ORGANIZATION OF CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

The Air Force organizes, trains, and equips its cyber forces to support the combatant commanders (CCDRs) and the joint warfighters, and to accomplish Service functions. Joint cyberspace forces are an integral part of military operations, and command relationships are crucial for ensuring timely and effective employment. Commander, US Strategic Command (CDRUSSTRATCOM) advocates, plans, and executes military cyberspace operations and has the responsibility to prioritize, deconflict, integrate, and synchronize military cyberspace operations for current and planned joint operations. The Air Force presents some cyberspace forces to CDRUSSTRATCOM for day-to-day operations via its Service element, 24th Air Force (AFCYBER). US Northern Command (USNORTHCOM) and US Pacific Command (USPACOM) may conduct the civil support and homeland defense (HD) missions with cyberspace operations during critical infrastructure protection.[1] Like all Air Force forces, Air Force cyberspace forces may be assigned or attached to other CCDRs, coalition or joint force commanders, as directed.

United States Strategic Command (USSTRATCOM)

USSTRATCOM is responsible for synchronizing the planning of cyberspace operations.[2] The foundational command relationship for Air Force cyberspace forces under USSTRATCOM,[3] which:

- Directs global information grid (GIG) operations and defense.
- Plans against designated cyberspace threats.
- Coordinates with other combatant commands and appropriate US government agencies prior to the creation of cyberspace effects that cross areas of responsibility (AORs).
- Provides military representation to US national agencies, US commercial entities, and international agencies for matters related to cyberspace, as directed.

[1] See JP 3-27, *Homeland Defense,* 12 July 2007, p. 32.
[2] The phrase "synchronizing planning" pertains specifically to planning efforts only and does not, by itself, convey authority to execute operations or direct execution of operations.
[3] Derived from the 2008 Unified Command Plan.

- Advocates for cyberspace capabilities
- Integrates theater security cooperation activities, deployments, and capabilities that support cyberspace operations, in coordination with the geographic combatant commands (GCCs), and makes priority recommendations to the Secretary of Defense (SecDef).
- Conducts operational preparation of the environment (OPE) and intelligence preparation of the operational environment (IPOE) and, as directed, synchronizes execution with GCCs.
- Executes cyberspace operations, as directed.
- Plans, coordinates, and executes kinetic and non-kinetic global strike as required.

Each of these missions assigned by the Unified Command Plan (UCP) has key functions, roles and responsibilities the Air Force accomplishes in order to support Joint Functional Commands (JFCs).

United States Cyber Command (USCYBERCOM)[4]

Mission: USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense (DOD) information networks and prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/allied freedom of action in cyberspace and deny the same to our adversaries.

Focus: USCYBERCOM fuses the Department's full spectrum of cyberspace operations and plans, coordinates, integrates, synchronizes, and conducts activities to lead day-to-day defense and protection of DOD information networks, coordinate DOD operations providing support to military missions, direct the operations and defense of specified DOD information networks, and prepare to, and when directed, conduct full spectrum military cyberspace operations. The command is charged with pulling together existing cyberspace resources and synchronizing warfighting effects to defend the information security environment.

USCYBERCOM centralizes command of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters the DOD's cyber expertise. USCYBERCOM's efforts support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.

---

[4] Fact Sheets "USCYBERCOM"

Forces: USCYBERCOM is a sub-unified command subordinate to USSTRATCOM. Service elements include:

USAF:	24th Air Force (AFCYBER)
USA:	Army Forces Cyber Command
USN:	Fleet Cyber Command
USMC:	Marine Forces Cyber Command

Air Force Space Command (AFSPC)

AFSPC organizes, trains, and equips Air Force cyberspace forces to conduct sustained operations in, through, and from cyberspace and fully integrates with air and space operations. It serves as the lead major command (MAJCOM) for Air Force cyberspace procedures and concepts of operations. As the Air Force Service component commander to CDRUSSTRATCOM for Air Force cyberspace forces, the commander, AFSPC (AFSPC/CC) exercises administrative control (ADCON) over active component and specified elements of ADCON over activated reserve component Air Force cyber forces assigned or attached to USSTRATCOM. This includes those Air Force forces assigned or attached as part of USCYBERCOM under 24th Air Force (24 AF). Operational control (OPCON) over assigned and attached Air Force cyberspace forces will be as directed by CDRUSSTRATCOM, normally through CDRUSCYBERCOM to the commander, 24 AF (24 AF/CC). AFSPC supports all joint warfighters in the cyberspace domain by providing forces, through 24 AF, that establish, maintain, operate, and defend Air Force cyberspace components; exploit adversary vulnerabilities; attack adversary systems; and provide command and control for assigned and attached cyberspace forces.[5]

See Volume 1, *Basic Doctrine* for additional doctrinal guidance on ADCON and specified ADCON responsibilities.

24th Air Force

This numbered Air Force serves as the component numbered Air Force (C-NAF) to USCYBERCOM. In this role, the C-NAF commander serves as the senior Air Force warfighter for employment of assigned and attached forces under USCYBERCOM. As commander of Air Force forces (COMAFFOR), the 24 AF/CC is normally delegated OPCON of assigned and attached Air Force forces and exercises control via the 624th Operations Center (624 OC).

The 24 AF/CC is further responsible for executing Air Force Service tasks as directed

[5] AFSPC Cyberspace PAD, Change 4.

by the Secretary of the Air Force (SECAF) and Chief of Staff of the Air Force (CSAF) in the role as the commander, Air Force Network Operations (AFNETOPS/CC). These tasks include overseeing the morale, welfare, safety, and security of assigned and attached forces. They also include tasks inherent in the responsibility to provide, establish, and maintain a secure and defensible network in accordance with Air Force Guidance Memorandum 13-01. Per this document, the AFNETOPS/CC is "the single commander responsible for the overall operation, defense, maintenance and control of the AF-GIG."

Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA)

Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) is a field operating agency subordinate to the Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2). AFISRA organizes, trains, equips, presents, and integrates all-source intelligence (e.g., signals intelligence [SIGINT], geospatial intelligence [GEOINT], measurement and signature intelligence, human intelligence, etc.) and full-spectrum capabilities to the intelligence community and to JFCs through the COMAFFOR. It provides customers at all echelons with multi-source intelligence products, applications, and services and provides intelligence expertise in the areas of SIGINT, IO (including information protection), acquisition, foreign weapons systems and technology, and treaty monitoring. In relation to cyberspace, AFISRA serves as the Air Force Service cryptologic component to the National Security Agency/Central Security Service (NSA/CSS), which authorizes SIGINT operations under Title 50, United States Code (U.S.C.). While NSA-derived analytic work roles are essential to cyber operations, employing full-spectrum cyber effects requires a multi-INT analysis approach. To enable 24 AF (AFCYBER) operations, AFISRA provides all-source cyber-focused ISR including digital network analysis to 24 AF through the 659th ISR Group. This support is generally characterized within five cyber-focused ISR areas: current intelligence and reporting, indications and warning, threat attribution and characterization, IPOE, and computer network exploitation.