

U.S. FLEET CYBER COMMAND

U.S. TENTH FLEET – FORT MEADE, MD



2014 FACT SHEET

We are Warfighters - First and foremost, the men and women who make up the U.S. Fleet Cyber Command/U.S. TENTH Fleet (FCC/C10F) team around the world are warriors who remain motivated and mission focused. FCC/C10F warfighters direct cyberspace operations to deter and defeat aggression while ensuring freedom of action in cyberspace. Operations are not limited to cyberspace alone, however, as FCC/C10F is the Navy’s central operational authority for cryptologic/signals intelligence, information operations, electronic warfare, and space capabilities in addition to cyber and networks operations.

We are Operational - U.S. Fleet Cyber Command serves as the Navy component command to U.S. Strategic Command and U.S. Cyber Command, and the Navy’s Service Cryptologic Component commander under the National Security Agency/Central Security Service. Fleet Cyber Command also reports directly to the Chief of Naval Operations as an Echelon II command.

U.S. 10th Fleet is the operational arm of Fleet Cyber Command and executes its mission through a task force structure similar to other warfare commanders. In this role, C10F provides operational direction through its Maritime Operations Center located at Fort George Meade Md., executing command and control over assigned forces in support of Navy or joint missions in cyber/networks, information operations, electronic warfare, cryptologic/signals intelligence and space.

Our Strategy Sets the Course - Navy Cyber Power 2020 is the road map for continued success and requires U.S. Fleet Cyber Command/U.S. TENTH Fleet (FCC/C10F) to address cyber threats, key trends, and challenges across four main areas, which are (1) integrated operations, (2) an optimized cyber workforce, (3) technology innovation, and (4) reforming development and execution of our requirements, acquisition, and budgeting. The NCP 2020 vision is assured access to cyberspace and confident command and control, preventing strategic surprise in cyberspace, and delivering decisive cyber effects.

Accountability - We must continue to transform the Navy’s culture with respect to the role of cyber in joint warfare. We will continue to develop standards of accountability for the cyber domain, like other warfighting domains, in step with the Navy’s long tradition of holding all hands responsible for their actions – cyber security is the responsibility of the entire Navy team.

Cyber Norm – The new cyber norm is the reality in which we operate and requires the entire Navy team to constantly stay ahead of the adversary in the cyber arena. The Navy’s network defenders must consistently and dynamically outpace the enemy, denying adversaries any benefit. As important, every user must understand their responsibility to also deny the enemy any advantage when on the network. After all, if the Navy has given you access to a keyboard, you are operating in the cyber domain.

With the stand-up of U.S. Fleet Cyber Command and re-commissioning of U.S. 10th Fleet in January 2010, the Navy recognized the need “...to confront a new challenge to our nation’s security in cyberspace.” Over the four years since then, as the Navy’s culture has begun to change with respect to cyber in Joint warfighting, the necessity for an active cyber defense has become more and more apparent. Late summer of 2013, the Navy expanded its aggressive campaign to enhance the security of its networks. Since then and moving forward, we will continually apply defensive measures and architectural hardening improvements (making the network more defensible) to strengthen the security of our networks.

FLTCYBERCOM Total Force

Active Military	10,496
Reserve & FTS Military	1,344
Civilians	2,469
Contractors	993
Totals	15,302

FY 13 Budget: \$904M