BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 10-17

31 JULY 2012

Operations

CYBERSPACE OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A3C-A6C

Certified by: AF/A3/5
(Lt Gen Burton M. Field)

Pages: 9

Supersedes: AFPD 13-3, 11 Jan 08

This policy directive implements DoDD O-8530.1, *Computer Network Defense (CND)*, and National Security Presidential Directive 38 (title classified at higher level), and provides direction for planning and conducting Air Force cyberspace operations to support the warfighter and achieve national security objectives. This policy directive applies to all military and civilian Air Force personnel, members of the Air Force Reserve, Air National Guard, and individuals or activities, authorized by an appropriate government official to conduct cyberspace operations or to access the Air Force-provisioned portion of the Global Information Grid (GIG) (AF-GIG). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the *Air Force Records Disposition Schedule (RDS)* located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the office of primary responsibility using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the submitting organization's chain of command. Waivers to this directive may be granted only by the United States Air Force Deputy Chief of Staff, Operations, Plans and Requirements (AF/A3/5).

1. Overview. This Directive establishes Air Force policy and assigns responsibilities for the planning and execution of cyberspace operations.

2. Policy. It is Air Force policy that:

2.1. Cyberspace is an operational domain.

2.2. The Air Force will conduct operations in, through and from cyberspace across the range of military operations.

2.3. The Air Force will conduct cyberspace operations in support of combatant commanders in the areas of offensive cyberspace operations, defensive cyberspace operations, and cyberspace support.

2.4. Cyberspace operations will be conducted by personnel trained and certified in accordance with applicable Air Force and intelligence community directives and authorities.

2.5. Decisions affecting the availability of any portion of the AF-GIG will be made by the responsible operational commander, with the advice and support of the responsible communications organization commander.

2.6. Providing policy, guidance, and oversight for cyberspace operations is a shared responsibility of the Office of Information Dominance and Chief Information Officer (SAF/CIO A6) and the AF/A3/5, in coordination with Commander, Air Force Space Command (AFSPC/CC) as the core function lead integrator (CFLI) for cyberspace operations. SAF/CIO A6 retains responsibility, with the support of AF/A3/5, for those activities and reporting requirements assigned to the CIO by public law.

3. Responsibilities.

3.1. AF/A3/5 and SAF/CIO A6, through a matrixed organization, will:

3.1.1. Provide Headquarters Air Force (HAF)-level policy, guidance, and oversight for cyberspace operations, integrating the activities of the Air Force's operations; intelligence, surveillance, and reconnaissance (ISR); and communications communities to ensure the delivery of Air Force cyberspace operational capabilities to warfighters.

3.1.2. Develop, coordinate, publish, implement, and enforce Air Force-wide guidance for cyberspace command and control (C2) and cyberspace operations.

3.1.3. Validate requirements for cyberspace operational capabilities through the Air Force Requirements Oversight Council.

3.1.4. Ensure development, coordination, publishing, implementation, and enforcement of procedures for conducting operations under conditions of diminished or denied network availability.

3.1.5. With the Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2), develop cyberspace processes and ensure that the force is trained and equipped to plan and assess cyberspace operations.

3.1.6. Ensure ISR capability requirements are identified to AF/A2 for incorporation into future cryptologic capability development.

3.1.7. Advise and assist in the development of organizational constructs that integrate cyberspace operational capabilities into Air Force and joint warfighting components.

3.1.8. Ensure operational assessment of current and future cyberspace operations and information superiority capabilities are integrated in the Air Force capability based planning process.

3.1.9. Advise and assist in the development, coordination, and integration of strategy, doctrine, and guidance for cyberspace operations capabilities into Air Force, Joint, combatant command, coalition, and national planning and operations.

3.1.10. Define Air Force guidance and standards for position descriptions, training and certification of personnel responsible for development, management, and repair of the AF-GIG.

3.1.11. Develop, coordinate, publish, implement, and enforce guidelines and procedures for network/system certification, accreditation, assessment, and authorization.

3.1.12. Serve as the functional authority for the 17D, 1B, and 3D Air Force specialty codes and related civilian career fields.

3.1.13. Develop certification criteria and identifiers for cyberspace expertise or experience and track personnel so identified.

3.1.14. Advocate for cyberspace operations funding and program support within the Air Force corporate structure.

3.2. AF/A2 will:

3.2.1. Ensure ability to provide collaborative analysis, fused intelligence, and cross-domain, integrated, and automated ISR PCPAD (planning and collecting, collection, processing and exploitation, analysis and production, dissemination) capabilities to enable cyberspace operations.

3.2.2. Provide cyber ISR expertise to influence national, Department of Defense (DoD), Joint, and Service policy and doctrine development for cyberspace operations.

3.2.3. Organize, train, and equip ISR forces for Air Force computer network exploitation (CNE) operations in the cyberspace domain.

3.2.4. Provide planning, programming, and budgeting oversight for ISR capabilities supporting cyberspace operations.

3.2.5. Ensure that operational commanders are provided with the information needed to plan and assess cyberspace operations.

3.2.6. Ensure provision of ISR CNE capabilities to enable multi-domain operations.

3.2.7. Ensure that ISR forces, assigned to Service Reserve Code 0U, are available to provide direct support to network warfare squadrons for execution of United States Cyber Command (USCYBERCOM) tasked/approved operations.

3.2.8. Oversee development of specialized ISR capabilities, resources, products, and services in direct support of stated cyberspace operational requirements.

3.2.9. Oversee, in partnership with Air Force ISR Agency (AFISRA), the collaboration of the Air Force Service Cryptologic Component (SCC) with the National Security Agency to conduct CNE and facilitate cryptologic signals intelligence (SIGINT) support for cyberspace operations, and cryptologic training.

3.2.10. Manage ISR capabilities and requirements and advocate them through the Air Force capabilities based planning process. Coordinate with 24th AF (AFCYBER) to

prioritize intelligence needs and employ forces, within resource and authority constraints, to satisfy those intelligence needs.

3.2.10.1. As the Air Force SCC, AFISRA is the service lead for all Air Force cryptologic activities and has management oversight of those elements of the Air Force performing cryptologic functions regardless of program to ensure these activities are compliant with national and departmental guidelines, including SIGINT security, training, authorities, accountability of resources, and oversight (inspections, skill evaluations, and reporting).

3.2.11. Manage ISR capabilities and requirements and advocate them through the Air Force capabilities based planning process. Coordinate with AFCYBER to prioritize intelligence needs and employ forces, within resource and authority constraints, to satisfy those intelligence needs.

3.2.12. Advocate and defend Air Force cyber ISR requirements to national level agencies. Review AFISRA, AFCYBER, USCYBERCOM, Defense Intelligence Agency (DIA), and national cyber requirements processes (i.e., validation, tasking, and satisfaction) for adequacy.

3.3. The Assistant Secretary of the Air Force for Acquisition (SAF/AQ) will develop and acquire cyberspace operational capabilities in response to validated requirements.

3.3.1. The Program Executive Office, Command, Control, Communications, Intelligence, and Networks (PEO C3I&N) will develop, acquire, and sustain cyberspace, communications, cryptologic and space/nuclear network capabilities across Air Force, Joint, and interagency communities. Additionally, the PEO C3I&N will develop and maintain an implementation baseline for the tactical and AFNET (Air Force network) communications and commoditized infrastructure supporting multiple capability areas to include cyberspace.

3.4. The General Counsel (SAF/GC) and The Judge Advocate General (AF/JA) will:

3.4.1. Advise the Air Force on legal matters related to cyberspace operations.

3.4.2. Provide advice and legal analysis to ensure operations and activities carried out in and through cyberspace are conducted in accordance with U.S., international, and other applicable law.

3.4.3. Conduct legal reviews of cyberspace operational capabilities. Those capabilities protected under special access programs (SAP) will be reviewed by SAF/GC; those not so protected will be reviewed by AF/JA.

3.4.4. Conduct legal reviews of rules of engagement for cyberspace capabilities.

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

3.5.1. Validate functional inspection criteria to ensure that Air Force cyberspace operational capabilities are properly developed in response to documented requirements, and that cyberspace operations are being properly executed.

3.5.2. Through the Air Force Office of Special Investigations, investigate allegations of criminal, fraudulent, and other illegal activities conducted over the AF-GIG, and perform

other criminal investigations and counterintelligence activities in accordance with applicable law, as needed, to protect the AF-GIG.

3.5.3. Assist the Secretary of the Air Force in his/her role as the Executive Agent for the DoD Cyber Crime Center, pursuant to DoDD 5505.13E, *DoD Executive Agent for the DoD Cyber Crime Center (DC3)*.

3.6. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) will serve as the senior security official for the Air Force with oversight and policy authority for all cyber-related Air Force SAPs.

3.7. Air Force Space Command (AFSPC) will:

3.7.1. Serve as the lead major command for Air Force cyberspace operations and the CFLI for the cyberspace superiority mission area. Develop departmental guidance and procedures for HAF release in departmental publications in accordance with AFI 33-360, *Publications and Forms Management*.

3.7.2. Organize, train, and equip Air Force cyberspace operations forces.

3.7.3. Present organized, trained and equipped cyberspace forces to combatant commanders as directed.

3.7.4. As directed by the Air Force Roadmap for the Development of Cyberspace Professionals (Change 1), and until updated guidance is published:

3.7.4.1. Serve as the cyberspace professional functional authority responsible to develop combat capability in the cyberspace warfighting domain.

3.7.4.2. Articulate cyberspace professional requirements to functional authorities.

3.7.4.3. Provide strategic level guidance to the functional communities that provide Air Force cyberspace capabilities.

3.7.5. Command, control, implement, configure, secure, operate, maintain, sustain, and defend the AF-GIG.

3.7.6. Command, control, and employ Air Force cyberspace operational capabilities.

3.7.7. Develop and implement measures of effectiveness and performance for cyber operations.

3.7.8. In coordination with Air Education and Training Command (AETC), develop and implement programs to educate Airmen on cyberspace operations, the employment of related capabilities, and the integration of those capabilities with capabilities of all other domains.

3.7.9. Recommend organizational constructs which facilitate the integration of cyberspace operational capabilities into Air Force and Joint warfighting components.

3.7.10. Define requirements for cyberspace operational capabilities.

3.7.11. Conduct operational tests of cyberspace systems in accordance with AFI 99-103, *Capabilities-Based Test and Evaluation*.

3.7.12. Develop, coordinate, publish, implement, and enforce network configuration management guidelines and standards.

3.7.13. Develop tactics, techniques, and procedures for the integration and employment of cyberspace operational capabilities.

3.7.14. Coordinate, delineate, and de-conflict cyberspace operations and ISR capabilities between the cyberspace superiority and global integrated ISR core function master plans (CFMP).

3.8. Air Force Materiel Command (AFMC) will:

3.8.1. Conduct technological research and materiel development activities to acquire, perform developmental testing of, field, and sustain current and future cyberspace capabilities.

3.8.2. Provide cyberspace environments for training and exercise of cyber units.

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

3.9.1. Provide initial skills training for cyberspace professionals.

3.9.2. In coordination with AFSPC, develop and implement programs to educate Airmen on cyberspace operations, the employment of related capabilities, and the integration of those capabilities with capabilities of all other domains.

Michael B. Donley
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 5505.13E, *DoD Executive Agent for the DoD Cyber Crime Center (DC3)*, 1 Mar 2010

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

DoDI 8410.02, *NETOPS for the Global Information Grid*, 19 Dec 2008

DoDI O-8530.2, *Support to Computer Network Defense*, 3 Mar 2001

Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 Nov 10, as amended through 31 Jan 11

AFDD 3-12, *Cyberspace Operations*, 15 Jul 10, with Change 1, 30 Nov 11

AFI 33-360, *Publications and Forms Management*, 11 Jun 09

AFI 51-402, *Legal Reviews of Weapons and Cyber Capabilities*, 27 Jul 11

AFI 99-103, *Capabilities-Based Test and Evaluation*, 26 Feb 08

AFMAN 33-363, *Management of Records*, 1 Mar 08

AFPD 16-7, *Special Access Programs*, 29 Dec 10

AFPD 33-1, *Cyberspace Infrastructure and Support*, in coordination.

AFPD 33-2, *Information Assurance (IA) Program*, 3 Aug 11

Air Force Roadmap for the Development of Cyberspace Professionals (Change 1), 13 Aug 10

National Security Presidential Directive 38, Title Classified at higher level, 7 July 2004

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 Sep 09.

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFCYBER—24th Air Force, as the Air Force component to USCYBERCOM

AF—GIG – The Air Force provisioned portion of the Global Information Grid

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AFSPC—Air Force Space Command

C2—Command and Control

CCDR—Combatant Commander

CFLI—Core Function Lead Integrator

CFMP—Core Function Master Plan

CIO—Chief Information Officer

CND—Computer Network Defense

CNE—Computer Network Exploitation

CONOPS—Concept of Operations

DC3—DoD Cyber Crime Center

DCO—Defensive Cyberspace Operations

DIA—Defense Intelligence Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

GIG—Global Information Grid

HAF—Headquarters Air Force, includes the Secretariat and the Air Staff

IA—Information Assurance

ISR—Intelligence, Surveillance, and Reconnaissance

OPR—Office of Primary Responsibility

PCPAD—Planning & Collecting, Collection, Processing & Exploitation, Analysis & Production, Dissemination

PEO C3I&N—Program Executive Office, Command, Control, Communications, Intelligence, and Networks

PKI—Public Key Infrastructure

RDS—Records Disposition Schedule

SCC—Service Cryptologic Component

SIGINT—Signals Intelligence

USCYBERCOM—United States Cyber Command

VCJCS—Vice Chairman of the Joint Chiefs of Staff

Terms

Air Force Global Information Grid (AF—GIG) - The Air Force-provisioned portion of the Global Information Grid (GIG) for which the Air Force has primary responsibility for the procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those services that enable Air Force commanders to achieve information and decision superiority in support of Air Force mission objectives. The AF-GIG consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information. (AFPD 13-3)

Computer Network Exploitation (CNE)— Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Joint Pub 3-13)

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

Cyber Capability— Any device or software payload intended to disrupt, deny, degrade, negate, impair, or destroy adversarial computer systems, data, activities, or capabilities. Cyber capabilities do not include a device or software that is solely intended to provide access to an adversarial computer system for data exploitation. (AFI 51-402)

Cyberspace (n. or adj.)— A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Joint Pub 1-02) NOTE: synonymous with *cyber* when used as an adjective.

Cyberspace Operations— The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (Joint Pub 3-0)

Cyberspace Superiority— The operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference. (AFDD 3-12)

Cyberspace Support— Foundational, continuous, or responsive operations in order to ensure information integrity and availability in, through, or from Air Force controlled infrastructure and its interconnected analog and digital portion of the battle space. (AFDD 3-12)

Defensive Cyberspace Operations (DCO)— DCO direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; outmaneuver adversaries taking or about to take offensive actions; and otherwise protect critical missions that enable our freedom of action in cyberspace. (USCYBERCOM Concept of Operations, v 1.0, 21 Sep 2010)

Global Information Grid (GIG)— The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. (Joint Pub 6-0)

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. (AFPD 33-2, Joint Pub 3-13)

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. (Joint Pub 3-13)

Offensive Cyberspace Operations (OCO)— The creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commanders' objectives and actively defend DoD or other information networks, as directed. (USCYBERCOM Concept of Operations, v 1.0, 21 Sep 2010)