BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 10-7

6 SEPTEMBER 2006

Operations

INFORMATION OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This AFPD is available for downloading from the e-Publishing website at **www.e-publishing.af.mil/**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A3I

Certified by: HQ USAF/A3/5
(Lt Gen Carrol H. Chandler)

Supersedes AFPD10-7, 12 August 1993;
AFPD10-11, 31 May 2001;
AFPD10-20, 1 October 1998

Pages: 26

This policy directive implements DoDD S-3600.1, *Information Operations (IO)* (U), dated 9 December 1996, DoDD O-8530.1, *Computer Network Defense (CND)*, dated 8 January 2001, DoDD 5205.2, *Operational Security (OPSEC) Program*, dated 29 November 1999, and applicable guidance from DoDD 5100.78, *United States Port Security Program*, dated 25 August 1986, and provides guidance for planning and conducting Air Force Information Operations (IO) to support the warfighter and achieve national strategy objectives. This policy applies to all military and civilian Air Force personnel, members of the Air Force Reserve, Air National Guard, DoD contractors, and individuals or activities under legal agreements or obligations with the Department of the Air Force. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* and disposed of in accordance with the *Air Force Records Disposition Schedule (RDS)* located at **https://afrims.amc.af.mil/**.

SUMMARY OF CHANGES

This document is substantially revised and reflects changes in IO doctrine found in AFDD 2-5, *Information Operations*, 11 January 2005. This updated policy directive replaces and renames AFPD 10-7, *Command and Control Warfare*, 12 August 1993, and incorporates policies from AFPD 10-11, *Operations Security (OPSEC)*, 31 May 2001, and AFPD 10-20, *Defensive Counterinformation Operations*, 1 October 1998, which are rescinded via this change. Applicable Air Force Instructions (AFIs) will be renumbered IAW this Air Force Policy Directive (AFPD). Note that USAF definitions of some IO terms vary from Joint definitions (see **Attachment 1**, Terms, and **Attachment 2**).

1. Introduction. Air Force IO consists of the integrated application of three capabilities: electronic warfare operations (EW Ops), network warfare operations (NW Ops), and influence operations (IFO).

1.1. Each capability is comprised of associated military capabilities:

1.1.1. EW Ops: Electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

1.1.2. NW Ops: Network attack (NetA), network defense (NetD), and network warfare support (NS).

1.1.3. IFO: Military deception (MILDEC), operations security (OPSEC), psychological operations (PSYOP), counterintelligence (CI), public affairs operations (PA), and counterpropaganda.

1.2. The Air Force applies the three IO capabilities in combinations for the purpose of both supporting and conducting the wide range of Air Force missions from global strike and global mobility to homeland security. The Air Force applies these three capabilities to influence, disrupt, or deny adversarial human and automated decision making while protecting our own. The Air Force may seek to use some of these capabilities to achieve effects similar to those achieved by kinetic weapons. Air Force IO, like air and space operations, are critically dependent on the following integrated control enablers (ICEs): intelligence, surveillance and reconnaissance (ISR), network operations (NetOps), predictive battlespace awareness (PBA), and positioning, navigation and timing (PNT). ICEs support operations and strive to provide commanders continuous decision-quality information to successfully employ air, space and information operations.

2. General. IO will integrate into military strategy; doctrine, operational concepts, operational and tactical planning and execution; across the range of military operations and exercises; communications-computer architectures and processing; weapons systems research, development, testing and evaluation (RDT&E); Air Force specialized training; inspections; acquisition and procurement; force development; and professional military education.

2.1. Success in military operations depends on the effective use of IO and information systems, on achieving and maintaining Information Superiority and Decision Superiority. Whether the target is national leadership, military command and control (C2), or an automated industrial process, how the observe, orient, decide, and act (OODA loop) process is implemented creates both opportunities and vulnerabilities. A primary focus of IO is to influence, disrupt, corrupt or usurp an adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations. The Air Force will employ a strategy to render an adversary's IO ineffective while preserving the effectiveness of our own, allied, and coalition IO.

2.2. The Air Force will maximize US, allied, and coalition military effectiveness by integrating IO into military strategy, plans, operations, exercises, training, communications architectures, information processing, systems development, and professional education while reducing friendly vulnerabilities.

2.3. The Air Force will organize, train, and equip its forces to conduct successful IO, creating desired effects for combatant commanders and national authorities.

2.4. The Air Force will implement procedures to defend the sources of friendly information that may be exploited by adversaries.

2.5. The Air Force will conduct IO activities in a manner to minimize undesired interpretations of intent.

2.6. The Air Force will ensure that Air Force IO activities that could adversely affect related US, allied, or coalition activities are coordinated to the maximum extent practicable.

3. Responsibilities. This directive establishes the following responsibilities and authorities:

3.1. The Deputy Chief of Staff, Air, Space and Information Operations, Plans and Requirements (HQ USAF/A3/5) will serve as the office of primary responsibility (OPR) for Air Force IO doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) considerations. The AF/A3/5 will serve as the senior Air Force IO officer and will represent Air Force IO at the DoD Space and IO Executive Committee. Other offices having responsibilities for individual capabilities of IO or IO ICE will coordinate with AF/A3/5 to ensure the consistent and standardized application of IO strategic planning, policy, guidance, and programmatic oversight.

3.1.1. AF/A3/5 will serve as the OPR for each of the IO capabilities (with the exceptions of Public Affairs and Counterintelligence[1]) and for integrating IO capabilities. AF/A3/5 will coordinate with SAF/AQ, SAF/XC, and SAF/US to ensure the incorporation of standardized IO requirements into Air Force acquisition activities. AF/A3/5 is the OPR for Headquarters Air Force (HAF) coordination for IO with the Joint Staff and the Office of the Secretary of Defense.

3.1.1.1. As the preferred forces (per AFDD 2-5) to execute NetA and NS operate under both Title 10 and Title 50 authorities, A3/5 will coordinate with A2 when appropriate to ensure those forces are optimally organized, trained, and equipped.

3.1.2. AF/A3/5, SAF/PA, SAF/IG, and AF/A2 will coordinate all programmatic actions related to IO with AF/A8, or other panel chairs as appropriate, and submit required changes through the Air Force Corporate Structure (AFCS) IAW AFI 16-501.

3.1.3. The Director of Information Operations (HQ USAF/A3I) will serve as AF/A3/5's OPR and lead for coordinating overall IO policy, doctrine, strategy and investment priorities. All other HAF offices with IO or IO ICE responsibilities will coordinate all IO-related matters to include promulgation of policy and guidance, requirements derivation, and programmatics with AF/A3I.

3.1.3.1. AF/A3I, in coordination with the appropriate Air Force career field managers (CFMs), will be responsible for management of the IO Career Force. The IO Career Force is comprised of the professionals who perform and/or integrate the core IO capabilities of EW Ops, NW Ops, and IFO. The IO Career Force consists of IO Capability Specialists and IO Planners.

3.1.3.2. Personnel assigned to IO billets have one or more of the following primary duties: training, testing, operational planning and/or execution, and standards/evaluation in one or more of the three IO capabilities. IO personnel are those individuals who meet the qualifications to fill an IO billet, whether currently occupying an IO billet or assigned to an IO organization.

3.1.3.3. AF/A3I will serve as the Functional Manager for Air Force designated IO programs and will provide inputs on policy and requirements prioritization guidance for activities with

1. See paragraphs **3.2.** (specifies SAF/PA as OPR for PA) and **3.3.** (SAF/IG (OSI) for CI).

ancillary IO capabilities (unless otherwise stated within this document). AF/A3/5 will resolve any questions regarding designation of Air Force programs as IO programs. AF/A3I will perform this duty in consultation with SAF/AQI as the OPR for IO Acquisition and AFMC in its role as Program Manager.

3.1.3.4. AF/A3I will coordinate with ACC, AF/A2I, AF/A5R, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSOC, AFSPC, and AMC to incorporate AF IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.1.3.5. AF/A3I will participate in the Air Force level IO Capabilities Team (IOCT) to ensure requirements and capabilities are integrated across the Air Force.

3.1.3.6. AF/A3I will coordinate with the Director of Operational Plans and Joint Matters (AF/A5X) to integrate IO into the Capabilities Review and Risk Assessment (CRRA) process.

3.1.4. The Director of Operational Capability Requirements (HQ USAF/A5R) will:

3.1.4.1. Serve as the OPR for defining and validating IO operational capability requirements for Air Force and Joint concepts of operation.

3.1.4.2. Serve as AF/A3/5's OPR for EW to include the full range of DOTMLPF and investment priorities.

3.1.4.3. Participate in the Air Force level IOCT and IO Steering Group to ensure requirements and capabilities are integrated across the Air Force.

3.1.5. The Director of Strategic Security (HQ USAF/A3S) is the HQ USAF lead for strategic security, to include Homeland Security, Force Protection, nuclear operations, space operations and integration, counter-proliferation issues and career-field management. AF/A3S develops sustainment, planning, programming, training, integration and policy guidance for strategic security capabilities. AF/A3S manages integration of strategic security capabilities into Air Force, joint, coalition, and national planning and operations. AF/A3S will coordinate with AF/A3I, SAF/USA, SAF/AQI, and SAF/AQL regarding efforts under its cognizance with ancillary IO capabilities.

3.2. The office of the Secretary of the Air Force, Office of Public Affairs (SAF/PA) will serve as the OPR for public affairs operations and will participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.3. The office of the Secretary of the Air Force, Inspector General Office (SAF/IG) will serve as OPR for counterintelligence (CI) through the Air Force Office of Special Investigations (AFOSI).

3.3.1. SAF/IG will participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.3.2. SAF/IG will assist the Secretary of the Air Force in his capacity as Executive Agent for a DoD Computer Forensics Laboratory (DCFL) and a DoD Computer Investigations Training Program (DCITP).

3.3.3. Commander AFOSI will provide overall program management for the DCFL and DCITP.

3.4. The office of the Secretary of the Air Force, Warfighting Integration and Chief Information Officer (SAF/XC) will serve as the OPR for information resources, to include ensuring effective/efficient acquisition, application, management and sustainment. In coordination with Commander, Air Force Network Operations (AFNetOps/CC) and AF/A3/5, SAF/XC will be responsible for develop-

ing, integrating, and implementing NetD solutions. SAF/XC will coordinate with AF/A3/5 and AF/A8 to ensure NetOps requirements, capabilities, and deficiencies are documented and will collaborate with AF/A3I Deputy for Network Warfare Operations (AF/A3IN) to do same for NetD requirements, capabilities, and deficiencies.

3.4.1. SAF/XC will participate in the Air Force level IOCT to ensure technical integration is addressed for the Air Force enterprise.

3.4.2. SAF/XCO will coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/USA, AFMC, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.4.3. SAF/XC will coordinate with AF/A3/5 to ensure the consistent and standardized application of strategic planning, policy, guidance, and programmatic oversight for NetOps, including Information Assurance (IA), as an ICE in support of IO.

3.5. The Deputy Chief of Staff for Intelligence (HQ USAF/A2) will:

3.5.1. Participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.5.2. Coordinate with ACC, AF/A3I, AF/A5R, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.5.2.1. As the preferred forces (per AFDD 2-5) to execute NetA and NS operate under both Title 10 and Title 50 authorities, A2 will coordinate with A3/5 when appropriate to ensure those forces are optimally organized, trained, and equipped.

3.5.3. Create, coordinate, and represent appropriate funding justification IAW decisions made by the AFCS for the Air Force, DoD and Congress, to include management of funds allocated for acquisition programs within the RDT&E appropriation

3.5.4. Review, coordinate and approve (where appropriate) IO program documentation (to include program management directives, initial capabilities documents, acquisition program baseline, security classification guides).

3.6. The Assistant Secretary of the Air Force, Acquisitions (SAF/AQ) through the Information Dominance Programs Directorate (SAF/AQI) and Special Programs Division (SAF/AQL), will serve as the OPR for the RDT&E of USAF IO acquisition activities, to include providing direction, guidance and supervision over all matters pertaining to the formulation, review, approval and execution of plans, policies, and programs relative to research, development, production and acquisition of IO programs and defense materiel. SAF/AQ will:

3.6.1. Participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.6.2. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/XCO, SAF/USA, AFMC, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.6.3. Create, coordinate, and represent appropriate IO funding justification IAW decisions made by the AFCS for the Air Force, DoD and Congress, to include management of funds allocated for acquisition programs within the RDT&E appropriation.

3.6.4. Work with AFMC to ensure that the IOCT is well informed of all relevant RDT&E efforts throughout the Air Force and other DoD and National Agencies.

3.6.5. Review, coordinate and approve (where appropriate) IO program documentation (to include program management directives, initial capabilities documents, acquisition program baseline, security classification guides).

3.6.6. Participate in the DoD Space and IO Executive Committee, as invited.

3.7. The office of the Undersecretary of the Air Force, Director of Space Acquisition (SAF/USA) will:

3.7.1. Participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.7.2. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, AFMC, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.8. The Deputy Chief of Staff, Manpower and Personnel, (HQ USAF/A1) and Air Force Personnel Center (AFPC), in coordination with AF/A3I and career field managers, will:

3.8.1. Develop a baseline of IO positions and an automated capability to identify and track Air Force IO billets and personnel.

3.8.2. Establish education, training, and experience standards.

3.8.3. Develop and implement procedures that provide appropriate education, training and career development opportunities for members of the IO Career Force.

3.8.4. Assign skilled and qualified IO personnel to IO positions.

3.8.5. Establish or supplement current professional development boards to monitor accession, training, education and career development for the IO Career Force.

3.9. The Office of the General Counsel, Division of International Affairs (SAF/GCI) is the OPR to ensure all Air Force applications of IO capabilities are consistent with US policy and law.

3.10. Air Combat Command (ACC) has IO responsibilities at the Air Force, combat air forces (CAF) and Major Command (MAJCOM) level.

3.10.1. At the Air Force level, ACC will serve as the Lead Command for Air Force IO with responsibilities as outlined in AFPD 10-9, *Lead Operating Command Weapon Systems Management*. ACC will ensure that all MAJCOM offices with IO or IO ICE responsibilities will coordinate all IO-related matters to include promulgation of policy and guidance, requirements derivation, and programmatics with AF/A3/5 and IAW AFI 16-501. ACC will:

3.10.1.1. In coordination with AMC, be responsible for development and management of the Air Force IO Capabilities Plan (IOCP). This consolidated plan documents, validates, and prioritizes the Air Force's identified IO capabilities gaps and shortfalls, and completes a solution search across each DOTMLPF category. In coordination with AF/A3/5 and with co-signature

from AMC, ACC will charter an IOCT to develop and manage the IOCP. ACC will serve as OPR for and chair of the IOCT. All Air Force commands, organizations, and agencies shall use the IOCP when addressing IO shortfalls. IOCT representatives will work with HQ USAF/A5X to incorporate IO capabilities into the Master Capabilities Library (MCL) and Requirements Analysis Team (RAT) process. ACC will coordinate the development of the Air Force IOCP with all IOCT members. The IOCT will collect, assess, prioritize, and advocate for IO solutions to be included in each members' Program Objective Memorandum (POM).

3.10.1.2. Establish and fund the IOCT and its supporting structure in order to develop the Air Force IOCP and to ensure its products are integrated into the Air Force Capability Review and Risk Assessment (CRRA) process.

3.10.1.3. Be responsible for the formation, manning, and training of IO forces to employ IO capabilities. Lead development of training for capability specialists to conduct IO tactics, techniques, and procedures and operational level planners to apply the doctrine and tenets of Air Force IO within the air and space operations centers (AOCs).

3.10.1.4. Establish sufficient vulnerability assessment and IO aggressor capabilities to satisfy RDT&E, operational test and evaluation (OT&E), exercises, training, and real world operations requirements.

3.10.1.5. Appoint an AFNetOps/CC.

3.10.2. At the CAF level, ACC will serve as the lead for all IO. As lead, ACC will organize, train, and equip IO forces and capabilities, to include readiness assessment and evaluation functions, and leading integration of IO into all CAF mission areas. ACC will:

3.10.2.1. Serve as OPR for the development of all Air Force IO enabling concepts, Operational Tactics, Techniques and Procedures (OTTP) and for the assessment of IO capabilities, including against potential threats.

3.10.2.2. Serve as OPR for planning, coordinating, and conducting all Air Force IO Initial Qualification Training (IQT), CAF Mission Qualification Training (MQT) and continuation training for IO forces.

3.10.2.3. Coordinate with AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.10.2.4. Facilitate inter-command IO standardization and incorporate Air Force IO capabilities into Joint/Air Force concepts, exercises, and AOC baselining.

3.10.3. At the MAJCOM level, ACC will provide programmatic oversight of IO programs and synchronize implementation among the three IO capabilities and their activities; establish and integrate IO within the AOC; coordinate specialized IO related ICE requirements; consolidate/integrate IO into theater air operations; standardize CAF IO organization, training and equipment; and integrate special access programs into operations and exercises.

3.11. Air Mobility Command (AMC) will serve as the lead command for IO at the mobility air forces (MAF) level.

3.11.1. As the MAF lead for IO, AMC is the office of collateral responsibility (OCR) for the Air Force IOCP.

3.11.1.1. AMC will support MAF integration into the IOCT and its supporting structure in accordance with AFPD 10-9 to develop the Air Force IOCP and to ensure its products are integrated into the Air Force CRRA process.

3.11.1.2. AMC will participate in the development of the IOCP and Commander, AMC, will be a signatory with Commander, ACC (COMACC).

3.11.2. At the MAF level, AMC will organize, train and equip IO capabilities to include IO assets supporting IO conducted by MAF organizations. AMC will lead centralized management of MAF IO capabilities; establish and integrate IO in the MAF Air Operations Centers (Tanker Airlift Control Center); coordinate specialized IO related ICE requirements; consolidate/integrate MAF IO requirements into theater air operations; standardize MAF IO organization, training and equipment; and integrate MAF special access programs into operations and exercises. AMC will:

3.11.2.1. Serve as MAF OPR for the development of OTTPs and for the assessment of IO capabilities.

3.11.2.2. Serve as OPR for planning, coordinating, and conducting MQT for MAF IO forces.

3.11.2.3. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSOC, and AFSPC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.12. Air Force Special Operations Command (AFSOC) will:

3.12.1. Serve as OPR for planning and coordinating MQT for assigned IO forces.

3.12.2. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.13. Air Force Materiel Command (AFMC) will:

3.13.1. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFSOC, AFSPC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.13.2. Provide the subject matter expertise necessary to assist the product center(s) and the system producers to explore alternative developmental courses of action for new IO capabilities as well as ensuring integration of IO into weapon systems' RDT&E.

3.13.3. Ensure that IO mid-term and long-term research and technology shortfall issues are adequately addressed through Air Force Research Laboratory activities, and advocate for solutions.

3.13.4. As requested by SAF/AQ, designate and man USAF System Program Offices (SPOs) for IO capabilities.

3.13.5. Serve as the Program Manager for USAF designated IO programs and provide policy and prioritization guidance for activities with ancillary IO capabilities. AF/A3/5 will resolve any questions regarding designation of programs. AFMC will perform this duty in consultation with AF/A3I in its role as Functional Manager and with SAF/AQI as the OPR for IO Acquisition.

3.13.6. Work with SAF/AQ to ensure that the IOCT is well informed of all relevant RDT&E efforts throughout the Air Force.

3.14. Air Education and Training Command (AETC) will:

3.14.1. Implement the approved life-cycle strategy, as defined by the Air Force IO Training Planning Team, that defines total force education and training needed to satisfy mission-generated IO requirements.

3.14.2. Participate in and chair, when appropriate, Utilization and Training Workshops (U&TWs) and Training Planning Teams (TPTs) which address IO training requirements for the core Air Force Specialty Codes (AFSCs) that feed the IO career force.

3.15. Air Force Space Command (AFSPC) will:

3.15.1. Serve as OPR for planning, coordinating, and conducting MQT for assigned IO forces.

3.15.2. Coordinate with ACC, AF/A3I, AF/A5R, AF/A2I, AF/A3S, SAF/AQI, SAF/AQL, SAF/XCO, SAF/USA, AFMC, AFSOC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.15.3. Serve as the Program Manager for USAF designated space programs and provide policy and prioritization guidance for activities with ancillary space capabilities. AF/A3/5 will resolve any questions regarding designation of programs. AFSPC will perform this duty in consultation with AF/A3I and AF/A3S.

3.15.4. Serve as lead command and advocate for capabilities required to organize, train, equip, and employ Air Force space and missile forces. This includes coordination on all IO capabilities related to Space Superiority.

3.15.5. Coordinate with ACC and AFMC to integrate development and presentation of IO forces with counterspace forces to achieve Information and Space Superiority

3.16. Commander, Air Force Network Operations (AFNetOps/CC) is the USAF NetOps/NetD C2 authority. AFNetOps/CC will:

3.16.1. Exercise specific compliance enforcement and directive authorities over MAJCOM units/assets.

3.16.2. Exercise Direct Liaison Authority (DIRLAUTH) to MAJCOM Directors of Communications (A6) or equivalent, System Control Centers, Network Operations Security Centers (NOSCs), and Deployable NOSCs (NOSC-D).

3.16.3. Exercise authority to task in response to events that involve multiple MAJCOMs, affect the preponderance of the Air Force network, or are time-critical to assure network availability and security. This authority extends to all systems and applications that expose AFNetOps to a vulnerability or impact operations.

3.17. All MAJCOMs and the Air National Guard (ANG) will:

3.17.1. Develop IO programs and policies aligned with Air Force IO program and policy guidance issued by AF/A3/5 and ensure subordinate organizations integrate applicable IO into day-to-day operations.

3.17.2. Use established requirements procedures and documentation, such as Initial Capabilities Documents, Capability Development Documents, inputs to the combatant commanders' Integrated Priority Lists and Joint Requirements Oversight Council reviews, Quadrennial Defense Reviews, lessons learned, and ad hoc studies to identify and document IO requirements and defi-

ciencies, and to provide those inputs to the IOCT in accordance with IOCT guidance. Submit potential solutions to the IOCT in accordance with IOCT guidance for vetting, visibility, and advocacy among all IOCT members. (See the IOCT charter for further information; contact ACC/A8I for details.)

3.17.3. When specifically authorized by HAF, organize, train and equip assigned IO forces. IO units shall not be created nor existing units become IO units, without specific authorization from HAF.

3.17.4. Participate in the Air Force level IOCT to ensure requirements and capabilities are integrated across the Air Force.

3.17.5. Coordinate with AFRC on IO matters pertaining to MAJCOM-gained units, total force integration, and IO requirements.

3.18. In coordination with AF/A3/5 and other appropriate agencies, commanders are responsible for IO implementation, posture and operations within their commands and units. Additionally, they are responsible for enforcing IO policies and directives, ensuring that IO plans and programs at every echelon are supported by ICEs at those levels.

3.19. Commanders at all levels are responsible for ensuring units and staffs act in accordance with US policy and public law.

4. See **Attachment 1** and **Attachment 2** for references and supporting information.

MICHAEL W. WYNNE
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD, *National Defense Strategy,* March 2005
(**http://www.defenselink.mil/pubs/**)

DoD Directive S-3600.1, *Information Operations (IO)* (U), 9 December 1996

DoD Directive 4640.6, *Communications Security Telephone Monitoring and Recording*, 26 June 1981

DoD Directive 5205.2, *DOD Operations Security (OPSEC) Program*, 29 November 1999 (under revision)

DoD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, December 1982

DoD Directive 8500.1, *Information Assurance*, 24 October 2002

DoD Directive O-8530.1, *Computer Network Defense (CND)*, 8 January 2001

DoD Instruction 3608.11, *Information Operations Career Force*, 4 November 2005

CJCS, *National Military Strategy of the United States of America*, 2004 (**http://www.defenselink.mil/pubs/**)

CJCS Instruction 3170.01E, *Joint Capabilities Integration and Development System (JCIDS)*, 11 May 05

CJCS Instruction 3210.01A, *Joint Information Operations Policy,* 6 November 1998

CJCS Instruction 3210.03B, *Joint Electronic Warfare Policy*, 31 July 2002

CJCS Instruction 3210.04, *Joint Electronic Warfare Reprogramming Policy*, 31 December 2003

CJCS Instruction 3211.01C, *Joint Policy for Military Deception*, 19 February 2002

CJCS Instruction 3213.01B, *Joint Operations Security*, 17 December 2003

CJCSI 6212.01C, *Interoperability and Supportability of National Security Systems (NSS) and Information Technology (IT)*, 20 November 03

CJCS Instruction 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 June 2004

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 Apr 2001 as amended through 31 August 2005

Joint Publication 2-0, *Doctrine for Intelligence Support to Joint Operations*, 9 March 2000

Joint Publication 3-13, *Information Operations,* 13 February 2006

Joint Publication 3-51, *Joint Doctrine for Electronic Warfare*, 7 April 2000

Joint Publication 3-54, *Joint Doctrine for Operations Security*, 27 January 1997

Joint Publication 3-58, *Joint Doctrine for Military Deception*, 31 May 1996

Joint Publication 3-61, *Public Affairs*, 9 May 2005

Air Force Doctrine Document 2-5, *Information Operations,* 11 January 2005

Air Force Doctrine Document 2-5.1, *Electronic Warfare*, 5 November 2002

Air Force Doctrine Document 2-5.3, *Public Affairs Operations*, 24 June 2005

AFPD 10-6, *Mission Needs And Operational Requirements,* 19 January 93

AFPD 10-7, *Command and Control Warfare (C2W)*, 12 August 1993 (superseded by this document)

AFPD 10-9, *Lead Operating Command Weapons System Management*, 13 June 2000

AFPD 10-11, *Operations Security*, 31 May 2001 (superseded by this document)

AFPD 10-20, *Air Force Defensive Counterinformation Operations*, 1 October 1998 (superseded by this document)

AFPD 33-2, *Information Protection,* 1 December 1996 (To become AFPD 33-2, *Information Assurance*)

AFPD 35-1, *Public Affairs Management,* 17 September 1999

AFPD 33-3, *Information Management*, 28 March 2006

AFPD 71-1, *Criminal Investigations and Counterintelligence,* 1 July 1999

AFI 10-601, *Capabilities Based Requirements Development*, 31 July 2006

AFI 10-701, *Operations Security (OPSEC),* 30 September 2005

AFI 10-703, *Electronic Warfare Integrated Reprogramming (EWIR),* 31 October 2001

AFI 10-704, *Military Deception Program*, 30 August 2005

AFI 10-706, *Electronic Warfare (EW),* 23 August 2001

AFI 10-707, *Spectrum Interference Resolution Program,* 20 June 2005

AFI 10-1105, *Port Security Instructions*, 19 May 1994 (To become AFI 10-7XX, *Port Security Instructions*.)

AFI 10-2001, *Defensive Counterinformation Planning, Operations and Assessment,* 4 October 2001 (To become AFI 10-7XX, *Information Planning, Operations and Assessment*)

AFI 10-2005, *Defensive Counterinformation Security Classification Guide*, 14 August 2002

AFI 14-104, *Oversight of Intelligence Activities*, 14 April 2005

AFI 16-501, *Control and Documentation of Air Force Programs*, 15 August 2006

AFI 33-115V1, *Network Operations (NETOPS)*, 24 May 2006

AFI 35-101, *Public Affairs Policies and Procedures*, 29 November 2005

AFI 71-101V4, *Counterintelligence*, 1 August 2000

AFMAN 37-123, *Management of Records*, 31 August 1994

Air Force Interim Computer Network Attack (CNA) Security Classification Guide, 3 June 2002
(Classified: contact AF/A3I)

Air Force Military Deception Security Classification Guide, 1 July 2005
(Classified: contact AF/A3I)

Abbreviations and Acronyms

ACC—Air Combat Command

AETC—Air Education and Training Command

AF—Air Force

AFCS—Air Force corporate structure

AFDD—Air Force doctrine document

AFI—Air Force instruction

AFMAN—Air Force manual

AFMC—Air Force Materiel Command

AFNetOps/CC—Commander, Air Force Network Operations

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force policy directive

AFRC—Air Force Reserve Command

AFSC—Air Force specialty code

AFSOC—Air Force Special Operations Command

AFSPC—Air Force Space Command

AMC—Air Mobility Command

ANG—Air National Guard

AOC—air and space operations center

C2—command and control

CAF—Combat Air Force

CFM—career field manager

CI—counterintelligence

CJCS—Chairman, Joint Chiefs of Staff

CNA—computer network attack

CND—computer network defense

CNE—computer network exploitation

CNO—computer network operations

COMACC—Commander, ACC

CONOPS—concept of operations

CP—Capabilities Plan

CT—Capabilities Team

CRRA—Capabilities Review and Risk Assessment

CSAF—Chief of Staff of the Air Force

DCFL—Department of Defense (DoD) Computer Forensics Laboratory

DCITP—Department of Defense (DoD) Computer Investigation Training Program

DIRLAUTH—direct liaison authority

DoD—Department of Defense

DoDD—Department of Defense Directive

DOTMLPF—doctrine, organization, training, materiel, leadership and education, personnel and facilities

DRU—direct reporting unit

EA—electronic attack

EP—electronic protection

ES—electronic warfare support

ESSA—Electronic Systems Security Assessments

EW—electronic warfare

EW Ops—electronic warfare operations

EWIR—Electronic Warfare Integrated Reprogramming

FOA—field operating agency

HAF—Headquarters Air Force

HQ—headquarters

HQ USAF/A1—Deputy Chief of Staff, Manpower and Personnel (formerly AF/DP)

HQ USAF/A3/5—Deputy Chief of Staff, Air, Space and Information Operations (formerly AF/XO)

HQ USAF/A3I—Director, Information Operations (formerly AF/XOIW)

HQ USAF/A3S—Director of Strategic Security (formerly AF/XOS)

HQ USAF/A5R—Director of Operational Capability Requirements (formerly AF/XOR)

HQ USAF/A5X—Director of Operational Plans and Joint Matters (formerly AF/XOX)

IA—information assurance

IAW—in accordance with

ICE—integrated control enabler

IFO—influence operations

IO—information operations

IOCP—Information Operations Capabilities Plan

IOCT—Information Operations Capabilities Team

IPT—integrated process team

IQT—initial qualification training

ISR—intelligence, surveillance, and reconnaissance

IT—information technology

IWF—information warfare flight

JOC—joint operating concept

JP—joint publication

MAF—Mobility Air Force

MAJCOM—Major Command

MCL—Master Capabilities Library

MILDEC—military deception

MQT—mission qualification training

NAF—Numbered Air Force

NetA—network attack

NetD—network defense

NetOps—network operations

NOSC—network operations security center

NOSC-D—deployable network operations security center

NS—network warfare support

NW Ops—network warfare operations

OCR—office of collateral responsibility

OODA—observe, orient, decide, act

OPR—office of primary responsibility

OPSEC—operations security

OTTP—operational tactics, techniques, and procedures

OT&E—operational test and evaluation

PA—public affairs

PBA—predictive battlespace awareness

PDO—Publishing Distribution Office

PNT—positioning, navigation, and timing

POM—program objective memorandum

PSYOP—psychological operations

RAT—Requirements Analysis Team

RAWG—Requirements Analysis Working Group

RDT&E—research, development, testing and evaluation

SAF/AQ—Secretary of the Air Force, Acquisitions

SAF/AQI—Directorate for Information Dominance Programs, Office of the Assistant Secretary of the Air Force for Acquisition

SAF/AQL—Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition

SAF/IG—Secretary of the Air Force, Inspector General Office

SAF/PA—Secretary of the Air Force, Office of Public Affairs

SAF/USA—Director of Space Acquisition, Office of the Undersecretary of the Air Force

SAF/XC—Secretary of the Air Force, Office of Warfighting Integration & Chief Information Officer

SEI—special experience identifier

SPO—system program office

TPT—training planning team

USAF—United States Air Force

U&TW—utilization and training workshop

Terms

counterintelligence (CI)—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. (AFDD 2-5; JP 1-02)

counterpropaganda operations—Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. (JP 1-02) [*Activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding*.] (AFDD 2-5) {Words in brackets apply only to the Air Force and are offered for clarity.}

decision superiority—A competitive advantage, enabled by an ongoing situational awareness, that allows commanders and their forces to make better-informed decisions and implement them faster than their adversaries can react. (AFDD 2-5)

electronic attack (EA)—That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of

weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). See electronic warfare. (AFDD 2-5; JP 1-02)

electronic protection (EP)—That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. See electronic warfare. (AFDD 2-5; JP 1-02)

electronic warfare (EW)—Any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. (AFDD 2-5; JP 1-02)

electronic warfare support (ES)—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. See electronic warfare. (AFDD 2-5; JP 1-02)

electronic warfare operations (EW Ops)—The integrated planning, employment and assessment of military capabilities to achieve desired effects across the electromagnetic targeting domain in support of operational objectives. (AFDD 2-5)

functional manager—The authority responsible for policy and procedures associated with systems within a given functional area. (Defense Finance and Accounting Service)

influence operations—Employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives. Influence operations capabilities include counterpropaganda operations, psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC), counterintelligence (CI) operations, and public affairs. (AFDD 2-5)

information—1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (AFDD 2-5; JP 1-02)

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. Also called IA. (JP 3-13)

information operations (IO)—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. Also called IO. (JP 3-13) [*Information operations are the integrated employment of the core capabilities of influence operations, electronic warfare operations, network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while*

protecting our own.] (AFDD 2-5) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

Information Operations Capability Plan (IOCP)—Defines, documents, advocates, and directs the modernization and sustainment of Air Force IO (DOTMLPF).

information resources—Information and related resources, such as personnel, equipment, and information technology. See also information. (JP 1-02)

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 3-13)

information system—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 3-13)

integrated control enablers (ICE)—Critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. Includes intelligence, surveillance, and reconnaissance (ISR), positioning navigation and timing (PNT), and network operations (NetOps). (AFDD 2-5)

intelligence, surveillance, and reconnaissance—Intelligence, surveillance, and reconnaissance are integrated capabilities to collect, process, exploit, and disseminate accurate and timely information that provides the battlespace awareness necessary to successfully plan and conduct operations. Also called ISR. (AFDD 2-5; AFDD 2-9)

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 forces mission. (AFDD 2-5; JP 1-02) [There are five categories of military deception. See JP 1-02 for the complete definition.]

network attack (NetA)—The employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. (AFDD 2-5) Network attack incorporates computer network attack (CNA) as defined in joint doctrine.

network defense (NetD)—The employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt or usurp it. (AFDD 2-5) Network defense incorporates computer network defense (CND) as defined in joint doctrine.

network operations (NetOps)—The integrated planning and employment of military capabilities to provide the friendly net environment needed to plan, control and execute military operations and conduct Service functions. NetOps provides operational planning and control. It involves time-critical, operational-level decisions that direct configuration changes and information routing. NetOps risk management and command and control decisions are based on a fused assessment of intelligence, ongoing operations, commander's intent, blue and gray situation, net health, and net security. NetOps provides the three capabilities of information assurance, network/system management, and information dissemination management. (AFDD 2-5)

network warfare operations (NW Ops)—The integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace. Network warfare operations are conducted in the information domain through dynamic combination of hardware, software, data, and human interactions. (AFDD 2-5) NW Ops capabilities include network attack (NetA), network defense (NetD), and network warfare support (NS).

network warfare support (NS)—Actions tasked by or under direct control of an operational commander to search for, intercept, identify, and locate or localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. NS provides information required for immediate decisions involving network warfare operations. NS data can be used to produce intelligence, or provide targeting for electronic or destructive attack. (AFDD 2-5) Closely related to the Joint term CNA Operational Preparation of the Environment (CNA OPE).

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 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. (AFDD 2-5; JP 1-02)

predictive battlespace awareness (PBA)—Knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions (AFDD 2-5; Air Force Pamphlet 14-118).

propaganda—Any form of communication in support of national or organizational objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. [The Joint definition in JP 1-02 omits "or organizational".]

psychological operations (PSYOP)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objectives 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 behaviors favorable to the originator's objectives. (AFDD 2-5; JP 1-02) [*PSYOP is an effects-based Influence Operation (IFO) capability that employs the full range of air and space power to produce specific cognitive, emotional, psychosocial, and behavioral effects in a approved foreign audiences, in furtherance of US strategic, operational, and tactical objectives.*] (IFO CONOPS) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

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. (AFDD 2-5; JP 1-02) Public affairs operations use timely and accurate information to help deter war, drive a crisis back to peace, or wage war.

public affairs operations—Operational activities that communicate unclassified information about Air Force activities to Air Force, domestic, and international audiences. The capabilities they give the warfighter include: providing counsel and guidance about the public information environment; enhancing Airman morale and readiness; gaining and maintaining public support for military operations; and communicating US resolve in a manner that provides global influence and deterrence. As a weapon in the commander's arsenal of information operations (IO), public affairs operations use timely and accurate information to help deter war, drive a crisis back to peace, or wage war. (AFDD 2-5.3)

Attachment 2

TAXONOMY OF INFORMATION OPERATIONS TERMINOLOGY

* Related Joint terms should *not* be assumed to be identical to USAF terms, but are offered for reference. See the Definition column and compare with current Joint definition of related term.

Air Force Term	Air Force Definition	Related Joint Term*
Operations		
- Air Operations	(not expanded here)	
- Space Operations	(not expanded here)	
- Information Operations (IO)	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. Also called IO. (JP 3-13) [*Information operations are the integrated employment of the core capabilities of influence operations, electronic warfare operations, network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.*] (AFDD 2-5) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}	Information Operations (IO)
- Electronic Warfare Operations (EW Ops)	electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. (JP 1-02) EW Ops: The integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives. Also called EW Ops. (AFDD 2-5)	Electronic Warfare (EW)

Air Force Term	Air Force Definition	Related Joint Term*
- Electronic Attack (EA)	That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). (JP 1-02)	Electronic Attack (EA)
- Electronic Protect (EP)	That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. (JP 1-02)	Electronic Protect (EP)
- Electronic Warfare Support (ES)	That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 1-02)	Electronic Warfare Support (ES)
- Network Warfare Operations (NW Ops)	Network warfare operations are the integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace. Network warfare operations are conducted in the information domain through the dynamic combination of hardware, software, data, and human interaction. Also called NW Ops. (AFDD 2-5)	Computer Network Operations (CNO)
- Network Attack (NetA)	The employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. Also called NetA. (AFDD 2-5)	Computer Network Attack (CNA)
- Network Defense (NetD)	The employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. Also called NetD. (AFDD 2-5)	Computer Network Defense (CND)

Air Force Term	Air Force Definition	Related Joint Term*
- Network Warfare Support (NS)	Actions tasked by or under direct control of an operational commander to search for, intercept, identify, and locate or localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. NS provides information required for immediate decisions involving network warfare operations. NS data can be used to produce intelligence, or provide targeting for electronic or destructive attack. Also called NS. (AFDD 2-5)	Computer Network Attack Operational Preparation of the Environment (CNA OPE)
- Influence Operations (IFO)	Employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives (AFDD 2-5)	
- 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. Also called OPSEC. (JP 1-02)	Operations Security (OPSEC)
- 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) [There are five categories of military deception. See JP 1-02 for complete definition.]	Military Deception (MILDEC)
- 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 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. Also called PSYOP. (JP 1-02)	Psychological Operations (PSYOP)
- Counterintelligence (CI)	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. Also called CI. (JP 1-02)	Counterintelligence (CI)

Air Force Term	Air Force Definition	Related Joint Term*
- Public Affairs (PA) Operations	Operational activities that communicate unclassified information about Air Force activities to Air Force, domestic, and international audiences. The capabilities they give the warfighter include: providing counsel and guidance about the public information environment; enhancing Airman morale and readiness; gaining and maintaining public support for military operations; and communicating US resolve in a manner that provides global influence and deterrence. As a weapon in the commander's arsenal of information operations (IO), public affairs operations use timely and accurate information to help deter war, drive a crisis back to peace, or wage war. (AFDD 2-5.3)	Public Affairs (PA) Operations
- Counterpropaganda	Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. (JP 1-02) [*Activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations and military forces situational understanding.]* (AFDD 2-5) {Words in brackets apply only to the Air Force and are offered for clarity.}	Counterpropaganda

* Related Joint terms should *not* be assumed to be identical to USAF terms, but are offered for reference. See the Definition column and compare with current Joint definition of related term.

* Related Joint terms should *not* be assumed to be identical to USAF terms, but are offered for reference. See the Definition column and compare with current Joint definition of related term.

Air Force Term	Air Force Definition	Related Joint Term*
Integrated Control Enablers (ICE)	Critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. Includes intelligence, surveillance, and reconnaissance, network operations, and positioning navigation and timing. Also called ICE. (AFDD 2-5)	
- Intelligence, Surveillance, and Reconnaissance (ISR)	Intelligence, surveillance, and reconnaissance are integrated capabilities to collect, process, exploit, and disseminate accurate and timely information that provides the battlespace awareness necessary to successfully plan and conduct operations. Also called ISR. (AFDD 2-9)	
- Network Operations (NetOps)	The integrated planning and employment of military capabilities to provide the friendly net environment needed to plan, control and execute military operations and conduct Service functions. NetOps provides operational planning and control. It involves time-critical, operational-level decisions that direct configuration changes and information routing. NetOps risk management and command and control decisions are based on a fused assessment of intelligence, ongoing operations, commander's intent, blue and gray situation, net health, and net security. NetOps provides the three operational elements of information assurance, network/system management, and information dissemination management. Also called NetOps. (AFDD 2-5)	Network Operations (NetOps)
- 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. Also called IA. (JP 3-13)	Information Assurance (IA)

Air Force Term	Air Force Definition	Related Joint Term*
- Network Management	The execution of the set of activities required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network, including performing actions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. (AFDD 2-5)	
- Information Dissemination Management	The subset of information management with a supporting infrastructure that addresses awareness, access, and delivery of information. The primary mission is to provide the right information to the right person, in the right format, at the right place and time in accordance with commanders' information dissemination policies while optimizing the use of information infrastructure resources. It involves the compilation, cataloging, caching, distribution, and retrieval of data; manages the information flow to users; and enables the execution of the commanders' information dissemination policy. (AFDD 2-5)	
- Predictive Battlespace Awareness (PBA)	Knowledge of the operational environment that allows the commander and staff to correctly anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions (AFDD 2-5; Air Force Pamphlet 14-118).	
- Positioning, Navigation, and Timing (PNT)	(not expanded here)	

* Related Joint terms should not be assumed to be identical to USAF terms, but are offered for reference. See the Definition column and compare with current Joint definition of related term.