

Cyberspace Doctrine Principles

Proficiency Code: A

Cyberspace, as defined in Air Force Doctrine Document (AFDD) 3–12 is a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace Operations (CO) is defined as the employment of cyberspace capabilities with the primary purpose of achieving military objectives or effects through the cyberspace domain. This lesson details how the Air Force employs some of those capabilities, and what many of the units assigned to cyberspace operations do to achieve those objectives. Before describing the structure and mission of cyberspace, you first need to know some of the policies governing the use of cyberspace operations.

There are three major considerations that apply to Cyberspace Operations:

- Policy (National, DOD, USAF).
- Authority.
- The law.

There are many policies and documents pertaining to cyberspace operations. The documents most relevant to Air Force cyberspace operations are contained in AFDD 3–12 *Cyberspace Operations, Appendix B, Policy and Doctrine Related to Cyberspace Operations*. The following table summarizes the different policies that apply to cyberspace operations.

Policies for Cyberspace Operations	
Type	Description
National	<p>The <i>National Strategy to Secure Cyberspace</i> is the comprehensive strategy for the US to secure cyberspace.</p> <p>It spells out three strategic priorities:</p> <ul style="list-style-type: none">• Prevent cyber-attacks against America’s critical infrastructure.• Reduce national vulnerability to cyber attacks.• Minimize damage and recovery time from cyber attacks. <p>The <i>National Strategy to Secure Cyberspace</i> outlines the framework for organizing and prioritizing US Government efforts in cyberspace. This strategy guides federal government departments and agencies that secure cyberspace. It identifies the steps every individual can take to improve our collective cyberspace security.</p> <p>More information on the national policy is located on the Department of Homeland Security’s website http://www.dhs.gov/.</p>
Military	<p>The <i>National Military Strategy for Cyberspace Operations</i> (NMS-CO) is the comprehensive strategy for US Armed Forces to ensure US superiority in cyberspace.</p> <p>There are four strategic priorities of the NMS-CO:</p>

	<ul style="list-style-type: none"> • Gain and maintain initiative to operate within adversary decision cycles. • Integrate cyberspace capabilities across the Range of Military Operations (ROMO). • Build capacity for cyberspace operations. • Manage risk for operations in cyberspace. <p>The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action.</p> <p>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 our people, is fundamental to this approach.</p>
--	---

Sources: JP 3-12