AIR FORCE DOCTRINE PUBLICATION 3-12

CYBERSPACE OPERATIONS

U.S. AIR FORCE

01 May 2026

Air Force Doctrine Publication 3-12, *Cyberspace Operations*

Table of Contents

Foreword i
Chapter 1: AIR FORCE CYBERSPACE OPERATIONS 1
UNDERSTANDING CYBERSPACE 2
CYBERSPACE OPERATIONS 7
CYBERSPACE OPERATIONS CHALLENGES 10
THREATS TO CYBERSPACE OPERATIONS 11
Chapter 2: ORGANIZATION, ROLES, AND RESPONSIBILITIES 13
DOW CYBERSPACE OPERATIONS FORCES 13
FORCE PRESENTATION AND EMPLOYMENT 16
COMMAND AND CONTROL OF CYBERSPACE FORCES 18
Chapter 3: PLANNING, EXECUTION, AND ASSESSMENT 22
CYBERSPACE OPERATIONS CONSIDERATIONS ACROSS THE COMPETITION CONTINUUM 22
CONSIDERATIONS FOR CYBER OPERATIONS 23
COORDINATING INTERAGENCY CYBERSPACE OPERATIONS 26
THREAT RESPONSE AND TARGETING 27
ASSESSMENT OF CYBERSPACE OPERATIONS 28
Appendix A: POLICY, DOCTRINE, AND AUTHORITIES RELATED TO CYBERSPACE OPERATIONS 30
Appendix B: ADDITIONAL AIR FORCE CYBERSPACE ROLES AND RESPONSIBILITIES 36
References 40

FOREWORD

The character of conflict has fundamentally changed. Cyberspace is no longer a supporting capability but a central, contested domain where national power is projected and defended. The ability to secure national interests and achieve mission success in the air, on land, in space, and at sea is now inextricably linked to the ability to operate and prevail in and through cyberspace. The speed, accessibility, and anonymity of this domain present both unparalleled opportunities for the joint force and significant challenges from a new generation of adversaries.

This publication, Air Force Doctrine Publication 3-12, *Cyberspace Operations*, provides the doctrinal foundation for how the United States Air Force thinks about, organizes for, and conducts operations in this critical domain. It establishes the core cyberspace operations, Offensive Cyberspace Operations, Defensive Cyberspace Operations, and Department of Defense Information Network Operations, as the pillars of our cyber power. This doctrine guides Airmen as they plan and execute operations across the competition continuum, from enabling day-to-day global activities to projecting power in armed conflict.

Success in the modern battlespace demands the full integration of cyberspace capabilities into joint all-domain operations (JADO). Together with combined joint all-domain command and control, JADO provides joint force commanders the means to integrate, synchronize, and deconflict the convergence of effects across all domains to achieve operational advantage. Cyberspace operations are not conducted in isolation, but as an integral part of operational planning and execution. Commanders, planners, and operators should understand the risks and opportunities inherent in a contested cyberspace environment and be prepared to fight and win.

CHAPTER 1: AIR FORCE CYBERSPACE OPERATIONS

Cyberspace is a global domain within the information environment (IE) consisting of the interdependent networks of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Joint Publication (JP) 3-12*, Joint Cyberspace Operations,* describes cyberspace operations as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Whether enabling peaceful military activities, supporting United States Air Force (USAF) information capabilities during competition, or used during armed conflict to gain operational advantage, cyberspace operations are conducted across the competition continuum to achieve assigned objectives and secure United States (US) national interests.

Cyberspace operations create effects consistent with Department of War (DoW), combatant command (CCMD), and service priorities. Cyberspace operations can be executed independently or integrated with operations in other domains to achieve primary, complementary, or enabling effects. Additionally, cyberspace operations ensure the confidentiality, integrity, and availability of vital command and control (C2) networks and the Department of Defense Information Network (DoDIN). Military operations in cyberspace are organized into missions through a combination of actions, which create effects to achieve a commander's objectives. USAF cyberspace forces support these objectives through offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoDIN operations.

All USAF operations rely on cyberspace, a domain that is increasingly challenged and contested. Like control of the air, control in cyberspace provides the joint force freedom of action and reduces vulnerability to enemy attacks, both within the cyberspace domain and across other domains. Achieving and maintaining advantage in cyberspace is a foundational component of overall operational and strategic advantage, especially for operations against peer adversaries. Because of cyberspace's complexity, achieving global superiority is unlikely. In some cases, even localized superiority may be achievable but impractical. Localized superiority in cyberspace refers to achieving a temporary and limited advantage over an adversary within a specific network, system, or geographic region. This advantage may be restricted by time, scope, or the specific capability employed. To ensure success in JADO, commanders should expect contested cyberspace operations and account for anticipated capabilities degradation.

The Six Pillars of America's Cyber Strategy

- **Pillar I.** Shape Adversary Behavior by deploying the full suite of US Government defensive and offensive cyber operations to detect, confront, and defeat cyber adversaries before they breach our networks and systems.
- **Pillar II.** Promote Common Sense Regulation by streamlining cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally to ensure that the private sector has the agility necessary to keep pace with rapidly evolving threats.
- **Pillar III.** Modernize and Secure Federal Government Networks by implementing cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition.
- **Pillar IV.** Secure Critical Infrastructure by identifying, prioritizing, and hardening America's critical infrastructure and supply chains, including defense critical infrastructure and adjacent vendors, private companies, networks, and services, such as the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals.
- **Pillar V.** Sustain Superiority in Critical and Emerging Technologies to protect user privacy from design to deployment–including supporting the security of cryptocurrencies and blockchain technologies–and secure the data, infrastructure, and models that underpin US leadership in AI while frustrating the spread of foreign AI platforms that censor, surveil, and mislead their users.
- **Pillar VI.** Build Talent and Capacity through existing avenues within academia, vocational and technical schools, corporations, and venture capital opportunities—to educate and train our existing cyber workforce across industries and occupations, and to recruit the next generation to design and deploy exquisite cyber technologies and solutions.

President Trump's Cyber Strategy for America (2026)

UNDERSTANDING CYBERSPACE

Cyberspace is a man-made domain, wholly contained within the IE, and encompasses the features of specificity, global scope, and an emphasis on the electromagnetic spectrum (EMS). Cyberspace segments are connected and supported by physical infrastructure, electronic systems, and portions of the EMS. Physical cyberspace nodes reside in every domain. Generally, cyberspace networks are interdependent. However,

parts of these networks are isolated via protocols, firewalls, encryption, and physical separation from other networks.

Activities in cyberspace can enable freedom of action in other domains, and activities in those domains can create effects in and through cyberspace. As new systems and capabilities are developed, they may use increasing portions of the EMS, have higher data processing capacity, speed, and leverage greater bandwidth.[1] Systems may also be designed to change frequencies (the places where they operate within the EMS) as they manipulate data. Thus, physical maneuver space exists in cyberspace.[2] Cyberspace-enabled capabilities are essential elements of military operations, critical enablers of all-domain synergistic effects.

CYBERSPACE OPERATIONS AND THE INFORMATION ENVIRONMENT

The USAF is responsible for developing, preparing, generating, employing, and presenting forces to support cyberspace-enabled operations in the information environment (OIE).[3] Because cyberspace is defined as wholly contained within the IE, cyberspace operations are often conflated with OIE. Rather, OIE combines cyberspace operations and other information activities and capabilities to create effects in support of joint operations throughout the operating environment, information being one of the seven joint functions of military operations.[4] Cyberspace operations can be conducted independently or synchronized, integrated, and deconflicted with other information capabilities and activities for more effective OIE.[5]

Cyberspace Operations Against ISIS

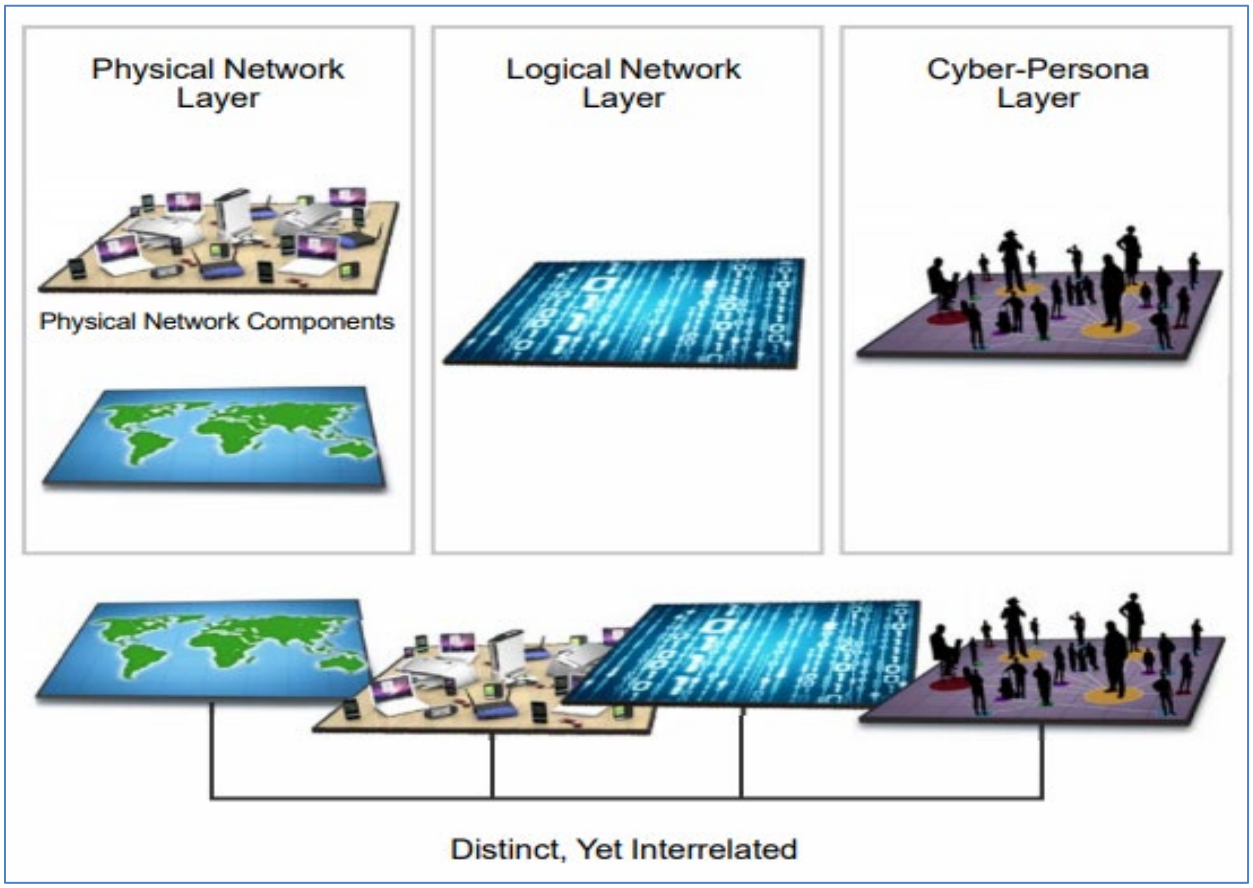
Integrating cyberspace operations with the other capabilities that leverage information enables scalable effects against targets commanders may otherwise lack options for. Joint Task Force Ares achieved this against the Islamic State of Iraq and Syria (ISIS) during Operation GLOWING SYMPHONY by integrating multiple disciplines to create confusion and distrust within ISIS and working closely with mission partners to dismantle its web-based operations.

THE OPERATIONAL ENVIRONMENT

The Cyberspace Layer Model. To aid understanding and assist in the planning and execution of cyberspace operations, JP 3-12 describes the cyberspace environment by presenting a cyberspace model comprising three interrelated layers: physical network, logical network, and cyber-persona. Each layer, by its nature, represents different aspects

[1] For additional information on USAF EMS systems and capabilities, see Air Force Doctrine Publication (AFDP) 3-85, *Electromagnetic Spectrum Operations*.
[2] For additional information on "Physical, Syntactic, and Semantic layers of Cyberspace," see *Conquest in Cyberspace*," Libicki, Martin C., RAND Corporation, Cambridge University Press, 2007.
[3] Per JP 3-04, *Information in Joint Operations*, OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior.
[4] See JP 3-0, *Joint Campaigns and Operations*, for additional information.
[5] See JP 3-12, *Joint Cyberspace Operations*, for additional information.

of cyberspace from which cyberspace operations should be planned, conducted, and assessed.



The Three Interrelated Layers of Cyberspace (JP 3-12)

Physical Network Layer. Comprised of IT devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, including data repositories and the connections that transfer data between network components. All physical components are owned by public or private entities capable of controlling or restricting access and require security measures to protect from physical damage or unauthorized access.

Logical Network Layer. Consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node but to their ability to be addressed logically and exchange or process data). Within the logical network layer, components are related by their ability to be logically addressed and to exchange or process data. Modern cloud-based networks offer an example. Though they span multiple servers across various physical locations comprise numerous dispersed components, they are viewed and function as a single entity from a logical perspective. Other examples are the DoW's Non-classified Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). These global, multi-segment networks can only be thought of as a single

network in a logical sense. Unlike physical network resources, logical layer targets can only be targeted by cyberspace capabilities: devices or computer programs, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

Cyber-persona Layer. A view of cyberspace created by abstracting and combining data from the logical network layer to develop descriptions of digital representations of an actor or entity's identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated (e.g., Non-Person Entity [NPE]), and their relationships to one another. Cyber-personas may relate directly to an actual person or entity and incorporate personal or organizational data (e.g., e-mail and Internet Protocol (IP) addresses, web pages, phone numbers, web forum logins, and financial account passwords). A single individual may create and maintain multiple cyber-personas. Conversely, a single cyber-persona can have multiple users. Cyber-personas can be complex, with elements distributed across multiple virtual locations that may not be linked to a single physical location. Identifying cyber-personas requires significant intelligence collection and analysis. As a result, adversarial use of cyber-personas can make it difficult to attribute responsibility for cyberspace activities.

Contested Cyberspace. A “contested cyberspace environment” exists when one or more adversaries attempt to change the outcome of a mission by denying, degrading, disrupting, manipulating, or destroying capabilities in cyberspace, or by altering the use, production, or confidence in those capabilities. Due to the nature of cyberspace, the low cost of entry, and the availability of viable commercial off-the-shelf (COTS) capabilities, commanders and planners should anticipate a contested environment.

Key Terrain in Cyberspace. Key terrain in cyberspace (KT-C) is analogous to key terrain in a physical domain, in that access to or control of it affords any combatant a position of marked advantage.[6] In cyberspace, it may only be necessary to maintain a secure presence at a particular location or within a particular process for a limited period. KT-Cs often have a virtual component identified in the logical network layer or the cyber-persona layer. Examples of KT-C include access points to major lines of communication, key waypoints for observing incoming threats, launch points for cyberspace attacks, and mission-relevant cyberspace terrain related to critical DoDIN connected assets.

The USAF may not own, control, or have access to the cyberspace terrain needed to conduct missions. To prepare, the USAF works with mission owners to identify mission-essential functions and associated hardware, software, and services that perform or enable them. Additionally, planners should be aware that sensitive cyber operations may be necessary to gain the KT-C access or infrastructure control required to support certain military missions.

Maneuver in Cyberspace. Maneuver is the employment of forces in the operational area through movement, combined with fires and information, to achieve a position of advantage. Once the KT-C has been identified, cyberspace forces should be positioned (physically or virtually) to generate desired effects, prevent or mitigate adversary effects.

[6] For additional information on Key Terrain Cyberspace, see JP 3-12, *Cyberspace Operations.*

Timelines for enacting planned cyberspace schemes of maneuver vary according to mission requirements and the commander's accepted level of risk.

Cyberspace Infrastructure Relationships. The USAF depends on US critical infrastructure and key resources (CI/KR) for many of its activities, including force deployment, training, transportation, and normal operations. Adversaries may attack these systems through espionage, denial of service, or more sophisticated, disruptive, and destructive attacks. Most critical infrastructure is under the control of networked, and interdependent supervisory control and data acquisition or distributed control systems. As such, physical protection alone is insufficient.

Characterized by interconnectedness and interdependency, authority and responsibilities for various CI/KR elements may overlap, creating vulnerabilities or causing friction and confusion. In response, DoW policies, memorandums of agreement, other coordination measures, and technical plans address this by delineating cyberspace by geographic regions and situations. The USAF coordinates regularly with utility owners, critical infrastructure operators, public and private sector partners, and other government agencies to ensure the availability and security of these resources.

CONTROL OF CYBERSPACE

Control of cyberspace is a key component of effective cyberspace operations. Control of cyberspace refers to a level of influence within the domain relative to that of an adversary. It can be categorized as parity, superiority, or supremacy, though the latter is unlikely to be achievable in cyberspace. Control can be achieved through many approaches, such as persistent engagement (which seizes and maintains the initiative), continuous risk assessment and management through protective actions, or by removing the adversary's will or capability to engage.

Offensive and defensive cyberspace operations will likely require some degree of cyberspace superiority. The joint force commander's (JFC) objectives and desired effects determine when, where, and how these operations are conducted to gain the required degree of cyberspace control. Control of cyberspace hinges on preventing prohibitive or effective cyberspace interference to friendly forces. Commanders should determine the level of cyberspace control required to accomplish the mission and direct actions, activities, or missions necessary to achieve it. The required or attainable level of cyberspace control may be limited spatially (physical and virtual) or temporally, and may be mission specific.

- **Cyberspace Parity.** A condition where opposing forces have roughly equal control of cyberspace. This represents a situation in which both friendly and adversary forces may encounter significant cyberspace interference. Parity is not a standoff, nor does it imply an inability to maneuver. On the contrary, parity may be typified by fleeting, intensely contested operations at critical points to achieve a sufficient level of control.
- **Cyberspace Superiority.** A 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. Cyberspace superiority may be critical to achieve superiority in other domains.

CYBERSPACE OPERATIONS

Every day, the cyberspace operations force conducts numerous cyberspace missions to secure and maintain freedom of action in cyberspace. These missions take on many forms, but can be categorized as either OCO, DCO, or DoDIN operations based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities employed.[7] To ensure unity of command and effort, missions are consolidated into a daily cyber tasking order (CTO). These core activities encapsulate a wide spectrum of capabilities and responsibilities to support all other domains and execute operations in cyberspace.

- **OCO.** Missions intended to project power in and through cyberspace.
- **DCO.** Missions to preserve the ability to utilize and protect friendly cyberspace capabilities and data, networks, devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity (MCA).
- **DoDIN Operations.** Operations to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the DoDIN.

OFFENSIVE CYBERSPACE OPERATIONS

OCO are missions intended to project power in and through gray and red cyberspace through actions taken in support of combatant commanders (CCDRs) or national objectives. OCO may exclusively target enemy cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading denial effects in the physical domains, affecting weapon systems, C2 processes, logistics nodes, and other high-value targets. All cyberspace operations missions conducted outside of blue cyberspace with intent other than defending blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions.[8]

USAF cyberspace forces and those assigned to the Cyber Mission Force (CMF) conduct OCO, when directed, in support of CCDR or national mission objectives. OCO consists of a range of operations enabled by intelligence, surveillance, and reconnaissance (ISR), cyberspace operational preparation of the environment (OPE), and cyberspace attack. OCO is planned, coordinated, and executed through either a Joint Force Headquarters-Cyber (JFHQ-C) or the Cyber National Mission Force (CNMF), in conjunction with CCMD cyberspace operations-integrated planning elements (CO-IPE). CO-IPEs provide direct support and reachback capability to coordinate between US Cyber Command (USCYBERCOM) forces and CCMD staff ensuring authorities are in place and deconfliction actions occur. The authorities for execution of each mission type reside at

[7] See JP 3-12, *Joint Cyberspace Operations*, for additional information.
[8] See JP 3-12, *Joint Cyberspace Operations*, for additional information.

different levels including, Commander, USCYBERCOM (CDRUSCYBERCOM), the Secretary of War (SecWar), or the President.

- **Cyberspace Intelligence, Surveillance, and Reconnaissance.** A military intelligence action conducted by the JFC, authorized by an execute order (EXORD). Cyberspace ISR is normally conducted to gather intelligence that may be required to support planning or execution of cyberspace operations.
- **Cyberspace Operational Preparation of the Environment.** Cyberspace OPE consists of non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. This mission includes identifying data, software, system/network configurations, identifiers, as well as physical structures connected to or associated with the network.
- **Cyberspace Attack.** Cyberspace actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) and manipulation effects and are considered a form of fires. These actions can be integrated with other fires to achieve greater effectiveness, such as using an EMS-enabled cyberspace attack to disrupt and degrade enemy air defense systems during an air operation.

OCO may affect adversary systems across multiple domains. Certain OCO may be conducted in conjunction with other components or special operations forces. Cyberspace targets include specific components, systems, networks, or even physical locations. Effects may be temporary, long-term, or permanent. By design, OCO may exclusively target adversary cyberspace functions or create cyberspace effects with manifestations in physical domains against adversary weapon systems, C2 processes, and logistics nodes. Some OCO missions may include cyberspace attack actions that are equivalent to physical damage or destruction of adversary systems and equipment. OCO missions require careful consideration regarding the scope of operations, rules of engagement (ROE), potential repercussions, and measurable progress towards the commander's objectives.

DEFENSIVE CYBERSPACE OPERATIONS

DCO missions are executed to defend blue cyberspace against imminent or active threats. DCO missions defeat threats that have bypassed, breached, or are threatening to breach security measures, thereby distinguishing DCO from DoDIN operations, which endeavor to secure DoW cyberspace from all threats in advance of any specific threat activity. The USAF organizes defensive cyberspace operations forces around networks, threats, or mission areas. This organizational practice aligns relevant capabilities with authority to execute operations and ensures defensive cyberspace airmen are familiar with the cyberspace terrain or mission area they are assigned to defend, or the threat they are assigned to defend against. Forces that are not part of the CMF, have a primary purpose to preserve the ability to utilize blue cyberspace capabilities and to protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity.

When a DCO activity is conducted on friendly cyberspace terrain, it constitutes a DCO-internal defensive measures (DCO-IDM) mission. When a DCO activity is conducted external to the defended network, in foreign cyberspace, and without the permission of the affected system's owner, it is considered a DCO-response action (DCO-RA) mission.

Adversaries rarely act overtly when conducting intelligence activities or offensive operations in cyberspace. For this reason, additional care should be taken to deliberately assess the operational effectiveness of DCO. Lack of evidence of a breach does not mean the network is secure. Proper assessment helps commanders avoid errors caused by misinterpretation of data. A deliberate operational assessment of the mission and terrain being protected, and the defensive cyberspace capabilities available, provides operational commanders with an accurate account of cyberspace risks to the mission.

DoW's Cyber Lines of Effort

- **Line of Effort 1.** Defend the Nation. Hardening against Cyber Threats by protecting critical infrastructure, disrupting MCAs, and working with interagency and international partners.
- **Line of Effort 2.** Prepare to Fight and Win the Nation's Wars. Campaigning in and through cyberspace by enhancing cyber resilience and the ability to fight in and through contested and congested cyberspace to meet the Joint Force's and generating asymmetric advantages.
- **Line of Effort 3.** Protect the Cyber Domain with Allies and Partners. Building capacity and capability of U.S. Allies and Partners and expand potential cyber cooperations continuing hunt forward operations to illuminate MCAs and encouraging adherence to international law and recognized cyberspace norms.
- **Line of Effort 4.** Build Enduring Advantage in Cyberspace. Investing in cyber workforce development, research and development, and innovation.

Department of Defense Cyber Strategy (2023)

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

For the purposes of this document, the AFIN is "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."[9]

[9] See JP 6-0, *Joint Communications*, and Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*, for additional information.

USAF DoDIN operations are standing missions that encompass day-to-day security, maintenance, threat response, and support to DCO forces. Although many of these activities are regularly scheduled events, they cannot be considered routine, as their aggregate effects establish the framework for most USAF missions. In addition to regular security efforts, an effective response to intrusions or other malicious activity on the USAF portion of the DoDIN, the Air Force Information Network (AFIN), requires coordinated action with DCO forces. Many associated tasks between DCO and DoDIN operations may overlap or require deconfliction. Support to DCO forces can include ensuring the appropriate levels of access and permissions to complete assigned defensive missions.

Daily operations are tasked by 16th Air Force (16 AF) elements or the AFIN Mission Assurance Center (AMAC) to appropriate units for execution. However, many systems within the AFIN are controlled by program offices or mission partners that do not report to 16 AF or AMAC. In such cases, authorities and responsibilities for security should be delineated and clarified to minimize AFIN vulnerabilities.

CYBERSPACE OPERATIONS CHALLENGES

COMMERCIAL OFF-THE-SHELF TECHNOLOGY

The expanded availability of COTS technology provides adversaries with increasingly flexible and affordable technology that can be adapted for nefarious purposes. Low barriers to entry (low cost, wide availability) significantly decrease the traditional capability gap between the US and its adversaries. Likewise, as technologies rapidly advance in areas such as the Internet of Things, artificial intelligence (AI), and quantum computing, adversaries can field newer, more sophisticated cyberspace systems, enabling experimentation with novel warfighting concepts. To keep pace with the COTS challenge, systems require continuous updates and significant effort to identify and fix vulnerabilities, bugs, and other performance concerns. Failure of USAF acquisitions, contracting, and operational planning efforts to align and keep pace with these changes increases the likelihood an adversary may exploit an unmitigated vulnerability.

Because private industry is the primary driver of technological advancements, the vast majority of USAF cyberspace operations components and capabilities are COTS. Such dependency creates potential vulnerabilities:

- **Foreign ownership, control, and influence of vendors.** Many COTS technologies (hardware and software) available for purchase are developed, manufactured, or have components manufactured in foreign countries. Adversaries may exploit this vulnerability by influencing foreign manufacturers, vendors, service providers, or developers to alter products with designed security weaknesses, such as modified chips or software modified to execute a blue pill (insider) attack on government systems. This vulnerability is present throughout a product's life cycle, from design and manufacture to delivery, and through product updates and support.
- **Supply chain.** Adversaries may also exploit security gaps in the global supply chain to intercept and alter products before delivery.

ATTRIBUTION

Perhaps the most challenging aspect of cyberspace-related intelligence is connecting an action to a real-world agent (individual or state) with sufficient confidence and verification to inform decision-makers. By design, the internet lends anonymity and complicates attribution. Likewise, government policies, international laws, and treaties can make it very difficult to determine the origin of a cyberspace attack. The ability to hide the source of an attack makes it difficult to find and identify the attacker in cyberspace. Successful attribution involves significant analysis and often requires collaboration with non-DoW agencies and organizations.

In addition to the factors above, the nature of attribution varies depending on the specifics of what can be identified. Identifying an IP address, location, or device may be sufficient for some actions, such as establishing deny lists. The more difficult action of connecting such identifiers to a specific actor (individual or otherwise) may be required for targeted offensive actions or other US Government or military response.

NETWORK VULNERABILITIES

The interconnected nature of cyberspace presents an inherent risk that requires constant attention and mitigation. Risks and vulnerabilities are often created by the lack of analyzed intelligence and interdependencies arising from system networking and integration. Systems may also be vulnerable to electronic attacks and structurally difficult to defend. DoW's Vulnerability Disclosure Program (VDP) works with ethical hackers and outside organizations to identify, notify, and rectify network owners of newly discovered vulnerabilities. Some examples of well-known vulnerabilities in cyberspace operations can be found in the 2023 Department of Defense Cyber Strategy. Operations like those planned and executed by Joint Task Force (JTF) ARES test our integration capabilities and identify vulnerabilities in a difficult, contested cyberspace environment. However, mitigation measures can decrease risk levels. Examples of risk mitigation include the implementation of firewalls, advanced training, education, policies, and intrusion detection and prevention systems.

INFRASTRUCTURE VULNERABILITIES

The physical infrastructure of cyberspace is routinely disrupted by operator errors, industrial accidents, and natural disasters. These unpredictable events can significantly impact operations. Planning efforts should highlight potential vulnerabilities and identify alternate or redundant pathways to increase system resiliency.

THREATS TO CYBERSPACE OPERATIONS

Cyberspace operations face many threats, ranging from nation-states to individual actors to accidents, and natural hazards.[10] To enable freedom of maneuver in cyberspace, cyberspace operations should reduce or eliminate threats and vulnerabilities and constantly assess, coordinate and deconflict cyberspace operations. In general,

[10] See JP 3-12, *Joint Cyberspace Operations*, for additional information.

cyberspace threats are divided into two major categories: MCA and adverse cyberspace activities (ACA).

- **Malicious Cyberspace Activities.** Activities, other than those authorized by or in accordance with (IAW) US law, which seek to compromise or impair the confidentiality, integrity, or availability of computers, information, or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident therein. Organized crime or other non-state, illegitimate organizations often make sophisticated malware available for purchase, free, or at little to no cost, allowing even unsophisticated threat actors to acquire advanced capabilities. Because of low barriers to entry and potentially high payoffs, an increasing number of adversaries use cyberspace capabilities to negate US advantages.

- **Adverse Cyberspace Activities.** The USAF term for friendly actions, natural events, disasters, or accidents that inadvertently achieve the same effects as MCA, providing adversaries the opportunity to capitalize on vulnerabilities and to degrade infrastructure. Friendly actions in one segment of the network may result in unintended damage in another. Likewise, natural events can damage and disrupt cyberspace with highly destructive effects requiring both proactive and reactive cyberspace operations to maintain or restore key systems. In addition to friendly actions, ACA also includes friendly negligence or deficiencies that create vulnerabilities or open systems to attack, such as failure to implement policy, implementing rushed or inadequate policy, and poor change management practices. There are also numerous examples of individuals (mission or system owners and operators) becoming insider threats with or without malign intent, by executing actions, policies, or changes that adversely affect operations.

CHAPTER 2: ORGANIZATION, ROLES, AND RESPONSIBILITIES

DOW CYBERSPACE OPERATIONS FORCES

DoW cyberspace operations forces (COF) are organized into eight operational groups.[11]

- Cyber Mission Force (CMF)
- USCYBERCOM and Subordinate Command Elements
- Military Services and DoW Defense Agencies and DoW Field Activities
- Cyberspace Assessment Elements
- Cyberspace Supporting Actions Elements
- CCMD Cyberspace Operations Elements
- DoW Intelligence Elements Supporting Cyberspace Operations
- Commander, United States Special Operations Command (CDRUSSOCOM)-Assigned Forces

Additionally, it is important to distinguish between forces assigned to the CMF and other elements within the DoW COF. While groups such as Military Service-retained forces, DoW Intelligence elements, and CDRUSSOCOM-assigned forces are formally recognized operational groups, they typically operate outside the CMF's direct tasking to fulfill Service-specific or other unique mission requirements.

CYBER MISSION FORCES

Forces presented to USCYBERCOM are organized into three CMF elements: Cyber Protection Force (CPF), CNMF, and Cyber Combat Mission Force (CCMF). AFCYBER presents cyberspace protection teams (CPT) to the CPF, national mission teams (NMT) to the CNMF, and combat mission teams (CMT) to the CCMF. USAF cyberspace operations forces not actively assigned to USCYBERCOM may be tasked to support the CMF via a request for forces or other appropriate order.

- **Cyber Protection Force.** The CPF, composed of CPTs, conducts cyberspace operations to protect the DoDIN or another friendly cyberspace.
- **Cyber National Mission Force:** The CNMF conducts cyberspace operations to defeat significant cyberspace threats to the DoDIN and, when ordered, to the nation. The CNMF comprises various numbered NMTs, National Support Teams (NSTs), and national-level CPT's for the protection of non-DoDIN blue-force cyberspace terrain.

[11] See Secretary of Defense Memorandum on *Department of Defense Cyberspace Operations Forces*, 24 July 2025, for additional information.

- **Cyber Combat Mission Force.** The CCMF conducts cyberspace operations to support the missions, plans, and priorities of the geographic and functional CCDRs. The CCMF comprises various numbered CMT and Combat Support Teams (CSTs).

In 2018, Joint Force Headquarters-Cyber (Air Force) (JFHQ-C [AF]) coordinated cyberspace operations in support of the CNMF. JFHQ-C (AF) operators and assigned intelligence forces conducted intelligence missions that rapidly enabled identification and tracking of cyberspace actors' intent to disrupt the 2018 election cycle. These missions enabled unity of effort across CCMDs, National Security Agency, Federal Bureau of Investigation, Department of Homeland Security, and the Department of Treasury.



SUBORDINATE COMMAND ELEMENTS

The subordinate headquarters of USCYBERCOM execute C2 of the CMF and other cyberspace forces. These include the following subordinate command elements:

- CNMF-HQ
- Department of Defense Cyber Defense Command (DCDC)
- JFHQ-C
  - Most services provide a JFHQ-C to USCYBERCOM, such as the JFHQ-C (AF). Additionally, DCDC, in coordination with all CCDRs and other DoW components, plans, directs, coordinates, and executes global DoDIN operations and DCO-IDM.
  - In coordination with USCYBERCOM, JFHQ-Cs provide steady state and contingency cyberspace operations planning and targeting support to aligned CCMDs and, when authorized, conduct OCO missions in support of those CCMDs. JFHQ-Cs direct, coordinate, synchronize, plan, and assess risk for current and future cyberspace operations, and ensure the integration of cyberspace security cooperation objectives into CCMD campaign plans.
  - USCYBERCOM aligns subordinate commands presented to it globally. Each JFHQ-C is aligned to support specified CCMDs and CCMD Integrated Joint Special Technical Operations-presented capabilities. CNMF and other service JFHQ-Cs support other CCMD objectives. C2 of JFHQ-C forces is directed by USCYBERCOM, normally through the 616th Operations Center (616 OC) for JFHQ-C Air Force forces.
- CO-IPEs
  - JFHQ-Cs lead and staff CO-IPEs to provide support to the CCMD with expert cyberspace planners. A CCDR's staff is tasked to execute cyberspace operations to secure, defend, and operate within DoDIN segments that affect the mission. To

address deficiencies in cyberspace experience, CO-IPEs provide expertise and reach-back capability, serving as liaisons between USCYBERCOM and the supported CCDR. CO-IPEs provide CCDRs with cyberspace operations planners and subject matter experts to support the development of cyberspace operations requirements, facilitate cyberspace operations C2 by advising planning teams on the best use of cyberspace forces, and assist with coordinating, integrating, and de-conflicting cyberspace operations. CO-IPEs are composed of USCYBERCOM, DCDC and JFHQ-C personnel and are fully integrated with each CCMD staff.

- Joint Mission Operations Centers (JMOCs).
- Service Cyberspace Component (SCC).
- JTFs created to support ongoing USCYBERCOM-led missions.

MILITARY SERVICES AND DOW AGENCIES AND FIELD ACTIVITIES

All total force cyberspace forces, units, and personnel in any military Service, DoW Agency, or Field Activity not assigned to USCYBERCOM. IAW DoD Directive (DoDD) 5100.01, those forces can perform actions to support service core functions.

- **Defensive Cyberspace Operations Forces.** Threat-informed forces that preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, and weapon systems with tailored actions to counter or mitigate specific MCA activities.
- **DoDIN Operations Cyberspace Forces.** Network or system-focused, threat-agnostic forces whose primary mission is to take actions to secure, configure, operate, extend, design, acquire, build, maintain, and sustain DoW cyberspace terrain.
  - Cyber Security Service Providers (CSSPs)
  - Network Operations Centers (NOCs)
  - Security Operations Centers (SOCs)
  - Network Operations and Security Centers (NOSCs)
- **Offensive Cyberspace Operations Forces.** Threat-informed forces not part of the CMF under the authority of the CCMD, which they are assigned, whose primary purpose is intended to project power in and through foreign cyberspace in support of CCDR or national objectives.

CYBERSPACE ASSESSMENT ELEMENTS

Forces organized to conduct independent assessments of DoW cyberspace to inform commanders of risk and the security posture of their assigned networks. These elements may execute operations in support of training, assessments, tests, inspections, and other cyber risk determinations, such as:

- DoW Cyber Assessment Teams

- DoW Cyber Red Teams

CYBERSPACE SUPPORTING ACTIONS ELEMENTS

Elements of the DoW components that perform enabling operations for cyber capabilities for the joint warfighter by provisioning IT architecture development, establishing standards, or designing, building, or operationalizing the DoDIN.

- Acquisition and Sustainment of cyberspace capabilities
- Business function elements (budget, logistics)
- DoW IT
- DoW Operational Technology (OT)

COMBATANT COMMAND CYBERSPACE OPERATIONS ELEMENTS

Elements of CCMDs, not assigned to USCYBERCOM, are responsible for planning, directing, coordinating, integrating, and synchronizing CCMD cyberspace operations activities, including cyberspace operations in support of, but not limited to: OIE, Psychological Operations (PSYOPS), space operations, and Electromagnetic Spectrum Operations (EMSO).

DOW INTELLIGENCE ELEMENTS SUPPORTING CYBERSPACE OPERATIONS

DoW intelligence related units or personnel whose primary mission requires the enabling or employment of cyberspace operations.[12]

COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND ASSIGNED FORCES

Forces assigned to the CDRUSSOCOM that are purposely organized, trained, and equipped to conduct OCO, DCO, and DoDIN operations.

FORCE PRESENTATION AND EMPLOYMENT

US CYBER COMMAND

CDRUSCYBERCOM's mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. The commander has three primary focus areas: Defend the DoDIN, support CCMD global mission execution, and strengthen our nation's ability to withstand and respond to cyberspace attacks. CDRUSCYBERCOM commands the preponderance of cyberspace forces not retained by the services. As the coordinating authority for global cyberspace operations, USCYBERCOM plans and executes activities to secure and defend the DoDIN and conducts cyberspace operations external to the DoDIN in support of national objectives. CDRUSCYBERCOM exercises directive

[12] See Secretary of Defense Memorandum on *Department of Defense Cyberspace Operations Forces*, 24 July 2025, for additional information.

authority for cyberspace operations (DACO), the authority to issue orders and directives to all DoW components for global DoDIN operations and DCO-IDM. Commander, DCDC (CDRDCDC) exercises DACO over all DoW components, agencies, and field activities. As DoDIN operational area commanders, SCC commanders exercise delegated DACO over their respective operational areas.

Individual services organize, train, and equip cyberspace units and present forces to USCYBERCOM through the JFHQ-C and directly via the service's respective SCC. Each SCC commander is dual-hatted by CDRUSCYBERCOM as a commander of one of the four JFHQ-Cs to enable synchronization of cyberspace operations C2 across all CCMDs. CDRUSCYBERCOM assigns or attaches these forces directly to a SCC commander or assigns them under their additional authority as Commander, JFHQ-C.

SERVICE CYBERSPACE COMPONENTS

SCC commanders exercise administrative control (ADCON) of assigned service forces and serve as the subject matter expert for service-specific cyberspace capabilities, forces, and operations.[13] In coordination with USCYBERCOM, they are responsible for developing tactics, techniques, and procedures (TTPs) and capabilities to support and enable cyberspace missions. SCCs presented to USCYBERCOM:

- US Air Force: Air Forces Cyber (AFCYBER)
- US Army: Army Cyber Command (ARCYBER)
- US Navy: Fleet Cyber Command (FLTCYBER)
- US Marine Corps: Marine Forces Cyber Command (MARFORCYBER)

16TH AIR FORCE/UNITED STATES AIR FORCE: AIR FORCES CYBER

The USAF's SCC, AFCYBER, is aligned with 16 AF, the component numbered air force, and the commander is dual-hatted as the cyberspace air component commander, the sole entity responsible for presenting USAF cyberspace forces to USCYBERCOM. The cyberspace air component commander is the senior Air Force warfighter for employment of assigned and attached USAF cyberspace forces under USCYBERCOM. Additionally, 16 AF/CC/CDRAFCYBER is designated Commander, Joint Forces Headquarters-Cyberspace (Air Force) (CDRJFHQ-C [AF]). Thus, 16 AF/CC/CDRAFCYBER is triple-hatted as commander of 16 AF, AFCYBER, and JFHQ-C (AF) with the following responsibilities:

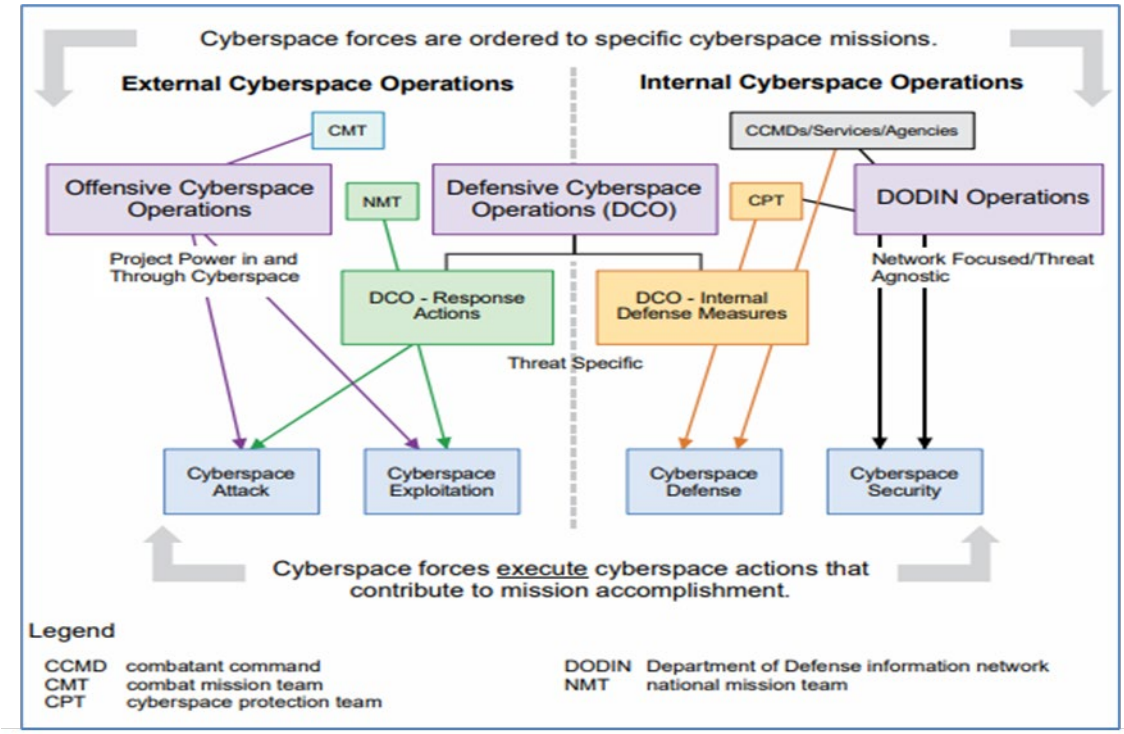
- **16 AF/CC.** Executes USAF service tasks as directed by the Secretary of the Air Force (SecAF) and Chief of Staff of the Air Force (CSAF), reports directly to Air Combat Command (ACC) and organizes, trains, and equips cyberspace operators and presents those forces to CCMDs, deploys USAF-approved weapon systems,

[13] Normally, service component commanders are also delegated operational control (OPCON) of assigned and attached forces. However, for cyber operations under USCYBERCOM, OPCON is delegated to each component's CDRJFHQ-C.

maintains and defends USAF portions of DoDIN, and provides, establishes, and maintains a secure and defensible network to support global USAF functions.

- **CDRAFCYBER.** As the USAF's SCC, presents cyber forces to CDRUSCYBERCOM, conducts operational-level planning, direction, coordination, execution, and oversight of DoDIN operations and DCO-IDM within USAF systems, maintains and defends the USAF portion of the DoDIN, exercises OPCON of forces as assigned by CDRUSCYBERCOM of service-aligned CPTs, and provides, establishes, and maintains a secure and defensible network to support operations in support of national security objectives.

- **CDRJFHQ-C (AF).** Enables synchronization of cyberspace operations C2 and reports directly to CDRUSCYBERCOM under combatant command (COCOM) authority. Analyzes, plans, and executes USCYBERCOM directed cyberspace missions.



JP 3-12, Cyberspace Operations Missions, Actions, and Forces

COMMAND AND CONTROL OF CYBERSPACE FORCES

COMMAND AND CONTROL OF AFCYBER FORCES

The 616 OC translates USCYBERCOM global and supports CCDR theater objectives, priorities, and intent into a coherent, executable plan for USAF cyberspace forces through the cyberspace tasking cycle. A derivative of the joint planning process for air (JPPA) and the air tasking cycle, the cyberspace tasking cycle is an iterative process for planning, coordinating, allocating, executing, and assessing the effectiveness of cyberspace operations. The cycle can be lengthened or shortened as needed to synchronize with a theater's battle rhythm.

Detailed plans for effectively employing cyberspace capabilities are produced through the cyberspace tasking cycle, culminating in the publication of the daily CTO. The CTO, derived from CDRUSCYBERCOM and supported by JFCs guidance, is analogous to the air tasking order (ATO) and tasks assigned and attached cyberspace forces. It provides special instructions and guidance necessary to execute and synchronize global and theater joint operations. All cyberspace operations executed during the period should be listed on the CTO for situational awareness (SA) and deconfliction purposes.

INTEGRATION AND SYNCHRONIZATION OF THEATER AND GLOBAL OPERATIONS

When supporting CCMD theater operations, commanders and planners should work closely with the appropriate operational C2 entities, such as the 616 OC or the assigned JFHQ-C, to synchronize the cyberspace tasking cycle with that theater's planning and tasking processes, including the CTO and ATO. In line with CDRAFCYBER's guidance, the 616 OC develops cyberspace courses of action to support theater operations. Using this guidance, ROE, the joint integrated prioritized target list, the target nomination list, and the approved master air attack plan, the 616 OC finalizes the CTO.

In addition to the deliberate process described above, dynamic cyberspace taskings can occur during the execution phase to meet supported commander requests. Within the 616 OC, daily AFCYBER mission execution is monitored and controlled by the combat operations division. Post-mission, the strategy division's operations assessment team receives mission reports and evaluates effects against established measures of effectiveness (MOEs) to determine if desired objectives have been achieved.

CYBERSPACE COMMAND AND CONTROL CHALLENGES

Though centralizing cyberspace operations (OCO, DCO, and DoDIN) under a single command offers distinct advantages, also poses significant challenges.

Relations for Global Support. AFCYBER executes a global mission through support relationships with various CCMDs and organizations that vary significantly.

Levels of Operation. AFCYBER balances competing objectives. This presents a challenge for organizing cyberspace forces, particularly at subordinate staff levels, since each entity requires a tactical C2 function (such as a cyberspace tactical operations center) or adequate representation at the headquarters level. In these cases, merging personnel roles and divergent command structures (e.g., A3 for DCO/DoDIN operations and J3 for OCO) present challenges for articulating unit tasking authorities.

Situational Awareness. Cyberspace operations SA cannot be maintained by a traditional common operational picture like those presented in air operations centers (AOCs). Instead, informed personnel are required to advise commanders on OCO, DCO, and DoDIN operations developments.

Remote Support. To ensure the required level of competency and representation within the 616 OC, AFCYBER CMF receives input and support from geographically separated entities: the 616 OC, AMAC, and 33rd Cyberspace Operations Squadron (33 COS).

Despite the advantages of dispersed operations, this presents significant challenges for coordination and communication.

Authorities. The authorities required to execute OCO normally exceed those held by operational level commanders, resulting in C2 challenges for mission execution. The authority to conduct OCO normally resides with CDRUSCYBERCOM. When authority for a specified OCO resides in another CCMD, USCYBERCOM remains the coordinating authority for global cyberspace operations. C2 of DCO and DoDIN operations fall under the purview of CDRAFCYBER's Title 10 USC responsibilities. However, this can be challenging for CMF personnel tasked to simultaneously prioritize resources for both local needs and AFCYBER-directed activities.

Security Classification. Ideally, a tasking order should be presented daily on a single document. However, the USCYBERCOM Dispatch has instances on SIPRNet and the Joint Worldwide Intelligence Communications System (JWICS).

LEGAL AUTHORITIES AND CONSIDERATIONS

There are several different United States Code Titles that are related to and/or provide authorities for cyberspace operations. These include, but are not limited to, Title 10, Title 18 (e.g., supporting Air Force Office of Special Investigations [AFOSI]), and Title 50. The nature of an operation may also require that CMF follow domestic law, international law, treaties, national and organizational policies, law of war, and established ROE. Airmen conducting or supporting coalition and allied cyberspace operations (e.g., North Atlantic Treaty Organization) should consider the authorities governing those operations as well. In all cases, the specific authority for each operation should be clearly defined in orders, typically an EXORD or operations order.

Operations within this varied legal landscape, which often require commanders to operate across various jurisdictions, highlight the need for clear command relationships. This is especially true for operations involving a total force mix of active duty Air Force, Air Force Reserve, and Air National Guard (ANG) forces, possibly in different duty statuses. When activated for federal service under Title 10 USC, ANG operates IAW the same authority as their active duty counterparts. Alternatively, duties performed under state authority are governed by Title 32 USC, *National Guard,* or any applicable state law under state active-duty status.

Total force legal considerations are not unique to ANG CMFs. However, given the ubiquitous nature of cyberspace and the tendency for operational lines between civil and military authorities to blur in cyberspace operations, it presents significant concerns and challenges not typically faced in traditional military operations. It is important for commanders conducting cyberspace operations under various authorities, especially those in dual status, to consult the appropriate servicing judge advocate for advice based on personnel status.

CMF Sources of Legal Authority

Title 10 USC—*Armed Forces*; section 2012, Support and services for eligible organizations and activities outside DOD.

Title 18 USC—*Crimes and Criminal Procedure*; section 592, Troops at polls; section 593, Interference by armed forces.

Title 32 USC—*National Guard.*

Title 50 USC—*War and National Defense*.

Presidential Policy Directives:

PPD-21: *Critical Infrastructure Security and Resilience*.

PPD-41: *US Cyber Incident Coordination Policy*.

Cybersecurity Act of 2015 (P.L. 114-213).

National Cybersecurity Protection Act of 2014 (P.L. 113-282).

National Defense Authorization Act.

National Defense Strategy.

National Cybersecurity Strategy.

National Military Strategy.

National Security Strategy.

Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities.

Executive Order 13800, Presidential Executive Order *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 11 May 2017.

Executive Order 14144 Amended, *Strengthening and Promoting Innovation in the Nation's Cybersecurity,* 6 June 2025

National Security Memorandum 8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*.

NSPM 13, *(U) United States Cyber Operation Policy*, as amended.

DOD Directives:

1100.20, *Support and Services for Eligible Organizations and Activities Outside the Department of Defense.*

3025.18, *Defense Support of Civil Authorities*.

3025.21, *Defense Support to Civilian Law Enforcement.*

DoDI 8530.02, Cyber Incident Response

CNGBI 3000.04, National Guard Bureau Domestic Operations.

**Additional sources of legal authority for CMF operations are outlined in Appendix A*

CHAPTER 3: PLANNING, EXECUTION, AND ASSESSMENT

DESIGN AND PLANNING OF CYBERSPACE OPERATIONS

Cyberspace operations may be planned as a part of major operations and campaigns, homeland operations, crisis response operations, or limited contingency operations. Taskings for cyberspace operations forces in each mission area, service, CCMD, federal, or state, vary in manner and nature. While the focus of each organization's planning element will vary according to the mission set or capability, the notional tasking cycle for all DoW operations will be derived from joint planning doctrine.[14]

Timing and tempo are key considerations for planning, use, and integration of cyberspace forces to ensure effects are available when needed. Successful cyberspace operations may require weeks, months, or even years of preparation before execution. The longest timelines require strategic understanding of cyberspace objectives against often theoretical problem sets projected many years in the future. This long-term view allows the development of technologies, infrastructures, and capabilities that reflect the understanding, analysis, and production time required to provide tools or capabilities when needed.

To account for potentially lengthened timelines, cyberspace planners should be present in the early stages of the joint planning process (JPP).[15] Incorporating cyberspace operations into early planning expands its capacity to support operations by presenting capabilities and targets susceptible to their effects, and provides commanders with an accurate estimate of the time required to deliver requested capabilities, whether through access, tools, or infrastructure.

CYBERSPACE OPERATIONS CONSIDERATIONS ACROSS THE COMPETITION CONTINUUM

ENGAGEMENT AND COOPERATION OPERATIONS

Multinational military operations are the norm, making intelligence and information sharing with allies and coalition partners increasingly important. Connectivity is essential, particularly when the US, allies, and coalition forces require mutual support during combat. Interoperability issues should also be considered and balanced with the USAF's need for information assurance. As a part of a larger networked team, the USAF should plan and execute in close concert with other services, states, and agencies.

HOMELAND OPERATIONS

Cyberspace operations support homeland operations, including homeland defense and defense support of civil agencies (DSCA). Once requested and authorized by the appropriate authorities, military assistance can be provided similar to direct support. Attack and exploitation operations in a homeland defense scenario may involve complex

[14], For additional information on joint targeting cycle, see JP 3-30, *Joint Air Operations*, JP 3-60, *Joint Targeting*, and JP 5-0, *Joint Planning*
[15] For additional information on JPP, see JP 5-0, *Joint Planning*.

legal and policy issues. Though these issues do not prevent all cyberspace operations, they will likely temper their applications. DoW forces cannot be used to conduct attack or exploit operations against US entities unless approved by appropriate authorities. Likewise, information sharing protocols (including protection of classified and sensitive information), laws, and policies regulate (and may at times prevent) data and information sharing between federal, state, and local agencies, non-governmental organizations, and partner nations.

MAJOR OPERATIONS AND CAMPAIGNS

In addition to other ongoing missions, cyberspace operations can be planned as part of major operations and campaigns. Incorporating a strategy for cyberspace superiority in formal planning offers commanders many additional options. Cyberspace operations can generate effects that historically required physical attack instead. Cyberspace operations can open avenues to exploit enemy capabilities, alter information the enemy receives, and influence an enemy's decisions.

When conducted at the theater level, cyberspace operations planning should be fully integrated into the JPP to expand planning and execution options to meet the JFC's objectives. Cyberspace planners should synchronize cyberspace operations with the air component commander's time-phased scheme of maneuver for a given tasking period. Effective cyberspace operations plans should include commander's guidance, desired effects, supported component schemes of maneuver, friendly capabilities, and likely adversary courses of action. The approved plan will guide operators employing cyberspace operations against approved targets. To the extent possible, cyberspace liaison officers should be made available to other components to synchronize component cyberspace requirements.

CONSIDERATIONS FOR CYBER OPERATIONS

OFFENSIVE CYBERSPACE OPERATIONS CONSIDERATIONS

Access. Gaining access to an adversary system or network can be an extremely arduous undertaking. Such operations require a great deal of technical understanding of adversary networks, systems, and TTPs to covertly gain and retain access without being discovered. Air planners should coordinate mission access requirements with their assigned director of cyberspace forces (DIRCYBERFOR or DC4) early in the planning process.

Technical Gain or Loss. For technical capabilities to be effective, they should continually evolve to stay ahead of the adversary's defenses. Maintaining this technological edge comes at a cost. Commanders authorized to employ OCO should weigh an operation's potential benefit against the risk of losing the technology and exposing friendly TTPs.

Intelligence Gain or Loss. OCO requires substantial investment to acquire the intelligence need to develop target packages and tools for a particular operation. Commanders should coordinate any proposed OCO with intelligence planners to ensure the anticipated results of an operation outweigh the risk of losing intelligence sources or methods.

Physical Effects. OCO, although conducted online, may also have physical effects. These physical effects need to be considered against CCDR ROE, the law of war, other legal considerations, and applicable international agreements and treaties. Such physical effects, especially when caused by OCO, can have wide-ranging second- and third-order effects. The unpredictable nature of such effects and the ability to cause wider collateral damage should be carefully considered and planned during the course of action development.

Integration into Joint Operations or Campaigns. OCO can increase the survivability or lethality of air and space operations. For optimal effectiveness, OCO should be fully integrated and synchronized with other applicable operational capabilities.

Reliance on Detailed Intelligence. From planning through assessment, OCO relies heavily on detailed intelligence collected through sensitive or unique methods. Intelligence is necessary to understand the adversary's systems, networks, capabilities, and TTPs. A lack of accurate, timely, and actionable intelligence in any of these areas could result in mission failure.

Targeting Lead Times. Because of cyberspace's complex and interconnected nature, targeting for OCO is often more time consuming than traditional operations. Developing initial target folders requires a significant time investment and relies heavily on the DIRCYBERFOR's access to the JFHQ-C. Minor incidents, like a software patch or a hardware update in a targeted network, can invalidate an entire operation, forcing a complete rebuild. Such events can be anticipated but are difficult to plan for in advance due to the specificity required by OCO.

Second- and Third-Order Effects. Effects in cyberspace are not limited by geography and may generate significant second- and third-order effects. Such effects are often difficult to predict. In planning, COA analysis should yield thorough detailed branches and sequels to inform risk awareness and decision-making.

De-confliction with Intelligence Community, Interagency, and Partner Nations. OCO should be thoroughly coordinated among key US and partner nation stakeholders. This coordination should begin early in the planning process to minimize risk to US and partner nation operations.

DEFENSIVE CYBERSPACE OPERATIONS CONSIDERATIONS

Critical Cyberspace Terrain and Key terrain in cyberspace. Effective defense of cyberspace systems and networks requires defenders and planners to have a clear understanding of critical cyberspace terrain and KT-C. With millions of potential targets and threat vectors available to adversaries, it is impossible to identify every potential intrusion or attack. Mission-relevant terrain in cyberspace (MRT-C) is another important cyberspace planning construct. MRT-C is an element of the mission assurance process, and it comprises the resources in cyberspace required to ensure the joint force can complete an assigned mission. DCO planning should focus on critical cyberspace terrain, MRT-C, and KT-C to maximize mission assurance and reduce mission risk by mitigating or eliminating threats to USAF systems. A focus on and clear understanding of the

defended terrain enhances analysts' and operators' ability to identify anomalous activity and respond in a timely manner.

Force Posture. Posturing forces allow operational and tactical planners to focus limited resources on solving the most important defensive challenges. Forces can be postured (or positioned) to defend against threats when tasked to defend against a specific adversary, against tactics when tasked to defend against specific, known cyberspace TTPs, or to protect missions or systems when tasked to defend a specific mission, network, or system. DCO activities against threats in a particular operational area may span across missions, systems, or networks. Forces should be given specific information and guidance on the threat, tactic, or mission to which they are postured.

Hypothesis-based Planning. Adversaries in cyberspace often act covertly. This creates specific challenges for accurately assessing DCO's effectiveness. Hypothesis-based planning mitigates these difficulties by leveraging cyberspace threat intelligence (CTI) and knowledge of adversary TTPs to emulate adversary activities. In situations where adversarial activity is expected but is hidden or obscured, emulation can aid assessment.

Intelligence and Technical Gain or Loss. It may not always be prudent to engage a threat. Monitoring the threat may protect friendly technical capabilities and provide critical insight into an adversary's capability, intent, or TTPs. For this reason, DCO planning and execution should be coordinated with intelligence planners, and consideration given to potential risks associated with intelligence and technical gain or loss.

Law Enforcement, Counterintelligence, Interagency, and Partner Integration. Effective DCO planning requires sharing newly discovered threat information and collaboration in planning and assessing defensive measures. As mission requirements dictate, planners should integrate with law enforcement, counterintelligence, and other relevant elements within the USAF and DoW, such as the AFOSI, Damage Assessment Management Office, the Cyber Resiliency Office for Weapon Systems, or the National Security Agency.

Effects of DCO on the Information Environment. Effective DCO can influence adversaries to change or abort operations targeting USAF systems and networks. What an adversary knows about our defensive plans may shape adversary plans and efforts to engage our networks and systems. Operational security, public affairs, and other OIE can be used to shape the adversary's understanding of our defense, thereby increasing friendly operational advantage.

Timeliness. Technologically sophisticated adversaries may seek to accomplish objectives quickly, emphasizing reduced duration of the targeted system or network intrusion. Once an anomalous activity or intrusion is discovered, priority should be placed on responding to the threat before it becomes difficult to trace. To enable a rapid response during operations, planning efforts should emphasize key areas to focus protection efforts against malware attacks, data loss, or physical damage to USAF capabilities.

Cyberspace Threat Intelligence. Timely, relevant, and actionable intelligence is imperative to the success of DCO missions and should be evaluated early in the mission

planning process. CTI avoid singular or transitory indicators and focus instead on adversary motivations, capabilities, and TTPs.

Coordination. DCO missions lack clear geographic boundaries and often span multiple CCDRs' areas of responsibility. For this reason, activities should be coordinated to minimize impact on global USAF operations. Identification of, and coordination with, affected mission system owners should be addressed early in the planning cycle.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS CONSIDERATIONS

Coordination and De-confliction. For nearly any operation, Airmen worldwide rely on DoDIN to conduct their missions. DoDIN maintenance operations should be coordinated and deconflicted with operational units to the greatest extent feasible to minimize impact on active missions.

Customer Needs and Mission Relevance. DoDIN operations are network and customer focused. Providing dependable communications to USAF users for the conduct of operations is the top priority. Improving the AFIN user experience and ability to conduct USAF operations should be the primary driver behind DoDIN operations.

COORDINATING INTERAGENCY CYBERSPACE OPERATIONS

UNITY OF EFFORT

Efforts across domains should be synchronized to produce an effective whole-of-government approach between DoW cyberspace operations, the US interagency community, allies, and coalition partners. Achieving unity of effort presents specific challenges, often manifesting in planning, including strategic identification, timelines, and authorities.

Strategic identification of aspects of cyberspace operations that may impact another government agency's operations or equities is critical to synchronizing effects. For example, financial information gathered as part of DoW cyberspace operations may also be used by the Department of the Treasury to freeze or otherwise limit access to illicit funds, creating additional effects against potential adversaries.

Timelines can often be difficult to synchronize across executive agencies and departments, primarily because of different internal planning and approval processes. These inefficiencies often extend the timelines required to synchronize efforts.

Authorities can often be confused when sensitive cyberspace operations involve various agencies and departments with competing legal or operational responsibilities. These issues require agencies or departments to deconflict responsibilities for targets and ensure proper support agreements and relationships are established.

THREAT RESPONSE AND TARGETING

TARGETING

A target is an entity that performs a function for the adversary for possible engagement or other action. The words target and targeting in reference to cyberspace operations may take on somewhat different meanings from those in doctrine, based on context. Though the term 'target' may be used colloquially across all cyberspace operations, importantly, targeting, as defined by JP 3-60, only applies to OCO.

Targeting is focused on creating effects against the adversary. Because they are defensively focused, DoDIN operations and DCO do not perform traditional targeting functions. However, each of these operations employs a modified target development process to develop and categorize relevant threats.

AFCYBER supports the joint targeting cycle by providing intelligence, operational teams, and support. There should be no difference between CCMD target development and service component target development functions, whether supporting OCO or another effort. Cyberspace targeting in support of validated CCMD targets should adhere to the same standards and procedures as outlined in JP 3-60, AFDP 3-60, *Targeting*, Chairman of the Joint Chiefs of Staff Instruction 3370.01C, *Target Development Standards*, and any applicable Air Force instructions.

DEFENSIVE CYBERSPACE OPERATIONS

Though not in an offensive context as described above, applicable Air Force instructions and US law (Title 10 USC) direct and authorize targeting of malicious activity and code within the DoDIN. The DCO modified targeting process depends primarily on the weapon system employed against the threat. For example: A kinetic strike on a target may require multiple intelligence disciplines, governed by intelligence collection laws, rules, and procedures, to fully develop the strike package. Even though a CPT may need similar information, those same rules may not apply because a significant portion of it is open-source data. If the DCO is tasked to the USAF, coordination will be through the USCYBERCOM Joint Operations Center and 616 OC. These actions should be coordinated to ensure deconfliction and limit potential fratricide in the cyberspace domain.

INTELLIGENCE SUPPORT TO CYBERSPACE OPERATIONS

DCO and DoDIN operations rely heavily on unclassified data to develop targets, as well as open-source information from industry partners, academia, and organizations focused on CTI, indications, and warnings. USAF cyberspace operations forces conduct cyberspace surveillance and reconnaissance activities to inform and produce intelligence products that support the joint targeting cycle and DCO. CMF also relies on traditional intelligence disciplines to build and validate threat assessments.

CYBERSPACE-INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

Cyberspace-ISR includes intelligence operations required to support OCO, DCO, and to some extent, DoDIN. Unlike traditional ISR, which operates within well-defined physical

boundaries, authorities, and capabilities, Cyberspace-ISR involves an almost infinite menu of possibilities within cyberspace. OCO operations under Title 50 USC have access to a full range of these Cyberspace-ISR tools and capabilities. However, Cyberspace-ISR in support of DCO may be complicated by the source of authority for, or entity performing the surveillance.

Under Title 10 USC authority, DCO operators can scan thousands of DoDIN devices to search for a specific threat or to scan individual network components for indications of compromise. CPTs can then deploy to any location to conduct operations on specific segments of the DoDIN. However, most relevant threat data lies beyond the boundaries of the DoDIN, requiring additional authorities or Title 10 authorization to access.

DCO using Title 50 USC methods and resources should adhere to strict intelligence oversight laws, rules, and regulations, which limit who can search for actionable cyberspace intelligence. Title 50 operations can address imminent threats by detecting network traffic hitting DoDIN boundaries within seconds of attempted malicious connections and activities. The adversary's use of unattributed or obscure connections complicates the collection and analysis of this information.

ASSESSMENT OF CYBERSPACE OPERATIONS

There are three primary types of assessment for cyberspace operations: tactical, operational, and strategic. Tactical assessments are generally performed by the operational C2 element, such as the OC's combat operations division and ISR division (ISRD). These divisions focus on the effectiveness of the tactical operations against the adversary, identifying key indicators of effects or secondary effects. The ISRD also reviews intelligence or other information gathered to determine if additional effects against other targets could be brought to bear. Operational-level assessment of strategy is normally conducted by the operational assessment team within the strategy and resources division, providing insights and recommendations on the types of effects created and if the effects meet the supported JFC's objective. If conducted in support of a combined operation, this assessment is coordinated with the JFC's C2 element for integrated operations. Strategic assessment within the CCMD determines whether the overall CCDR objectives are met.

TACTICAL ASSESSMENT

Assessment planning is a critical component of the planning process and should be conducted early, as objectives, effects, and guidance are developed. During the tactical planning process, operators and planners should develop a tactical assessment plan, outlining the MOEs and measures of performance (MOPs) associated with respective operations and assigned tasks. This information is disseminated via tasking orders to ensure cyberspace forces, mission partners, and tactical planning elements have sufficient information to plan missions effectively and prioritize cyberspace terrain identification.

MOPs for tactical assessment are typically measured using a variety of intelligence and analytical methods, such as signals intelligence (SIGINT) for OCO and local network logs

for DCO, as well as other means. Indirect or secondary effects, such as potential behavioral changes that are difficult to assess in a timely manner, are best assessed at the operational level and above.

OPERATIONAL-LEVEL ASSESSMENT

Operational assessment is a judgment, supported by analysis, of a commander's strategy (ends, ways, means, and risk). At this level, progress toward cyberspace operational and strategic objectives are measured, recommendations for strategy adjustments or future actions beyond re-attack are made, and complex indirect effects may be evaluated.

Assessment at the operational level focuses on both effects and performance via MOEs and MOPs against an operational task. Operational MOEs are largely similar to those in tactical assessment but often involve longer reporting timelines to assess effectiveness. Operational MOPs are established prior to execution and measured through end of mission reports and tactical assessments from subordinate teams or units. Such measures should be linked to the JFC's approved success criteria.

Given the interrelated and complex nature of cyberspace operations, operational cyberspace planners and analysts should develop an intimate understanding of the linkage between the relevant cyberspace terrain and other supported or dependent operations. For operations supporting theater CCMDs, this often requires direct feedback from theater cyberspace forces.

Operational assessments feed into the larger, more complex strategic assessment process conducted at the CCMD level to determine the operation's effectiveness in achieving strategic or campaign objectives against the associated risk to friendly forces. The cyberspace air component commander is uniquely suited to advise the commander on the proper theater-wide balance between OCO and DCO, and strategic, operational, and tactical applications to best accomplish the JFC's objectives.

APPENDIX A: POLICY, DOCTRINE, AND AUTHORITIES RELATED TO CYBERSPACE OPERATIONS

The USAF carefully examines US National, DoW, and USAF policies, domestic and international laws, and international obligations, where applicable, when conducting cyberspace operations to meet the requirements outlined in the National Security Strategy, National Defense Strategy, and National Military Strategy. This section captures the overarching national and DoW cyberspace operations policies.[16]

National-Level Documents	
National Security Strategy of the United States of America, November 2025	The *National Security Strategy of the United States of America* is a document prepared periodically by the Executive Branch of the US government for Congress that outlines the major national security concerns of the US and how the administration plans to deal with them. The legal foundation for the document is spelled out in the Goldwater-Nichols Act. The document is purposely general in content (in contrast with the *National Military Strategy* [NMS]) and its implementation relies on elaborating guidance provided in supporting documents (including the NMS).
FY2022 National Defense Authorization Act (NDAA), Section 1527, Cyber Data Management, 27 December 2021	Addresses roles and responsibilities for USCYBERCOM to acquire and use data for the conduct of offensive cyber, defensive cyber, and DoDIN operations.
President Trump's Cyber Strategy for America, March 2026	The 2026 strategy outlines six pillars of action: 1) Shape Adversary Behavior, 2) Promote Common Sense Regulation, 3) Modernize and Secure Federal Government Networks, 4) Secure Critical Infrastructure, 5) Sustain Superiority in Critical and Emerging Technologies, and 6) Build Talent and Capacity. This represents a shift towards making our networks more defensible and resilient, unleashing innovation, accelerating economic growth, and securing American technology dominance.

[16] For additional information on operational cyberspace operations authorities, see JP 3-12, *Joint Cyberspace Operations*.

National-Level Documents	
United States International Cyberspace and Digital Strategy 2024	The United States International Cyberspace and Digital Strategy outlines the U.S. vision for a global digital ecosystem centered on "digital solidarity.". The strategy focuses on four action areas: (1) promoting an open, inclusive, secure, and resilient digital ecosystem; (2) aligning rights-respecting digital and data governance with international partners; (3) advancing responsible state behavior and countering threats by building coalitions; and (4) strengthening the digital and cyber capacity of partners. It aims to advance economic prosperity, enhance security, and protect democracy and human rights, while countering the influence of authoritarian states in cyberspace.
Presidential Executive Order on Improving the Nation's Cybersecurity, 12 May 2021	Directs the Federal government to improve its efforts to identify, deter, protect against, detect, and respond to malicious cyberspace actions and actors.
National Security Presidential Memorandum-13, (U) United States Cyber Operations Policy, 2018, as amended	Allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace.
NIST Cybersecurity Framework 2.0 February 2024	Version 2.0 expands the scope to all organizations and places increased emphasis on cybersecurity governance, supply chain risk management, and cybersecurity measurement. It also introduces a new "Govern" function.

Department of War Documents	
2023 Department of Defense Cyber Strategy (Summary)	The 2023 DoD Cyber Strategy Summary discusses: Achieving enduring advantage in cyberspace, integrating cyber across all warfighting domains, and building a resilient cyber ecosystem. This indicates a shift towards long-term competitive advantage and domain integration.
Unified Command Plan (UCP), 25 April 2023 with Change 2 dated May 2025	The UCP assigns USCYBERCOM the mission of synchronizing planning for cyberspace operations, in coordination with other CCDRs, the services, and, as directed, other US government agencies; execution authority for selected cyberspace operations.

Department of War Documents	
Secretary of Defense Memo on Department of Defense Cyberspace Operations Forces, 24 July 2025	This memorandum defines "Department of Defense Cyberspace Operations Forces (DoD COF)." DoD COF is interchangeable with the term "cyberspace forces" and refers to any forces in any DoD Component (as defined in the DoD Dictionary of Military and Associated Terms) that plan, conduct, or enable Offensive Cyberspace Operations, Defensive Cyberspace Operations, or DoDIN Operations.
DODD 3600.01, *Information Operations*, 4 May 2017	Covers some of the computer network aspects of cyberspace operations, classifying them as part of information operations. 3600.01 discusses “computer network operations,” comprised of “computer network attack,” “computer network defense,” and “computer network exploitation,” but does not discuss networks or cyberspace operations in a more holistic sense. Some further guidance may be found in the *2023 Department of Defense Cyber Strategy*, but the details are not provided in the summary.
DODD 3020.40, *Mission Assurance (MA)*, 11 September 2018	Establishes policy and assigns responsibilities to meet the goals of refining, integrating, and synchronizing aspects of DOD security, protection, and risk-management programs that directly relate to mission execution as described in the DOD Mission Assurance Strategy and Mission Assurance Implementation Framework. Maintains a Defense Critical Infrastructure (DCI) line of effort within mission assurance to sustain programming, resources, functions, and activities supporting those responsibilities formerly under the Defense Critical Infrastructure Program (DCIP).
DOD Instruction (DODI) 8500.01, *Cybersecurity*, 7 October 2019	Establishes policy and assigns responsibilities for the DOD cybersecurity program through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DODI 8530.01 *Cybersecurity Activities Support to DoD Information Network Operations*, 25 July 2017	Establishes policy, definition, and responsibilities to protect DOD information systems and computer networks against unauthorized activity, threats, or vulnerabilities.
DODI 8410.02, *Support to DOD Information Network Operations*, 8 December 2021	Incorporates and cancels DOD chief information officer Guidance and Policy Memoranda No. 10-8460 and No. 4-8460. Establishes policy and assigns responsibilities for implementing and executing NetOps, the DOD-wide operational, organizational, and technical capabilities for operating and defending the GIG. Institutionalizes NetOps as an integral part of the GIG.

Department of War Documents	
Deputy Secretary of Defense Memo, Satellite Communications Segment of the DOD Information Network, 11 January 2021	Addresses how all of DOD SATCOM is within the DoDIN and the relationships between space and cyberspace operations.
DODD 3025.18 *Defense Support of Civil Authorities (DSCA)*, 19 March 2018	Provides guidance for the execution and oversight of DSCA when requested by civil authorities or by qualifying entities and approved by the appropriate DOD official, or as directed by the President, within the US, including the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any territory or possession of the US or any political subdivision thereof.
DODI 3025.21 *Defense Support of Civilian Law Enforcement Agencies*, 8 February 2019	Establishes DOD policy, assigns responsibilities, and provides procedures for DOD support to Federal, State, tribal, and local civilian law enforcement agencies, including responses to civil disturbances within the US, including the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any territory or possession of the US or any other political subdivision thereof.
JP 3-12, *Joint Cyberspace Operations*, 19 December 2022	This publication provides doctrine for cyberspace operations planning, preparation, execution, and assessment in support of joint operations.
JP 3-04, *Information in Joint Operations*, 14 September 2022	This publication provides doctrine for OIE planning, preparation, execution, and assessment in support of joint operations.
JP 3-55, Joint Operations Security, 20 February 2025	This publication provides doctrine for planning, preparing, executing, and assessing operations security in joint operations, with an increased emphasis on cyberspace, information operations, and emerging technologies.
JP 3-60, *Joint Targeting*, 20 September 2024	This publication provides doctrine for joint targeting planning, preparation, execution, and assessment in support of joint operations.
JP 6-0, *Joint Communications*, 4 December 2023	This publication is the keystone document for the communications system series of publications. It provides fundamental principles and guidance to plan, execute, and assess communications system support to joint operations.

Department of the Air Force Documents	
AFDP 3-13, *Information in Air Force Operations*, 1 May 2025	This AFDP establishes doctrinal guidance for information in USAF operations and details the use of cyberspace operations to conduct OIE. Other AFDPs, such as, AFDP 3-61, *Public Affairs Operations,* and AFDP 3-85, *EMSO* also discuss OIE as they apply to those specific airpower functions.
Department of the Air Force Policy Directive (AFPD) 17-2, *Cyber Warfare Operations*, 27 October 2020	Establishes USAF policy for planning and executing operations to create offensive and defensive effects in cyberspace and for providing communications capability to warfighting forces under proper DOD authorities. Cyberspace is critical to all Department of the Air Force operations and cyberspace warfare operations are key to enabling successful multi-domain operations while supporting Combatant Command objectives. Assigns the responsibilities for cyberspace operations to specific deputy chiefs of staff: ✪ Cyberspace ISR to Headquarters Air Force (HAF) A2. ✪ DCO-IDM, DCO-RA, and C2 to HAF A3 and A6. ✪ USAF cyberspace domain policy and guidance to the Office of the Chief Information Officer (CISO), Department of the Air Force.

United States Code-based Authorities

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of U.S. government portion of cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip, U.S. forces to conduct military operations in cyberspace
Title 18	*Crimes and Criminal Procedures*	Federal offenses	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and DSCA training and operations in the U.S.	Army National Guard, Air National Guard	Domestic consequence management when in a Title 32 status
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All federal departments and agencies	Establish and enforce standards for acquisition and security of IT
Title 44	*Public Printing and Documents*	All federal agencies	All federal departments and agencies	Information security and information resource management
Title 47	*Tele-communications*	All federal agencies	All federal departments and agencies	Use of the electromagnetic spectrum
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, services, and agencies under the DOD and intelligence community aligned under the Office of the Director of National Intelligence	Secure U.S. interests by conducting military and foreign intelligence operations in cyberspace

APPENDIX B: ADDITIONAL AIR FORCE CYBERSPACE ROLES AND RESPONSIBILITIES

SAF/CA–PRINCIPAL CYBER ADVISOR

SAF/CA is the Principal Cyber Advisor to SecAF on all cyber matters and is responsible for advising the SecAF, CSAF, and Chief, Space Operations (CSO) on the implementation and execution of the Department of War Cyber Strategy within the DAF. SAF/CA's key focus areas are recruitment, resourcing, and training of military cyberspace operations forces, acquisition of offensive, defensive, and IT capabilities, and evaluating and improving DAF culture of cybersecurity accountability.

SAF/CN-CHIEF INFORMATION OFFICER

SAF/CN serves as the senior technical advisor to the SecAF, CSAF, CSO, and senior USAF leadership on IT, Cyberspace, and national security systems. SAF/CN provides oversight of the DAF IT portfolio, including the investment strategy, networks, and network-centric policies, communications, information resources management, information assurance, and other related matters. Other responsibilities include delivering enterprise architecture, enforcing the Freedom of Information Act and Privacy Act, integrating DAF warfighting and mission support capabilities by networking air, space, and terrestrial assets, and shaping strategy and policy for all cyberspace security operations and support activities.

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

The DAF Office of the Chief Information Security Officer (CISO) serves as the advisor for SAF/CN on cybersecurity policy, cybersecurity programs, and cyber force development, risk management, and cybersecurity for information systems, weapon systems, and OT supporting military cyberspace operations. The CISO's mission is to ensure the effectiveness of the USAF's five core missions by increasing the cybersecurity and resiliency of systems and information. The CISO facilitates risk management decisions by:

- Creating policy for enterprise cybersecurity and cybersecurity risk management.
- Overseeing the implementation of cybersecurity controls.
- Maintaining, monitoring/reporting, and enforcing compliance with US, DoW, and USAF cybersecurity policies.
- Advocating cybersecurity issues within the USAF corporate process.

HAF A3

The HAF A3 is the USAF's Deputy Chief of Staff for Operations. HAF A3 is responsible for the development and implementation of policy directly supporting global operations, force management, training, and readiness of air and cyberspace forces.

HAF A6

The HAF A6 is the USAF's Deputy Chief of Staff for Warfighter Communications and Cyber Systems. HAF A6 is responsible for guidance, oversight, and advocacy of USAF warfighter command, control, communications, and cyber systems implementation.

AIR FORCE MAJOR COMMAND A6 DIRECTORATES

Major command (MAJCOM) A6 manage and provide support for command-unique programs, systems, and equipment. They coordinate policy, procedures, and technical orders affecting cyberspace support activities. MAJCOM A6 operate as liaisons between 16 AF and individual communications squadrons and installations. MAJCOM A6 prioritize actions within their respective MAJCOMs and coordinate with the 616 OC and 16 AF/A6 to appropriately posture resources to accomplish MAJCOM A6 priorities.

MAJCOM communication coordination centers (MCCC) liaise with operations centers. They provide daily DoDIN operations priorities on behalf of the MAJCOM A6 to give commanders SA of MAJCOM-unique system availability and compliance with network taskings. The MCCC tracks, assigns, and monitors cyberspace orders issued by or through operations centers. The MCCC provides updates and advises commanders on MAJCOM network status and operational impacts of cyberspace orders to component missions.

AIR COMBAT COMMAND

ACC organizes, trains, and equips USAF cyberspace forces to conduct sustained operations in and through cyberspace. It serves as the lead MAJCOM for USAF cyberspace procedures and concepts of operations. The ACC commander exercises ADCON of 16 AF and specifies elements of ADCON over activated USAF reserve cyberspace forces assigned or attached to USCYBERCOM. ACC supports the cyberspace domain by providing USAF forces to AFCYBER, through 16 AF, which then presents forces to the Joint Force to establish, maintain, operate, and defend USAF cyberspace components, exploit adversary vulnerabilities, attack adversary systems, and provide C2 for assigned and attached cyberspace forces.

AIR NATIONAL GUARD READINESS CENTER

The Air National Guard Readiness Center (ANGRC) organizes, trains, and equips all ANG cyberspace forces and retains ADCON over all Air National Guard personnel regardless of status. Operational control (OPCON) is transferred to the relevant CCDR upon activation or mobilization.

AIR FORCE CYBERSPACE OPERATIONS SQUADRONS

USCYBERCOM's efforts to establish the CMF, which includes CPTs, aim to address cyberspace threats to the joint force. Joint priorities do not always align with USAF priorities. USAF cyberspace operations squadrons address the need for an organic, wing level organization to enable mission assurance of specific weapon systems and critical infrastructure resiliency at the base or wing level. MDTs provide mission assurance

capabilities to their associated base or wing level assets at the direction of their respective Wing or AOC Commander. MDTs complement enterprise-level DCO units by providing SA and expertise in their local KT-C. Information and data fed from MDTs to enterprise-level DCO units support analysis of enterprise-level trends and execution of solutions that may transcend the local MDT's scope of responsibility.

DIRECTOR OF CYBERSPACE FORCES

Given the dependence on cyberspace, JFACCs require a single focal point for planning, developing, and integrating OCO, DCO, and DoDIN operations across all domains. To meet this need, the USAF utilizes a DIRCYBERFOR to bridge the gap between a JFACC and the cyberspace air component commander.

A DIRCYBERFOR's three primary roles supporting a JFACC and cyberspace air component commander:

- Advise and serve as the single point of contact for SA of full-spectrum cyberspace operations within the operational environment.
- Advocate for cyberspace operations support and integration of cyberspace operations across all domains.
- Serve as the primary conduit to external entities (ACC, AFCYBER, other SCCs, CO-IPE, Defense Information Systems Agency, CCMD staffs, Joint Cyber Center), for cyberspace support to CMF and AOC cyberspace operations and priorities.

AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

The AFOSI is a federal law enforcement and counterintelligence agency responsible for conducting criminal and counterintelligence investigations and operations, specialized investigative activities, protective service operations, and integrated force protection for the DAF. As part of its mission, AFOSI conducts cyberspace intrusion investigations and operations to identify, exploit, and neutralize criminal, terrorist, and intelligence threats. AFOSI is the sole USAF organization authorized to employ law enforcement and counterintelligence authorities and capabilities to thwart hostile cyberspace activities by malicious cyberspace actors. Threat actors who have committed actions in violation of US law, including intrusions into DoDIN, or execution of malicious code in, through, or against such systems, fall within AFOSI's purview. All appropriate USAF elements should notify AFOSI of any indicators of such activity. AFOSI works closely with AFCYBER forces, domestic law enforcement and counterintelligence agencies, and foreign partners to pursue and prosecute threats.

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

Department of Defense Cyber Crime Center (DC3) supports DAF cyberspace operations through its digital forensics analysis, cyber threat analysis, and vulnerability management. DC3 provides technical and all-source intrusion and forensics analysis of digital devices and media, cyber threat reporting, and cyber threat information sharing in support of the Defense Critical Infrastructure, law enforcement and counterintelligence investigations

and operations, the US Intelligence Community, and federal agencies conducting cyberspace operations and national cyber incident response. In support of the DoW Cyber Strategy, the DC3 VDP identifies, notifies, and rectifies newly discovered DoDIN vulnerabilities. The DC3 Cyber Training Academy provides specialized cyber and investigative training to cyberspace operations forces in the areas of digital forensics, malware analysis, and cyber investigative techniques and procedures.

REFERENCES

All websites accessed 20 April 2026.

US AIR FORCE DOCTRINE: *https://www.doctrine.af.mil/*

- AFDP 3-60, *Targeting*
- AFDP 3-85, *Electromagnetic Spectrum Operations*

JOINT DOCTRINE

- JP 3-0, *Joint Campaigns and Operations*
- JP 3-04, *Information in Joint Operations*
- JP 3-12, *Joint Cyberspace Operations*
- JP 3-30, *Joint Air Operations*
- JP 3-60, *Joint Targeting*
- JP 5-0, *Joint Planning*
- JP 6-0, *Joint Communications*

MISCELLANEOUS PUBLICATIONS

- *President Trump's Cyber Strategy for America (2026)*
- *Secretary of Defense Memorandum on Department of Defense Cyberspace Operations Forces, 24 July 2025*
- Department of the Air Force Policy Directive 17-2, *Cyber Warfare Operations*
- CJCSI 3370.01, *Target Development Standards*