



# Department of Defense DIRECTIVE

NUMBER 3600.01

August 14, 2006

*Incorporating Change 1, May 23, 2011*

~~USD(A)~~ USD(P)

SUBJECT: Information Operations (IO)

References: (a) DoD Directive S-3600.1, "Information Operations (U)," December 9, 1996 (hereby cancelled)

~~(b) Section 165 of title 10, United States Code~~

*(b) Under Secretary of Defense for Intelligence Memorandum, "Coordination and Deconfliction of Information Operations and Human Intelligence (HUMINT)," August 17, 2010 (hereby cancelled)*

*(c) DoD Directive S-5200.37, "Management and Execution of Defense Human Intelligence (HUMINT)," February 9, 2009*

*(d) Assistant to the Secretary of Defense (Intelligence Oversight) Memorandum to Secretary of Defense, June 25, 2010, endorsed by Secretary, July 22, 2010*

*(e) through (l), see Enclosure 1*

## 1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues Reference (a) to update IO policy, definitions, and responsibilities in the ~~Department of Defense (DoD)~~ to support the objective of making IO a core military competency; *and cancels Reference (b).*

1.2. Provides authority to develop separate instructions for implementation of the guidance contained in this Directive.

*1.3. Directs the coordination and deconfliction of information gathering activities in support of IO and Human Intelligence (HUMINT) and other intelligence activities within the Combatant Commands, consistent with References (c) through (g).*

*1.4. Distinguishes HUMINT and related intelligence activities from other human-derived information gathering activities, such as foreign cultural analysis, human terrain analysis, and the collection of information on a given population, human factors, atmospheric, and socio-cultural dynamics.*

## 2. APPLICABILITY

This Directive applies to ~~the Office of the Secretary of Defense (OSD)~~, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the ~~Department of Defense DoD~~, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the ~~Department of Defense DoD~~ (hereinafter referred to collectively as the “DoD Components”).

## 3. DEFINITIONS

3.1. ~~Information Operations (IO)~~. The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), ~~Psychological Operations (PSYOP)~~ *Military Information Support Operations (MISO)*, Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

3.2. Other terms used in this Directive are defined in Enclosure 1.

## 4. POLICY

It is DoD policy that:

4.1. IO shall be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

4.1.1. In peacetime, IO supports national objectives primarily by influencing adversary perceptions and decision-making. In crises short of hostilities, IO can be used as a flexible deterrent option to demonstrate resolve and communicate national interest to affect adversary decision-making. In conflict, IO may be applied to achieve physical and psychological results in support of military objectives. During post conflict or stability operations, IO continues to support national objectives and influence foreign perceptions.

4.1.2. IO contributes to information superiority by both defending military decision-making from adversary attacks and by influencing and degrading an adversary’s decision-making capability, thereby producing an information advantage. IO contributes directly to the national security strategy, which uses all elements of national power in a synchronized and coordinated manner to influence adversary perceptions and behavior.

4.2. IO capabilities shall be developed that can be employed in concert with various core, supporting, related, and intelligence capabilities to provide a fully integrated warfighting capability.

4.2.1. Core IO Capabilities. IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: EW, CNO, ~~PSYOP~~ *MISO*, MILDEC, and OPSEC. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

#### 4.2.2. Supporting Capabilities

4.2.2.1. Counterintelligence (CI) investigations, operations, collection, analysis, production, and dynamic functional services shall be employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.

*4.2.2.2. HUMINT and related intelligence activities are those deriving information collected from human sources, and shall be used to support IO.*

*4.2.2.2.1 For collection of information that may endanger the source or the collector, or meet other conditions specified in DoD Directive (DoDD) 5200.37 (Reference (c)), then the information shall only be collected by trained and certified HUMINT collectors who are assigned to organizations with a mission to collect HUMINT in response to validated intelligence requirements.*

*4.2.2.2.2 The direction and control of HUMINT activities is an inherently governmental function and may only be performed by USG civilian or military personnel.*

*4.2.2.2.3 Any person observing suspected violations of U.S. criminal law, Executive Orders (E.O.s), Presidential Directives, Intelligence Community Directives and DoD Issuances by any other person, shall report immediately through the chain of command to the Defense HUMINT Manager, the Assistance Secretary of Defense for Intelligence Oversight, the DoD Component's General Counsel or Inspector General as required by section 1.6(b) and (c) of E.O. 12333 (Reference (h), the 1995 Crimes Reporting Memorandum of Understanding (Reference(i)), procedure 15 of DoD 5240.1-R (Reference (j) and DoDD 5148.11 (Reference (k)). Each employee shall report suspected violations of U.S. Federal criminal law by an employee, and of specified U.S. Federal criminal laws by any other person, immediately through the chain of command to the Defense HUMINT Manager, the Assistant to the Secretary of Defense for Intelligence Oversight, and the DoD Component's General Counsel or Inspector General in accordance with the procedures described in Reference (c).*

4.2.2.~~3~~. Physical (kinetic) attack may be employed alone or integrated with non-kinetic attack options to influence or disrupt adversary decision-makers or groups and provide support for full spectrum dominance.

4.2.2.~~3~~.4. Physical Security shall support IO by preventing unauthorized physical access to personnel, equipment, installations, material, and documents, and by safeguarding information and information systems against espionage, sabotage, damage, and theft.

4.2.2.4.5. Information Assurance (IA) shall provide capabilities to protect and defend information and information systems. IA activities shall be conducted independently to achieve these objectives or combined with specific CNO activities.

4.2.2.5.6. Combat Camera shall provide clear, timely, unaltered documentation of military operations to the Combatant Commander. This documentation provides a source of video and still images that can be used to counter disinformation, misinformation, and propaganda.

#### 4.2.3. Related Capabilities

4.2.3.1. Public Affairs (PA), as a function of command, shall support the continuing public information and communication requirements of the ~~Department~~DoD. PA activities contribute to the broader ~~U.S. Government~~(USG) communications effort by providing truthful, accurate and timely information to the public, the domestic and international media, military members, and their families. PA shall provide operational capabilities to communicate military objectives, counter misinformation and disinformation, deter adversary actions, and maintain the trust and confidence of the U.S. population, as well as our friends and allies. Effective military operations shall be based on credibility and shall not focus on directing or manipulating U.S. public actions or opinion.

4.2.3.2. Civil-Military Operations (CMO) activities shall support DoD informational objectives by influencing, developing, or controlling indigenous infrastructures in foreign operational areas and can be an alternate means to communicate with the host nation and foreign public. CMO shall be performed by designated civil affairs personnel, other military forces, or a combination of both.

4.2.3.3. Defense Support to Public Diplomacy (DSPD) ensures the ~~Department~~DoD sends a coherent and compelling message in concert with other USG agencies. The prevalence of access to global communications requires a comprehensive and proactive USG communication strategy. The Department of State maintains the lead for public diplomacy with the ~~Department of Defense~~DoD in a supporting role. Through DSPD, the ~~Department~~DoD collaborates with other USG agencies for public diplomacy programs that directly support the DoD mission. It is critical that all DoD information activities be conducted in concert with the broader USG communications strategy and support the National Security Strategy.

4.2.4. Intelligence Support. Intelligence shall be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

#### 4.2.5. Other Human-Derived Information Gathering Activities

4.2.5.1. *Other human-derived information gathering activities provide “atmospherics” in support of IO and include polling, surveys, opinion research, spot reports,*

*and consolidation of other information relevant to prevailing moods, attitudes, and influences among a population.*

*4.2.5.2. IO planning and execution incorporate atmospheric and all forms of intelligence to target decision makers and effect decision making.*

*4.2.5.3. Because of the close relationship to HUMINT, other human-derived information gathering activities for atmospheric in support of IO planning and execution shall be coordinated and deconflicted with the Intelligence Community (IC).*

*4.2.5.4. All contracts to support human-derived information gathering activities shall have proper USG oversight of the development of the statement of work, of the placement of work on the contract, and of the performance of such contract, and undergo a policy review in accordance with subparagraph 4.2.5.3.*

4.3. To achieve the objective of establishing IO as a core military competency, a cadre of IO Capability Specialists and IO Planners shall be developed.

4.4. IO shall be integrated into Security Cooperation Guidance for theater planning, as well as deliberate and contingency planning, to support national policy and strategy.

4.5. IO *planning and execution* shall be coordinated and appropriately synchronized during peacetime and crisis actions and will include interagency coordination to ensure deconfliction with other agency programs, operations, and activities, *in accordance with DoDD S-3321.1 (Reference (1)).*

4.6. Tactics, techniques, procedures, and technologies shall be shared among the DoD Components to fully facilitate synchronization and integration of IO.

4.7. IO capabilities shall be integrated into joint exercises and joint training regimes to the maximum extent possible.

4.8. The DoD Information Operations and Space Executive Committee shall serve as the senior corporate body advising the Secretary of Defense on issues relating to IO.

## 5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall:

5.1.1. Serve as the Principal Staff Assistant to the Secretary of Defense for IO.

5.1.2. Develop and oversee DoD IO policy and integration activities.

5.1.3. Assess the performance of Defense and Military Intelligence and the responsiveness of intelligence activities to support DoD IO.

5.1.4. Serve as the DoD lead within the IC regarding IO issues, *and provide guidance for the coordination and deconfliction of HUMINT and related intelligence activities and other human-derived information gathering activities (e.g., in support of IO).*

5.1.5. Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.

5.1.6. Establish specific policies for the development and integration of CNO, MILDEC, and OPSEC as core IO capabilities.

5.1.7. Ensure the Director, National Security Agency, will:

5.1.7.1. Support IO planning and operations with Signals Intelligence, technology, and access.

5.1.7.2. Support proposed IO courses of action with the intelligence gain/loss assessments and potential targeting strategies.

5.1.7.3. Host and serve as Executive Secretary for the process to deconflict Department CNO activities with the IC.

5.1.7.4. Assess the overall security posture of national security systems and conduct CND activities as directed.

5.1.7.5. Provide OPSEC assistance, products, and services.

5.1.8. Ensure the Director, Defense Intelligence Agency, will: ~~manage DoD all-source intelligence collection, analysis, and dissemination in support of DoD IO intelligence requirements.~~

*5.1.8.1. Manage DoD all-source intelligence collection, analysis, and dissemination in support of DoD IO intelligence requirements.*

*5.1.8.2. Provide guidance for the coordination and deconfliction of HUMINT and related intelligence activities and other human-derived information gathering activities (e.g., in support of IO).*

*5.1.8.3. Ensure the Director, Defense CI and HUMINT Center (DCHC), provides oversight and management of the coordination and deconfliction of HUMINT and related intelligence activities and other human-derived information gathering activities (e.g., in support of IO) and take appropriate action to remedy issues that cannot be resolved at lower levels.*

5.2. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) shall:

5.2.1. Establish specific policies for the development and integration of EW as a core IO capability.

5.2.2. Develop and maintain a technology investment strategy to support the development, acquisition, and integration of EW capabilities.

5.2.3. Incorporate IO threat countermeasures in acquisition programs.

5.2.4. Invest in and develop the science and technologies needed to support IO capabilities.

5.3. The Under Secretary of Defense for Policy (USD(P)) shall:

5.3.1. Provide DoD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs submitted by Combatant Commanders to verify that proposed employment of IO capabilities are appropriately coordinated and consistent with DoD policy and the National Military Strategy.

5.3.2. Lead interagency coordination, exclusive of the IC, and international cooperation involving the planning and employment of IO capabilities.

5.3.3. Establish specific policy and oversight for the development and integration of ~~PSYOP~~ *MISO* as a core IO capability.

5.3.4. In coordination with USD(I) and ASD(PA), establish specific policy and oversight for the development and integration of DSPD as a related IO capability.

5.4. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall:

5.4.1. Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.

5.4.2. Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

5.5. The Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer shall:

5.5.1. Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.

5.5.2. Oversee and assess the efforts of the Heads of the DoD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.



5.6. The Assistant Secretary of Defense for Public Affairs shall:

5.6.1. Establish specific policy for the relationship of PA to IO.

5.6.2. Oversee PA planning and coordination efforts as related to IO within the ~~Department of Defense~~*DoD*.

5.6.3. Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for PA and visual information personnel at the Defense Information School.

5.6.4. In coordination with USD(I) and USD(P), oversee and develop DoD policy that addresses DoD efforts to communicate information to the public and the media.

5.7. The Heads of the DoD Components shall:

5.7.1. Assign responsibilities and establish procedures within their organizations to implement the policies in ~~S~~section 4 of this Directive.

5.7.2. Inform PA officials of military plans and operations and establish synchronized IO and PA efforts.

5.7.3. Develop policy, doctrine, and the capabilities to execute IO across the range of military operations.

5.7.4. Develop and conduct education, training, and exercise programs to provide for the successful planning, integration, and execution of IO, *to include the provision of intelligence oversight training for IO staffs*.

*5.7.5. Provide proper USG oversight of the development of the statement of work, of the placement of work on the contract, and of the performance of all contracts that support other human-derived information gathering activities (e.g., in support of IO).*

*5.7.6. Coordinate and deconflict DoD HUMINT and related intelligence activities and other human-derived information gathering activities (e.g., in support of IO) within their command or area of responsibility through the joint force staff counterintelligence and human intelligence element of the intelligence directorate of a joint staff or the equivalent intelligence staff, consistent with Reference (c). Notify the DCHC of any issue requiring action consistent with subparagraph 5.1.8.3.*

5.8. The General Counsel of the ~~Department of Defense~~*DoD* shall provide legal advice and assistance to the Secretary of Defense and other DoD officials on DoD IO, including the IO planning process and execution.

5.9. The Secretaries of the Military Departments and Commander, U.S. Special Operations Command, shall develop IO doctrine and tactics, and organize, train, and equip for IO within



their respective responsibilities pursuant to ~~S~~ection 165 of title 10, U.S. Code (Reference (~~b~~g)), and Major Force Program 11 responsibilities, respectively.

5.10. The Chairman of the Joint Chiefs of Staff shall:

5.10.1. Serve as the principal military advisor to the President of the United States, the National Security Council, and the Secretary of Defense on IO.

5.10.2. Validate capability-based IO requirements through the Joint Requirements Oversight Council.

5.10.3. Develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations.

5.10.4. Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

5.11. The Commanders of the Combatant Commands shall integrate, plan, *coordinate*, *deconflict*, and execute IO when conducting campaigns across the range of military operations and shall identify and prioritize IO requirements. IO shall be integrated into appropriate Security Cooperation plans and activities. The following Combatant Commanders have these specific responsibilities:

5.11.1. The Commander, U.S. Strategic Command (USSTRATCOM), shall integrate and coordinate DoD IO core capabilities of EW, CNO, *PSYOP MISO*, MILDEC, and OPSEC that cross geographic areas of responsibility or across the core IO areas, in addition to the responsibilities in paragraph 5.11.

5.11.2. The Commander, U.S. Special Operations Command (USSOCOM), shall, in addition to the responsibilities in paragraph 5.9 and 5.11.:

5.11.2.1. Integrate and coordinate DoD *PSYOP MISO* capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' *PSYOP MISO* planning and execution.

5.11.2.2. Employ other special operations force IO capabilities as directed.


*6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.*

67. EFFECTIVE DATE

This Directive is effective immediately.

  
Gordon England 8/14/06

*Change 1 Approved:*

  
William J. Lynn III  
Deputy Secretary of Defense

Enclosure – 12

*E1. References, continued*

*E2. Definitions*

E1. ENCLOSURE 1

DEFINITIONS/REFERENCES, continued

- (e) *“Trilateral Memorandum of Agreement among the Department of Defense and the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Exploitation Activities,” May 9, 2007*
- (f) *DoD Instruction S-5240.23, “Counterintelligence (CI) Activities in Cyberspace,” December 13, 2010*
- (g) *Section 165 of title 10, United States Code*
- (h) *Executive Order 12333, “United States intelligence Activities (as amended),” July 30, 2008*
- (i) *Memorandum of Understanding between the Department of Defense and the Department of Justice, “Reporting of Information Concerning Federal Crimes,” September 8, 1995<sup>1</sup>*
- (j) *DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,” December 7, 1982*
- (k) *DoD Directive 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight, September 20, 2010*
- (l) *DoD Directive S-3321.1, “Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War, July 26, 1984*

---

<sup>1</sup> Copies are available to authorized users via the Defense SECRET Internet Protocol Router Network (SIPRNET)  
[http://usdi.dia.smil.mil/usdi\\_st/usdi\\_docs/keyref/usdi\\_keyref.cfm](http://usdi.dia.smil.mil/usdi_st/usdi_docs/keyref/usdi_keyref.cfm)

~~E1.2.~~ ENCLOSURE 12

DEFINITIONS

*E2.1.1. Atmospherics. Information regarding the surrounding or pervading mood, environment, or influence on a given population.*

~~E1.1.4.~~ *E2.1.2. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.*

~~E1.1.2.~~ *E2.1.3. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DoD information systems and computer networks in response to a CND alert or threat information. Note: CND also employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DoD information and computer networks.*

~~E1.1.3.~~ *E2.1.4. Computer Network Exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.*

~~E1.1.4.~~ *E2.1.5. Computer Network Operations (CNO). Comprise CNA, CND, and related CNE enabling operations.*

~~E1.1.5.~~ *E2.1.6. Defense Support to Public Diplomacy (DSPD). Those activities and measures taken by the DoD Components to support and facilitate the overt public diplomacy efforts of USG Departments and Agencies designed to promote U.S. foreign policy objectives.*

~~E1.1.6.~~ *E2.1.7. Electronic Warfare (EW). Any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy.*

*E2.1.8. Foreign Cultural Analysis. Analysis of information on the demographics, norms, values, institutions, and artifacts of a population used to assist in anticipating the actions of that population within the operating environment.*

*E2.1.9. Foreign Intelligence. Defined in Reference (h).*

~~E1.1.7.~~ *E2.1.10. 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 at any level in a state or organization.*

*E2.1.11. HUMINT. A category of intelligence derived from information collected and provided by human sources.*

*Change 1, 05/23/2011*

ENCLOSURE 12

~~E2.1.12.~~ *Human Terrain Analysis.* A multidisciplinary approach to describe and predict geospatial and temporal patterns of human behavior by analyzing the attributes, actions, reactions, and interactions of groups or individuals in the context of their environment.

~~E1.1.8-E2.1.13.~~ Information. Facts, data, or instruction in any medium or form with context comprehensible to the user.

~~E1.1.9-E2.1.14.~~ Information Assurance (IA). 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. Note: CND provides operational direction and guidance through global network operations and defense for employment of IA in response to a CND alert or specific threats.

~~E1.1.10-E2.1.15~~ Information Operations Specialists and Planners. Functional experts in one or more of the highly specialized core capabilities of CNO, EW, or **PSYOP MISO**, who plan and execute the full spectrum of IO. IO planners shall understand basic principles associated with EW, CNO, and **PSYOP MISO**, as well as understand an adversary's cultural and political context, in order to be capable of integrating IO effects into Combatant Commanders' plans and orders. Both IO Capability Specialists and IO Planners should be fully educated and trained to understand the planning principles associated with OPSEC and MILDEC.

~~E1.1.11-E2.1.16~~ 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.

~~E1.1.12-E2.1.17.~~ Information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, and disseminate information.

~~E1.1.13-E2.1.18.~~ Military Deception (MILDEC). Those measures designed to mislead an adversary by manipulation, distortion, or falsification to induce him to react in a manner prejudicial to his interests.

~~E1.1.15-E2.1.19.~~ Psychological Operations (PSYOP) 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 government, organizations, groups, and individuals. The purpose of **PSYOP MISO** is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

~~E1.1.14-E2.1.20.~~ Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

~~E1.1.14.1-E2.1.20.1.~~ Identify those actions that can be observed by adversary intelligence systems.

*Change 1, 05/23/2011*

ENCLOSURE ~~12~~

~~E1.1.14.2.E2.1.20.2.~~ 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.

~~E1.1.14.3.E2.1.20.3.~~ Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

~~E1.1.15. Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.~~

~~E1.1.16.E2.1.21.~~ Public Affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal audiences with interest in the ~~Department of DefenseDoD~~. Effective PA is based on credibility and shall not focus on directing or manipulating public actions or opinion.

~~E1.1.17.E2.1.22.~~ Public Diplomacy. Those overt information activities of the USG designed to promote united foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers and by broadening the dialog between American citizens and institutions and their counterparts abroad.

~~E1.1.18.E2.1.23.~~ Security Cooperation. Those activities conducted with allies and friends, in accordance with Secretary of Defense Guidance, to:

~~E1.1.18.1.E2.1.23.1.~~ Build relationships that promote specified U.S. interests.

~~E1.1.18.2.E2.1.23.2.~~ Build allied and friendly capabilities for self-defense and coalition operations.

~~E1.1.18.3.E2.1.23.3.~~ Provide U.S. forces with peacetime and contingency access.

~~E2.1.24. Socio-Cultural Dynamics. Information about the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment.~~

~~E2.1.25. Source. A person from whom information or services are obtained.~~