BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE POLICY DIRECTIVE 17-2

27 OCTOBER 2020

Cyberspace

CYBER WARFARE 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/A2/6CX / A3C

Certified by: AF/A2/6
(Lt Gen Mary F. O'Brien)

Supersedes: AFPD 17-2, 12 April 2016

Pages: 11

This publication implements Department of Defense Instruction (DoDI) 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*; DoDI O-3710.02, *Secretary of Defense Communications (SDC)*; DoDI 3780.01, *Senior Leader Communications Modernization*; DoDI 4630.09, *Communication Waveform Management 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 4650.10, *Land Mobile Radio (LMR) Interoperability and Standardization*; DoDI 8320.05, *Electromagnetic Spectrum Data Sharing*; and DoDI 8420.02, *DoD Satellite Communications (SATCOM)*. It establishes Cyber Warfare Operations policy to support the warfighter and achieve national security objectives. This publication applies to all Department of the Air Force organizations, employees, including civilian and contractor personnel. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program* and are disposed in accordance with the Air Force Records Disposition Schedule which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility using the Air Force Form 847, *Recommendation for Change of Publication;* route Air Force Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include organizational changes and the division of former Information Dominance and Chief

Information Officer (SAF/CIO A6) responsibilities between the Deputy Chief Information Officer (SAF/CN) and the Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6). It also recognizes the redesignation of Air Force Space Command as the United States Space Force. This publication defines the term "Cyber Warfare Operations" and is not intended to expand the role of Air Force cyberspace activities beyond the current scope authorized by Department of Defense, Chairman Joint Chief of Staff, and Combatant Command operational authorities. It formalizes the shift of Lead Command responsibilities for the Cyber Warfare Operations mission area from Air Force Space Command to Air Combat Command, assignment of Lead Service responsibilities for enterprise satellite communications to the United States Space Force, and defines those responsibilities.

1. OVERVIEW.

1.1. This Directive establishes Air Force policy for planning and executing operations to create offensive and defensive effects in cyberspace and for providing communications capability to warfighting forces under proper Department of Defense authorities. Cyberspace is critical to all Department of the Air Force operations and cyber warfare operations are key to enabling successful multi-domain operations while supporting Combatant Command objectives. Synchronization and unity of effort are critical in the cyberspace domain, which is trans-regional and enables instantaneous global effects.

1.2. In addition, cyber warfare operations includes operations to extend or modify the Air Force's portion of the Department of Defense Information Network for the purpose of providing communications capability to warfighting forces. **Note:** Such operations do not include, or refer to, cyberspace activities, investigations, operations or the conduct of cyber effects operations and activities conducted by the Air Force Office of Special Investigations for law enforcement or counterintelligence purposes.

2. POLICY. The Department of the Air Force will:

2.1. Contribute to the joint force's attainment of cyberspace superiority by fully exploiting cyberspace to execute, enhance and support Department of the Air Force core missions directly supporting joint objectives.

2.2. Provide global, assured, resilient satellite, airborne, and terrestrial communications networks for warfighters in support of Department of the Air Force core missions.

2.3. Execute cyber warfare operations to support joint warfighter requirements, increase effectiveness of its core missions, and increase resiliency and survivability of its information, systems, and missions.

2.3.1. The Department of the Air Force will develop cyberspace weapons and weapon systems; cyberspace capabilities; operational tactics, techniques, and procedures; and maintenance procedures to fully support assigned and authorized roles and missions.

2.3.2. Cyber warfare operations will be conducted by Airmen trained and certified in accordance with applicable Department of Defense, Joint, and Intelligence Community directives and authorities.

2.4. Establish Air Combat Command as the lead command for the cyber warfare operations mission area via this directive, with Department of the Air Force responsibilities for organizing, training, and equipping forces to conduct cyber warfare operations. United

States Space Force and United States Air Force will realign roles and responsibilities for Service-Retained forces (such as Mission Defense Teams) which have not been designated as a cyber operational force. Forces that enable tactical command and control or weapons systems and critical infrastructure will be designated at a later date.

2.5. Establish the United States Space Force as the lead service for Department of the Air Force enterprise satellite communications operations via this directive, with service-wide responsibilities for organizing, training, and equipping forces to conduct those operations. United States Space Force, in concert with Department of the Air Force commands, will maintain clear, detailed, and measurable standards in this mission area to ensure efficient employment and interoperability of forces.

2.6. Integrate cyber warfare operations with the separate and distinct activities of electromagnetic warfare; information operations; and intelligence, surveillance, and reconnaissance, as well as other relevant operational activities, to produce information warfare capabilities to support combatant command objectives.

3. ROLES AND RESPONSIBILITIES.

3.1. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6)** will:

3.1.1. In coordination with the Deputy Chief of Staff, Operations (AF/A3), develop cyber warfare operations doctrine, requirements, strategy, policy, guidance, standards, and concepts, and integrate them where appropriate with the separate and distinct Air Force Intelligence, Surveillance, and Reconnaissance enterprise.

3.1.2. In coordination with the Deputy Chief Information Officer (SAF/CN), develop doctrine, requirements, strategy, policy, guidance, standards, and concepts to support global, assured, resilient satellite, airborne, and terrestrial communications networks for warfighters in support of Air Force core missions.

3.1.3. Provide functional oversight, force development, and talent management for cyber-focused Department of the Air Force career fields.

3.1.3.1. When United States Space Force has been authorized, it will provide functional oversight, force development, and talent management for cyber-focused United States Space Force assigned career fields.

3.1.4. Oversee development and cybersecurity of Intelligence, Surveillance, and Reconnaissance capabilities, resources, products, and services to support cyberspace operational requirements.

3.1.5. Ensure development of Cyberspace Intelligence, Surveillance, and Reconnaissance tactics, techniques, and procedures; guidance; and policies.

3.1.6. Retain responsibility for policy, as well as oversight of lead command implementation of DoDI 3222.03; DoDI O-3710.02; DoDI 3780.01; DoDI 4630.09; DoDI 4650.01; DoDI 4650.02; DoDI 4650.10; DoDI 8320.05; and DoDI 8420.02.

3.1.7. In accordance with Department of Defense Directive S-3710.01, *National Leadership Command Capability (NLCC) (U)*, coordinate with and support the Deputy Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10) and other

Department of Defense agencies to provide guidance and policy for cyber warfare operations on behalf of the Nuclear Enterprise. This includes the nuclear command, control and communications mission area, as well as nuclear delivery platforms and systems.

3.1.8. Provide oversight of Department of Air Force senior leader communications modernization efforts as executed through and by the major commands in accordance with DoDI 3780.01.

3.1.9. Ensure Department of Air Force compliance with Department of Defense waveform management policy and processes in accordance with DoDI 4630.09.

3.1.10. Provide policy, guidance, resource advocacy and oversight for the management of Air Force electromagnetic spectrum in accordance with DoDI 4650.01 and DoDI 8320.05.

3.1.11. Oversee the Military Auxiliary Radio System in accordance with DoDI 4650.02.

3.1.12. Ensure Air Force compliance with Department of Defense land mobile radio interoperability and standardization policy and processes in accordance with DoDI 4650.10.

3.1.13. Coordinate with United States Space Force and AF/A3 to ensure Air Force compliance with Department of Defense satellite communications policy and processes in accordance with DoDI 8420.02.

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

3.2.1. In coordination with the AF/A2/6, provide guidance and oversight for the command and control and conduct of cyber warfare operations, develop plans, and provide guidance to integrate cyberspace operational capabilities with air and space capabilities.

3.2.2. Have primary responsibility for oversight of Air Force day to day operations, including cyberspace operations. This responsibility in no way should be read to infringe upon operations and activities assigned or reserved to a Functional or Combatant Command, to the Air Force Deputy Chief Information Officer by law or in Air Force Policy Directive 17-1, *Information Dominance Governance and Management;* to the Air Force Chief Data Officer by law or in Air Force policy; or to the Commander, Air Force Office of Special Investigations (AFOSI/CC) by law, regulation, or in Air Force policy.

3.2.3. Coordinate allocation of Air Force cyber forces and cyber warfare operations capabilities as requested via the Global Force Management process.

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

3.3.1. Develop test policy and provide guidance and oversight to ensure comprehensive cyber test of Department of the Air Force assets, consistent with Department of the Air Force and Department of Defense policies.

3.3.2. Ensure Department of the Air Force test and evaluation infrastructure utilizes latest cyber-related intelligence data to provide an operationally representative cyber environment for test and evaluation.

3.4. **The Deputy Chief Information Officer (SAF/CN)** will provide policy and guidance to foster an operationally resilient, reliable, and secure Department of the Air Force Information Network which meets Department of Defense and Department of the Air Force requirements.

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

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

3.6.1. Validate functional inspection criteria in coordination with respective Combatant Command Inspector General to ensure that Department of the Air Force cyberspace capabilities are properly developed in response to documented requirements, and cyberspace operations are being executed appropriately.

3.6.2. Through the AFOSI/CC, investigate allegations of criminal, fraudulent, espionage, and other illegal activities conducted in cyberspace. Conduct the full range of counterintelligence cyber activities to protect the Department of the Air Force's core missions and when properly authorized, support cyber warfare operations.

3.6.2.1. Law enforcement and counterintelligence cyber activities, investigations, operations, and capabilities developed by Air Force Office of Special Investigations to conduct missions pursuant to the Air Force Mission Directive 39, *Air Force Office of Special Investigations (AFOSI)*, are approved by the AFOSI/CC according to the delegated independent authority of the AFOSI/CC in the Air Force Policy Directive 71-1, *Criminal Investigations and Counterintelligence*.

3.6.2.2. Counterintelligence in cyberspace activities, operations, and capabilities developed by Air Force Office of Special Investigations to conduct missions pursuant to Air Force Mission Directive 39, *Air Force Office of Special Investigations (AFOSI)*, are approved by the AFOSI/CC according to the delegated independent authority of the AFOSI/CC in Air Force Policy Directive 71-1, *Criminal Investigations and Counterintelligence.*

3.6.2.3. These cyber capabilities are not used in military operations, but under law enforcement or counterintelligence authorities; as such, Air Force Office of Special Investigations may execute cyber warfare operations for counterintelligence purposes.

3.6.3. Oversee execution of Executive Agent responsibilities regarding the Department of Defense Cyber Crime Center digital and multimedia forensics, threat analysis, and cyber training functions in support of criminal investigations and counterintelligence, as delegated in Headquarters Air Force Mission Directive 1-20, *The Inspector General,* to support Air Force cyber warfare operations.

3.7. **Commander, Air Combat Command (ACC/CC)** will:

3.7.1. Serve as the Lead Command for the cyber warfare operations mission area.

3.7.1.1. Be responsible for publishing any implementing Departmental-level guidance required by DoDI 3222.03; DoDI O-3710.02; DoDI 3780.01*;* DoDI 4630.09; DoDI 4650.01; DoDI 4650.02; DoDI 4650.10, and DoDI 8320.05.

3.7.1.2. In coordination with other commands, develop tactics, techniques, and procedures and mission essential task lists necessary to effect cyber warfare operations integration, to include complementary and interoperable command relationships and command and control procedures.

3.7.1.3. Oversee deployment and management of Department of the Air Force-approved cyberspace weapon systems and cyberspace capabilities, other than those employed for law enforcement or counterintelligence purposes. In concert with other commands, maintain clear, detailed, and measurable standards in the cyber warfare operations mission area to ensure efficient employment and interoperability of forces.

3.7.1.4. Manage and oversee the sustainment, modernization and future force development of cyber warfare operations capabilities and weapon systems, and ensure their inclusion in appropriate processes, such as: strategic planning, programming, budgeting and execution cycles; Air Force corporate governance; joint capabilities integrations and developments; and defense acquisition systems.

3.7.1.5. Manage the process to identify future cyberspace requirements and modernization needs, and incorporate them into the Air Force and joint modernization planning processes to include the Joint Capabilities Integration and Development System.

3.7.1.6. Establish, in coordination with the other commands, the command and control process for cyber warfare operations, to include the interfaces with United States Cyber Command, the theater-level air operations centers, and air expeditionary task forces.

3.7.1.7. Formulate and manage cyber warfare operations baseline inspection and evaluation standards, regardless of command.

3.7.1.8. Develop and publish, with the full participation and coordination of other supported commands and in coordination with mandatory and appropriate offices at Headquarters Air Force, related publications supporting this directive. Specific guidance for lead command guidance may be found in Department of Air Force Instruction 33-360, *Publications and Forms Management*.

3.7.1.9. Issue cyberspace orders on behalf of the Secretary of the Air Force for the command and control, implementation, operation, maintenance, sustainment, configuration, and defense of the Air Force Information Network. **Note:** For clarification of the distinction between cybersecurity and cyberspace defense, see **Attachment 1**.

3.7.1.10. In coordination with the Chief Information Security Officer, issue direction for the security of the Department of the Air Force Information Network.

3.7.1.11. Manage the Department of the Air Force Cyber Mission Force enterprise, to include funds and force presentation to United States Cyber Command through Air Forces Cyber Forces.

3.7.1.12. Manage the Mission Defense Team program to enable tactical command and control of weapons systems and critical infrastructure resiliency. Enable Mission Defense Teams with information/intelligence, access, authority, and capability.

3.8. **United States Space Force** will:

3.8.1. Serve as lead service for Department of the Air Force enterprise satellite communications operations.

3.8.2. Be responsible for publishing implementing guidance required by DoDI 8420.02 in accordance with authority delegated from the Secretary of the Air Force.

3.8.3. Develop and publish, with the full participation and coordination of other supported commands and in coordination with AF/A2/6 and AF/A3, related publications supporting this directive.

3.8.4. When fully authorized, develop service-specific implementing policies and guidance unique to United States Space Force for assigned roles and responsibilities.

3.8.5. Direct United States Space Force-assigned mission defense teams when agreed between Chief of Staff of the Air Force and Chief of Space Operations to manage Service-level organize, train and equip of mission defense teams in support of United States Space Force space mission systems.

3.9. **Headquarters Air Force Functionals, Major Commands, Direct Reporting Units, and Field Operating Agencies** will:

3.9.1. Retain responsibility for accomplishing the above duties for command or mission-unique equipment, modifications, and missions.

3.9.2. Participate in the development of Lead Command or Lead Service guidance, and adhere to such guidance when it is specified to apply to all commands.

3.9.3. Follow applicable policy, including Lead Command or Lead Service guidance, and cyberspace orders when executing cyberspace operations.

Barbara M. Barrett
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 50, Code of Federal Regulations, Section 44

DoDI 3222.03, *DoD Electromagnetic Environmental Effects (E3) Program*, 10 October 2017

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

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

DoDI O-3780.01, *Senior Leader Secure Communications Modernization (SLSCM)*, 22 May 2014

DoDI 4630.09, *Communication Waveform Management and Standardization*, 15 July 2015

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

DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, 17 October 2017

DoDI 4650.10, *Land Mobile Radio (LMR) Interoperability and Standardization*, 28 July 2015

DoDI 8320.05, *Electromagnetic Spectrum Data Sharing*, 22 November 2017

DoDI 8420.02, *DoD Satellite Communications (SATCOM)*, 15 September 2016

DoDI 8500.01, *Cybersecurity*, 14 March 2014

Chairman of the Joint Chiefs of Staff PLANORD, 181807Z, 18 April 2017

JP 1, *Doctrine for the Armed Forces of the United States*, 25 March 2013

JP 2-01, *Joint and National Intelligence Support to Military Operations*, 5 July 2017

JP 3-0, *Joint Operations*, 22 October 2018

JP 3-12, *Cyberspace Operations*, 8 June 2018

JP 3-13, *Information Operations*, 27 November 2012

JP 3-13.1, *Electronic Warfare*, 8 February 2012

JP 3-30, *Joint Air Operations*, 25 July 2019

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

Air Force Doctrine Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*, 30 July 2019

HAFMD 1-20, *The Inspector General*, 7 May 2015

AFMD 39, *Air Force Office of Special Investigations (AFOSI)*, 14 April 2020

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 1 July 2019

DAFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 51-401, *The Law of War,* 3 August 2018

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

adj.—Adjective

AFI—Air Force Instruction

AFMD—Air Force Mission Directive

AFPD—Air Force Policy Directive

DoDI—Department of Defense Instruction

HAFMD—Headquarters Air Force Mission Directive

n.—Noun

Terms

Air Expeditionary Task Force—A deployed numbered air force or command echelon immediately subordinate to a numbered air force provided as the United States Air Force component command committed to a joint operation. (JP 3-30)

Air Force Information Network—The set of Air Force information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, 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 6-0 definition of Department of Defense Information Network)

Command and Control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1)

Cyber (adj.)—Of or pertaining to the cyberspace environment, capabilities, plans, or operations.

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 Attack—Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires. (JP 3-12)

Cyberspace Defense—Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. (JP 3-12)

Cyberspace Exploitation—Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (JP 3-12)

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 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. (JP 3-12)

Cyber Warfare Operations—Operations undertaken by Air Force forces to conduct Cyberspace Attack, Cyberspace Exploitation, or Cyberspace Defense, when assigned or attached to and authorized by a Combatant Command, and to extend or modify the Department of Defense Information Network for the purpose of providing communications capability to warfighting forces. Such operations do not include cyber warfare operations activities conducted by Air Force Office of Special Investigations for counterintelligence purposes. (DAFPD 17-2)

Department of Defense Information Network—The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 6-0)

Electromagnetic Spectrum—The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

Electromagnetic Warfare—Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (Air Force Doctrine Annex 3-51)

Information Operations—The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

Information Warfare—The employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and conflict.

Intelligence Community—See 50 U.S.C. §3003 (4)

Intelligence, Surveillance, and Reconnaissance (ISR)—1. An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. 2. The organizations or assets conducting such activities. (JP 2-01)

Mission-Relevant Terrain in Cyberspace—Defined as but not limited to all devices, internal/external links, operating systems, services, applications, ports, protocols, hardware, and software on servers required to enable the function of a critical asset. Mission-relevant terrain in cyberspace may exist external to the Department of Defense cyberspace. (Chairman of the Joint Chiefs of Staff PLANORD, 181807Z Apr 17)

Weapon—A device designed to kill, injure, disable or temporarily incapacitate people or destroy, damage, disable or temporarily incapacitate property or materiel. The term "weapon" does not include a device developed and used for training, or launch platforms to include aircraft and intercontinental ballistic missiles. (AFI 51-401)

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) **Note:** The term "Cyberspace Weapon System" is used in this directive as a means to identify requirements and critical resources requiring program-associated funding, but is not dispositive as to whether a particular resource is actually a "weapon system" as defined in JP 3-0, or a "weapon" as defined in AFI 51-401.