BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 17-2

12 APRIL 2016

Cyberspace

CYBERSPACE OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AF/A3CO-A6CO

Certified by: SAF/CIO A6 (Lt Gen Bender)

Supersedes: AFPD 10-17, 31 July 2012; AFPD 33-1, 9 August 2012

Pages: 11

This Air Force (AF) Policy Directive (PD) (AFPD) consolidates cyberspace operations policy previously included in superseded AFPDs and implements: Presidential Policy Directive-20, *U.S. Cyber Operations Policy*; Department of Defense (DoD) Directive (DoDD) 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*; DoDD 3700.01, *DoD Command and Control (C2) Enabling Capabilities*; DoDD 3710.01, *National Leadership Command Capability (NLCC)*, DoDD 8000.01, *Management of the Department of Defense Information Enterprise*; DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid (GIG);* DoDD O-8530.1, *Computer Network Defense;* DoD Instruction (DoDI) O-3710.02, *Secretary of Defense Communications (SDC)*; DoDI 4630.09, *Communications Waveform Development and Standardization*; DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum;* DoDI 4650.02, *Military Auxiliary Radio System (MARS)*; DoDI 5000.02, Operation of the Defense Acquisition System, DoDI 8100.04, *DoD Unified Capabilities (UC)*; DoDI 8140.01, *Cyberspace Workforce Management*; DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense;* DoDI 8410.01, *Internet Domain Name Use and Approval;* DoDI 8410.02, *NetOps for the Global Information Grid (GIG)*; DoDI 8410.03, *Network Management*; DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies;* DoDI 8500.01, *Cybersecurity;* DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling;* DoDI 8520.03, *Identity Authentication for Information Systems;* DoDI 8523.01, *Communications Security (COMSEC);* DoDI O-8530.2, *Support to Computer Network Defense (CND)*; *and,* CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*.

SUMMARY OF CHANGES

This AFPD, published along with AFPD 17-1, supersedes AFPDs 10-17, 33-1, and portions of AFPD 33-5. It aligns and consolidates policies on cyberspace operations with current AF doctrine, statutory, and regulatory guidelines.

This AFPD provides policy guidelines for planning and conducting AF cyberspace operations to support the warfighter and achieve national security objectives. It applies to all information, information systems (ISs), and information technology (IT) infrastructure within Air Force purview, excluding non-Air Force space, Special Access Programs (SAP), and Intelligence Community ISs. Non-Air Force space systems are multi-Component space systems (e.g., those supporting more than one DoD Component) and are under the purview of United States Strategic Command. It applies to all military and civilian AF personnel, members of the AF Reserve, Air National Guard, and individuals or organizations authorized by an appropriate government official to conduct cyberspace operations or to access the AF Information Network (AFIN). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the AF Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the submitting organization's chain of command.

1. Overview. This Directive establishes AF policy for planning and executing operations to achieve Information Dominance in cyberspace.

2. Policy. It is AF policy that:

2.1. The AF will achieve Information Dominance by fully exploiting the man-made domain of cyberspace to execute, enhance and support Air Force core missions.

2.2. The AF will execute Cyberspace Operations to support joint warfighter requirements, increase effectiveness of its core missions, increase resiliency, survivability, and cybersecurity of its information and systems, and realize efficiencies through innovative IT solutions.

2.2.1. Successful execution of Cyberspace Operations requires integrated and synchronized execution of Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and DoD Information Networks (DoDIN) Operations (DoDIN Ops) as described in Joint Publication (JP) 3-12, *Cyberspace Operations*.

2.2.2. The AF will develop cyberspace weapon systems; capabilities; operational tactics, techniques, and procedures (TTPs); and maintenance procedures to execute AF and Joint cyberspace operations.

2.2.3. AF Cyberspace Operations will be conducted by Airmen trained and certified in accordance with applicable DoD, Joint, and Intelligence Community directives and authorities.

2.2.4. The AF will develop weapons systems, capabilities, and TTPs to "fight through" enemy offensive cyberspace operations to ensure continued mission assurance in hostile cyber environments.

2.3. AFIN Operations are actions taken to design, build, configure, secure, operate, maintain, and sustain AF IT, to include Platform IT (PIT), cyber enabled systems/weapons systems, and National Security Systems (NSS), in a way that creates and preserves data availability, integrity and confidentiality.

2.4. AFIN Operations will be planned and conducted to ensure enhanced information sharing, collaboration, and situational awareness within the Joint Information Environment.

2.5. Data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles for all authorized users.

2.6. The AF will centrally command, control, and manage the AFIN infrastructure and enterprise services.

3. Responsibilities.

3.1. Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2) will:

3.1.1. Oversee development of specialized ISR capabilities, resources, products, and services to support cyberspace operational requirements.

3.1.2. Ensure development of ISR TTPs to enable cyberspace operations.

3.1.3. Develop policy and provide guidance and oversight for Cyberspace ISR.

3.2. Deputy Chief of Staff, Operations (AF/A3) will:

3.2.1. Develop policy and provide guidance and oversight for OCO, DCO Response Actions, DCO Internal Defensive Measures, and C2 of cyberspace operations, integrating the activities of the AF's operations, ISR, and cyberspace communities to ensure the delivery of cyberspace operational capabilities to warfighters. Cyberspace operational capabilities include, but are not limited to, the deployment and employment of cyber weapon systems, non-kinetic operations, cyber-electronic warfare support, cyber ISR, combatant commander-directed/prioritized operational planning, cyber mission force (CMF) operations, and cyber operations conducted by other than CMFs (e.g., counterintelligence operations conducted by the AF Office of Special Investigations (AFOSI)).

3.2.2. Have primary responsibility for oversight of AF cyberspace operations, except for activities assigned or reserved to SAF/CIO A6 as the Chief Information Officer by law or in AFPD 17-1.

3.2.3. Develop plans and provide guidance to integrate cyberspace operational capabilities with air and space capabilities.

3.3. The AF Director of Test and Evaluation (AF/TE) will:

3.3.1. Develop and implement a comprehensive test strategy, that includes cyber testing, and institute policy consistent with AF and DoD policies.

3.3.2. Ensure AF test and evaluation (T&E) infrastructure utilizes latest cyber intelligence data to provide an operationally representative cyber environment for T&E.

3.4. The Chief of Information Dominance and Chief Information Officer (SAF/CIO A6) will provide policy and guidance to enable an operationally resilient, reliable, and secure cyberspace domain which meets AF operational requirements.

3.5. The General Counsel (SAF/GC) and The Judge Advocate General (AF/JA) will advise the AF on legal matters related to cyberspace operations.

3.6. The Inspector General (SAF/IG) will:

3.6.1. Validate functional inspection criteria to ensure that AF cyberspace capabilities are properly developed in response to documented requirements, and that cyberspace operations are being properly executed.

3.6.2. Through AFOSI, investigate allegations of criminal, fraudulent, and other illegal activities conducted in cyberspace, perform other criminal investigations to protect AF resources in accordance with applicable law, and conduct the full range of cyber counterintelligence activities to protect the AF core missions and enable or engage in cyberspace operations.

3.7. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) will:

3.7.1. Provide oversight and policy authority for cyberspace-related AF special access programs (SAPs) IAW AFPD 16-7, *Special Access Programs*, and AF Instruction (AFI) 16-701, *Management, Administration, and Oversight of Special Access Programs*.

3.7.2. Appoint authorizing officials for AF SAP information systems, platforms, networks, and technologies.

3.8. Air Force Space Command will:

3.8.1. Serve as the core function lead (CFL) for cyberspace superiority.

3.8.2. Issue cyberspace orders on behalf of the Secretary of the Air Force for the overall C2, security and defense of the AFIN; and the C2, implementation, security, operation, maintenance, sustainment, configuration, and defense of the Air Force Network and Air Force Network-Secure (AFNET/AFNET-S).

3.8.3. Manage funds for the AF CMF enterprise.

3.8.4. Present integrated CMF teams to USCYBERCOM through AFCYBER.

3.8.5. Deploy AF-approved cyber weapon systems.

3.9. Air Force Materiel Command will conduct technological research and materiel development activities to acquire, perform developmental testing of, field and sustain current and future cyberspace capabilities.

3.10. Air Education and Training Command will, in coordination with the SAF/CIO A6 Functional Authorities Career Field Managers, develop and implement programs to educate all Airmen on cyberspace operations, the employment of related capabilities, and the integration of those capabilities with capabilities of all other domains.

3.11. The Air Force Operational Test and Evaluation Center (AFOTEC) or MAJCOM Operational Test Units will:

3.11.1. Perform operational test and evaluation (OT&E) in support of cyberspace capabilities development activities.

3.11.2. Execute cyber test policy and guidance as directed by DoD and AF/TE.

3.12. Headquarters AF Functionals, Major Commands, Direct Reporting Units, and Field Operating Agencies will:

3.12.1. Follow AF policy and cyberspace orders when executing cyberspace operations.

3.12.2. Include required cyber testing resources, plans, and measures in all T&E Master Plans to ensure adequate testing of cyber suitability, interoperability, supportability, resiliency, and survivability.

DEBORAH L. JAMES
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Presidential Policy Directive 20, *U.S. Cyber Operations Policy,* undated

NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003

DoDD 3700.01, *DoD Command and Control (C2) Enabling Capabilities,* October 22, 2014

DoDD 3710.01, *National Leadership Command Capability (NLCC)*, May 27, 2015

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, April 14, 2004, certified current as of April 23, 2007

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

DoDI 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*, January 8, 2015

DoDI O-3710.02, *Secretary of Defense Communications (SDC),* October 20, 2014

DoDI 4630.09, *Communications Waveform Development and Standardization*, July 15, 2015

DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, January 9, 2009

DoDI 4650.02, *Military Auxiliary Radio System (MARS)*, December 23, 2009

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

DoDI 8100.04, *DoD Unified Capabilities (UC)*, December 9, 2010

DoDI 8140.01, *Cyberspace Workforce Management*, August 11, 2015

DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*, August 5, 2013

DoDI 8410.01, *Internet Domain Name Use and Approval*, April 14, 2008

DoDI 8410.02, *NetOps for the Global Information Grid,* December 19, 2008

DoDI 8410.03, *Network Management,* August 29, 2012

DoDI 8500.01, *Cybersecurity*, March 14, 2014

DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, May 24. 2011

DoDI 8520.03, *Identity Authentication for Information Systems*, May 13, 2011

DoDI 8523.01, *Communications Security (COMSEC)*, April 22, 2008

DoDI O-8530.2, *Support to Computer Network Defense,* March 9, 2001

CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*, June 13, 2005, current as of 18 June 2008.

Joint Publication (JP) 1-02*, Department of Defense Dictionary of Military and Associated Terms,* November 8, 2010, as amended through September 15, 2015

JP 3-12*, Cyberspace Operations,* February 5, 2013

JP 6-0, *Joint Communications System*, June 10, 2015

AFPD 16-7, *Special Access Programs*, February 19, 2014

AFI 16-701, *Management, Administration, and Oversight of Special Access Programs*, February 18, 2014

AFMAN 33-363*, Management of Records,* March 1, 2008

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF —Air Force

AFI —Air Force Instruction

AFIN —Air Force Information Network

AFMAN – Air Force Manual

AFNET – Air Force Network

AFNET-S – Air Force Network**-**Secure

AFOSI —AF Office of Special Investigations

AFPD —Air Force Policy Directive

AFRIMS —Air Force Records Information Management System

C2 —Command and Control

CFL —Core Function Lead

CIO —Chief Information Officer

CMF —Cyber Mission Force

CND —Computer Network Defense

COMSEC —Communications Security

DCO —Defensive Cyberspace Operations

DoD – Department of Defense

DoDD – Department of Defense Directive

DoDI —Department of Defense Instruction

DoDIN —Department of Defense Information Networks

E3 —Electromagnetic Environmental Effects

GIG —Global Information Grid

ISR —Intelligence, Surveillance, and Reconnaissance

IT —Information Technology

JP —Joint Publication

MARS —Military Affiliate Radio System

NLCC —National Leadership Command Capability

NSS —National Security System

OCO —Offensive Cyberspace Operations

OPR —Office of Primary Responsibility

PD —Policy Directive

PIT— Platform Information Technology

PK —Public Key

PKI —Public Key Infrastructure

RDS —Records Disposition Schedule

SAF —Secretary of the Air Force

SAP —Special Access Program

SCF —Service Core Function

SDC —Secretary of Defense Communications

T&E —Test and Evaluation

TTP —Tactics, Techniques, and Procedures

UC —Unified Capabilities

WLAN —Wireless Local Area Network

Terms

AF Information Network (AFIN) — The globally interconnected, end-to-end set of AF information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to AF warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems." (Derived from the JP 3-12 definition of DoDIN).

AFIN Infrastructure—The AF cyberspace infrastructure consisting of AF-owned/leased and controlled components (hardware, software, networks, systems, equipment, facilities, and

services) operated by DoD, AF, contractor or other entity on behalf of the AF, which stores, transmits, receives, or processes information, regardless of classification or sensitivity.

AFIN Operations—AF actions taken to design, build, configure, secure, operate, maintain, and sustain AF IT, to include Platform IT (PIT), cyber enabled systems/weapons systems, and National Security Systems (NSS), in a way that creates and preserves data availability, integrity and confidentiality. (Derived from definition of DoDIN Operations).

AF Network (AFNET) —The AF's underlying Nonsecure Internet Protocol Router Network that enables AF operational capabilities and lines of business, consisting of physical medium and data transport services. (Air Force definition).

AF Network-Secure (AFNET-S) — The AF's underlying Secure Internet Protocol Router Network (SIPRNet) that enables AF operational capabilities and lines of business, consisting of physical medium and data transport services. (Air Force definition).

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

Core Function Lead—SecAF/CSAF-appointed senior leader responsible for specific Core Functions (CF) providing AF-level, long-term views. CFLs integrate Total Force concepts, capabilities, modernization, and resourcing to ensure future assigned core capabilities across the range of military operations as directed by AF Strategy and Strategic Planning Guidance. CFLs are responsible for the Core Function Support Plan and recommendations for the development of the POM for the assigned CF. CFLs have tasking authority regarding CF issues to identify enabling capabilities and integration requirements/opportunities. (AFPD 90-11).

Cyber (adj.) — of or pertaining to the cyberspace environment, capabilities, plans, or operations. (Air Force definition).

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoDI 8500.01).

Cyberspace (n. or adj.) — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12) NOTE: synonymous with *cyber* when used as an adjective.

Cyberspace Operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives or effects in or through cyberspace (JP 3-0). Cyberspace Operations are categorized as Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and DoD Information Networks (DoDIN) Operations (DoDIN Ops). (Described in JP 3-12).

Cyberspace Superiority — The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12).

Defensive Cyberspace Operations (DCO) — Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and net-centric capabilities, and other designated systems. (JP 3-12).

Defensive Cyberspace Operations —Internal Defensive Measures (DCO-IDM) – Those DCO that are conducted within the DoDIN. They include actively hunting for advanced internal threats as well as the internal responses to those threats. (JP 3-12).

Defensive Cyberspace Operations Response Actions (DCO-RA) — Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DoD cyberspace capabilities or other designated systems. Also called DCO-RA.

Department of Defense Information Networks (DoDIN) — The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 3-12).

Department of Defense Information Network (DoDIN) Operations—. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12).

Information Dominance. —The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects. (AF Information Dominance Vision).

Information Technology (IT)—Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is required by a Federal contractor incidental to a Federal contract. Note: The above term is considered synonymous with the term “information system” as defined and used in AF programs. The term “IT” does not include National Security Systems (NSS) according to 44 USC 3502.

National Security System (NSS)—Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria

established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Adapted from NIST SP 800-59 & 44 USC 3542).

Offensive Cyberspace Operations (OCO) — Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 3-12).

Service Core Functions—Functional areas that delineate the appropriate and assigned core duties, missions, and tasks of the USAF as an organization, responsibility for each of which is assigned to a CFL. SCFs express the ways in which the USAF is particularly and appropriately suited to contribute to national security, although they do not necessarily express every aspect of what the USAF contributes to the nation. (AFPD 90-11).

Platform Information Technology (PIT) — a special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services). Examples include, but are not limited to: SCADA type systems, training simulators, diagnostic test and maintenance equipment. (AFI 33-210).

Unified Capabilities (UC)—The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. (DoDI 8100.04).

Weapon System—A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (JP 3-0).