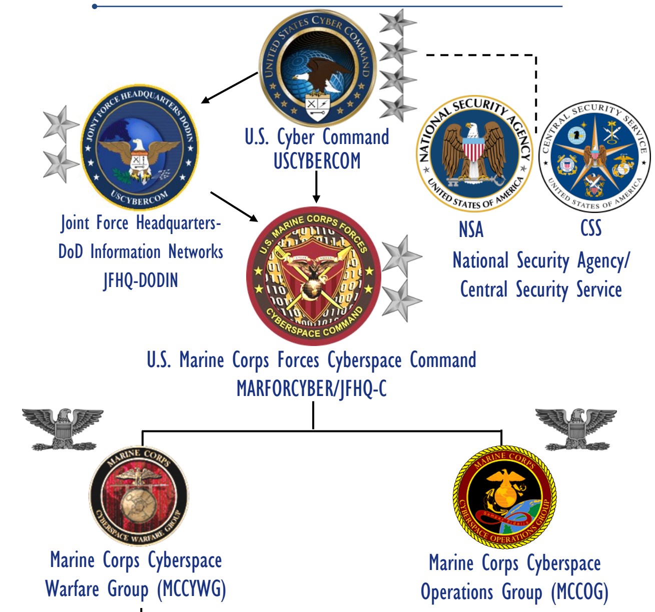
CYBERSPACE COMMAND RELATIONSHIPS



Cyber Mission Force (CMF):

- National Mission Teams (NMT)
- Combat Mission Teams (CMT)
- Cyber Protection Teams (CPT)
- Combat Support Teams (CST)

Cyber Service Components

OVERVIEW: The Secretary of Defense recognized the significance of the cyberspace domain to national security, and directed the establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command under U.S. Strategic Command (USSTRATCOM). In response, the Marine Corps established U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER) in October 2009 as the Marine Corps' service component to USCYBERCOM. This was complemented by the establishment of the Navy's U.S. Fleet Cyber Command, Army Cyber Command, Air Force Cyber Command, and Coast Guard Cyber Command.

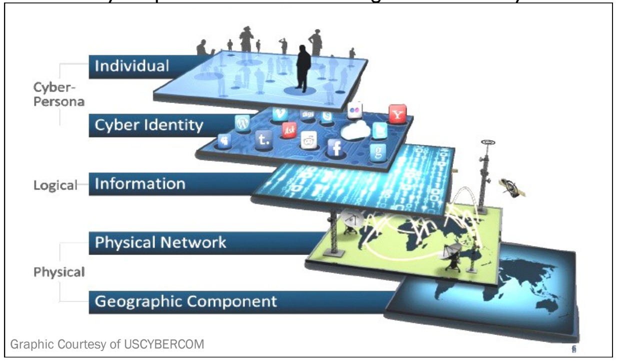
> *"As a force, we will remain ready to fight and win across the range of military operations and in all five warfighting domains– maritime, land, air, cyber, and space."*
>
> *- General Neller, Commandant of the Marine Corps, 1 March 2016*

UNDERSTANDING CYBERSPACE

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data; including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JP 3-12).

Cyberspace intersects with and enables all operational missions in all domains.

The cyberspace domain can be thought of in three layers:



Graphic Courtesy of USCYBERCOM

Cyber-persona layer: comprised of individuals and entities on the network. An individual (e.g. "Jane Smith") is digitally represented through his/her cyber identities.

Logical network layer: comprised of the code—"the 1s and 0s"—that conveys information; but is not tied to a specific individual, path, or node.

Physical network layer: comprised of the geographic and physical network components. This includes the location of where elements of the network reside and is comprised of the hardware, systems software, and infrastructure that support the network (routers, switches, transmitters).

CYBERSECURITY BATTLEGROUND

There are three battle spaces in cyberspace:

Blue Spaces: friendly force battle spaces mostly formed by DODIN environments.

Grey Spaces: widely considered to be the Internet as a whole and considered neutral maneuver space.

Red Spaces: network of networks that an adversary can use to conduct attacks.

U.S. Marine Corps Forces Cyberspace Command

Commander: MajGen Lori E. Reynolds
Executive Director : SES Gregg R. Kendrick
Chief of Staff: Col Daniel J. Haas
Sergeant Major: SgtMaj John W. Scott

U.S. Marine Corps Forces Cyberspace Command

UNDERSTANDING THE THREAT

We face a growing cyber threat—one that is increasingly persistent, diverse, and dangerous. The traditional fight we have envisioned across the domains of air, land, sea, and space has expanded to the cyberspace domain. In the domain of cyberspace, the United States' technical superiority is not established: we have to earn superiority in each fight. Marines understand the actions required to achieve superiority in a physical battlespace. In order to fight and win in the cyber battlespace, we must apply the same principles.

MARFORCYBER'S MISSION

To conduct full spectrum Cyberspace Operations, to include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (DCO) within the MCEN and Joint Force networks, and when directed, conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces; in order to enable freedom of action across all warfighting domains, and deny the same to adversaries.

MARFORCYBER LINES OF EFFORT

There are three priority efforts outlined within MARFORCYBER's campaign plan. The campaign plan serves as a framework for organizing activities, allocating resources, growing capability, and measuring progress.

LOE 1: Secure, Operate, and Defend the MCEN

LOE 2: Provide Warfighting Capabilities

LOE 3: Provide Value to the MAGTF

MARFORCYBER'S VISION IS TO BE THE NATION'S FORCE OF CHOICE TO DEFEND CYBER EQUITIES, ENABLE FREEDOM OF ACTIONS, AND PROVIDE EFFECTS IN THE CYBERSPACE DOMAIN, MAINTAINING THE MARINE CORPS' LEGACY OF THE NATION'S FORCE IN READINESS. WE ARE THE FIRST TO FIGHT—IN ALL DOMAINS.

SEMPER IN PROELIO LATIN FOR "ALWAYS IN BATTLE" IS NOT ONLY OUR MOTTO, BUT THE REALITY OF CYBERSPACE. CYBERSPACE IS AND ALWAYS WILL BE A CONTESTED DOMAIN. CYBERSPACE INTERSECTS WITH AND ENABLES ALL OPERATIONAL MISSIONS IN ALL DOMAINS. ALWAYS FAITHFUL, ALWAYS IN BATTLE.

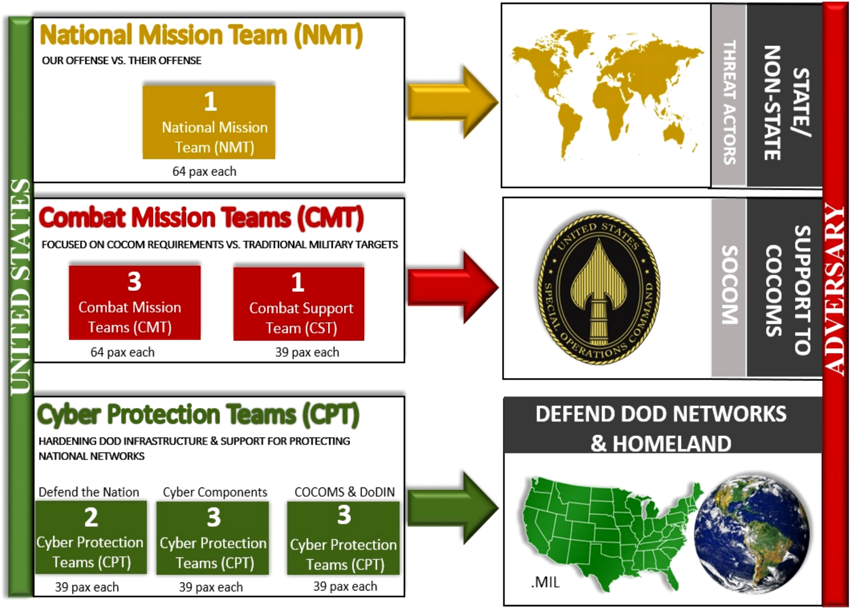
MARINE CORPS CYBERSPACE WARFARE GROUP

The MCCYWG has the responsibility to man, train, and equip personnel for all Marine Cyber Mission Force (CMF) teams and retains administrative control of the teams even after they are provided to USCYBERCOM for operational control. Upon completion of the initial CMF build, it is envisioned that the MCCYWG will transition their role into one of serving as the Cyber Warfighting Center for the Marine Corps - providing standardized advanced cyber training and certifications that supports Marine cyber training and readiness across the Corps.

MARINE CORPS CYBERSPACE OPERATIONS GROUP

The MCCOG is responsible for directing global network operations and computer network defense of the MCEN. The MCCOG executes DoD Information Network (DODIN) operations and DCO in order to enhance freedom of action across warfighting domains, while denying the efforts of adversaries to degrade or disrupt our advantage through cyberspace.

MARINE CORPS CYBER MISSION FORCE



UNITED STATES

National Mission Team (NMT)

OUR OFFENSE VS. THEIR OFFENSE

1 National Mission Team (NMT) — 64 pax each

Combat Mission Teams (CMT)

FOCUSED ON COCOM REQUIREMENTS VS. TRADITIONAL MILITARY TARGETS

3 Combat Mission Teams (CMT) — 64 pax each

1 Combat Support Team (CST) — 39 pax each

Cyber Protection Teams (CPT)

HARDENING DOD INFRASTRUCTURE & SUPPORT FOR PROTECTING NATIONAL NETWORKS

Defend the Nation: 2 Cyber Protection Teams (CPT) — 39 pax each

Cyber Components: 3 Cyber Protection Teams (CPT) — 39 pax each

COCOMS & DoDIN: 3 Cyber Protection Teams (CPT) — 39 pax each

STATE/ NON-STATE THREAT ACTORS

SUPPORT TO COCOMS SOCOM

DEFEND DOD NETWORKS & HOMELAND

ADVERSARY

JOINT FORCE HEADQUARTERS - CYBER

In support of joint military commanders' objectives, each Cyber Service Component is tasked to establish a Joint Force Headquarters-Cyber (JFHQ-C). In 2017, MARFORCYBER established a standing JFHQ-C and will begin to man a JFHQ-FWD. Combat Mission Teams support their assigned Combatant Command/s under the JFHQ-C construct by planning and conducting cyberspace operations. JFHQ-C MARFORCYBER supports U.S. Special Operations Command.

DEFENSE OF THE MCEN

Joint Force Headquarters—DoD Information Networks (JFHQ-DODIN) provides command and control of DODIN operations and defensive cyber operations internal defensive measures to coordinate the protection of DoD component capabilities enabling power projection and freedom of action across all warfighting domains. MARFORCYBER is responsible for the defense of the MCEN, the Marine Corps' portion of the DODIN.