OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

PERSONNEL AND READINESS

June 5, 2024

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum 24-002 – "Assessing Joint Force Readiness to Perform Designed and Assigned Missions in Contested and Congested Cyberspace Environments"

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive 5124.02 this directive-type memorandum (DTM):

- Provides DoD Components guidance to establish standardized policy, terminology, and metrics to assess the readiness of the joint force to perform designed and assigned missions in contested and congested cyberspace environments.

- Updates readiness reporting policy to include the joint force's ability to execute designed and assigned missions in contested and congested cyberspace environments.

- Provides guidance to update relevant existing policies.

- Is effective June 5, 2024; must be incorporated into Joint Publications (JPs) 3-0, 3-12, and 5-0, Chairman of the Joint Chiefs of Staff (CJCS) Instruction 3500.01, and DoD Instruction 3110.05. This DTM will expire June 5, 2025.

Applicability.

- This DTM applies to OSD, the Military Departments, the Office of the CJCS and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this DTM as the "DoD Components").

- Does not apply to:

    - Cybersecurity service providers. This policy is addressed in United States Cyber Command DoD Cybersecurity Service Provider Training and Readiness Framework.

- Electromagnetic spectrum policy. This policy is addressed in DoD Directive 3610.01.

- Cybersecurity activities in support of Department of Defense Information Networks operations. This policy is addressed in DoD Instruction 8530.01.

Definitions. See Glossary.

Policy.

- To posture the joint force to be operationally ready to accomplish designed and assigned missions in contested and congested cyberspace environments.

- Readiness reporting will be expanded to include a unit's ability to operate in contested and congested cyberspace environments.

- Terminology across the DoD related to contested and congested cyberspace environments will be standardized.

- The joint force must incorporate the risks of operating in contested and congested cyberspace environments when assessing and exercising their operational plans.

Responsibilities. See Attachment 2.

Releasability. **Cleared for public release**. The DTM is available on the Directives Division website at https://www.esd.whs.mil/DD/.

Ashish S. Vazirani,
Performing the Duties of the Under Secretary of Defense for Personnel and Readiness

Attachments:
As stated

ATTACHMENT 1

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3500.01, "Joint Training Policy for the Armed Force of the United States," current edition

DoD Directive 3610.01, "Electromagnetic Spectrum Enterprise Policy," September 4, 2020

DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008

DoD Directive 7730.65, "DoD Readiness Reporting System," May 31, 2023

DoD Instruction 3110.05, "Sustainment Health Metrics in Support of Materiel Availability," April 24, 2024

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

Joint Publication 3-0, "Joint Campaigns and Operations," June 18, 2022

Joint Publication 3-12, "Joint Cyberspace Operations," December 19, 2022

Joint Publication 5-0, "Joint Planning," December 1, 2020

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

United States Cyber Command, DoD Cybersecurity Service Provider Training & Readiness Framework, May 8, 2023[1]

[1] Available on the Internet at https://www.milsuite.mil/book/docs/DOC-1250311

ATTACHMENT 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R):

a. Incorporates the joint force's ability to execute assigned or designed missions in contested and congested cyberspace environments into readiness reporting policy.

b. Implements joint force standards in the Defense Readiness Reporting System (DRRS), in coordination with the Directors of the Combat Support Agencies, the CJCS, and the Secretaries of the Military Departments for operating in contested and congested cyberspace environments.

2. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) develops standardized terms for joint force operations in contested and congested cyberspace environments, in coordination with the DoD Component heads.

3. DOD COMPONENT HEADS. The DoD Component heads provide support to the USD(P), as requested, to develop standardized terms for joint force operations in contested and congested cyberspace environments in accordance with Paragraph 2.

4. DIRECTORS OF THE COMBAT SUPPORT AGENCIES (CSAS). In addition to the responsibilities in Paragraph 3., the Directors of the CSAs implement joint force standards in DRRS for operating in contested and congested cyberspace environments. Additionally, they update their standardized mission essential tasks when specific contested and congested cyberspace standards and conditions are applicable, to enable CSAs to assess operational capability for assigned and designed mission in contested and congested cyberspace environments.

5. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 3., the Secretaries of the Military Departments:

a. Update relevant Service component standardized mission essential tasks when specific contested and congested cyberspace standards and condition are applicable, to enable the Military Services to assess operational capability for assigned and designed missions in contested and congested cyberspace environments.

b. Capture the ability to operate in contested and congested cyberspace environments into unit readiness reporting metrics.

c. Implement joint force standards in the DRRS, in coordination with the USD(P&R), the Directors of the CSAs, and the CJCS.

d. In coordination with the Chief, National Guard Bureau (NGB), incorporate into training exercises for their respective Military Services the challenges of operating in contested and congested cyberspace environments.

e. In coordination with the Combatant Commanders (CCDRs), define requirements to address the challenges of operating in contested and congested cyberspace environments and incorporate those requirements into Service training exercises.

f. In coordination with the CJCS and the CCDRs, update doctrine to include how to achieve assigned and designed missions in contested and congested cyberspace environments.

6. CHIEF, NGB. In addition to the responsibilities in Paragraph 3., the Chief, NGB, in coordination with the Secretaries of the Military Departments, incorporates the challenges of operating in contested and congested cyberspace environments into Service training exercises.

7. CJCS. In addition to the responsibilities in Paragraph 3., the CJCS:

a. Updates relevant readiness reporting guidance and policy to include joint force operations in contested and congested cyberspace environments.

b. Provides policy guidance and supports CCDRs joint training programs and joint exercises to achieve assigned and designed missions in contested and congested cyberspace environments.

c. Implements joint force standards and conditions in DRRS for operating in contested and congested cyberspace environments.

d. Updates joint doctrine, in coordination with Secretaries of the Military Departments and the CCDRs, to include how to achieve assigned and designed missions in contested and congested cyberspace environments in accordance with the joint force standards referred to in Paragraph 1.b.

e. In coordination with the CCDRs, defines requirements to address the challenges of operating in contested and congested cyberspace environments and incorporates those requirements into joint training exercises.

8. CCDRs. In addition to the responsibilities in Paragraph 3., the CCDRs:

a. Account for challenges of operating in contested and congested cyberspace environments and relevant mitigations in joint and Service training exercises.

b. Serve as lead agents, in coordination with the Secretaries of the Military Departments, to define requirements to address the challenges of operating in contested and congested cyberspace environments and incorporates those requirements into Service training exercises.

c. Serve as lead agents, in coordination with the CJCS, to define requirements to address the challenges of operating in contested and congested cyberspace environments and incorporates those requirements into joint training exercises.

d. In coordination with the CJCS and the Secretaries of the Military Departments, update doctrine to include how to achieve assigned and designed missions in contested and congested cyberspace environments.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
CCDR	Combatant Commander
CJCS	Chairman of the Joint Chiefs of Staff
CSA	combat support agency
DRRS	Defense Readiness Reporting System
DTM	directive-type memorandum
JP	joint publication
NGB	National Guard Bureau
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
assigned mission	Defined in DoDD 7730.65.
congested cyberspace	A disconnected, intermittent, or limited environmental aspect of cyberspace where operations might be degraded by unintentional interference from private sector or military use, or by natural events. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
contested cyberspace	A disconnected, intermittent, or limited operational aspect of cyberspace in which malicious activity threatens or impacts mission effectiveness by degrading information, data exchange, or network capability. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
cyberspace	Defined in JP 3-12.
degrade	Defined in Paragraph 2.c.(5)(a)1 of Chapter II of JP 3-12.

TERM	DEFINITION
designed mission	Defined in DoDD 7730.65.