle.

Also see DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials*, 15 Jan 1986, in particular enclosure 4.

Preliminary Inquiry. An unobtrusive review of the facts and circumstances of an incident or allegation to determine if the preliminary information or circumstances is sufficient to warrant the initiation of an investigation or referral to an investigative entity. The limited objective will be determined by the policy of individual agencies and may include the collection of information from other agencies and/or other records such as travel, financial, HR, security, and badgeing, etc.; which may be used to make an informed determination if the incident involved is part of a pattern. (ONCIX Insider Threat Detection – Glossary) Also see *counterintelligence investigation*, counterintelligence preliminary inquiry, *investigation*; *Section 811 referral*.

Preparation of the Environment (PE). An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. (JP 3-05, Special Operations, 18 Apr 2011; approved for inclusion in JP 1-02.)

Preventive Deployment. The deployment of military forces to deter violence at the interface or zone of potential conflict where tension is rising among parties. Forces may be employed in such a way that they are indistinguishable from a peace operations force in terms of equipment, force posture, and activities. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Preventive Diplomacy. Diplomatic actions taken in advance of a predictable crisis to prevent or limit violence. (JP 1-02 and JP 3-0)

Priority Intelligence Requirement (PIR). An intelligence requirement stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. (JP 1-02 & JP 2-0)

Prisoner of War (POW or PW). A detained person as defined in Articles 4 and 5 of the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949. In particular, one who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts which do not amount to breaches of the law of armed conflict. For example, a prisoner of war may be, but is not limited to, any person belonging to one of the following categories who has fallen into the power of the enemy: a member of the armed forces, organized militia or volunteer corps; a person who accompanies the armed forces without actually being a member thereof; a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment; or individuals who, on the approach of the enemy, spontaneously take up arms to resist the invading forces. (JP 1-02)

Probable Cause. 1) To search: A reasonable belief that a crime has been committed and that the person, property, or evidence sought in connection with the crime is located in the place or on the person to be searched; and/or 2) To apprehend: A reasonable belief that a crime has been committed and that the person to be apprehended committed it. (AR 190-20, Military Police Investigations)

Probe. In information operations, any attempt to gather information about an automated information system or its on-line users. (JP 1-02 & JP 3-13) Also see *information operations*.

Processing and Exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 1-02 & JP 2-01)

Production. The preparation of reports based on analysis of information to meet the needs of intelligence users (Consumer's) within and outside the Intelligence Community. (CIA, *A Consumer's Guide to Intelligence*, July 1995) Also see *intelligence production*.

-- Also, conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of data from all available sources and the preparation of intelligence products in support of known or anticipated user requirements. (AR 381-20, Army CI Program, 25 May 2010)

Production results in the creation of intelligence, that is, value-added actionable information tailored to a specific customer. In government parlance, the term "finished intelligence" is reserved for products issued by analysts responsible for synthesizing all available sources of intelligence, resulting in a comprehensive assessment of an issue or situation, for use by senior analysts or decision makers.

– DIA, *Intelligence Essentials for Everyone*, June 1999

Production Requirement. A customer's formal request for analytic support, identifying the topic or issue of interest, type of information or analysis required, date required, preferred format, and classification. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Proliferation. The transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors. (JP 1-02 & JP 3-40)

Prominent Individual. Someone who is widely known and has a favorable public reputation. (DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009)

Propaganda. Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 1-02 & JP 3-13-2)

Protection. The ability to prevent, mitigate adverse effects of attacks on personnel (combatant /non-combatant) and physical assets of the United States, allies, and friends. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 1-02 and JP 3-0)

Provocation. Activity intended to cause an individual, organization, intelligence service, or government to take actions that can cause damage to itself. (Spy Book) Also see *dangle*.

-- Also, [aka *dangle*] an agent deployed by you to be recruited by an opponent and to perform his or her secret work *under your control* as a channel to and weapon against your opponent. (William R. Johnson, *Thwarting Enemies at Home and Abroad*, 2009)

Pseudonym. A code name assigned to an individual, place, or activity to enhance operational, administrative, and communication security. (AFOSI Manual 71-142, 9 Jun 2000)

Psychological Operations (PSYOP). *None; rescinded term; see Military Information Support Operations (MISO)*.

Term changed to MISO IAW SECDEF Memo dated 3 Dec 2010.

Public Affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. (JP 1-02 and JP 3-61)

Public Diplomacy. 1). Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2). In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. Its objective is to promote and sustain consent for peace building both within the host nation and externally in the region and in the larger international community. (JP 1-02 and 3-07.3)

Public Information. Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or nonobjectionable to the responsible releasing agency. (JP 1-02 and JP 3-13)

Publicly Available Information. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any vent that is open to the public. (Attorney General Guidelines for National Security Investigations and Foreign Intelligence Collection, 31 Oct 2003)

Quit Claim. A document in which an asset acknowledges that all commitments due have been met by the handler's organization. (HDI Lexicon, April 2008)

Rabbit. [Tradecraft jargon --] The target in a surveillance operation. (CI Centre Glossary)

Radiogram. Coded bursts of data sent by a radio transmitter that can be picked up by a radio receiver that has been set to the proper frequency; as transmitted, radiograms generally sound like the transmission of Morse code. (FBI Affidavit, 25 June 2010)

Radar Intelligence (RADINT). Intelligence derived from data collected by radar. (JP 1-02 & JP 2-0)

Reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

Reactive Operation. An operation initiated in response to a FIS personal contact. (AFOSI Manual 71-142, 9 Jun 2000)

Real Time. Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (JP 2-0) Also see *near real time*.

Reasonable Belief. A reasonable belief arises when the fact and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on the facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. (DoD 5240.1-R, December 1982)

Recognition Signal. Any prearranged signal by which individuals or units may identify each other. (JP 1-02)

-- Also, prearranged visual indicator used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, 9 Jun 2000)

Records Check. The process whereby a Special Agent obtains relevant information about Sources or Subjects from the records and information holdings of military, civilian or government agencies, as well as certain commercial companies and vendors, during the conduct of an investigation or operation. Types include military agency checks (MACs), local agency checks (LACs) and national agency checks (NACs).

-- *Military Agency Check (MAC):* a records or files check conducted at any military agency within the jurisdiction of the CI element conducting the check.

-- *Local Agency Check (LAC):* a records or files check of official or publically available information retained by any local office or government agency within the jurisdiction of the CI element conducting the check. Records may include holdings and databases maintained by local and state law enforcement agencies, local courts, local offices of federal agencies, etc.

-- *National Agency Check (NAC):* formal requests to federal agencies for searches of their records and supporting databases and files for information of investigative or operational interest. NACs include DoD agencies, as well as other federal agency holdings, e.g., FBI, CIA, DHS, IRS, OPM, State Department, FINCEN, etc.

Recovery Operations. Operations conducted to search for, locate, identify, recover, and return isolated personnel, human remains, sensitive equipment, or items critical to national security. (JP 1-02 & JP 3-50)

Recruitment. The deliberate and calculating effort to gain control of an individual and to induce him or her to furnish information and/or to carry out intelligence tasks for an intelligence or counterintelligence service. (CI Community Lexicon and DoDI S-5240.17, CI Collection, 12 Jan 2009)

-- Also, authorized personnel establishing control over an foreign individual who, witting or unwitting of USG involvement, accepts tasking as a result of the established relationship; authorized personnel establishing control over a U.S. person who, fully aware of USG involvement, accepts tasking as a result of the established relationship. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009 w/ chg 1 16 Aug 2010)

-- Also, the acquisition of an individual's services who, witting or unwitting of U.S. Government involvement, accepts directions and control thus obligating both parties to an act in a prescribed manner. (HDI Lexicon, April 2008)

-- Also, term for the tradecraft process of enlisting a target individual to work for an intelligence or security service. (*The CIA Insider's Dictionary*, by Leo D. Carl, 1996)

Agent recruiting is the most important task of both strategic and operational intelligence. No real problems can be solved without agent penetration in basic government, military and technological centres of the enemy.

-- Victor Suvorov, *Inside Soviet Military Intelligence* (1984); see Chapter 4 - Agent Recruiting.

Recruitment Cycle. The... process by which intelligence services recruit agents (aka the agent acquisition process). (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

"The recruitment cycle is the essence of spying"

Seven steps of the recruitment cycle: 1) Spotting; 2) Assessing; 3) Developing; 4) Pitching; 5) Formalizing; 6) Producing; and 7) Terminating.

-- James M. Olson (CIA Retired)

Seven basic areas: 1) Spotting; 2) Evaluation; 3) Recruiting; 4) Testing; 5) Training; 6) Handling; and 7) Termination.

- + Spotting: *the process of identifying foreigners or other persons who might be willing to spy...*
 - + Evaluation: *a thorough review of all information available...*
 - + Recruiting: *the recruitment "pitch"... People volunteer or agree to spy on their governments for many reasons. It is the task of the recruiter to determine what reason—if one exists—is most likely to motivate the potential agent. .*
 - + Testing: [testing the asset's] *loyalty and reliability ...*
 - + Training: [tradecraft training] *instructed in one of several methods of covert communications... learn the use of clandestine contacts. And... will be given training on security precautions, such as the detection and avoidance of surveillance.*
 - + Handling: *Successful handling of an agent hinges on the strength of the relationship that the case officer is able to establish with the agent.a good case officer must combine the qualities of a master spy, a psychiatrist, and a father confessor. ...One of the biggest problems in handling an agent is caused by the changeover of case officers.*
 - + Termination: *All clandestine operations ultimately come to an end. ...[need for] resettlement*
- Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence*, 2nd Edition (1980), pp 215-228

Agent recruitment: 1) Spot; 2) Assess; 3) Develop & Recruit; 4) Test; 5) Train; 6) Handle; and 7) Terminate
-- Jefferson Mack, *Running a Ring of Spies* (1996)

Recruitment-in-Place (RIP). An official who overtly continues to work for his government and clandestinely provides information of intelligence value to a foreign government; will in many instances be connected with a foreign government's intelligence service. (CI Community Lexicon) Also see *penetration*.

-- Also, 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. (ICS Glossary)

It is axiomatic in intelligence work that 'there is no better counterintelligence than recruiting the other side's intelligence officers.'
-- James M. Olson (CIA Retired)

Red Team. An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (JP 1-02 & JP 2-0)

Red Team Analysis. Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

Red Team analysis tries to consciously place the analyst in the same cultural, organizational, and personal setting -- "putting them in their shoes" -- in which the target individual or group operates. Red Team analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary.

Contrarian methods and "Red Teams" should be a routine part of the analytical process.
-- Jeffrey R. Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 43

Refugee. A person who owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country. See also *dislocated civilian; displaced person; evacuee; expellee; stateless person*. (JP 1-02 & JP 3-29)

Regional Security Officer (RSO). A security officer responsible to the chief of mission (ambassador), for security functions of all US embassies and consulates in a given country or group of adjacent countries. (JP 1-02 & JP 3-10)

-- Also, Diplomatic Security Special Agents of the U.S. Department of State (DoS), assigned to U.S. diplomatic missions overseas as the personal advisor to the ambassador or chief of mission on all security issues and coordinate all aspects of a mission's security program. They develop and implement effective security programs to protect DoS employees from terrorist, criminal, and technical attack both at work and at home. The RSO serves as the primary liaison with foreign police and security services overseas in an effort to obtain support for U.S. law enforcement initiatives and investigations. (DoS)

See DoS website at: <<http://www.state.gov/m/ds/protection/c8756.htm>>

Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Rendition. An extra-territorial activity to apprehend and return a person to the US or another country, with or without permission from the country in which the subject is apprehended. (National HUMINT Glossary)

The term "rendition" in the counterterrorism context means nothing more than moving someone from one country to another, outside the formal process of extradition.

-- Daniel Benjamin, Former Director for Counterterrorism, National Security Council

Repatriate. A person who returns to his or her country or citizenship, having left said native country either against his or her will, or as one of a group who left for reason of politics, religion, or other pertinent reasons. (JP 1-02)

Repatriation. 1) The procedure whereby American citizens and their families are officially processed back into the United States subsequent to an evacuation. (JP 3-68); and 2) The release and return of enemy prisoners of war to their own country in accordance with the 1949 Geneva Convention Relative to the Treatment of Prisoners of War. (JP 1-0)

Reportable Incident. Any suspected or alleged violation of Department of Defense policy or of other related orders, policies, procedures or applicable law, for which there is credible information. (JP 3-63)

Request For Assistance (RFA). A request based on mission requirements and expressed in terms of desired outcome, formally asking for assistance.

Request For Information (RFI). 1) Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A RFI can be initiated to respond to operational requirements and will be validated in accordance with the combatant command's procedures. 2) The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. (JP 1-02 & JP 2-0)

Residency. An office or location in a country used by foreign intelligence officers from which to plan, coordinate, and execute intelligence activities. Also refers to the number of foreign intelligence agents present in a given area. (AR 381-20, Army CI Program, 25 May 2010)

Resistance Movement. An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability. (JP 1-02 & (JP 3-05, Special Operations, 18 Apr 2011)

Responsible Analytical Center (RAC). The Intelligence organization that has responsibility for providing integrated all-source analysis, or application of analysis, to produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. DoD organizations that qualify as RACs

include: DIA analytical offices [including DAC-1C] and Intelligence Centers, the COCOM Joint Intelligence Operations Centers (JIOCs), and the Service intelligence production centers (MCIA, NASIC, NGIC, and ONI). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Restraint. In the context of joint operation planning, a requirement placed on the command by a higher command that prohibits an action, this restricting freedom of action. (JP 1-02 & JP 5-0)

Restricted Area. An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, 1) An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize interference between friendly forces; and 2) An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. (JP 1-02)

Restricted Target. A valid target that has specific restrictions placed on actions authorized against it due to operational considerations. Also see *restricted target list*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Restricted Target List (RTL). A list of restricted targets nominated by elements of the joint force and approved by the joint force commander. This list also includes restricted targets directed by higher authorities. Also see *restricted target*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Returnee. A displaced person who has returned voluntarily to his or her former place of residence. (JP 3-29)

Revolution. The overthrow or renunciation of one government or ruler and the substitution of another by the governed. (Army FM 3-24-2, Tactics in Counterinsurgency, April 2009)

Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, a measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability). (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a measure of the potential degree to which protected information is subject to loss through adversary exploitation. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Risk, in the context of critical infrastructure and terrorism, can be defined as the potential consequence associated with a particular kind of attack or event against a particular target, discounted by the likelihood that such an attack or event will occur (threat) and the likelihood that the target will sustain a certain degree of damage (vulnerability).

Threat includes not only the identification of specific adversaries, but also their intentions and capabilities (both current and future). Consequences include lives and property lost, short term financial costs, longer term economic costs, environmental costs, etc.

Given this definition, risk is not threat, nor vulnerability to a threat, nor the estimated consequences associated with a specific attack, but some integration of the three.

-- CRS Report, RL30153, 8 Jan 2007

Risk Assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.

(DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, the identification and assessment of hazards (first two steps of risk management process). (JP 1-02 & JP 3-07.2)

-- Also, a process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, a defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation. (IC Standard 700-1, 4 Apr 2008)

Risk Management (RM). The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 1-02 & JP 2-0)

-- Also, a process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, process and resultant risk of systematically identifying, assessing and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of selecting and implementing security countermeasures to accept or mitigate the risk of a known or suspected threat to an acceptable level based on cost and effectiveness. (IC Standard 700-1, 4 Apr 2008)

-- Also, *Antiterrorism (AT) risk management*: the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. The end products of the AT program risk management process shall be the identification of areas and assets that are vulnerable to the identified threat attack means. Three critical components of AT risk management: threat assessment, asset criticality assessment, and vulnerability assessment. (DoDD 2000.12, DoD AT Program, 18 Aug 2003)

*The basic concept for a cost effective security system is **risk management** rather than the unattainable and unaffordable goal of risk avoidance.*

-- Joint Security Commission II Report, 24 August 1999, p.12

Rolling Car Pickup. A clandestine car pickup executed so smoothly that the car hardly stops at all and seems to have kept moving forward. (CI Centre Glossary) Also see *car pick-up*.

Rule of the Least Intrusive Means. The collection of information by a DoD intelligence component must be accomplished by the **least intrusive means** or lawful investigative technique reasonably available. (DIA Intelligence Law Handbook, Sep 1995)

This rule prescribes a hierarchy of collection techniques which must be considered before an intelligence component engages in collection of information about US persons. The methodologies below become progressively more intrusive as one proceeds through this hierarchical framework:

- First, to the extent feasible, information must be collected from publically available materials, or with the consent of the person or persons concerned.
- Second, if collection from these sources is not feasible, then cooperating sources may be used.
- Third, if neither publically available information nor cooperating sources are sufficient or feasible, and then collection may be pursued using other lawful investigative techniques that require neither a judicial warrant nor the approval of the Attorney General of the United States.
- Finally, when none of the first three approaches has been sufficient or feasible, then the collecting intelligence component may seek approval for use of one of the techniques that require a warrant or approval of the Attorney General.

Rules of Engagement (ROE). Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 1-02 & JP 1-04)

Ruse. In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 3-13.4)

Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources. (JP 1-02)

-- Also, the willful destruction of government property with the intent to cause injury, destruction, or defective production of national defense or war materials by either an act of commission or omission. (IC Standard 700-1, 4 Apr 2008)

Sabotage is a violation of Title 18 USC, §§ 2151-2156.

Safe House. An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (JP 1-02 & JP 3-07.2)

-- Also, a facility use to afford security for operations. (HDI Lexicon, April 2008)

-- Also, house or premises controlled by an intelligence service that affords at least temporary security for individuals engaged in intelligence operations. (CI Community Lexicon)

-- Also, any house, apartment, office, or other building or quarters used to afford security for persons engaged in clandestine activities or for intelligence collection purposes. Safe houses may be used as refuge for or holding of agents or defectors; lodging and feeding of couriers, escapees, or evaders; lodging and working space for agents; rendezvous training, briefing, or questioning; or storage of supplies and equipment. (National HUMINT Glossary)

-- Also, a secure facility, unknown to adversary intelligence and security services, used for agent meetings, defector housing or debriefing, and similar support functions. (CIA in D&D Lexicon, 1 May 2002)

-- Also, [safehouse] a secure location used by intelligence services to meet with agents or for other clandestine purposes. The renter or purchaser of a safehouse is usually a cutout, someone who has no visible connection with intelligence work or with any official organization. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Sanction Enforcement. Operations that employ coercive measures to interdict the movement of certain types of designated items into or out of a nation or specified area. (JP 1-02 and JP 3-0)

Sanitize. To revise a report or other document in such a fashion as to prevent identification of sources, or of the actual persons and places with which it is concerned, or of the means by which it was acquired. Usually involves deletion or substitution of names and other key details. (JP 1-02)

Sanitization. The editing of intelligence to protect sources, methods, capabilities, and analytical procedures to permit wider dissemination (IC Standard 700-1, 4 Apr 2008)

Scattered Castles. The IC [Intelligence Community] security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, DoD civilians, and contractor personnel. DoD information is furnished by JPAS. (IC Standard 700-1, 4 Apr 2008)

Scientific and Technical Intelligence (S&TI). The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. (JP 1-02 & JP 2-01)

Scientific Method. [One of the four basic types of reasoning applied to intelligence analysis, it] combines deductive and inductive reasoning: induction is used to develop the hypothesis, and deduction is used to test it. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; induction.*

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003).

Screening. In intelligence, [the] evaluation of an individual; or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile coupled with the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. (JP 1-02 & JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Search. An examination, authorized by law, of a specific person, property, or area for specified property or evidence, or for a specific person for the purpose of seizing such property, evidence, or person. (AR 190-20) Also see *search warrant, seizure.*

Search Warrant. An express authorization to search and seize issued by competent civilian authority. (AR 190-20) Also see *search, seizure.*

Seizure. The taking or dispossession of property from the possessor by an authorized person or the restriction of the freedom of movement of an individual against his or her will by an agent of the Government. (AR 190-20)

SECRET Internet Protocol Router Network (SIPRNet). The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. (JP 1-02 & JP 6-0)

Secret Writing (SW). Any tradecraft technique employing invisible messages hidden in or on innocuous materials. This includes invisible inks and microdots, among many other variations. (CI Centre Glossary)

The simplest secret writing uses organic inks: milk, vinegar, lemon juice, even urine. These inks dry invisibly and can be developed by applying heat. Espionage agencies have produced many inks made of chemicals that could be developed only by a specific chemical. -- Spy Book

The chief difficulty with secret inks was their inability to handle great volume of information that spies had to transmit in a modern war. -- David Kahn, *The Codebreakers* (1967)

For an explanation of secret inks, see Robert Wallace and H. Keith Melton, *Spycraft: The Secret History of the CIA's Spyspechs from Communism to Al-Qaeda* (2008), pp. 427-437.

Section 811 Referral. Section 811 of the Intelligence Authorization Act of 1995 (50 USC 402a) is the legislative act that governs the coordination of counterespionage investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are the reports – made by the Executive Branch agencies or departments to the FBI under Section 811(c)(1)(a) – that advise the FBI of any information, regardless of origin, which may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power. (CI Community Lexicon)

Section 811 was enacted in response to the damage to US national security caused by the Aldrich Ames espionage case. The Ames case led to a legislative call for agencies to share data in counterespionage investigations and for the FBI to be involved earlier in the process of evaluating information concerning the possible compromise of classified information.

Security. 1) Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (JP 1-02, JP 2-0, and JP 3-10)

Security is not counterintelligence – counterintelligence is not security.

“People like to confuse counterintelligence (CI) with security. In practice, the two are related but not identical.” -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

“Security is a dimension of clandestinity in espionage, counterespionage, counterintelligence, adultery, and poker. It is to these activities what style is to a writer, an athlete, or a musician, but it is not itself a work, a game, or a performance. Its purpose is prophylactic: it excludes toxic and infectious organisms and conserves vital fluids.”

-- William R. Johnson, “Clandestinity and Current Intelligence.” *Studies in Intelligence*, vol 20, no. 3, (Fall 1976), pp. 15-69. Originally classified “Secret / No Foreign Dissem” [declassified].

*“Counterintelligence investigates the enemy, or if you will in the modern world, the opposition, to learn their capabilities, intentions, methods and focus. **It is not security work. Security protects. It does not attack.** [Emphasis added] CI attacks the actor. It attacks the opposition intelligence structures. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security.”*

-- Robert P Hanssen (Soviet Spy, Former FBI Agent and current Federal inmate) as quoted in “Diary of a Spy” by Paul M. Rodriquez, *Insight on the News*, 16 July 2001.

Security Classification. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. (JP 1-02)

There are three categories of security classification:

- 1) *Top Secret*--National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.
- 2) *Secret*--National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.
- 3) *Confidential*--National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Security Clearance. An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information. (JP 1-02)

Within DoD, a security clearance is a determination that a person is eligible under DoD policy for access to classified information. Clearances allow personnel to access classified information categorized into three levels: top secret, secret, and confidential. The damage to national defense and foreign relations that unauthorized disclosure could reasonably be expected to cause ranges from "exceptionally grave damage" for top secret information to "damage" for confidential information.

Security Countermeasures (SCM). Actions, devices, procedures, and/or techniques to reduce security risks. (IC Standard 700-1, 4 Apr 2008)

Security Detainee. Those detainees who are not combatants, but who may be under investigation or pose a threat to US forces if released. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

Security In-Depth. A concept of security calling for layered and complementary controls sufficient to detect and deter infiltration and exploitation of an organization, its information systems and facilities. (IC Standard 700-1, 4 Apr 2008)

Security Organizations. Military law enforcement, military criminal investigative organizations, and DoD-contracted security personnel. (DoDD 2000.12, DoD AT Program, 18 Aug 2003)

Security Service. Entity or component of a foreign government charged with responsibility for counterespionage or internal security functions. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011; and CI Community Lexicon)

Sedition. Willfully advocating or teaching the duty or necessity of overthrowing the US government or any political subdivision by force or violence. (JP 1-02)

Sedition and criminal subversion of military forces are violations of Title 18 USC, §§ 2384-2390 and is a punishable offense under UCMJ Article 94. It is a term of law which refers to overt conduct that is deemed by the legal authority as tending toward insurrection against the established order. It is the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. Sedition often includes subversion of a constitution and

incitement of discontent (or resistance) to lawful authority. A seditionist is one who engages in or promotes the interests of sedition.

The difference between sedition and treason consists primarily in the subjective ultimate object of the violation to the public peace. Sedition does not consist of levying war against a government nor of adhering to its enemies, giving enemies aid, and giving enemies comfort. Nor does it consist, in most representative democracies, of peaceful protest against a government, nor of attempting to change the government by democratic means (such as direct democracy or constitutional convention).

Sedition is the stirring up of rebellion against the government in power. Treason is the violation of allegiance to one's sovereign or state, giving aid to enemies, or levying war against one's state. Sedition is encouraging one's fellow citizens to rebel against their state, whereas treason is actually betraying one's country by aiding and abetting another state.

Senate Select Committee on Intelligence (SSCI). Created pursuant to Senate Res. 400, 94th Congress: to oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs. Provides legislative oversight over US intelligence activities to assure that such activities are in conformity with the Constitution and laws of the United States. (www.intelligence.senate.gov)

The 1980 Intelligence Oversight Act charged the SSCI and the House Permanent Select Committee on Intelligence (HPSCI) with authorizing the programs of US intelligence agencies and overseeing their activities.

Senior Defense Official / Defense Attaché (SDO/DATT). Principal DoD official in a U.S. embassy, as designated by the Secretary of Defense. (DoDD 5105.75, DoD Operations at Defense Embassies, 21 Dec 2007) Also see *Defense Attaché Office*.

The SDO/DATT is the Chief of Mission's (COM's) principal military advisor on defense and national security issues, the senior diplomatically accredited DoD military officer assigned to a US diplomatic mission, and the single point of contact for all DoD matters involving the embassy or DoD elements assigned to or working from the embassy.

All DoD elements assigned or attached to or operating from U.S. embassies are aligned under the coordinating authority of the SDO/DATT. See DoDD 5105.75.

Sensitive. Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity. (JP 1-02)

Sensitive Compartmented Information (SCI). All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. These controls are over and above the provisions of DoD 5200.1-R, Information Security Program Regulation. (JP 1-02)

-- Also, classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DNI. (National Intelligence: A Consumer's Guide - 2009).

-- Also, classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the DNI. (DoDI 5200.01, 9 Oct 2008)

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons

unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. (JP 1-02 and JP 2-01)

-- Also, an accredited area where Sensitive Compartmented Information may be stored, used, discussed, and/or processed. Only those Intelligence Community Agencies with SCIF Accreditation Authority may officially accredit facilities to handle, process, and store SCI materials. (National Intelligence: A Consumer's Guide - 2009).

For additional information on SCIFs see *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, IC Standard Number 705-1, 17 Sep 2010, and *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information*, IC Standard Number 705-2, 17 Sep 2010.

Sensitive Information. Information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Sensitive Site. A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets. (JP 1-02 & JP 3-31)

-- Also, a designated, geographically limited area with special diplomatic, informational, military, and economic sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money-laundering areas, and document storage areas for secret police forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

Sensitive Site Exploitation (SSE). Within DoD, none. See *site exploitation*.

This term was previously defined in JP 1-02 as: a related series of activities inside a captured sensitive site to exploit personnel documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents.

Note: Army Tactics, Techniques and Procedures (ATTP) 3-90.15 [FM 3-90.15], 8 Jul 2010 rescinded "*sensitive site exploitation*" as a doctrinal term.

Sensitive Sources and Methods. A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support US intelligence activities. (ICS Glossary)

Shape. The ability to conduct activities to affect the perceptions, will, behavior, and capabilities of partner, competitor, or adversary leaders, military forces, and relevant populations to further U.S. national security or shared global security interests. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Short-Range Agent Communication (SRAC). A device that allows agent and [case] officer to communicate clandestinely over a limited distance. (Spycraft)

Signal Flags. The IC [Intelligence Community] database containing information used to assist security and counterintelligence professionals conducting National Agency Checks on individuals applying for positions with IC organizations. (IC Standard 700-1, 4 Apr 2008)

Signal Security. A generic term that includes both communications security and electronics security. (JP 1-02)

Signal Site. A covert means of communications using a nonalerting signal, such as a chalk mark on a lamppost, to either initiate or terminate a clandestine act, (Spycraft) Also see *signals*.

Signals. Any form of clandestine tradecraft using a system of marks, signs, or codes for signaling between operatives. (CI Centre Glossary) Also see *signal site*.

Signals Intelligence (SIGINT). 1) A category of intelligence comprising either individually or in combination all communications intelligence [COMINT], electronic intelligence [ELINT], and foreign instrumentation signals intelligence [FISINT], however transmitted. 2) Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 1-02 and JP 2-0, Joint Intelligence)

For DoD policy see DoDI O-3115.07, Signals Intelligence (SIGINT), 15 Sep 2008

-- Also, information derived from intercepted communications and electronic and data transmissions. (WMD Report, 31 Mar 2005)

The Intelligence Community refers to the collection and exploitation of signals transmitted from communication systems, radars, and weapon systems as signals intelligence or SIGINT. SIGINT consists of Communications Intelligence (COMINT) – technical and intelligence information derived from intercept of foreign communications; Electronic Intelligence (ELINT) – information collected from systems such as radars and other weapons systems; and Foreign Instrumentation Signals Intelligence (FISINT) – signals detected from weapons under testing and development.

SIGINT is collected in a variety of ways depending on the type of signal targeted. The National Security Agency (NSA) collects the raw SIGINT and then NSA translators, cryptologists, analysts, and other technical experts turn the raw data into something that an all-source analyst can use. Once the NSA has collected, processed, and analyzed SIGINT, it is passed on to CIA and Intelligence Community analysts who use it to complement information from other sources to produce finished intelligence.

The volume and variety of today's signals adds challenges to the timely production of finished intelligence for policymakers. It is a lot of work to track and analyze all the SIGINT collected.

-- www.cia.gov (accessed, 30 Nov 2010)

Signatures. [In CI usage,] indicators of potential FISS and ITO [international terrorist organizations] methods of operations, including static surveillance of U.S. forces [and] installations.... (Army FM 2-22.2, CI, Oct 2009)

Silver Triangle. The South American region consisting of Peru, Bolivia, and Colombia that is historically known to be a major illegal drug production area. (JP 3-07.4)

Single Scope Background Investigation (SSBI). Investigation for individuals requiring a top secret clearance or working in a critical sensitive position; normally covers a 5-year period and consists of a subject interview, NAC, credit checks, character references, and employment records checks and references.

-- Also, a personnel security investigation consisting of all the elements prescribed in Standard B of ICPG 704.1. The period of investigation for a SSBI varies, ranging from the immediate preceding 3 years for neighborhood checks to immediately preceding 10 years for local agency checks. (IC Standard 700-1, 4 Apr 2008)

Singleton. Intelligence operations conducted by a single intelligence officer or agent. These operations include intelligence collection, servicing agents, and courier services. (Spy Book)

Site Exploitation. A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. (JP 1-02 & 3-31)

-- Also, systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution. (Army Tactics, Techniques & Procedures 3-90.15 [FM 3-90.15], Site Exploitation Operations, 8 Jul 2010)

Situation Report (SITREP). A report giving the situation in the area of a reporting unit or formation. (JP 1-02)

Situational Awareness. Immediate knowledge of the conditions of the operation, constrained geographically and in time. (Army FM 3-0, Operations, Feb 2008)

Sleeper. [Tradecraft jargon] A spy placed in a target area but does not engage in espionage until he or she is activated at a future time. (Spy Book)

Sociocultural Factors. The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 1-02 & JP 2-01.3)

Source. 1) A person, thing, or activity from which information is obtained; 2) in clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes; or 3) in interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (JP 1-02) Also see *asset, controlled source; human source; HUMINT source*.

-- Also, a person, device, system, or activity from which services or information are obtained. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

Source Directed Requirement (SDR). A HUMINT collection requirement based upon the placement and access of a source to collect and report on a specific person, place, thing, or event. (DIA HUMINT Manual, Vol I, DHE-M 3301.001, 30 Jan 2009)

Source Management. The process of registering and monitoring the use of sources involved in counterintelligence and human intelligence operations to protect the security of the operations and avoid conflicts among operational elements. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Source Registry. A source record/catalogue of leads and sources acquired by collectors and centralized for management, coordination and deconfliction of source operations. (JP 1-02 & JP 2-01.2)

Source Validation. Vetting to determine if a source is who he/she claims to be, is free of external control, is capable of behaving in a secure manner, and possesses placement and access consistent with tasking. (HDFI Lexicon, April 2008) Also see *vetting* and *counterintelligence flags*.

All DoD human sources are vetted in accordance with Intelligence Community Policy Memorandum 2006-300-1 (Validation of National Intelligence Community Human Intelligence Sources) and National HUMINT Manager Directive 001.08 (HUMINT Source Validation).

For DoD policy see DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U)*, 22 Jun 2009.

Special Access Program (SAP). A sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program. (JP 1-02 & JP 3-05.1)

-- Also, a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

Special Access Program Central Office (SAPCO). The office within a DoD Component or OSD PSA that, when directed, executes, manages, administers, oversees, and maintains records on the SAPs for which it has been assigned CA. Responsibilities may also include developing and implementing policies and procedures for oversight, management, execution, administration, SAP security, IA for SAP IS, and records management of SAPs under their cognizance, as directed. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

The DoD SAPCO is the office charged by the Deputy Secretary of Defense with responsibility as the designated proponent for developing and implementing policies and procedures for DoD SAP execution, management, and administration.

For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), these functions shall be exercised by the Director of National Intelligence.

-- EO 13526, *National Security Information*, 29 Dec 2009

Special Actions. Those functions that due to particular sensitivities, compartmentation, or caveats cannot be conducted in normal staff channels and therefore require extraordinary processes and procedures and may involve the use of sensitive capabilities. (JP 1-02 & JP 3-05.1)

Special Activities. *Term rescinded by JP 3-05, Special Operations, 18 Apr 2011.*

As previously defined, it was a term synonymous with "covert action." See *covert action*.

Special Agent. Within DoD, none. See *Counterintelligence Special Agent*.

This term was previously defined in JP 1-02 as: a person, either United States military or civilian, who is a specialist in military [law enforcement,] security or the collection of intelligence or counterintelligence information. *Term rescinded by JP 2-01.2, dated 11 Mar 2011.*

Special Area Clearance. The required concurrence granted to DoD personnel by the Department of State and the Office of the USD(P) for travel to certain overseas areas designated by the Department of State as special areas. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Special Collection Techniques. Those lawful investigative techniques which are employed by a DoD intelligence component under the rule of the least intrusive means, after a determination has been made that the required information is not publicly available, available with the consent of the person or persons concerned, or available from cooperative sources. (DIA Intelligence Law Handbook, Sep 1995) Also see *rule of the least intrusive means*.

At times "special collection techniques" are also referred to as "special investigative techniques" with CI channels. "Special collection techniques" are addressed in DoD 5240.1-R (7 Dec 1982), Procedures 5-10:

- * Procedure 5 - Electronic Surveillance
- * Procedure 6 - Concealed Monitoring
- * Procedure 7 - Physical Searches
- * Procedure 8 - Searches and Examination of Mail
- * Procedure 9 - Physical Surveillance
- * Procedure 10 - Undisclosed Participation in Organizations

Special Communication. See definition provided in DTM 08-019, Establishment of the DoD Special Communication Enterprise Office (SCEO), 11 Jun 2008, marked FOUO.

Special Event. An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

Special Information Operations (SIO). Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (JP 1-02 & JP 3-13) Also see *information operations*.

Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination. (IC Standard 700-1, 4 Apr 2008)

Special Limiting Criteria (SLC). [Term used in document/media exploitation activities]. A narrowly-defined set of criteria intended to restrict access to data that, if compromised, could imperil planned operations, contain evidence of espionage or counterintelligence operations, identify sources and methods, and/or contain illegal or inappropriate material. (NMEC)

Special Mission Unit (SMU). A generic term to represent a group of operations and support personnel from designated organizations that is task-organized to perform highly classified activities. (JP 1-02 & JP 3-05.1)

Special Operations (SO). Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. (JP 3-05, Special Operations, 18 Apr 2011)

Special Reconnaissance (SR). Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. (JP 3-05, Special Operations, 18 Apr 2011)

Specific Intelligence Collection Requirement (SICR). An identified gap in intelligence holdings that may be satisfied only by collection action, and that has been validated by the appropriate requirements control authority. (JP 1-02 & JP 2-01)

Specified Task. In the context of joint operation planning, a task that is specifically assigned an organization by its higher headquarters. (JP 5-0, Joint Planning, 26 Dec 2006)

Spot. [In intelligence usage,] to locate and recruit people demonstrated access to intelligence targets. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Spotter. In intelligence, an agent or illegal assigned to locate and assess individuals in positions of value to an intelligence service. (JP 1-02, JP 2-01.2; and CI Community Lexicon)

Spotter / Assessor. An asset assigned to locate and/or assess individuals of intelligence or operational interest. (HDI Lexicon, April 2008)

Spotter / Assessor Operation. Those actions taken to identify persons who may be in contact with or placed in contact with opposition intelligence and counterintelligence services, and to determine the potential value of these persons as intelligence or counterintelligence sources. (AR 381-47, OFCO, 17 Mar 2006)

Spy. A generic term that refers... to either a professional intelligence officer work works for an intelligence service, or to a foreign source or asset who steals secrets on behalf of that intelligence service. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

The spy is the greatest of soldiers. If he is the most detested by the enemy, it is only because he is the most feared.

— King George V (1865-1936)

A U.S. intelligence officer that handles clandestine human sources is normally referred to as a “case officer (C/O)” or “operations officer (OO).” The people that case officers or OOs recruit as penetrations of foreign governments and organizations are their “agents.” Agents have access to important information and pass that information secretly to their case officers.

In the circumstances of espionage and betrayal, one county's heroic spy is another's traitor.

-- Frederick P. Hitz, Former Inspector General of the CIA (1990 - 1998)

“What do you think spies are: priests, saints, and martyrs? They're a squalid procession of vain fools, traitors too, yes; pansies, sadists and drunkards, people who play cowboys and Indians to brighten their rotten lives...”

-- Alec Leamas, the protagonist in LeCarre's *The Spy Who Came in From the Cold*.

Spying. During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere. (DoDI 5240.06, 7 Aug 2004)

Spying in time of war is a violation of Article 106, Uniform Code of Military Justice (UCMJ).

One spy in the right place is worth 20,000 men in the field

-- Napoleon

Like war, spying is dirty business. Shed of its alleged glory, a soldier's job is to kill. Peel away the claptrap of espionage and the spy's job is to betray trust. -- William Hood, *Mole* (1993)

Spyware. A wide range of unwanted programs that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information (including financial information such as credit card numbers), monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites. (McAfee.com, accessed 15 Nov 2010)

Stability Operations. An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 1-02 & JP 3-0)

Staff Judge Advocate (SJA). A judge advocate so designated in the Army, Air Force, or Marine Corps, and the principal legal advisor of a Navy, Coast Guard, or joint force command who is a judge advocate. (JP 1-04)

Star-Burst Maneuver. A countersurveillance ploy in which more than one target car or target officer is being followed and they suddenly go in different directions, forcing the surveillance team to make instant choices about whom to follow. (CI Centre Glossary)

State-Directed Terrorism. Terrorist groups that operate as agents of a government, receiving substantial intelligence, logistical, and operational support from the sponsoring government. (DoDD 2000.12, DoD AT Program, 18 Aug 2003)

State-Supported Terrorism. Terrorist groups that generally operate independently, but receive support from one or more governments. (DoDD 2000.12, DoD AT Program, 18 Aug 2003)

Station. A CIA operational center overseas... usually, but not always, located under cover in a U.S. official installation. The senior officer in charge of a station is known as the chief of station, or COS. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Status of Forces Agreement (SOFA). An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. (JP 1-02 & JP 3-16)

-- Also, an accord, either bilateral or multilateral, that defines the legal position of a visiting military force deployed in the territory of a friendly state, usually delineating matters affecting the relationship between the military force and the civilian authorities and population. (AR 381-20, Army CI Program)

Stay Behind. Agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied. (JP 1-02)

Steganography. The process of hiding information by embedding messages within other, seemingly harmless messages. The process works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. (Wikipedia, accessed 4 April 2011)

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

With the advent of digital media, steganography has come to include the hiding of digital information within digital files. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

-- Wikipedia (accessed 4 April 2011)

Steganography is the process of secreting data in an image. Moscow Center uses steganographic software that is not commercially available. The software package permits the SVR clandestinely to insert encrypted data in images that are located on publicly-available websites without the data being visible. The encrypted data can be removed from the image, and then decrypted, using SVR-provided software. Similarly, SVR-provided software can also be used to encrypt data, and then clandestinely to embed the data in images on publicly-available websites.

-- FBI Affidavit, 25 June 2010

Strategic Communication. Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 1-02)

Strategic Debriefing. Debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011; and Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

Sources for strategic debriefing operations include but are not limited to émigrés, refugees, displaced persons, defectors, and selected U.S. personnel.

Strategic Intelligence. Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. (JP 1-02) Also see *intelligence; operational intelligence; tactical intelligence.*

Sherman Kent defined *strategic intelligence* as “high-level foreign positive intelligence.”

Strategic Level of War. The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, and develops and uses national resources to achieve these objectives. Activities at this level establish national and multinational military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of national power; develop global plans or theater war plans to achieve those objectives; and provide military forces and other capabilities in accordance with strategic plans. (JP 1-02 & JP 3-0) Also see also *operational level of war; tactical level of war.*

Strategic Planning Guidance (SPG). Provides direction for DoD components to develop the future years defense program and the President's budget submission. The four defense policy goals are to assure, dissuade, deter, and decisively defeat. The goals are articulated in a planning construct of deterring forward and winning decisively while defending at home. (JP 3-28)

Strategy. A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 1-02 and JP 3-0)

-- *Military Strategy.* The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force. (JP 1-02)

-- *National Military Strategy.* The art and science of distributing and applying military power to attain national objectives in peace and war; also called NMS. (JP 3-0, Joint Operations, 17 Sep 2006)

-- *National Strategy.* The art and science of developing and using the diplomatic, economic, and informational powers of a nation, together with its armed forces, during peace and war to secure national objectives; also called national security strategy or grand strategy. (JP 1-02)

Subject Interview. Interview with the subject of an investigation; it may be non-custodial or custodial.

Subversion. Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. (JP 1-02 & JP 3-24) Also see *subversive activity.*

-- Also, Actively encouraging military or civilian personnel to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline of the US military forces. Lending aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of the U.S. Government. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. (Dictionary.com)

Subversion refers to an attempt to overthrow structures of authority, including the state. It is an overturning or uprooting. Subversive activity is the lending of aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by force and violence. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage are placed in the category of subversive activity.

Subversion of Department of Defense personnel. Actions designed to undermine the loyalty, morale, or discipline of DoD military and civilian personnel. (JP 1-02)

-- Also, an act or acts inciting military or civilian personnel of the DoD to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, [or] discipline, of the Military Forces of the United States. (DoDI 5240.06, 7 Aug 2004)

Criminal subversion of military forces is a violation of Title 18 USC, §§ 2384-2390.

Subversive Activity. Anyone lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity. (JP 1-02)

Supply Chain. The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product. (JP 1-02 & JP 4-09)

Supply Chain Risk. The risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT [information and communication technology] components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications. (DTM 09-016, 25 Mar 2010) Also see *supply chain vulnerabilities; supply chain vulnerabilities*.

The increased dependence of the United States on global inputs in the manufacturing and service sectors, especially relating to information technology, opens the door to greater supply-chain vulnerabilities. As international companies and foreign individuals play a greater role in the information-technology supply chain, the specter of persistent, stealthy subversion is raised—particularly by foreign intelligence and military services, as well as international terrorists and criminal groups. – ONCIX website <<http://www.ncix.gov/sections/carc/index.html>>

See DCID 7/6, *Community Acquisition Risk Center*, 2 Mar 2005.

Within DoD, DTM 089-016 establishes policy and a defense-in-breath strategy for managing supply chain risk to information and communications technology (ICT) with DoD critical information systems and weapon systems in accordance with NSD-54/HSPD-23.

DoD computing systems, are a constant target of foreign exploitation. A 2007 Defense Science Board report noted that the software industry has become increasingly and irrevocably global. Much of the code is now written outside the United States, some in countries that may have interests inimical to those of the United States. The combination of DoD's profound and growing dependence upon software and the expanding opportunity for adversaries to introduce malicious code into this software has led to a growing risk to the Nation's defense.

See report of the *Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software*, Sep 2007.

Supply Chain Risk Management (SCRM). The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport). (DTM 09-016) Also see *supply chain risk*; *supply chain vulnerabilities*.

Supply Chain Vulnerabilities. An assessment of the supply chain related to CPI [critical program information] to determine if an adversary has the capability and intent to affect it in a manner that compromises the military effectiveness of the given platform, weapon system, or network. (DoDI 5200.39, 16 Jul 2008) Also see *supply chain risk*; *supply chain risk management*.

Supplier Assurance. Evidence demonstrating the level of confidence that a supplier is free from vulnerabilities. (DoDI 5200.39, 16 Jul 2008)

Support Asset. An asset who acquires, maintains, and/or provides services. (HDI Lexicon, April 2008)

Supported Commander. 1) The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. In the context of joint operation planning, this term refers to the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. 2) In the context of a support command relationship, the commander who receives assistance from another commander's force or capabilities, and who is responsible for ensuring that the supporting commander understands the assistance required. (JP 1-02 & JP 3-0) Also see *support*; *supporting commander*.

Supporting Commander. 1) A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate. 2) In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander. (JP 1-02 & JP 3-0) Also see *support*; *supported commander*.

Surreptitious Entry. Entry by stealth. (Spycraft)

Surveillance. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. JP 1-02, JP 3-0, and Army FM 34-1) Also see *counter surveillance*, *electronic surveillance*, *physical surveillance*, *surveillance detection*.

“Surveillance is a valuable investigative tool [emphasis added]....”

“Investigators always should assume that subjects engaged in operational, terrorist, or criminal activity will attempt to detect surveillance by employing a variety of methods and techniques.... During surveillances, participants must remain vigilant and alert to the possibility of countersurveillance techniques being employed against them.”

-- John T. Nason, “Conducting Surveillance Operations” in *FBI Law Enforcement Bulletin*, May 2004

-- Also, the continuous watching or listening (overtly or covertly) of people, vehicles, places, or objects to obtain information concerning the activities and identities of individuals. (Peter Jenkins, *Surveillance Tradecraft: The Professional's Guide to Covert Surveillance Training*, 2010)

-- Also, the monitoring of the behavior of a person or group of people, often in a surreptitious manner. (Wikipedia)

The word surveillance comes from the French *surveiller*, to watch over. The term is often used for all forms of observation or monitoring, not just visual observation.

Surveillance, physical: term for the universal tradecraft of undetected observation conducted by humans versus technical means.

Surveillance, technical: generic term for surveillance using various forms of visual, auditory and electronic aids in covering a designated target.

Surveillance, close: tradecraft jargon term for surveillance maintained where the prevention of loss of the subject is paramount.

Surveillance, discreet: tradecraft jargon term for surveillance maintained on a "loose" basis, the prevention of detection being paramount, even to the loss of the subject being tailed. Generally, the guiding rule is to discontinue surveillance rather than risk actions which make the subject aware of the surveillance.

Surveillance, fixed: tradecraft jargon term for a stationary or static surveillance. Also *stakeout*, tradecraft jargon for the static surveillance of a given target.

Surveillance, foot: tradecraft jargon term for, as the words imply, a surveillance conducted on foot.

Surveillance, mobile: tradecraft jargon term for surveillance conducted with the use of various mobile platforms, e.g., vehicles, aircraft, boats, etc.

-- Adapted from *The CIA's Insider's Dictionary* by Leo D. Carl (1996)

Surveillance, by definition, is intrusion into the affairs of other people.

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

-- Also [as used within DoD concerning force protection], monitoring the activity of DoD personnel, facilities, processes, or systems including showing unusual interest in a facility, infrastructure, or personnel (e.g., observations through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit. (DTM 08-007, DoD Force Protection Threat Information, 22 Jul 2008)

Surveillance Detection. Measures taken to detect and/or verify whether an individual, vehicle, or location is under surveillance. (DoDI S-5240.15, 20 Oct 2010) Also see *counter surveillance, surveillance.*

-- Measures taken to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, self-initiated actions taken by a target/subject to identify surveillance. Conducted by taking advantage of screen and flow, couple with detailed route selection, and noting possible surveillance against time and distance relationships. (CI Community Lexicon)

Surveillance Detection Route (SDR). A carefully crafted route, of varying lengths and complexity depending on the operational environment, used by a case officer and/or agent to get to a meeting site, and after leaving the meeting site, determine that the case officer and agent are not under surveillance before going to and after the ops meeting. (National HUMINT Glossary)

-- Also, a preplanned route used to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, *surveillance detection run*; a route designed to erode or flush out surveillance without alerting them to an operative's purpose. (CI Centre Glossary)

-- Also, a planned route taken by an agent or handler prior to conducting a clandestine act... designed to identify or elude surveillance. (Spycraft)

Professional case officers of all services, conduct lengthy SDRs before engaging in operational acts. A good SDR gives a case officer the opportunity to flush out surveillance if it is there and to make a determination of his or her surveillance status. The CIA jargon for completing an SDR and verifying without any doubt that surveillance is not there is "getting black."

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

Suspicious Activity. Observed behavior that may be indicative of intelligence gathering or other pre-operational planning related to a terrorist or other security threat to DoD interests worldwide. (DTM 10-018, Law Enforcement Reporting of Suspicious Activity, 1 Oct 2010)

-- Also, observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5)

Suspicious Activity Report (SAR). Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5)

eGuardian -- the FBI's law enforcement-centric threat reporting system -- rapidly disseminates SARs dealing with information regarding a potential threat or suspicious activity throughout the national law enforcement community to include DoD. For DoD policy see DTM 10-018, *Law Enforcement Reporting of Suspicious Activity*, 1 Oct 2010.

Synchronization. 1) The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2) In the intelligence context, application of intelligence sources and methods in concert with the operation plan to ensure intelligence requirements are answered in time to influence the decisions they support. (JP 1-02 and JP 2-0, Joint Intelligence)

Synthesis. In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 1-02)

System Assurance. The justified measures of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. (DoDI 5200.39, 16 Jul 2008)

Tactical Control (TACON). Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. TACON is inherent in operational control. TACON may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP 1 & JP 1-02) Also see *combatant command*; *combatant command (command authority)*; *operational control*.

Tactical Intelligence. Intelligence required for planning and conducting tactical operations. (JP 1-02)

Tactical Intelligence and Related Activities (TIARA). Those activities outside the National Foreign Intelligence Program that accomplish the following: 1) respond to operational commanders' tasking for time-sensitive information on foreign entities; 2) respond to national intelligence community tasking of systems whose primary mission is support to operating forces; 3) train personnel for intelligence duties; 4) provide an intelligence reserve; or 5) are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data. (JP 1-02)

Tactical Level of War. The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives. (JP 1-02 & JP 3-0) Also see *operational level of war*; *strategic level of war*.

Tactical Questioning (TQ). Direct questioning by any Department of Defense personnel of a captured or detained person to obtain time-sensitive tactical intelligence, at or near the point of capture or detention and consistent with applicable law. (JP 1-02 & JP 3-63)

For Do D policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 9 Oct 2008

-- Also, expedient initial questioning for information of immediate tactical value. (Army FM 2-22.3, Human Intelligence Collector Operations, Sep 2006)

Tag. Something that is attached to the item to be located and/or tracked, which increases its ability to be detected or its probability of identification by a surveillance system suitably tuned to the tag. (Defense Science Board 2004 Summer Study, *Transition to and from Hostilities*, Dec 2004)

Tags can be either active (such as radio-emitting tags) or passive (such as radio frequency identification [RFID] tags). Passive tags can also be chemical (such as infrared fluorescent) or biological in nature.

Target. 1) An entity or object considered for possible engagement or other action; 2) **in intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed**; 3) an area designated and numbered for future firing; and 4) in gunfire support usage, an impact burst that hits the target. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

Target Audience (TA). An individual or group selected for influence. (JP 1-02 and JP 3-13)

Target Folder. A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02 & JP 3-60)

Targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, considering commander's objectives, operational requirements, capabilities, and limitations. (JP 1-02, JP 3-0, and JP 5-0, Joint Planning, 26 Dec 2006)

-- Also, the act of focusing on a country, organization, non-state actor, installation, system, or person to identify an operational or intelligence goal. (National HUMINT Glossary)

See JP 3-60, Joint Targeting, for additional information.

Note: The doctrinal targeting process that has been adopted by the Army is denoted by the acronym "D3A," which stands for "Decide, Deliver, Detect, and Assess" and is covered in-depth in FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, 8 May 1996.

Target Intelligence. Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 1-02 & 3-60)

Task Force Counterintelligence Coordinating Authority (TFCICA). An individual that affects the overall coordination of counterintelligence activities (in a joint force intelligence directorate counterintelligence and human intelligence staff element, joint task force configuration), with other supporting CI organizations, and supporting agencies to ensure full CI coverage of the task force operational area. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

Tasking. The assignment or direction of an individual or activity to perform in a specified way to achieve an objective or goal. (S-DoDI 5240.17, CI Collection, 12 Jan 2009)

-- Also, directing or requesting a source to perform in a specific manner to achieve an objective or conduct an activity. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009)

-- Also, the process associated with acceptance of a validated collection requirement and assigning it to organic collection assets for action. (DIA HUMINT Manual, Vol I, DHE-M 3301.001, 30 Jan 2009)

Tear Line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release. (JP 1-02 & JP 2-0)

The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with "need-to-know", need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

Tearline Reporting. An automated or manual technique for separating an intelligence report into multiple portions separated by machine- or human-readable tearlines. A tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located. The sanitized information within the tearlines contains the substance of the more detailed information without identifying the sensitive sources and methods, allowing wider dissemination of substantive intelligence information to authorized users. (ICD 206, 17 Oct 2007)

Technical Intelligence (TECHINT). Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. (JP 1-02 & JP 2-0)

-- Also, the identification, assessment, collection, exploitation, and evacuation of captured enemy materiel (CEM) in support of national and immediate technical intelligence requirements. TECHINT provides rapid performance and vulnerability assessments of enemy equipment, giving a critical edge to US forces in current and future operations. (Army FM 2-22.401, TECHINT, 9 Jun 2006)

Technical Penetration. The use of technological means to conduct an intentional, unauthorized interception of information-bearing energy. (DoDI 5240.05, TSCM Program, 22 Feb 2006)

-- Also, *technical penetrations* include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

-- Also, a deliberate, unauthorized, clandestine emplacement of a device or modification of existing government equipment, or the clandestine employment of a technique, which allows the technical monitoring within an area for the purpose of gaining information. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Technical Security. A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies. This discipline mandates training in various countermeasure techniques. (IC Standard 700-1, 4 Apr 2008)

Technical Surveillance. Surveillance accomplished through the use of electronic listening devices, vehicle trackers, and signaling devices. (CI Community Lexicon)

Technical Surveillance Countermeasures (TSCM). Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (JP 1-02)

-- Also, techniques and measures to detect, neutralize and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information. (DoDI 5240.05, TSCM Program, 22 Feb 2006)

-- Also, physical, electronic, and visual techniques used to detect and counter technical security devices, technical security hazards, and related physical security deficiencies. (IC Standard 700-1, 4 Apr 2008)

TSCM represents the convergence of two distinct disciplines -- counterintelligence and security countermeasures. These techniques and countermeasures are designed to detect and nullify a wide variety of technologies used to gain unauthorized access to classified national security information, restricted data, or otherwise sensitive information.

-- ICD 702, *TSCM*, 18 Feb 2008

TSCM shall be conducted in DoD using techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information.

-- See DoDI 5240.05, *Technical Surveillance Countermeasures (TSCM)*

Technical Surveillance Device. A device covertly installed to monitor (visually, audibly, or electronically) sensitive activities and/or information processing within a target area. (ICS Glossary)

Technical Threat Analysis. A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence collection groups which could target personnel, information, operations, and resources. (DoDI 5240.05, TSCM Program, 22 Feb 2006)

Technology Targeting Risk Assessment (TTRA). A country-by-country assessment conducted by the Defense Intelligence Community that quantifies risks to CPI [critical program information] and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), and military installations. The TTRA evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: Technology Competence, National Level of Interest, Risk of Technology Diversion, Ability to Assimilate, and Technology Protection Risk. (DoDI 5200.39, 16 Jul 2008)

The TTRA and CI Assessment provide laboratory/technical directors and Program Managers with information required to establish a comprehensive security program for the protection of identified critical program information (CPI).

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (JP 1-02)

-- Also, an unclassified term that refers to the investigation and study of compromising emanations. (IC Standard 700-1, 4 Apr 2008)

-- Also, short name referring to investigation, study, and control of compromising emanations from information system equipment (CNSS Instruction No. 4009)

-- Also, Transient Electro Magnetic Pulse Emanation Standard (TEMPEST): the investigation, study, and control of compromising emanations from telecommunication and automated information systems equipment. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, the evaluation and control of compromising emanations from telecommunications and automated information systems. TEMPEST countermeasures are designed to prevent FISS and ITO [international terrorist organization] exploitation of compromising emanations by containing them within the space of the equipment or facility processing classified information. (Army FM 2-22.2, CI, Oct 2009)

TEMPEST – *the problem of compromising radiation*. Any time a machine is used to process classified information electrically... that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio beacons, may radiate through free space for considerable distances.... Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or waste pipes and be conducted along those paths for some distance.... When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was processed by the source equipment. The phenomenon affects not only cipher machines but any information-processing equipment—teletypewriters, duplicating equipment, intercoms, facsimile, computers...
-- Source: *TEMPEST: A Signal Problem*, NSA, undated; see <www.nsa.gov/public/crypt-spectrum.cfm>

Terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (JP 1-02 and JP 3-07.2)

-- Also, premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents (22 USC §2656f(d) and the National Strategy for Combating Terrorism, Feb 2003) [Definition used by Department of State, NCTC and CIA].

-- Also, the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR §0.85) [Definition used by FBI, which reflects its mission, identifying a terrorist incident as a violation of the criminal laws of the United States and a suspected terrorist would, therefore, be subject to arrest and prosecution.]

***There is no universally accepted definition of terrorism.
It remains the subject of continuing debate in international bodies.***
-- Lord Carlile of Berriew Q.C. (March 2007)

Terrorist. An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives. (JP 1-02)

Terrorist Extremist. An extremist that uses terrorism -- the purposeful targeting of ordinary people -- to produce fear to coerce or intimidate governments or societies in the pursuit of political, religious, or ideological goals. Extremists use terrorism to impede and undermine political progress, economic prosperity, the security and stability of the international state system, and the future of civil society. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

Terrorist Group. Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives. (JP 1-02)

Terrorists with Global Reach – Transnational Terrorists. Terrorist organizations with an operational and support network in multiple countries that possess the capability to recruit, plan, resource, and execute terrorist acts worldwide. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

Terrorism [the federal crime]. An offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. This includes terrorist acts committed within and outside U.S. national boundaries. See 18 USC 2332b(g)(5)(A).

The Federal Bureau of Investigation (FBI) is the lead agency for investigating the federal crime of terrorism. If another federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI. The extraterritorial jurisdiction for terrorism crimes is specified in 18 U.S.C. 2332b(e) and (f).

Pursuant to 28 C.F.R. 0.85(1), the Attorney General has assigned responsibility to the Director of the FBI to "Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate."

-- Congressional Research Service (CRS) Report # R41780 (27 Apr 2011)

Terrorism Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; [or] the product of a threat analysis for a particular unit, installation, or activity. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

TFCICA. See *Task Force Counterintelligence Coordinating Authority*.

Theater. The geographical area for which a commander of a geographic combatant command has been assigned responsibility. (JP 1 & JP 1-2))

Theater Clearance. Clearance for official travel within a geographic combatant command area of responsibility granted by the responsible geographic combatant commander or other delegated authority. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Theater of War. Defined by the Secretary of Defense or the geographic combatant commander, the area of air, land, and water that is, or may become, directly involved in the conduct of the war. A theater of war does not normally encompass the geographic combatant commander's entire area of responsibility and may contain more than one theater of operations. (JP 1-02)

Theater Strategy. The art and science of developing integrated strategic concepts and courses of action directed toward securing the objectives of national and alliance or coalition security policy and strategy by the use of force, threatened use of force, or operations not involving the use of force within a theater. (JP 1-02 & JP 3-0)

Third Agency Rule. An agreement among the US Government agencies participating in the exchange of intelligence data forbidding one agency to disseminate to another agency information which originated with a third agency. (National HUMINT Glossary)

-- Also, the tenet that information, usually classified or sensitive, originating in one U.S. agency not be disseminated by another agency to which the information has not been made available without the consent of the originating agency. (AR 381-20, Army CI Program, 25 May 2010)

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to the interest of the U.S. (IC Standard 700-1, 4 Apr 2008)

-- Also, the sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness. (DoDD 5200.1-M, Acquisition Systems Protection Program, March 1994)

-- Also, an adversary having the intent, capability, and opportunity to cause loss or damage. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, the perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations. (IOSS OPSEC Glossary of Terms, 27 Aug 2003)

-- Also see *threat to national security; transnational threat; foreign intelligence collection threat; insider threat.*

Threat Advisory. An advisory is a one-time product or produced on a recurring schedule – daily, weekly, or monthly. The advisory informs authorized recipients of an immediate or the potential for a foreign intelligence or terrorist threat. The advisory typically contains information of a perishable nature. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

A threat advisory is distinguishable from an assessment and an analysis report in that it is prepared when there is an imminent or near-term intelligence or terrorist threat. A threat advisory often contains perishable information with only limited study or research conducted prior to publication.

Threat Analysis. In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (JP 1-02 & DoDD 2000.12)

-- Also, a process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities. (DoDM 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Threat Assessment. A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, *DCIP Threat Assessment:* [in Defense Critical Infrastructure Protection (DCIP) usage] a compilation of strategic intelligence information incorporating multi-faceted threats facing defense critical assets (DCAs). DCIP threat assessments address threats posed to DCAs from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction. (DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 27 Aug 2007)

-- Also, an evaluation of the current or projected capability of a foreign intelligence service or international terrorist group to limit, neutralize, or negate the effectiveness of a friendly mission, organization, or material item through multidisciplinary intelligence collection, espionage, or sabotage. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, in antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. (JP 1-02 & JP 3-07.2)

-- Also, [in antiterrorism usage] the process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; it is the product of a threat analysis for a particular unit, installation, or activity. (DoDD 2000.12, DoD Antiterrorism Program, 18 Aug 2003)

Threat Finance. The covert movement of the profits of illicit acts or of funds that will support illicit acts. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *counter threat finance (CTF)*.

The covert movement of money is the underlying facilitator of all threat activity.

Within DoD, see DTM 08-034, *DoD Counterthreat Finance (CTF) Policy*, 2 Dec 2008

Threats to the National Security. 1) International terrorism; 2) espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; 3) foreign computer intrusion; and 4) other matters determined by the Attorney General consistent with Executive Order 12333 or a successor order. (AG Guidelines for Domestic FBI Operations, 29 Sep 2008)

Threat Warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 1-02)

Time-Sensitive Collection Requirement (TSCR). A HUMINT collection requirement (HCR) needing immediate or time-specific action. Those organizations tasked with the time sensitive collection requirement should provide initial intelligence reports or a report stating an inability to collect on the requirement with 48 hours of issuance. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Tosses (hand, vehicular) [e.g., hand toss, car toss]. Tradecraft techniques for placing drops by tossing them while on the move. (CI Centre Glossary)

Tradecraft. Specialized methods and equipment used in the organization and activity of intelligence organizations, especially techniques and methods for handling communications with agents. Operational practices and skills used in the performance of intelligence related duties. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011; and CI Community Lexicon)

***The methods of the clandestine operator...
Principles and techniques of clandestine operations***

In general, tradecraft is the sum total of the skills the Case Officer or agent must master in order to securely operate in the field and preserve security of operational activity.

"The spy who does not take tradecraft seriously is unlikely to remain a spy for very long."

-- H.H.A. Cooper and Lawrence J. Redlinger, *Making Spies: A Talent Spotter's Handbook*

-- Also, the art, discipline and methodology of conducting secure clandestine operations and intelligence collection. (National HUMINT Glossary)

-- Also, the tactics, techniques, and procedures used in executing HUMINT, counterintelligence, or related activities to obscure, protect, or otherwise frustrate detection. (HDI Lexicon, April 2008)

-- Also, the techniques, technology, and methodologies used in covert intelligence operations. Tradecraft applies to both the procedures, such as surveillance detection routes, as well as the use of devices in covert audio and agent communications. (Spycraft)

-- Also, the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business. Elements of tradecraft, in general terms, include the ways in which an intelligence officer arranges to make contact with an agent, the means by which the agent passes on information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way. (<<http://www.espionageinfo.com/Te-Uk/Tradecraft.html>>)

Successful espionage is impossible without good tradecraft

The techniques adopted by spies to conceal their activities are lumped together under the catch-all term "tradecraft." It refers to a vast range of protective measures devised to preserve the operational security of spying.

-- Frederick P. Hitz (Former CIA IG 1990-1998), *The Great Game* (2005)

Pillars of Tradecraft: assessment; cover and disguise; concealments; clandestine surveillance; and covert communications.

-- *Spycraft* (pg. 363)

Tradecraft - Analytical. The term "tradecraft" usually applied to espionage techniques, but there is also *analytical tradecraft*: techniques, methods, and standards of the practice of analysis, e.g., framing questions, marshaling evidence, making concise arguments, identifying intelligence gaps, etc. Analytical tradecraft affords some criteria by which to judge analytical products and analysts.

Transnational Threat. Any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery for such weapons, and organized crime) that threatens the national security of the United States. (50 USC §401a)

-- Also, any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens United States national security or interests. (JP 1-02 & 3-26)

Trap and Trace. A device which capture the incoming electronic or other impulses which identify the origination number of an instrument or device from which a wire or electronic communication was transmitted; see 18 USC §3127(4). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *pen register*.

A trap and trace device shows all incoming phone numbers to a particular telephone.

Treason. Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. (JP 1-02)

-- Also, whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason [in war time, treason is a violation of Title 18 USC, § 2381]. (DoDI 5240.06, 7 Aug 2004)

Treason was specifically defined in the U.S. Constitution, the only crime so defined. Article III Section 3 delineates treason as follows: "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court."

The crime is prohibited by legislation passed by Congress; 18 U.S.C. § 2381 states "whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than \$10,000; and shall be incapable of holding any office under the United States." In the history of the United States there have been fewer than 40 federal prosecutions for treason and even fewer convictions.

Trojan Horse. Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. (CNSS Instruction No. 4009) Also see *malicious code*.

-- Also, a computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse). (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, a malicious program that pretends to be a benign application; it purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive. (McAfee.com, accessed 15 Nov 2010)

Two-Person Integrity. A provision that prohibits one person from working alone. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Two-Person Rule. A system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed. (JP 1-02)

Unacknowledged SAP. A SAP [Special Access Program] having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient. (EO 13526, National Security Information, 29 Dec 2009, DoDD 5210.50, Unauthorized Disclosure of Classified Information to the Public, 22 Jul 2005, and National Intelligence: A Consumer's Guide - 2009)

-- Also, intentionally conveying classified documents, information, or material to any unauthorized person (one without the required clearance, access, and need to know). (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Unauthorized disclosure of classified information is an increasingly common occurrence.

The harm caused by... frequent unauthorized disclosures is manifold. Particular items of information appearing in the press provide valuable intelligence for our adversaries concerning the capabilities and plans of the United States for national defense and foreign relations.... Disclosures about US intelligence programs are particularly damaging, because they may cause sources to dry up. Lives of human agents are endangered and expensive technical systems become subject to countermeasures.

—The Willard Report (Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information), 31 Mar 1982)

Leaking sensitive information is like giving the enemy our play book.

Each year, countless unauthorized leaks cause severe damage to our intelligence activities and expose our capabilities. The fact of the matter is, some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information.... The threat leaks pose to our national security is alarming, and it is imperative we do more to protect our national secrets.

-- Congressman Rep. Pete Hoekstra at the Heritage Foundation, 25 July 2005.
See full remarks at <<http://www.fas.org/sgp/news/2005/07/hoekstra072505.html>>

Intelligence requires secrets. And secrecy is under assault.... When secrecy is breached, foreign targets of US intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, US intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve.

— James B. Bruce, Former CIA Officer

See Bruce's excellent article, entitled "The Consequences of Permissive Neglect: Laws and Leaks of Classified Intelligence" in *Studies of Intelligence* (Vol 47 No 1) available online at:

<<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article04.html>>

Leaks are a problem that has plagued intelligence agencies throughout modern history – they can undermine intelligence operations, jeopardize intelligence sources and methods, and have a terrible impact on the lives of covert agents who are publicly exposed.

-- Senator Ron Wyden, cited in Senate Report 112-12, 4 April 2011, p. 12

The unauthorized release of classified documents in 2010 by major newspapers and the Wikileaks website underscore the risks of widespread dissemination of sensitive information.

-- CRS Report RL33539, *Intelligence Issues for Congress*, 20 Jun 2011

Uncertainty. Doubt resulting from awareness of imperfect knowledge. This may arise from information absence, perceived error, deception, unpersuasive nature of evidence, complexity, etc. (*A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d. - circa 2007)

In analysis, uncertainty can derive from seeing plausible alternatives to the truth (the latter of which may be unknown or unknowable). Moreover, emotional and motivational factors attend cognitive uncertainty. Analysts can feel anxiety or discomfort if they lack confidence or self-esteem generally, feel an aversion to ambiguity, or have a need to please, or have a hypersensitivity to criticism. This affective element can exist even in the presence of sufficient evidence to make a reasonable judgment. Some analyst may well estimate the truth, but—in contrast to the inscription on the wall of the CIA lobby (*John* 8:32)—the truth.

-- *A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d., p. 375

Unconventional Warfare (UW). A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery. (DoDD 3000.07, 1 Dec 2008)

-- Also, activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. (JP 3-05, Special Operations, 18 Apr 2011; approved for incorporation into JP 1-02.)

Undeclared. An officer, asset, agent, or action whose agency affiliation is not formally identified to a foreign intelligence or security service, government or organization, or other US Government entity. (National HUMINT Glossary)

-- Also, an individual or action whose intelligence affiliation is not disclosed. (HDI Lexicon, April 2008)

Understand. The ability to individually and collectively comprehend the implications of the character, nature, or subtleties of information about the environment and situation to aid decision-making. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Unified Action. The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

Unified Command Plan (UCP). The document, approved by the President, that sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. (JP 1-02)

Six combatant commands have geographic area responsibilities: U.S. Northern Command (NORTHCOM), U.S. Central Command (CENTCOM), U.S. European Command (EUCOM), U.S. Pacific Command (PACOM), U.S. Southern Command (SOUTHCOM), and U.S. Africa Command (AFRICOM).

Four combatant commands have worldwide functional responsibilities not bounded by geography: U.S. Special Operations Command (SOCOM), U.S. Strategic Command (STRATCOM), U.S. Joint Forces Command (JFCOM), and U.S. Transportation Command (TRANSCOM).

Note: USJFCOM will be disestablished o/a August 2010.

Uniform Code of Military Justice (UCMJ). The criminal code governing the Armed Services of the United States. (CI Community Lexicon)

Unilateral Operation. A clandestine activity conducted without the knowledge or assistance of a foreign intelligence or security service, host country, foreign organization, or non-state actor. (National HUMINT Glossary)

Unity of Effort. Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization - the product of successful unified action. (JP 1 & JP 1-02)

Unknown Subject (UNSUB). The subject of an investigation, whose identity has not been determined, commonly referred to as an "UNSUB." Also see *DoD unknown subject*.

Unlawful Enemy Combatant. Persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict. For purposes of the war on terrorism, "unlawful enemy combatant" includes, but is not limited to, an individual who is or was part of or supporting Taliban or al Qaeda forces or associated forces that are engaged in hostilities against the United States or its coalition partners. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 9 Oct 2008)

Unload Signal. A visual signal to indicate the departure of an individual or removal of an object from a given locale. (HDI Lexicon, April 2008)

Unsolicited Correspondence. Request for information from a person which may range from direct inquiries by phone, e-mail, fax, or letter in which the recipient is asked to provide seemingly innocuous data. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Typical requests include solicitation of research papers, requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, and so forth; correspondence where the actual purpose may be to identify by name and position any individual who might be targeted later by a foreign intelligence service, and to elicit targeted information not readily obtainable by other means.

Unwitting. Not aware of US Government sponsorship or affiliation. (National HUMINT Glossary) Also see *witting*.

-- Also, unaware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

U.S. Coast Guard (USCG). A military, multi-function, maritime service that is the principal Federal agency responsible for safety, security, and stewardship with the maritime domain. It has diverse missions: national defense, homeland security, maritime safety, and environmental & natural resources stewardship. In March 2003, pursuant to the Homeland Security Act, the USCG was transferred from the Department of Transportation to the Department of Homeland Security (DHS).

The CI component of the USCG is the Coast Guard Counterintelligence Service (CGCIS).

U.S. Homeland. The physical territory of the United States: the 50 states, District of Columbia, US territories and territorial waters; significant infrastructure linked to the United States; and major commercial air, land and sea corridors into the country. Also see *homeland*.

U.S. National. US citizen and US permanent and temporary legal resident aliens. (JP 1-02)

U.S. Person. For intelligence purposes, a US person is defined as one of the following: 1) a US citizen; 2) an alien known by the intelligence agency concerned to be a permanent resident alien; 3) an unincorporated association substantially composed of US citizens or permanent resident aliens; or 4) a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments. (JP 1-02)

Validation. **1) A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied.** 2) A part of target development that ensures all vetted targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of armed conflict and rules of engagement. 3) In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. 4) Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and United States Transportation Command that all the information records in a time-phased force and deployment data not only are error free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. (JP 1-02 & JP 3-35)

Vehicle-Borne Improvised Explosive Device (VBIED). A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Otherwise known as a car bomb. (JP 1-02)

VENONA. Code name for the U.S. codebreaking project that deciphered portions of the texts of Soviet intelligence messages between Moscow and other cities in the 1940s. Most messages concerned spy activities in the United States. (Spy Book)

For additional information: <www.nsa.gov/public_info/declass/venona/index.shtml> and <<http://web.archive.org/web/20060614231955/http://www.nsa.gov/publications/publi00039.cfm>>

Also see *The FBI-KGB War: A Special Agent's Story* by Robert J. Lamphere and Tom Shachtman.

Vetting. A generic term to describe the full spectrum of asset evaluation for authenticity, reliability and hostile control. It includes ops testing, caser officer and psychological assessment, polygraph, security, counterintelligence interview, production review and personal record questionnaires. (National HUMINT Glossary) Also see *asset validation*, *source validation* and *counterintelligence flags*.

-- Also, as related to *source validation*, an ongoing process the purpose of which is to continually determine, by means of specific operational acts and analytical assessments, the motivation, veracity, and control of a reporting source. (DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009)

-- Also, a process of examination and evaluation, generally referring to performing a background check on someone before offering him or her employment, conferring an award, etc. In addition, in intelligence gathering, assets are vetted to determine their usefulness. (en.wikipedia.org/wiki/Vetting)

"Vetting" literally means getting a sick animal examined by a veterinarian; it has evolved into a term meaning to test or scrutinize. -- Spy Book

Vetting is used in agent/source authentication. The vetting process is one of testing and examining the agent to determine the degree of the agent's/source's reliability and truthfulness in reporting information. It is designed to weed out fabricators and double agents.

Virus. Malicious software; a form of Trojan horse that reproduces itself in other executable code. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995) Also see *computer virus*.

-- Also, a software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

A virus is a computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates the files. Some viruses display symptoms, and others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.

– McAfee.com, accessed 15 Nov 2010

Volunteer. A person who initiates contact with a government, and who volunteers operational or intelligence information and/or request political asylum; includes call-ins, walk-ins, virtual walk-ins, and write-ins. (National HUMINT Glossary)

Vulnerability. 1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished; 2) The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment; and 3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02 & JP 3-60)

-- Also, a situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

Vulnerability Analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Vulnerability Assessment (VA). A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. (JP 1-02 & JP 3-07.2)

-- Also, [regarding infrastructure] a systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010)

-- Also, the comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and /or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management. (DoD 5200.08-R, 9 Apr 2007)

-- Also, the process of identifying weaknesses in the protection of friendly operations and activities which, if successfully exploited by foreign intelligence, could compromise current or future plans, capabilities, or activities, including RDA [research, development and acquisition]. (AR 381-20, Army CI Program, 25 May 2010)

Vulnerability Study. An analysis of the capabilities and limitations of a force in a specific situation to determine vulnerabilities capable of exploitation by an opposing force. (JP 1-02)

Walk-in. An unsolicited contact who provides information. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011; and DHE-M 3301.002, Vol II Collections OPerations, 23 Nov 2010) Also see *volunteer*.

-- Also, an individual who offer his/her services to an intelligence service without being solicited. (CIA, D&D Lexicon, 1 May 2002)

This term applies universally to agents who volunteer their services to a hostile intelligence agency by making an approach to an adversary at its premises. The KGB recognized that some of its best sources including John Walker, Aldrich Ames, and Robert Hanssen, acted in this way, but did not use the same term, preferring "self-recruited agents."

-- *Historical Dictionary of Cold War Counterintelligence* (2007)

For the story of a walk-in, see Barry G. Royden, "Tolkachev, A Worthy Successor to Penkovsky," *Studies in Intelligence*, v 47, n 3: pp. 5-33. Full article available at: <<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html>>

...it should be emphasized once more that work with "walk-ins" is an important part of agent operations for strategic intelligence and when properly planned and conducted can be very fruitful. -- Ivan A. Serov, GRU General (1962)

See Ivan A. Serov, "Work with Walk-Ins,"* *Studies in Intelligence*, Vol 8, No. 1. This article, originally published in 1962, is adapted from one of several on Soviet intelligence doctrine written by high-ranking officers of the GRU (Soviet Military Intelligence). The article shows that Soviet/Russian problems in assessing and handling the walk-in are not unlike our own. The full article available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no1/html/v08i1a02p_0001.htm>

* Note: Russian term *dobrozheleatel* ("well-wisher") is virtually the same as our "walk-in."

Warning. 1) A communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantial increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation; and 2) operating procedures, practices, or conditions that may result in injury or death if not carefully observed or followed. (JP 1-02)

Waived SAP. A SAP [Special Access Program] for which the Secretary of Defense has waived applicable reporting in accordance with [Section 119 of Title 10 US Code] following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

Weapons of Mass Destruction (WMD). Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. WMD can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the system. (JP 3-26, Homeland Security, 2 Aug 2005)

-- Also defined in US Code as: (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (USC Title 18 §2332a)

-- Also, chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. (JP 1-02 & JP 3-40)

White List. The identities and locations of individuals who have been identified as being of intelligence or counterintelligence interest and are expected to be able to provide information or assistance in existing or new intelligence areas of interest. (CI Community Lexicon) Also see *Gray List*; *Black List*.

Window Dressing. [Tradecraft jargon] Ancillary materials that are included in a cover story or deception operation to help convince the opposition or casual observers that what they are observing is genuine. (CI Centre Glossary)

Witting. A term of intelligence art that indicates that one is not only aware of a fact or piece of information but also aware of its connection to intelligence activities. (JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) Also see *unwitting*.

-- Also, a person is aware of USG sponsorship or affiliation. (National HUMINT Glossary)

-- Also, aware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

-- Also, knowledgeable as to certain aspects of a clandestine organization and its activities. (AFOSI Manual 71-142, 9 Jun 2000)

Worms. Parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via Internet Relay Chat (IRC). (McAfee.com, accessed 15 Nov 2010)

Write for Maximum Utility (WMU). An approach that guides the way that intelligence organizations conceive, format, produce, and disseminate intelligence products in order to increase their usability for the intended customers. (ICD 208, 17 Dec 2008) Also see *write-to-release*.

Utility is maximized when customers receive or are able to expeditiously discover and pull or request intelligence, information, and analysis in a form they are able to easily use and able to share with their colleagues, subordinates, and superiors. WMU ensures intelligence, information, and analysis are produced in a manner to facilitate reuse—either in its entirety or in coherent portions—thereby enabling wider dissemination and enhancing its usability.

WMU shares certain goals as well as techniques with previous and ongoing IC WTR [write-to-release] efforts. WMU goes further than WTR in linking knowledge of the customer's operating environment to the intelligence production effort. The resulting effort is not "one size fits all" or production of all intelligence products at the lowest classification, but products tailored to best meet a customer's requirements. This may mean producing the definitive assessment on a given topic area based on all available intelligence, regardless of classification.

-- ICD 208, *Write for Maximum Utility*, 17 Dec 2008

Write-to-Release (WTR). A general approach whereby intelligence reports are written in such a way that sources and methods are protected so that the report can be distributed to customers or intelligence partners at lower security levels. In essence, write-to-release is proactive sanitization that makes intelligence more readily usable by a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and tearline reporting. (ICD 208, 17 Dec 2008) Also see *tearline reporting* and *write for maximum utility*.

Zombie. A computer that is infected with a virus or Trojan horse that puts it under the remote control of an online hijacker. The hijacker uses a zombie to generate spam or launch denial of service attacks. (McAfee Labs – Threat Glossary)

Counterintelligence A variety of views...



CI... the most secret of secret intelligence activities....

-- Senate Report 94-755, Church Committee Report, 26 April 1976, p.163

“...countering the intelligence efforts of an adversary is the central function of counterintelligence.”

-- Roy Godson, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence* (Washington: Brassey's 1995), pp. xii, 15 & 304

“...intelligence of a special kind, plus something else.... Counterintelligence collects, stores, analyzes and disseminates information about certain foreign threats to U.S. security and then acts to destroy or neutralize them.... Its end purpose is not the mere collection and analysis of information, but action, and successful action, against those who threaten the security of the United States.”

-- Francis McNamara, *U.S. Counterintelligence Today*, The Nathan Hale Institute (1985), p. 18

“[CI] ...must strive to know everything possible about an adversary's intelligence capabilities, including his sources, and methods of collection, his covert actions at influencing and managing our actions and perceptions, and even his culture and thought processes.”

-- S. Eugene Poteat, “Counterintelligence Spy vs. Spy, Traitor vs. Traitor,” *American Intelligence Journal* (Winter 2000-2001), p. 62

“...information about an adversary's intelligence operations, capabilities, agents, collection technology, and so on. It is *not* security. It is intelligence on which security policies should be based. Nor is it intelligence about an adversary's policy making or military operations or other nonintelligence capabilities and activities.”

-- William E. Odom, *Fixing Intelligence For a More Secure America* (New Haven: Yale University Press 2003), p. xxix

“...efforts taken to protect one's own intelligence operations from penetration and disruption by hostile nations or their intelligence services. It is both analytical and operational. ...not a separate step in the intelligence process but an important function throughout the process.”

-- Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington: CQ Press 2000), p. 98

“...national effort to prevent foreign intelligence services... from infiltrating our institutions and establishing the potential to engage in espionage, subversion, terrorism, and sabotage.”

-- Newton Miller, “Counterintelligence at the Crossroads,” *Intelligence Requirements for the 1980's: Elements of Intelligence*, ed. Roy Godson (Washington, DC: National Strategy Information Center, Inc., 1983), p. 50

“...involves the use of both offensive and defensive measures to: protect sensitive US information and operations from compromise and penetration by foreign intelligence services and other hostile entities; ensure the security and integrity of ongoing US diplomatic, military and intelligence operations; and penetrate, compromise and neutralize hostile operations mounted by foreign intelligence services, terrorist organizations and drug cartels.”

-- “Richard L. Haver, “The Ames Case: Catalyst for a National Counterintelligence Strategy,” *Defense Intelligence Journal*, Vol. 4 No. 1 (Spring 1995), p. 12

“...includes all information gathered and activities conducted by the government aimed at detecting, analyzing, and countering threat. ...the term refers to active operations conducted to counter--through detection, assessment, neutralization, and manipulation--the intelligence operations of foreign countries and groups. ...it includes recruitment of foreign intelligence officers, disruption of activities, prosecution of criminal espionage, and manipulation and deception. ...it involves the use of surveillance, double agents, and other clandestine techniques.”

-- Kenneth E. deGraffenreid, “Countering Hostile Intelligence Activities as a Strategic Threat,” National Strategy Information Center, Inc., Sep 1989, p. 3

“Counterintelligence is a term often associated with catching spies. ... [it is also] information gathered and activities conducted with the purpose of disrupting and neutralizing the activities of hostile intelligence services.”

-- Jeffery Richelson, The US Intelligence Community, 2d ed. (Ballinger Publishing Co., Cambridge MA, 1989), pp. 317 - 330

“Counterintelligence is a critical part of nearly all intelligence activities. When performed properly, the CI function is integral to the intelligence activity itself and part of the overall security of the organization.”

-- Aspin-Brown Commission Report, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, 1 March 1996

“...the most arcane and organizationally fragmented, the least doctrinally clarified, and legally, and thus politically, the most sensitive intelligence activity.”

-- William E. Odom, Fixing Intelligence For a More Secure America (New Haven: Yale University Press 2003), p. 167

Need for Counterintelligence...



But there will always be espionage and there will always be counter-espionage. Though conditions may have altered, though difficulties may be greater..., there will always be secrets which one side jealously guards and which the other will use every means to discover; there will always be men who from malice or for money will betray their kith and kin and there will always be men who, from love of adventure or a sense of duty, will risk a shameful death to secure information valuable to their country.

W. Somerset Maugham, *Ashenden: or the British Agent*, (1928: New York: Doubleday, Doran, 1941)

Inescapable Truth... there will always be Spies

“...the counterintelligence community is performing its wartime mission every day as agents counter foreign intelligence threats – that’s why we call it the silent war.”

-- COL Stuart Herrington, USA (Ret)

“In the spy game, when you’re penetrated – when someone is working for the other side inside your security world – they own you.”

-- Richard Haver, Former Exec Dir for IC Affairs and Former Special Asst to USD(I)

“There are far too many in the Intelligence Community who either do not understand counterintelligence or, who understanding its concepts, have climbed to the top of their career ladders by opposing it.”

-- Senator Malcolm Wallop, Senate Intelligence Committee (1985)

CI... A Never-Ending Necessity

The Ten Commandments of Counterintelligence

- ▶ I -- Be Offensive
- ▶ II -- Honor Your Professionals
- ▶ III -- Own the Street
- ▶ IV -- Know Your History
- ▶ V -- Do Not Ignore Analysis
- ▶ VI -- Do Not Be Parochial
- ▶ VII -- Train Your People
- ▶ VIII -- Do Not Be Shoved Aside
- ▶ IX -- Do Not Stay Too Long
- ▶ X -- Never Give Up



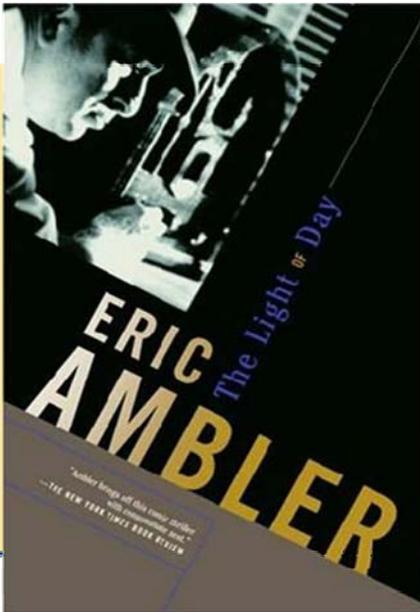
-- James M. Olson, served 31 years in the CIA*

* James M. Olson, “The Ten Commandments of Counterintelligence,” *Studies in Intelligence*, 2001, Vol. 54 No. 5; available online at <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol45no5/html/v45i5a08p.htm>



We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us.

-- Doolittle Report (1954)*



I think if I were asked to single out one specific group of men, one category as being the most suspicious, unbelieving, unreasonable, petty, inhuman, sadistic, double-crossing set of bastards in any language, I would say without hesitation the people who run counterespionage departments.

-- Eric Ambler. *Light of Day* (1962)

* *Report on the Covert Activities of the Central Intelligence Agency* (aka Doolittle Report), 30 Sep 1954, redacted copy (originally classified TOP SECRET). Lt Gen James H. Doolittle was the Chairman of this Presidential directed Special Study Group. Redacted copy available online at: <http://www.foia.cia.gov/helms/pdf/doolittle_report.pdf>

Counterintelligence officers—people who specialize in catching spies—work in a part of the profession so labyrinthine that it is often referred to as a “wilderness of mirrors”...

-- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)

One final perspective...



Counterintelligence... a wilderness of mirrors

"A wilderness of mirrors," a description of counterintelligence attributed to James J. Angleton. It comes from T.S. Eliot's poem "Gerontion" (1920); also the title of a 1980 book authored by David C. Martin about CIA counterintelligence.

Angleton was CIA's Chief of the Counterintelligence from 1954 until his retirement in 1974. In December 1974, Angleton was basically forced into retirement by the Director of CIA (William Colby), who became convinced that Angleton's "labyrinthine" approach to counterintelligence was severely hampering the Agency's clandestine HUMINT collection mission.

Sources

A Consumer's Guide to Intelligence (PAS 95-00010), CIA, Public Affairs Staff, July 1995; updated, 2d ed. 1996; replaced with ***National Intelligence: A Consumer's Guide - 2009***, Office of Director National Intelligence (ODNI). Copy available online at: <www.dni.gov/reports/IC_Consumers_Guide_2009.pdf>

Code of Laws of the United States of America, Title 18, et al, available online from the Government Printing Office. Access online data base at: <<http://www.gpoaccess.gov/uscode/index.html>>

Counterintelligence Community Lexicon (CI Community Lexicon), National Counterintelligence Center, NACIC 2000-10004, June 2000 – cited as CI Community Lexicon.

DoD Dictionary of Military and Associated Terms, Joint Publication 1-02. Copy available online at: <http://www.dtic.mil/doctrine/dod_dictionary/> (also available at <<https://jdeis.js.mil/>>) -- cited as JP 1-02

DoD Issuances (e.g., Directives, Instructions) available online at: <<http://www.dtic.mil/whs/directives/>>

Fair Play: The Moral Dilemmas of Spying by James M. Olson, Potomac Books, Inc., Washington, D.C., 2006.

Glossary of Intelligence Terms and Definitions, The Intelligence Community Staff (ICS), Office of the Director of Central Intelligence, 1978; updated June 1989 – cited as ICS Glossary.

Glossary of Security Terms, Definitions, and Acronyms, Intelligence Community Standard - Number 700-1 (previously numbered ICS 2008- 700-1), 4 April 2008 – cited as IC Standard 700-1.

Glossary of Spy Term, CI Centre -- cited as CI Centre Glossary.

Note: originally available online at <http://cicentre.com/LINKS_Reference_Material.htm> -- site now requires membership to access, see <<http://www.cicentre.com/>>

Historical Dictionary of Cold War Counterintelligence by Nigel West, Scarecrow Press, Inc., Maryland, 2007

Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and related Activities, April 2008 – cited as HDI Lexicon

Intelligence Community Intelligence Directives (ICDs), unclassified ICDs available online at: <http://www.dni.gov/electronic_reading_room.htm>

Intelligence Essentials for Everyone, by Lisa Krizen, Occasional Paper Number Six, DIA (Joint Military Intelligence College), June 1999. Copy available online at: <<http://www.dia.mil/college/pubs/8342.htm>>

McAfee Labs - Threat Glossary, undated.

Copy available online at: <<http://mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx>>

National Intelligence: A Consumer's Guide - 2009.

Copy available online at: <http://www.dni.gov/reports/IC_Consumer's_Guide_2009.pdf>

National HUMINT Glossary, unclassified, 15 pages, undated.

Copy available on JWICS at: <<http://jwc-nhb-nhc03.idiss.cia.ic.gov/intelink/NationalHUMINTGlossary.pdf>>

OPSEC Glossary of Terms. Interagency OPSEC Support Staff.

Copy available online at: <<http://www.iooss.gov/docs/definitions.html>>

Spy Book -- The Encyclopedia of Espionage by Norman Polmar and Thomas B. Allen, Random House, New York, Updated and Revised Edition, 2002 – cited as Spy Book.

Spycraft: The Secret History of the CIA's Spys from Communism to Al-Qaeda by Robert Wallace and H. Keith Melton, Penguin Group, New York, 2008 – cited as Spycraft.

Note: DoD issuances (e.g., directives, instructions, DTMs) approved for public release are available on the Internet from the DoD Issuances Website at: <<http://www.dtic.mil/whs/directives/>>

Army Field Manuals (FMs) are available online at: http://armypubs.army.mil/doctrine/active_fm.html (requires an AKO account). Selected FMs also at: <<http://www.fas.org/irp/doddir/army/index.html>>

Intelligence Community & Misc. Government Websites

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI): www.dni.gov

NATIONAL COUNTER INTELLIGENCE EXECUTIVE (NCIX): www.ncix.gov

NATIONAL COUNTERTERRORISM CENTER (NCTC): www.nctc.gov

DEPARTMENT OF DEFENSE (DoD): www.defense.gov (also see: www.defenselink.mil)

- Defense Intelligence Agency (DIA): www.dia.mil
- Defense Security Service (DSS): www.dss.mil
- Army: www.army.mil
 - Intelligence & Security Command (INSCOM): www.inscom.army.mil
- Air Force: www.af.mil
 - Air Force Office of Special Investigations (AFOSI): www.osi.andrews.af.mil
 - Air Force ISR Agency: www.afisr.af.mil
- Navy: www.navy.mil
 - Office of Naval Intelligence (ONI): www.nmic.navy.mil
 - Naval Criminal Investigative Service (NCIS): www.ncis.navy.mil
- Marine Corp: www.marines.mil
 - USMC Intelligence: hqinet001.hqmc.usmc.mil/DirInt/default.html

NATIONAL SECURITY AGENCY (NSA): www.nsa.gov

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA): www.nga.mil

NATIONAL RECONNAISSANCE OFFICE (NRO): www.nro.gov

CENTRAL INTELLIGENCE AGENCY (CIA): www.cia.gov

DEPARTMENT OF JUSTICE (DoJ): www.usdoj.gov

- Federal Bureau of Investigation (FBI): www.fbi.gov
- Drug Enforcement Agency (DEA): www.dea.gov
- DoJ Office of Legal Counsel (OLC): www.usdoj.gov/olc
- DoJ National Security Division (NSD): www.usdoj.gov/nsd

DEPARTMENT OF HOMELAND SECURITY (DHS): www.dhs.gov

- U.S. Coast Guard (USCG): www.uscg.mil
- Customs and Border Protection (CBP): <http://cbp.gov/>
- Immigrations and Customs Enforcement (ICE): <http://www.ice.gov/>
- Transportation Security Administration (TSA): <http://www.tsa.gov/>
- U.S. Secret Service (USSS): <http://www.secretservice.gov/>
- DHS Office of Intelligence & Analysis: http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm

DEPARTMENT OF STATE: www.state.gov

- Bureau of Diplomatic Security: <http://www.state.gov/m/ds>

DEPARTMENT OF TREASURY: www.ustreas.gov

- Office of Terrorism and Financial Intelligence: <http://www.ustreas.gov/offices/enforcement/>
- Financial Crimes Enforcement Network (FinCEN): <http://www.fincen.gov/>

DEPARTMENT OF ENERGY: www.energy.gov

WHITE HOUSE: www.whitehouse.gov

U.S. SENATE: www.senate.gov

- Senate Select Committee on Intelligence (SSCI): intelligence.senate.gov

U.S. HOUSE OF REPRESENTATIVES: www.house.gov

- House Permanent Select Committee on Intelligence (HPSCI): intelligence.house.gov

LIBRARY OF CONGRESS: www.loc.gov

- Federal legislative information available at: thomas.loc.gov