



ANNEX 3-12 CYBERSPACE OPERATIONS

APPENDIX B: POLICY AND DOCTRINE RELATED TO CYBERSPACE OPERATIONS

Last Updated: 30 November 2011

National-Level Documents	
<u>National Security Strategy</u>	The National Security Strategy of the United States of America is a document prepared periodically by the executive branch of the government of the United States for congress that outlines the major national security concerns of the United States 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 (contrast with the National Military Strategy) and its implementation relies on elaborating guidance provided in supporting documents (including the National Military Strategy [NMS]).
US <i>National Strategy to Secure Cyberspace</i> , February 2003	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.” ¹

Department of Defense Documents	
<u>National Defense Strategy</u> (NDS)	The NDS is issued periodically and the last one was published in June 2008. It outlines how the Department supports the President’s National Security Strategy and informs the National Military Strategy and other subordinate strategy documents. The strategy builds on lessons learned and insights from previous operations and strategic reviews such as the 2006 Quadrennial Defense Review.

¹ *National Strategy for Securing Cyberspace*, The White House, February 2003.

Department of Defense Documents	
<p><u>National Military Strategy</u></p>	<p>The NMS is issued by the Chairman of the Joint Chiefs of Staff as a deliverable to the Secretary of Defense briefly outlining the strategic aims of the armed Services. The NMS's chief source of guidance is the National Security Strategy document.</p> <p>The Chairman of the Joint Chiefs of Staff, in consultation with the other members of the Joint Chiefs of Staff, the Commanders of the Unified Combatant Commands, the Joint Staff, and the Office of the Secretary of Defense, prepares the National Military Strategy in accordance with 10 U.S.C., Section 153. Title 10 requires that not later than February 15 of each even-numbered year, the Chairman submit to the Senate Committee on Armed Services and the House Committee on Armed Services a comprehensive examination of the national military strategy. This report must delineate a national military strategy consistent with the most recent National Security Strategy prescribed by the President; the most recent annual report of the Secretary of Defense submitted to the President and Congress; and the most recent Quadrennial Defense Review conducted by the Secretary of Defense.</p>
<p><u>National Military Strategy for Cyberspace Operations</u> (NMS-CO), December 2006</p>	<p>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 our people, is fundamental to this approach.</p>
<p><u>Unified Command Plan</u> (UCP) 6 April 2011</p>	<p>The UCP assigns USSTRATCOM the mission of synchronizing planning for cyberspace operations, in coordination with other CCDRs, the Services, and, as directed, other US government agencies; and executing selected cyberspace operations.</p>

Department of Defense Documents	
<p>Joint Operations Planning and Execution System (JOPES)</p>	<p>The JOPES is the Department of Defense's (DOD's) principal means for translating national security policy decisions into military plans and operations. JOPES Functional Managers grant permissions, restrict access to operation plans on the database, and perform periodic reviews of user IDs and the content of the JOPES database to ensure outdated plans and accounts are removed when no longer required.</p>
<p>CJCS Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) v1 31 Oct 2005</p>	<p>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 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 rapidly and dynamically share knowledge 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. The NCOE will translate information superiority into combat power by effectively linking (both horizontally and vertically) knowledgeable entities throughout the battlespace, thus making possible dramatically new ways of operating and, by extension, decisive advantages in warfighting. The timeframe is 8 to 20 years in the future, with an illustrative focus on the year 2015.</p>
<p>DOD Directive 3600.01, <i>Information Operations</i>, 23 May 2011 (Secret; title and information extracted are unclassified)</p>	<p>Covers some of the computer network aspects of cyberspace operations, classifying them as part of IO. 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.</p>
<p>SecDef Memorandum, <i>Command and Control for Military Cyberspace Missions</i>, 12 November 2008,</p>	<p>Specifies that USSTRATCOM's JTF-GNO falls under the operational control of USSTRATCOM's USCYBERCOM, which directly impacts the organization of the global functional combatant command responsible for much joint cyberspace activity.</p>

Department of Defense Documents	
<p>DODD 3020.40, <i>Defense Critical Infrastructure Program</i> (DCIP), 14 January 2010</p>	<p>This Directive cancels DOD Directive 5160.54, "Critical Asset Assurance Program," January 20, 1998 (hereby canceled), updates policy, and assigns responsibilities for the DCIP, incorporating guidance from the President in Homeland Security Presidential Directive #7, December 17, 2003 to function as the Sector-Specific Agency for the Defense Industrial Base with the following responsibilities: collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.</p> <p>This Directive cancels Deputy Secretary of Defense Memorandum, "Critical Infrastructure Protection Responsibilities and Realignments," August 11, 1999 (hereby canceled) and supersedes The Department of Defense Critical Infrastructure Protection Plan, November 18, 1998 (hereby superseded), and the Deputy Secretary of Defense Memorandum, "Realignment of Critical Infrastructure Protection Oversight to the Assistant Secretary of Defense for Homeland Defense," September 3, 2003 (hereby superseded).</p>
<p>DODD 3020.26, <i>Department of Defense Continuity Programs</i>, January 9, 2009</p>	<p>DOD policy that all defense continuity-related activities, programs, and requirements of the DOD Components, including those related to continuity of operations, continuity of government, and enduring constitutional Government, shall ensure the continuation of current approved DOD and DOD component mission essential functions all circumstances across the spectrum of threats</p>
<p>DODD 8500.01E, <i>Information Assurance</i>, 24 October 2002</p>	<p>Establishes policy and assigns responsibilities to achieve Department of Defense (DOD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare</p>

Department of Defense Documents	
DODD O-8530.01 <i>Computer Network Defense</i> , 1 January 2001	Establishes policy, definition, and responsibilities for CND within DOD information systems and computer networks
DODI O-3600.02 <i>Information Operations Security Classification Guidance</i> , 28 Nov 1995	Provides DOD-level security classification guidance relevant to some cyberspace operations
DODI 8410.02, <i>Network Operations for the GIG</i> , 19 Dec 08	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
JP 1, <u>Doctrine for the Armed Forces of the United States</u> , 14 May 2007, Change 1 20 March 2009	This publication is the capstone joint doctrine publication. It provides doctrine for unified action by the Armed Forces of the United States. As such, it specifies the authorized command relationships and authority that military commanders can use, provides guidance for the exercise of that military authority, provides fundamental principles and guidance for command and control, prescribes guidance for organizing joint forces, and describes policy for selected joint activities. It also provides the doctrinal basis for interagency coordination and for US military involvement in multiagency and multinational operations.
JP 2-0, <u>Joint Intelligence</u>	This publication is the keystone document of the joint intelligence series. It provides fundamental principles and guidance for intelligence support to joint operations and unified action.
JP 2-01, <u>Joint and National Intelligence Support to Military Operations</u> , 07 October 2004	This publication establishes doctrinal guidance on the provision of joint and national intelligence products, services, and support to military operations.

Department of Defense Documents	
JP 2-01.3, <u>Joint Intelligence Preparation of the Operational Environment</u>	This publication describes the process in which the adversary and other relevant aspects of the operational environment are analyzed to identify possible adversary courses of action and to support joint operation planning, execution, and assessment.
JP 3-0, <u>Joint Operations</u> , 11 August 2011	This publication is the keystone document of the joint operations series. It provides the doctrinal foundation and fundamental principles that guide the Armed Forces of the United States in the conduct of joint operations across the range of military operations.
JP 3-08, <u>Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I and II</u> , 17 March 2006	Volume I discusses the interagency, intergovernmental organization (IGO), and nongovernmental organization (NGO) environment and provides fundamental principles and guidance to facilitate coordination between the Department of Defense, and other US Government agencies, IGOs, NGOs, and regional organizations. Volume II describes key US Government departments and agencies, IGOs and NGOs — their core competencies, basic organizational structures, and relationship, or potential relationship, with the Armed Forces of the United States.
JP 3-13, <u>Information Operations</u>	This publication provides doctrine for information operations planning, preparation, execution, and assessment in support of joint operations.
JP 3-13.1, <u>Electronic Warfare</u> , 25 January 2007	This publication provides joint doctrine for electronic warfare planning, preparation, execution, and assessment in support of joint operations across the range of military operations.
JP 3-13.3, <u>Operations Security</u> , 29 June 2006	This publication provides doctrine for planning, preparation, execution, and assessment of operations security in joint operations.
JP 3-13.4, <u>Military Deception</u> , 13 July 2006	This publication provides joint doctrine for the planning and execution of military deception at the combatant command and/or subordinate joint force level.
JP 3-14, <u>Space Operations</u> , 6 January 2009	This publication provides joint doctrine for planning, executing, and assessing joint space operations.

Department of Defense Documents	
JP 3-13.2 Military Information Support Operations	This publication addresses military psychological operations planning and execution in support of joint, multinational, and interagency efforts across the range of military operations
JP 5-0, Joint Operation Planning 11 August 2011	This publication is the keystone doctrine for joint operation planning throughout the range of military operations.
JP 6-0, Joint Communications System	This publication is the keystone document for the communications system series of publications. This publication presents approved doctrine for communications system support to joint and multinational operations and outlines the responsibilities of Services, agencies, and combatant commands with respect to ensuring effective communications system support to commanders.

Air Force-Level Documents	
HQ USAF Program Action Directive 07-08 (Change 4), <i>Phase I of Implementation of Secretary of Air Force Direction to Organize Air Force Cyberspace Forces</i> , 20 February 2009	Organization of the Air Force's Service contribution to cyberspace operations.
Volume 1, Basic Doctrine	This document is the premier statement of US Air Force basic doctrine. It has been prepared under the direction of the CSAF. It establishes general doctrinal guidance for the application of air and space forces in operations across the full range of military operations

Air Force-Level Documents	
<p>Annex 3-0, <u>Operations and Planning</u></p>	<p>This document has been prepared under the direction of the CSAF. It establishes doctrinal guidance for organizing, planning, and employing air, space, and cyberspace forces at the operational level of conflict across the full range of military operations. It is the capstone of US Air Force operational-level doctrine publications. Together, these publications collectively form the basis from which commanders plan and execute their assigned air and space missions and their actions as a component of a joint Service or multinational force.</p>
<p>Annex 3-13, <u>Information Operations</u></p>	<p>This annex establishes doctrinal guidance for information operations. More detailed doctrinal discussions of information operations concepts are explained in Annex 3-13.1, <i>Electronic Warfare Operations</i>; and Annex 3-61, <i>Public Affairs Operations</i>. The nomenclature of these publications is subject to change. Other annexes also discuss information operations as they apply to those specific airpower functions.</p>
<p>Annex 3-61, <u>Public Affairs</u></p>	<p>This document articulates fundamental Air Force principles for conducting public affairs operations and provides commanders with operational-level guidance for employing and integrating those capabilities across the range of air, space, and information operations.</p>
