AIR FORCE DOCTRINE PUBLICATION 3-12

CYBERSPACE OPERATIONS

U.S. AIR FORCE

1 February 2023

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

Table of Contents

"The Air Force organizes, trains, and equips forces to be an air component to a joint force commander (JFC). As part of the joint force's air component, our forces must be prepared to accomplish JFC objectives**.** The air component commander's administrative authorities are derived from Title 10, U.S. Code, and exercised as the commander, Air Force forces (COMAFFOR). The air component commander's operational authorities are delegated from the JFC and exercised as both the COMAFFOR, over Air Force Forces, and as the functional joint force air component commander (JFACC), over joint air forces made available for tasking. Thus, the air component commander leads Air Force forces as the COMAFFOR and the JFC's joint air operations as the JFACC. This duality of authorities is expressed in the axiom: Airmen work for Airmen and the senior Airman works for the JFC."

-- Air Force Doctrine Publication (AFDP) 1, *The Air Force*

For simplicity, the Air Force service component commander (COMAFFOR) to the Joint Force Headquarters-Cyber (JFHQ-C) will be referred to as the "cyberspace air component commander" throughout this AFDP.

CHAPTER 1: AIR FORCE CYBERSPACE OPERATIONS

We must train Airmen to bring air, space, and cyber capabilities together with all the other elements of a strategic military campaign…cyber forces protect the nation every day…and the Air Force is central to the way the nation operates relative to defending the networks and having those capabilities available to a president.

-- General David Goldfein, 21st Chief of Staff, United States Air Force

Cyberspace is a global domain within the information environment (IE) consisting of the interdependent networks of information technology 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 during cooperation, supporting Air Force 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 US national interests.

Cyberspace operations create effects along lines of operation and lines of effort consistent with 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 (DOD) Information Network (DODIN). Military operations in cyberspace are organized into missions, through a combination of actions, that create effects to achieve a commander's objectives. Air Force cyberspace forces support these objectives through the conduct of offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD information network (DODIN) operations.

All Air Force 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 and near-peer adversaries. Because of cyberspace's complexity, global superiority is not achievable. In some cases, even localized superiority may be impractical. To ensure success in joint all-domain operations (JADO), commanders should expect contested cyberspace operations and account for anticipated capabilities degradation.

UNDERSTANDING CYBERSPACE

Cyberspace is unlike the naturally-bounded domains of air, land, maritime, and space. To persist, cyberspace requires continued attention from humans. 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 for activities in the other domains, and activities in the other 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, and speed, and leverage greater bandwidth. 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.[1] Cyberspace-enabled capabilities are essential elements of military operations—critical enablers of all-domain synergistic effects.

CYBERSPACE OPERATIONS, THE INFORMATION ENVIRONMENT, AND INFORMATION WARFARE

For the USAF, cyberspace operations are considered one of six principle information warfare (IW) capabilities presented to the joint force to conduct and support operations in the information environment (OIE)[2]. 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. Cyberspace operations can be conducted independently or synchronized, integrated, and deconflicted with other information capabilities and activities for more effective OIE.[3]

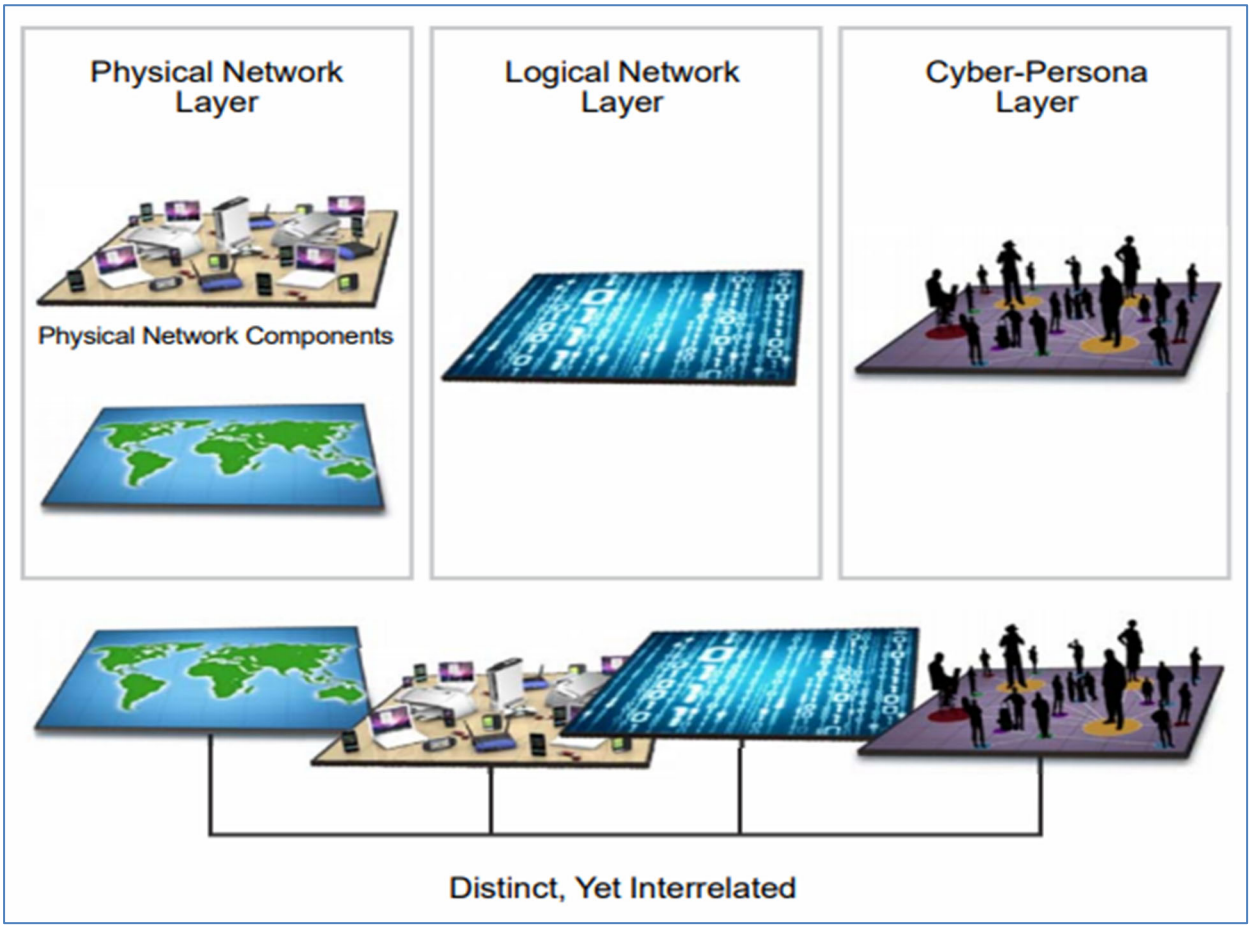
Cyber-enabled OIE Against ISIS

Integrating cyberspace operations with the employment of other information capabilities 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.

[1] For additional information on the "Physical, Syntactic, and Semantic layers of Cyberspace" see *Conquest in Cyberspace*," Libicki, Martin C., RAND Corporation, Cambridge University Press, 2007.
[2] 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.
[3] JP 3-12. *Joint Cyberspace Operations*.

THE OPERATIONAL ENVIRONMENT

The Cyberspace Layer Model. To aid understanding and assist planning and execution of cyberspace operations, JP 3-12 describes the cyberspace environment by presenting the cyberspace layer model—constituted by three interrelated layers: physical network, logical network, and cyber-persona. Varying characteristically, each layer represents different aspects of cyberspace from which cyberspace operations should be planned, conducted, and assessed.



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

The **physical network layer** consists of the information technology (IT) devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components. The physical network also includes hardware and infrastructure (e.g., computing devices, storage devices, network devices, and network links [wired and wireless]). 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.

The **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 addressed logically and exchange or process data. Modern cloud-based networks offer an example. Though they exist on multiple servers in various physical locations and consist of numerous dispersed components, from a logic perspective, they are viewed and function as a single entity. Other examples are the DOD's Nonclassified Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol 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.

The **cyber-persona layer** is 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 identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, 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 in various 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 attributing responsibility for cyberspace activities difficult.

Contested Cyberspace. A "contested cyberspace environment" involves circumstances in which 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 usage, 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 (JP 3-12). In cyberspace, it may only be necessary to maintain a secure presence on a particular location, or in 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 communications, key waypoints for observing incoming threats, launch points for cyberspace attacks, and mission-relevant cyberspace terrain related to critical DODIN connected assets.

The Air Force may not own, control, or have access to the cyberspace terrain needed to conduct missions. To prepare, the Air Force 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 in combination 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. Timelines for enacting planned cyberspace schemes of maneuver will vary according to mission requirements and the commander's accepted level of risk.

Cyberspace Infrastructure Relationships. The Air Force 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 and create vulnerabilities or cause friction and confusion. In response, DOD policies, memorandums of agreement, other coordination measures, and technical plans address this by delineating cyberspace by geographic regions and situations. The Air Force 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 describes a level of influence in the domain relative to that of an adversary. It can be categorized as parity, superiority, or supremacy, although the latter is probably not achievable in cyberspace. Control can be achieved through many approaches, such as persistent engagement (which seizes and maintains the initiative), continuous assessment and management of risk 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 JFC's 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. Though desirable, achieving cyberspace supremacy in any operation is probably unattainable. Rather, 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 in which no force has 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 Supremacy**: A degree of cyberspace control that permits operations wherein the opposing force is incapable of effective interference. Interference may still exist but can be easily countered or has little or no effect on operations.

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.[4] 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 friendly cyberspace capabilities and protect data, networks, devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.
- **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 CCDR or national objectives. OCO may exclusively target enemy cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading denial effects into the physical domains to affect 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.[5]

[4] JP 3-12.
[5] JP 3-12.

Air Force cyberspace mission forces (CMF) conduct OCO, when directed, in support of combatant commander (CCDR) or national mission objectives. OCO consist of a range of operations enabled by intelligence, surveillance, and reconnaissance (ISR), cyberspace operational preparation of the environment (C-OPE), and cyberspace effects operations. OCO is planned, coordinated, and executed through either a 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 to ensure authorities are in place and deconfliction actions occur. Authorities for execution of each mission type reside at different levels including Commander, USCYBERCOM (CDRUSCYBERCOM); the Secretary of Defense (SecDef), or the President.

- **Cyberspace ISR:** A military intelligence action conducted by the JFC, authorized by an execute order (EXORD). Cyberspace ISR is normally conducted to gather intelligence which may be required to support planning or execution of cyberspace operations.

- **C-OPE:** consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. This mission includes identifying data, software, system / network configurations and identifiers, or physical structures connected to, or associated with, the network.

- **Cyberspace Effects Operations:** Cyberspace actions that create various direct effects in cyberspace (i.e., denial, degradation, disruption, or destruction) and manipulations that can manifest as denial actions in the physical domains.

OCO may create effects on 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, logistics nodes, etc. The employment of OCO should be viewed as an application of military force. Regarding the use of force, some OCO missions may rise to the same level as physical damage or destruction of adversary systems and equipment. OCO missions require careful consideration regarding 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 from imminent or active threats in cyberspace. 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 DOD cyberspace from all threats **in advance** of any threat activity. The Air Force organizes defensive cyberspace 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.

Air Force DCO actions generally consist of protective, investigative, or response activities conceptually similar to counterintelligence.

- **Protective DCO** activities minimize risk to Air Force networks, systems, and data through threat-informed cyberspace security actions.
- **Investigative DCO** activities identify, illuminate, and characterize threats that have breached Air Force networks and provide options for response.
- **Response DCO** activities are conducted by cyberspace operations forces, on or off DODIN systems in friendly- or adversary-controlled cyberspace terrain.

When a protective, investigative or response DCO activity is conducted on friendly cyberspace terrain, it constitutes a **DCO-internal defensive measures (DCO-IDM)** mission. When a DCO response 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 that result from misinterpretation of data. Deliberate operational assessment of the mission and terrain being protected, and the defensive cyberspace capabilities available, provides operational commanders an accurate account of cyberspace risks to the mission.

DOD INFORMATION NETWORK OPERATIONS

Air Force DODIN operations are standing missions that involve day-to-day security and maintenance operations, 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 Air Force missions. In addition to regular security efforts, effective response to intrusions or other malicious activity on the Air Force portion of the DODIN—the Air Force Information Network (AFIN)[6]—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.

[6] 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." Derived from JP 6-0, *Joint Communications System*, and Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*.

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 various 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 ensure AFIN vulnerabilities are minimized.

CYBERSPACE OPERATIONS CHALLENGES

COMMERCIAL OFF-THE-SHELF TECHNOLOGY

The expanded availability of COTS technology provides adversaries with progressively more flexible and affordable technology that can be adapted for military purposes. Low barriers to entry (low cost, widely availability, etc.) significantly decrease the traditional capability gap between the US and its adversaries. Likewise, as these technologies rapidly advance, adversaries are able to 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 Air Force acquisitions, contracting, and operational planning efforts to align and keep pace with these changes increases the likelihood an adversary may exploit an unmitigated vulnerability.

Private industry is the primary driver of technological advancements. Because of this, the vast majority of Air Force cyberspace operations components and capabilities are COTS. Such dependence 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. 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 take advantage of 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 and 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 fix an attacker within cyberspace. Successful attribution involves significant analysis and often requires collaboration with non-DOD agencies and organizations.

In addition to the factors above, the nature of attribution varies according to specifics of what can be identified. The identification of an IP address, location, or device, etc., may be enough for some actions, such as establishing blacklists. 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 which requires constant attention and mitigation. Risks and vulnerabilities are often created by the lack of analyzed intelligence and interdependencies created through systems networking and integration. Systems may also be vulnerable to electronic attack and difficult to defend structurally. Due to the domain's nature, a risk assumed by one is potentially assumed by all. Some examples of well-known vulnerabilities in cyberspace operations can be found in the declassified 2006 *National Military Strategy for Cyberspace Operations* (NMS-CO). Operations like those planned and executed by Joint Task Force Ares test our integration means and identify vulnerabilities within a difficult contested cyberspace environment. However, mitigation measures can decrease risk levels. Examples of risk mitigation can include implementation of firewalls and advanced training, education, 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 have significant impact on 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, anywhere from nation-states to individual actors, to accidents and natural hazards (see JP 3-12). To enable freedom of maneuver in cyberspace, cyberspace operations must reduce or eliminate threats and vulnerabilities and constantly assess, coordinate and deconflict cyberspace operations. In general, cyberspace threats are divided into two major categories: malicious cyberspace activity and adverse cyberspace activities.

- **Malicious Cyberspace Activities:** Activities, other than those authorized by or in accordance with 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 or free, allowing even unsophisticated threat actors to acquire advanced capabilities at little to no cost. Because of the low barriers to entry and the potentially high payoff, an increasing number of adversaries use cyberspace capabilities to attempt to negate US advantages.

- **Adverse Cyberspace Activities (ACA):** The Air Force term for friendly actions or natural events, disasters, or accidents that inadvertently achieve the same effects as malicious cyberspace activity; providing adversaries the opportunity to capitalize on vulnerabilities and infrastructure degradation. 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 cyberspace 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 where individuals (mission or system owners and operators) can, with or without malign intent, become insider threats by executing actions, policies, or changes which adversely affect operations.

U.S. NATIONAL CYBERSPACE POLICY

There are numerous policy documents that establish and support US national cyberspace policy. From the Air Force's perspective, the list below outlines the principal documents and summarizes each policy's significance for cyberspace operations.

Four pillars established by *The National Cyber Strategy of the United States of America*, (Sep 2018):

- Pillar I: Defend the homeland by protecting networks, systems, functions, and data.
- Pillar II: Promote US prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation.
- Pillar III: Preserve peace and security by strengthening the ability of the US—in concert with allies and partners—to deter and, if necessary, punish those who use cyberspace tools for malicious purposes.
- Pillar IV: Expand US influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet.

Four strategic priorities of the NMS-CO[7]:

- Gain and maintain initiative to operate within adversary decision cycles.
- Integrate cyberspace capabilities across the range of military operations.
- Build capacity for cyberspace operations.
- Manage risk for operations in cyberspace.

[7] The 2006 NMS-CO is the only declassified example available for the purposes of this document.

DOD's objectives for cyberspace (*Summary, DOD Cyber Strategy* (2018) [linked in Appendix A]):

- Ensure the joint force can achieve its missions in a contested cyberspace environment.
- Strengthen the joint force by conducting cyberspace operations that enhance US military advantages.
- Defend US critical infrastructure from malicious cyberspace activity that could cause a significant cyberspace incident.
- Secure DOD information and systems against malicious cyberspace activity, including DOD information on non-DOD-owned networks.
- Expand DOD cyberspace cooperation with interagency, industry, and international partners.

DAFPD 17-2 assigns the responsibilities for cyberspace operations to specific deputy chiefs of staff:

- Cyberspace ISR to Headquarters Air Force (HAF) A2/6A.
- DCO-IDM, DCO-RA, and C2 to HAF A2/6C and A3C.
- Air Force cyberspace domain policy and guidance to the Office of the Chief Information Officer (CISO), Department of the Air Force

For additional details, reference Appendix A of this document: "Policy, Doctrine, and Authorities Related to Cyberspace Operations".

CHAPTER 2: ORGANIZATION, ROLES, AND RESPONSIBILITIES

DOD CYBERSPACE OPERATIONS FORCES

DOD cyberspace operations forces are organized into five operational groups:

- **Cyberspace mission forces**
- **Subordinate command elements**
- **DOD component network operations centers and cyberspace security service providers**
- **Special capability providers**
- **Specially designated units**

Additionally, some service cyberspace forces and capabilities are not considered a part of the formal DOD CMF. This includes DOD business function elements; service retained forces (e.g., Air Force mission defense teams [MDTs]); joint cyberspace centers; intelligence units and activities; and US Special Operations Command (USSOCOM) assigned forces.

CYBERSPACE 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. Air Force cyberspace operations forces not actively assigned to a USCYBERCOM mission remain subject to tasking as part of the CMF.

- **Cyber Protection Force:** The CPF, composed of CPTs, conducts cyberspace operations for internal protection of the DODIN or other friendly cyberspace.
- **Cyber National Mission Force:** The CNMF conducts cyberspace operations to defeat significant cyberspace threats to the DODIN and, when ordered, to defeat significant cyberspace threats to the nation. The CNMF comprises various numbered NMTs, associated national support teams, and national-level CPT for protection of non-DODIN blue-force cyberspace terrain.
- **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 associated combat support teams.

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.
- JFHQ-DODIN.
- JFHQ-C:
  - Most services provide a JFHQ-C to USCYBERCOM, such as the JFHQ-C (AF) (AFCYBER). Additionally, JFHQ-DODIN, in coordination with all CCDRs and other DOD 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 aligned 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. JFHQ-C (AF) is aligned to support US Space Command, US Transportation Command, US Strategic Command, US European Command, 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).
- Service cyberspace component (SCC)[8] HQs' CO-IPEs:
  - A CCDR's staff is tasked to execute cyberspace operations to secure, defend, and operate within DODIN segments that affect the mission. However, CCMDs

[8] Throughout this document SCC refers to the service cyberspace component. However, 16 AF/CC also serves as the USAF service cryptologic component commander. The service cryptologic component also uses the acronym SCC.

have not historically had a pool of cyberspace experience to pull from. To fill this deficiency, CO-IPEs provide expertise and reach-back capability, serving as a liaison between USCYBERCOM and the supported CCDR. CO-IPEs are constituted by USCYBERCOM, JFHQ-DODIN and JFHQ-C personnel, and are fully integrated with each CCMD staff. CO-IPEs provide CCDRs with cyberspace operations planners and subject matter experts to support 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.

DOD COMPONENT NETWORK OPERATIONS CENTERS AND CYBERSPACE SECURITY SERVICE PROVIDERS

DOD component network operations centers and cyberspace security providers consist of units designated by the Secretaries of Military Departments, in coordination with other DOD component heads, to conduct cyberspace operations in support of DODIN operations, including DCO-IDM. They also include service forces dedicated to managing the Joint Cyber Common Access Platform.

SPECIAL CAPABILITY PROVIDERS

Special capability provider is the designation given to any force purposely organized to execute OCO or DCO-RA.

SPECIALLY DESIGNATED UNITS

Specially designated units are designated by the President or the SecDef, as part of the DOD cyberspace operations forces, to conduct activities in support of specific cyberspace operations.

The roles and organizations detailed above comprise a majority of the significant offices and organizations that play an active role in daily cyberspace operations. However, this list is not exhaustive. For detail and description of additional Air Force positions and their respective cyberspace roles and responsibilities, refer to *Appendix B: "Additional Air Force Cyberspace Roles and Responsibilities."*

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 attack. 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

authority for cyberspace operations (DACO)—the authority to issue orders and directives to all DOD components for global DODIN operations and DCO-IDM. JFHQ-DODIN exercises DACO over all DOD components, agencies, and field activities. As DODIN operational area commanders, SCC commanders exercise 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.

SERVICE CYBERSPACE COMPONENTS

SCC commanders exercise administrative control (ADCON)[9] of assigned forces and serve as the subject matter expert for service-specific cyberspace capabilities, forces, and operations. In coordination with USCYBERCOM, they are responsible for developing tactics, techniques, and procedures (TTPs) and capabilities to support and enable accomplishment of cyberspace missions. SCCs presented to USCYBERCOM include:

- 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).

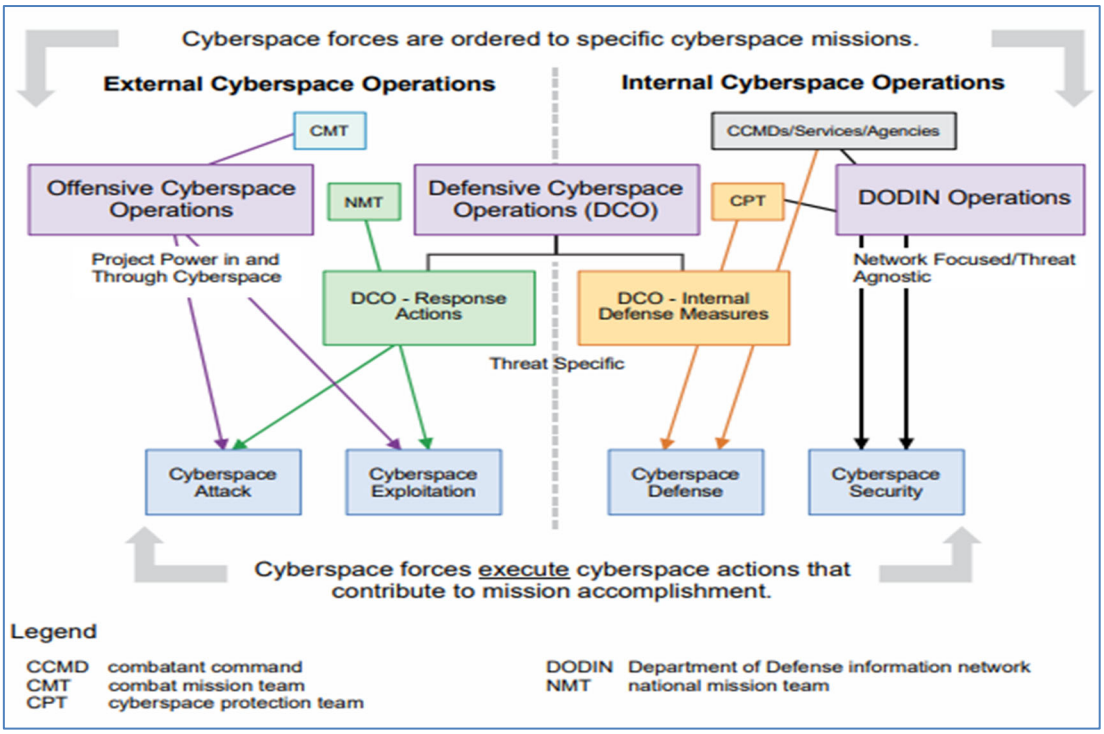
16TH AIR FORCE / AFCYBER

The USAF's SCC, AFCYBER is aligned with 16 AF, the component numbered air force, and its commander is dual hatted as the cyberspace air component commander; the sole entity responsible for presenting Air Force cyberspace forces to USCYBERCOM. The cyberspace air component commander is the senior Air Force warfighter for employment of assigned and attached Air Force 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 Air Force 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; maintains and defends Air Force portions of DODIN; and provides, establishes, and maintains a secure and defensible network to support global Air Force functions.

[9] 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.

- **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 Air Force systems; maintains and defends the Air Force portion of the DODIN; exercises OPCON of service CPTs; provides, establishes, and maintains a secure and defensible network to support Air Force operations around the world.
- **CDRJFHQ-C (AF):** Enables synchronization of cyberspace operations C2 and reports directly to CDRUSCYBERCOM under combatant command (COCOM) authority. Analyzes, plans, and executes CYBERCOM 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 616th OC translates USCYBERCOM global, and supported CCDR theater objectives, priorities, and intent into a coherent, executable plan for Air Force 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 cyberspace operations effectiveness. The cycle can be lengthened or shortened as needed, to synchronize with a theater's battle rhythm.

Detailed plans required to effectively employ cyberspace capabilities are produced through the cyberspace tasking cycle, culminating with publication of the daily CTO. The

CTO, derived from CDRUSCYBERCOM and supported JFCs, 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 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 assigned JFHQ-C, to synchronize the cyberspace tasking cycle with that theater's planning and tasking processes, including synchronization of the CTO and ATO. In line with the cyberspace air component commander's guidance, the 616 OC aids development of 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 operations) under one command offers distinct advantages, doing so also poses significant challenges identified below:

- **Varied Relations for Global Support:** AFCYBER executes a global mission through support relationships with various CCMDs and organizations that vary significantly.
- **Varied 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., an A3 for DCO / DODIN operations and a J3 for OCO) present challenges for articulating unit tasking authorities.
- **Situational Awareness (SA**): 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 Network Warfare Squadron (33 NWS). 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. Under Title 50 USC or, when applicable, Title 10 USC, the authority to conduct OCO resides with CDRUSCYBERCOM. 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 commander needs and AFCYBER-directed activities.

- **Security Classification:** Ideally, a CTO should be presented daily on a single document. However, due to varying classification levels, the Cyber C2 Mission System produces a CTO on SIPRNet, whereas necessary portions of cyberspace operations are disseminated via USCYBERCOM-mandated channels on the Joint Worldwide Intelligence Communications System (JWICS).

LEGAL AUTHORITIES AND CONSIDERATIONS

Generally, Airmen assigned duties, responsibilities, and tasks for cyberspace operations are governed by Title 10, United States Code (USC*)—Armed Forces*, or Title 50 USC—*War and National Defense.* In some situations, CMF tasked with law enforcement authorities may conduct cyberspace operations under Title 18 USC—*Crimes and Criminal Procedure* (e.g., Air Force Office of Special Investigation). 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) must 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 operate in accordance with the same authority as their active duty counterparts. Alternately, 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 in cyberspace operations for operational lines between civil and military authorities to blur, it does present 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.

Sample 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 Cyber Strategy.
- National Military Strategy.
- National Security Strategy.
- **Presidential Executive Order 14028**, *Improving the Nation's Cybersecurity*, 12 May 2021.
- **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.
- **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.*
- **Directive Type Memorandum 17-007**, Interim Policy and Guidance for Defense Support to 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 particular mission set or capability, the notional tasking cycle for all DOD operations will be derived from planning doctrine described in JP 5-0, *Joint Planning*, the joint targeting cycle as defined in JP 3-60, *Joint Targeting;* and the air tasking cycle outlined in JP 3-30, *Joint Air Operations*.

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 sometimes years of preparation prior to 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)[10]. 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, infrastructure, etc.

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 Air Force's need for information assurance. As a part of a larger networked team, the Air Force should plan and execute in close concert with other services, states, and agencies.

[10] JP 5-0, *Joint Planning*.

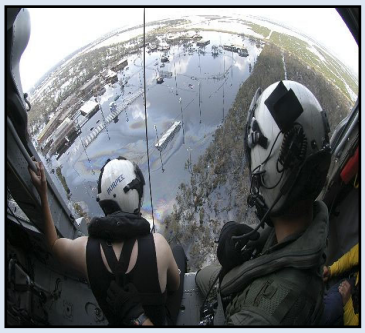
Establishing the Cyberspace Infrastructure in Afghanistan

In 2007, in support of Operation ENDURING FREEDOM, the 3rd Combat Communication Group (3 CCG) deployed to Kabul, Afghanistan and established an enterprise network for Afghanistan's Ministry of Interior (MoI), which provided capabilities such as e-mail, telephone service through "voice over internet protocol" and video teleconferencing capability between the National Police Coordination Center, six joint regional coordination centers, 12 Kabul headquarters buildings, 38 provincial command centers, as well as about 200 other locations like medical and fire stations. Also, 3 CCG provided the infrastructure to allow network technicians to protect MoI's computers against viruses and provided a platform from which they could defend against cyberspace attack.

HOMELAND OPERATIONS

Cyberspace operations support homeland operations, including homeland defense and defense support of civil agencies (DSCA). Once requested and authorized through appropriate authorities, military assistance can be provided similar to direct support. Attack and exploitation operations in a homeland defense scenario may involve complex legal and policy issues. Though these issues do not prevent all cyberspace operations, they will likely temper their applications. DOD forces cannot be used to perform attack or exploit operations on 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, local agencies, non-governmental organizations, and partner nations.

Reconstituting the Cyberspace Infrastructure during Disaster Relief



In 2005, the Gulf of Mexico region was devastated by Hurricane Katrina which destroyed critical infrastructure in Mississippi, Louisiana, and Texas. This disaster displaced tens of thousands of people seeking to escape the impact of the storm. Based on their expertise for extending the cyberspace domain, Air Force combat communications groups deployed throughout the Gulf region to reconstitute the cyberspace domain and allow military and US government organizations to communicate and be connected for situational awareness and C2.

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 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 OCO, DCO, AND DODIN 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 OCO software (tools) to be effective, they must continually evolve to stay ahead of the adversary's ability to defend against them. 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 necessary intelligence for development of 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 for potential loss of intelligence sources or methods.

- **Physical Effects.** OCO, although conducted through cyberspace, may have physical effects as well. 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 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 when compared to 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 produce thorough and 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 government and partner nation operations.

DEFENSIVE CYBERSPACE OPERATIONS CONSIDERATIONS

- **Critical Cyberspace Terrain and KT-C.** 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 Air Force 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 allows 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 they are postured around.

- **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 instead 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 of newly discovered threat information and collaboration on planning and assessment of defensive measures. As mission requirements dictate, planners should integrate with law enforcement, counterintelligence, and other relevant elements within the Air Force and DOD, such as the Air Force 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 Air Force 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 and public affairs can be used to shape the adversary's understanding of our defense, resulting in increased 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 Air Force 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 should shy away from singular or transitory indicators, and focus instead on adversary motivations, capabilities, and TTPs.

- **Coordination.** DCO missions do not have clear geographic boundaries and often span multiple CCDRs' areas of responsibility. For this reason, activities should be coordinated to minimize impact on global Air Force operations. Identification of, and coordination with affected mission system owners should be addressed early in the planning cycle.

DOD INFORMATION NETWORK OPERATIONS CONSIDERATIONS

- **Coordination and De-confliction**. For nearly any operation, Airmen across the globe rely on DODIN to conduct their operational 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 Air Force users for the conduct of operations is the top priority. Improving the AFIN user experience and ability to conduct Air Force 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 DOD cyberspace operations, the US interagency community, allies, and coalition partners. Achieving unity of effort presents specific challenges, often manifested in planning, that include strategic identification, timelines, and authorities.

- **Strategic identification** of aspects of cyberspace operations which may impact another government agency's operations or equities is critical to synchronizing effects. For example, financial information gathered as part of DOD 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 between executive agencies and departments, primarily due to different internal processes for planning and approval cycles. These inefficiencies often extend the timelines required to synchronize efforts.

- **Authorities** can often be confusing 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.

Since they can often create equivalent or complimentary effects against a target, the National Defense Strategy encourages cooperation with allies and partners. For US government entities, unity of effort is derived through national strategy documents approved by

the President. However, achieving unity of effort with allies and partner forces presents additional challenges including treaty requirements, legal agreements, foreign disclosure rules[11], and establishment of common communications standards.

THREAT RESPONSE AND TARGETING

TARGETING

A target is an entity or object 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. As 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 support, intelligence, and operational teams. 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 must 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 mostly on what weapon system is 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 ninety percent of it is open-source data. If the DCO is assigned to the Air Force, coordination will be through the USCYBERCOM Joint Operations Center and 616 OC. These actions must be coordinated to ensure deconfliction and limit potential fratricide in the cyberspace domain.

INTELLIGENCE

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 cyberspace threat intelligence, indications, and warnings. Air Force cyberspace

[11] Department of the Air Force (DAF) Manual 16-201, *DAF Foreign Disclosure and Technology Transfer Program*, and DOD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

operations forces conduct cyberspace surveillance and reconnaissance activities to inform and produce intelligence products that support the joint targeting cycle and DCO. CMF also rely on traditional intelligence disciplines to build and validate threat assessments.

CYBER-INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

C-ISR includes those intelligence operations required to support OCO, DCO, and to some extent, DODIN operations. Unlike traditional ISR, which operates within well-defined physical boundaries, authorities, and capabilities, C-ISR involves an almost infinite menu of possibilities within cyberspace. OCO operations under Title 50 USC. have access to a full range of these C-ISR tools and capabilities. However, C-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 scan individual pieces of the network 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 authorization beyond Title 10 to access.

DCO using Title 50 USC. methods and resources must 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 from network traffic hitting DODIN boundaries seconds after attempted malicious connections and activities are executed. The adversary's use of unattributed or obscure connections complicates how this information can be collected and analyzed.

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 takes place within the CCMD to determine if 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 through 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 changes in behavior that are very difficult to assess in a time-sensitive 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 reported by 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 toward 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 Air Force carefully examines US National and DOD policies, domestic and international laws, and international obligations, where applicable, when conducting cyberspace operations to meet the requirements as outlined in the National Security Strategy, National Defense Strategy and National Military Strategy. This section captures the overarching national and DOD cyberspace operations policies. This section does not address cyberspace operations authorities, please see cyberspace operations authorities in JP 3-12.

National-Level Documents	
National Security Strategy, October 2022	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.
National Cyber Strategy of the United States of America, September, 2018	Covers the necessity for vigilance in cyberspace, many defensive aspects of cyberspace operations, and the general principles that should guide national response to a cyberspace “crisis.”
United States International Strategy for Cyberspace	Covers the goals of the US for the internet on the international stage.
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-Level Documents	
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.
National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity	Optional, 2014.

Department of Defense Documents	
National Military Strategy for Cyberspace Operations (NMS-CO)	The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of Airmen, is fundamental to this approach.
DOD Cyber Strategy and Cyber Posture, 2018	Emphasizes on the use of cyberspace to amplify military lethality and effectiveness; to defend forward by confronting threats before they reach the US networks; proactively engaging in day-to-day great power competition in cyberspace; protecting military advantage and prosperity; recognizing partnerships; contesting the exfiltration of sensitive DOD information; embracing technology, automation and innovation; defending critical infrastructure; and recruiting, developing and managing critical cyberspace talent.
2018 Department of Defense Cyber Strategy (DOD-CS)	The DOD-CS describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The DOD-CS is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of Airmen, is fundamental to this approach.

Department of Defense Documents	
Unified Command Plan (UCP), 13 January, 2021	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.
CJCS Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) v1 31 October, 2005	This document provides a conceptual look at how the NCOE will enhance the overall performance of warfighters at every level. Its focus is supporting a joint task force (JTF), including the JTF commander, JTF mission partners, and warfighters at the "first tactical mile." The goal is for the entire joint force and mission partners to have the technical connectivity and interoperability necessary to share knowledge rapidly and dynamically amongst decision-makers, communities of interest, and others, while protecting information from those who should not have it—all to facilitate the coherent application of joint action.
DOD Directive (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 NMS-CO, but the details are not releasable at this time.
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.

Department of Defense Documents	
DODI 3600.02 *Information Operations Security Classification Guidance*, 6 August, 1998	Provides DOD-level security classification guidance relevant to some cyberspace operations.
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.
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 3-13.3, *Operations Security*, 21 February, 2018	This publication provides doctrine for planning, preparation, execution, and assessment of operations security in joint operations.

Department of Defense Documents	
JP 6-0, *Joint Communications System*, 4 October, 2019	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.

United States Air Force Documents	
HQ Air Force Program Action Directive 07-08 (Change 4), *Phase I of Implementation of Secretary of Air Force Direction to Organize Air Force Cyberspace Forces*, 20 February 2009	Organization of the Air Force's service contribution to cyberspace operations.
AFDP 3-13, *Information in Air Force Operations*, 1 February 2023	This AFDP establishes doctrinal guidance for information in Air Force operations and details the use of cyberspace operations to conduct OIE. Other AFDPs, such as AFDP 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations,* and AFDP 3-61, *Public Affairs Operations* 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 Air Force policy for planning and executing operations to create offensive and defensive effects in cyberspace and for providing communications capability to warfighting forces under proper 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.

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	*Telecommunications*	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/CN - CHIEF INFORMATION OFFICER

The Department of the Air Force Chief Information Officer (SAF/CN) serves as the principal advisor to the SECAF, the CSAF, the Chief of Space Operations, and senior Air Force leadership on IT, Cyberspace, and national security systems. SAF/CN provides oversight of the DAF information technology 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 Freedom of Information Act and Privacy Act laws; 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

Established in 2016, the CISO's mission is to assure the effectiveness of the US Air Force'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 risk management.
- Overseeing the implementation of cybersecurity controls.
- Enforcing compliance of US, DOD, and Air Force policies.
- Advocating cybersecurity issues within the Air Force corporate process.

AIR FORCE MAJOR COMMAND A6 DIRECTORATES

Major command (MAJCOM) A6s manage and provide support for command-unique programs, systems, and equipment. They coordinate policy, procedures, and technical orders affecting cyberspace support activities. MAJCOM A6s operate as liaisons between 16 AF and individual communications squadrons and installations. MAJCOM A6s 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 situational awareness 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 Air Force cyberspace forces to conduct sustained operations in and through cyberspace. It serves as the lead MAJCOM for Air Force cyberspace procedures and concepts of operations. The ACC commander exercises ADCON of 16 AF, and specified elements of ADCON over activated Air Force reserve cyberspace forces assigned or attached to USCYBERCOM. ACC supports all joint warfighters in the cyberspace domain by providing Air Force forces, through 16 AF, to establish, maintain, operate, and defend Air Force 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 is transferred to the relevant CCDR upon activation or mobilization.

AIR FORCE CYBERSPACE OPERATIONS SQUADRONS

Efforts by USCYBERCOM to establish the CMF, which includes CPTs, are aimed at addressing cyberspace threats to the joint force. Joint priorities do not always align with Air Force priorities. Air Force 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 situational awareness and expertise in their local KT-C. Information and data fed from MDTs to enterprise-level DCO units supports analysis of enterprise-level trends and execution of solutions that may transcend the local MDT's scope of responsibility. When necessary, CPTs can be deployed to enhance the Wing's mission assurance capabilities.

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 Air Force 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 situational awareness 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.

OFFICE OF SPECIAL INVESTIGATIONS

The Office of Special Investigations (OSI) is a federal law enforcement and counterintelligence agency with responsibility to conduct criminal and counterintelligence investigations and operations, specialized investigative activities, protective service operations, and integrated force protection for the DAF. As part of its mission, OSI conducts cyberspace intrusion investigations and operations to identify, exploit, and neutralize criminal, terrorist, and intelligence threats. OSI is the sole Air Force 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, to include intrusions into DODIN, or execution of malicious code in, through, or against such systems, fall within OSI's purview. All appropriate Air Force elements must notify OSI of any indicators of such activity. OSI works closely with AFCYBER forces, domestic law enforcement and counterintelligence agencies, and foreign partners to pursue and prosecute threats.

REFERENCES

All websites accessed 1 February 2023.

Doctrine can be accessed through links provided at: https://www.doctrine.af.mil/

US AIR FORCE DOCTRINE

- AFDP 3-60, *Targeting*

JOINT DOCTRINE

Joint Electronic Library (JEL):

https://www.jcs.mil/Doctrine/

JEL+:

https://jdeis.js.mil/jdeis/index.jsp?pindex=2

- 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 System*

MISCELLANEOUS PUBLICATIONS

- Department of the Air Force Policy Directive 17-2, *Cyber Warfare Operations*
- Department of the Air Force Manual 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*
- Department of Defense Directive 5230.11, *Disclosure of classified Military Information to Foreign Governments and International Organizations*