

Titled: USCYBERCOM ANNOUNCEMENT MESSAGE

DTG: 212106Z May 10

MSGID/GENADMIN/CDRUSSTRATCOM//

REFERENCES

REF/a/Doc/SecDef/23Jun2009//

AMPN/Memo Directing USSTRATCOM'S Establishment of a Subordinate Unified Command for Cyber Operations//

REF/b/Doc/USSTRATCOM/01Sep2009//

AMPN/Implementation Plan for Establishing USCYBERCOM//

REF/c/Doc/CDRUSSTRATCOM/29Jun2009//

AMPN/Terms of Reference for Establishing USCYBERCOM//

REF/d/Doc/CDRUSSTRATCOM/21May2010//

AMPN/Operational Directive 10-001, USCYBERCOM//

REF/e/Doc/White House/17Dec2008//

AMPN/Unified Command Plan 2008//

GENTEXT/SITUATION/

1. **SITUATION:** Per ref a, the Secretary of Defense (SecDef) directed the establishment of United States Cyber Command (USCYBERCOM), a new subordinate unified (subunified) command to United States Strategic Command (USSTRATCOM) for cyberspace operations. In accordance with (IAW) refs a, b and c, Commander (CDR) USSTRATCOM established USCYBERCOM with an initial operational capability (IOC) on 21 May 2010 to plan, execute, command, and control operations and training missions in and through cyberspace. The purpose of this message is to inform all DoD Components of USCYBERCOM's mission, roles, responsibilities, authorities, and command relationships within the Department of Defense.//

GENTEXT/MISSION/

2. **MISSION:** USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense (DoD) information networks; and when directed, prepares to conduct full-spectrum military cyberspace operations, in order to enable actions in all domains, ensure U.S. and Allied freedom of action in cyberspace, and deny the same to our adversaries.//

GENTEXT/EXECUTION/

3. **EXECUTION:**

a. **Operational Capability.** USCYBERCOM has assumed the tasks, missions, and operations of Joint Functional Component Command Network Warfare (JFCC NW) and has begun to consolidate them with the tasks, missions, and operations of Joint Task Force-Global Network Operations (JTF-GNO). USCYBERCOM continues to service all existing and incoming operational support requirements submitted for action to JFCC NW and JTF-GNO, according to current processes.

b. **Responsibilities.**

(1) CDRUSCYBERCOM tasks are delineated in ref d. Specifically, CDRUSSTRATCOM has delegated authority to CDRUSCYBERCOM to conduct the following Unified Command Plan (UCP) cyberspace mission tasks (ref e):

(a) Directing DoD Global Information Grid (GIG) operations and defense.

(b) Planning against designated cyberspace threats.

(c) Coordinating with other combatant commands and appropriate U.S. government agencies prior to the planning and execution of cyberspace operations having effects that cross areas of responsibility.

(d) Planning Operational Preparation of the Environment (OPE), and as directed, executing OPE or synchronizing execution of OPE in coordination with the Geographic Combatant Commanders (GCC).

(e) Providing military representation to U.S. national agencies, U.S. commercial entities, and international agencies for matters related to cyberspace, as directed.

(f) Executing cyberspace operations, as directed.

(2) Prior to FOC, USCYBERCOM will:

(a) Create a robust, transparent process to receive, adjudicate, service, and provide feedback on operational support requirements submitted by the combatant commands, services, and agencies (CC/S/A).

(b) Consolidate the requirements processes of JFCC NW and JTF-GNO.

(c) Be delegated USSTRATCOM UCP authorities to synchronize cyberspace planning with other CC/S/As.

(d) Transform the cyber LNO structure into CSEs for each combatant command. CSEs will ensure comprehensive situational awareness of the cyberspace domain and provide faster, enhanced early warning capabilities to global watch centers.

c. Organization.

(1) USCYBERCOM was formed at IOC by merging the staff elements of JFCC NW and JTF-GNO, adhering to the traditional organizational structure of J-Code directorates and special/personal staffs.

(a) CDRUSCYBERCOM is dual-hatted as the Director of the National Security Agency (DIRNSA).

(b) CDRUSCYBERCOM has operational control (OPCON) of JTF-GNO, which will be de-activated prior to FOC, and CDRUSCYBERCOM will fully subsume JTF-GNO's mission and capabilities.

(c) DCDR, JTF-GNO is dual-hatted as the USCYBERCOM J33, who directs the execution of current cyberspace operations.

(d) JTF-GNO J-codes will assume coincident USCYBERCOM roles within USCYBERCOM's J-code structure. JTF-GNO retains its current J-code structure, and adopts USCYBERCOM J-codes as directed by CDRUSCYBERCOM.

(2) Joint Operations Center (JOC). The USCYBERCOM J3 operates the JOC, which is composed of JTF-GNO NetOps Center and USCYBERCOM watch center personnel. The JOC will focus on directing the operation and defense of the DoD GIG, and Overseas Contingency Operations. Additionally, the JOC:

(a) Leads crisis action planning.

(b) Synchronizes, directs, and executes current cyberspace operations, as directed by the J33.

(c) Achieves and maintains DoD cyberspace situational awareness, and provides indications and early warning support to the Integrated Cyber Center (ICC); also coordinates GCC cyber support requirements.

(d) Maintains 24/7 operational capability and provides direction to assigned and/or attached forces for DoD operations.

(3) Joint Intelligence Operations Center (JIOC). USCYBERCOM will establish a JIOC to plan, prepare, direct, integrate, synchronize and manage continuous, full-spectrum intelligence operations to satisfy command requirements at or before FOC. Formed primarily from personnel formerly assigned to the JTF-GNO J2 and JFCC NW J2, the JIOC will:

(a) Operationally integrate with National Security Agency (NSA) and the Defense Intelligence Agency (DIA) to leverage their capabilities and expertise.

(b) Provide direct support to USCYBERCOM intelligence and joint planning operations, and support cyber intelligence requirements submitted by other combatant commands.

(c) Incorporate an NSA/CSS Cryptologic Support Group and DIA forward elements.

(4) (U) Service Components. CDRUSCYBERCOM will execute the preponderance of cyberspace operations through Service Components. See para 5.a.3.a for service components supporting USCYBERCOM.

(5) Adaptive JTFs. CDRUSCYBERCOM will establish JTFs in response to emergent situations, or to deliver long-term planning and execution support to Combatant Commanders (CCDRs). These JTFs include specialized planners and operators who can provide "expeditionary CNO" to CCDRs through a combination of forward-deployed and reachback capabilities.

(6) Cyberspace Support Elements (CSE) and LNOs. USCYBERCOM's support to CCDRs will range from regionally and functionally focused planning conducted by USCYBERCOM headquarters staff to dedicated, robust, and empowered cyber-planning elements deployed to combatant commands. Accordingly, CDRUSCYBERCOM will:

(a) Establish LNOs at each combatant command with reachback capability to HQ J5, USCYBERCOM. This forward presence will grow with the capability to coordinate and facilitate operations and defense of networks, cyber planning, targeting, and analysis.

UNCLASSIFIED//~~FOUO~~

(b) Provide larger, more capable CSEs tailored to the unique operational environment of individual combatant commands, as resources become available.

(7) USCYBERCOM will maintain relationships with its interagency partners through three bodies:

(a) Joint Interagency Task Force-Cyber (JIATF-Cyber). Formed from the JFCC NW JIATF-Cyber at IOC, the USCYBERCOM JIATF-Cyber is a multi-functional interagency coordination working group that coordinates and deconflicts cyberspace operations with interagency and key partner nations. JIATF-Cyber ensures situational awareness among its members and provides a forum for collaboration and planning.

(b) Joint Interagency Coordination Group-Cyber (JIACG-Cyber). Formed from the JIATF-Cyber after IOC, JIACG-Cyber is a multi-functional, advisory element that represents civilian departments and agencies at USCYBERCOM and facilitates information sharing between agencies and key partner nations. The JIACG-Cyber Director is the USCYBERCOM J3. The Deputy Director of the JIACG-Cyber will be an interagency member with a commensurate civilian rank. The JIACG-Cyber:

1. Provides regular, timely, and collaborative day-to-day support for planning, coordination, preparation, and implementation of interagency activities.

2. Participates in contingency and crisis-action planning, and supports Defense Support to Civil Authorities (DSCA).

(c) Interagency Executive Steering Council (IA ESC). The IA ESC, co-chaired by DCDRUSCYBERCOM and a senior representative from each interagency partner, is comprised of senior-level leaders from participating agencies. The USCYBERCOM Chief of Staff, Political Advisor, Special Staff, and JIACG-Cyber Director attend as required. The IA ESC:

1. Provides face-to-face interaction between senior interagency operational leaders to overcome bureaucratic obstacles to cooperation and further develop understanding before a crisis develops.

2. Meets periodically and reviews interagency posture, operations and plans, and offers a forum for issue resolution, communication facilitation, and the elevation of issues to senior U.S. Government leadership.//

GENTEXT/ADMIN AND LOG/

UNCLASSIFIED//~~FOUO~~

4. ADMINISTRATION AND LOGISTICS:

a. **Administration**. USCYBERCOM has limited capacity to execute all administrative tasks required of a subunified command; and therefore will require continued USSTRATCOM assistance and/or augmentation, as stated in ref b.

b. **Public Affairs (PA) Guidance**. PA posture is active. USSTRATCOM/PA has lead and will coordinate with NSA/SC and OASD/PA until USCYBERCOM/PA is established. PA guidance is detailed in ref b.//

GENTEXT/COMMAND AND CONTROL/

5. COMMAND AND SIGNAL:

a. Command Relationships:

(1) (U) DIRLAUTH relationships granted to JFCC NW and JTF-GNO convey to USCYBERCOM.

(2) Combatant Commanders:

(a) Task: Comply with CDRUSSTRATCOM's direction, as delegated to CDRUSCYBERCOM, for operation and defense of the DoD GIG.

(b) Requests:

1. Unless otherwise specified by SecDef, maintain a mutual support relationship for planning, coordinating, and executing cyberspace operations.

2. Coordinate with CDRUSCYBERCOM to prioritize mission requirements and force capabilities. Conflicts that cannot be resolved through coordination with CDRUSCYBERCOM to be forwarded to CDRUSSTRATCOM.

3. Review Ref b, Annex J Appendix 1, Command and Control for Network Operations (NetOps C2) at IOC and FOC.

(3) Services:

(a) Per Ref a, the military departments have identified the following organizations to serve as components to USCYBERCOM. Upon SECDEF approval, these organizations will be assigned to CDRUSSTRATCOM with OPCON delegated to CDRUSCYBERCOM prior to FOC.

(1) ARFORCYBER

UNCLASSIFIED//~~FOUO~~

(2) FLTCYBERCOM

(3) MARFORCYBER

(4) AFCYBER

b. **Contact Information:**

(1) **Battle Captain/JOC:** DSN: [Not Responsive]; **COMM:** [Not Responsive]
[Not Responsive]; **Red Switch** [Not Responsive]; **NSTS** [Not Responsive]; **SIPR:**
[Not Responsive], **JWICS:** [Not Responsive] (**Future address contact info:**
SIPR: [Not Responsive]; **JWICS:** [Not Responsive])

(2) **J0:** DSN: [Not Responsive] **COMM:** [Not Responsive]

(3) **CAG:** DSN: [Not Responsive] **COMM:** [Not Responsive];

(4) **SJA:** DSN: [Not Responsive] **COMM:** [Not Responsive]

(5) **J1:** DSN: [Not Responsive] **COMM:** [Not Responsive];

(6) **J2:** DSN: [Not Responsive]; **COMM:** [Not Responsive];

(7) **J3:** DSN: [Not Responsive]; **COMM:** [Not Responsive];

(8) **J4:** DSN: [Not Responsive]; **COMM:** [Not Responsive];

(9) **J5:** DSN: [Not Responsive]; **COMM:** [Not Responsive];

(10) **J6:** DSN: [Not Responsive]; **COMM:** [Not Responsive];

(11) **J7:** DSN: [Not Responsive]; **COMM:** [Not Responsive]

(12) **J8:** DSN: [Not Responsive]; **COMM:** [Not Responsive]