Even though we can respond to cyber attacks in any domain, this force is expanding the president’s options with full-spectrum cyber capabilities that can complement other military assets.¹


Cyber is and has been such an integral part of the maritime operational level of war (OLW)³ over the past two decades that its impact at times has perhaps been taken for granted. The reality of the new cyber norm in which we operate however has eliminated any room for complacency. From systems that are foundational to the operations of our ships and aircraft to the way we command and control platforms and weapons, cyber and network maneuver are essential to Navy operations.

Contrary to past practices and beliefs, cyberspace is much more than an administrative domain for email and business functions. From satellites orbiting above the earth to the “Silent Service” below the seas, and everything in between, cyber is part of maritime operations. Navy and Joint commanders depend on cyberspace for assured command and control (C2), integrated fires, battle space awareness/intelligence, maneuver, protection, and sustainment. For example, carrier aviation maintenance programs rely upon it to deliver mission-ready aircraft and weapon systems such as the Tactical Tomahawk use cyberspace to receive in-flight targeting data⁴. Additionally, cyberspace empowers naval maneuvers with positioning, navigation, and timing support (e.g., the Global Positioning and Navigation systems).

While the Navy’s TENTH Fleet team is charged to operate and defend Navy and DoD networks, all hands contribute to our overall cybersecurity posture through their actions and behaviors while on the net. If you use a keyboard, you are an operator in cyberspace.

To ensure operational success in the maritime environment therefore, defense of Navy and DoD networks and information is essential and cannot be separated from the overall maritime OLW. Put another way, defensive cyber operations and cyber security are paramount to the maritime OLW and we cannot afford to underestimate the impact.

The Navy’s strategic interest in the cyber realm extends beyond of the Department of Defense Information Networks (DODIN) – the .mil domain - and includes commercial and academic institutions that provide design, manufacturing, research and other sensitive
products and services for the Navy. Although outside of the .mil domain, securing sensitive but unclassified Navy data from either theft or espionage is key to maintaining our warfighting advantage.

Sensitive unclassified data can be used against us to improve kinetic and non-kinetic targeting of our platforms. Furthermore, it can be used to improve the warfighting capabilities of potential future adversaries through enhanced knowledge of how we man, train and equip for warfighting.

Defensive capabilities exist to oppose a threat. The probing and espionage of U.S. networks by our adversaries is in a constant state of play. Unfortunately, cyber capabilities can also be used as a weapon and could potentially do great harm to U.S. assets. Moreover, operational preparation of the environment (OPE) for potential cyber attack may be masked as espionage.

Secretary Hagel outlined our requirement to prepare for the worst during his March 28 comments for General Alexander’s retirement ceremony at Fort Meade:

“Our military’s first responsibility is to prevent and de-escalate conflict and that is DOD’s overriding purpose in cyberspace as well. General Alexander has helped leaders across DOD recognize that cyberspace will be a part of all future conflicts. And if we don’t adapt to that reality, our national security will be at great risk.”

As Fleet Cyber Command continues to build the Navy component to the Cyber Mission Force, it is clear that the scope of cyber’s impact on the maritime OLW does not end with network operations and defense. It also includes an ability to deliver cyber fires integrated with joint force kinetic and non-kinetic fires in support of commanders’ objectives.

On this full-spectrum side of cyberspace operations, there is much work yet to be done. The Joint community, we, and our sister Services are still refining and exercising the integration of cyber missions with geographic combatant command operations; additionally, we continue to clarify the necessary authorities associated with delivering these critical effects, while we build capacity and capability in the Cyber Mission Force.

In the meantime, the Navy continuously evaluates adversary actions in cyberspace through steadfast cyber intelligence collection and analysis, and integrates cyber information and threat warnings into the commanders’ operational view.

The holistic picture that emerges is thus one in which the Navy operates, defends, exploits, and engages in cyberspace -consistently and effectively- to ensure our maritime forces retain access to cyberspace for all mission critical functions and to provide Navy and Joint commanders with assured C2, integrated fires, and battle space awareness.

In an era when our country faces many national security challenges, we cannot afford to overlook the impact of cyber on the operational level of war. While there are challenges, the Fleet Cyber Command/TENTH Fleet team sees this as an opportunity to make a difference to our Navy and the Nation by transforming ourselves to meet these challenges.

This will be more apparent as we expand the capabilities and options that maritime and Joint commanders can draw upon in the electromagnetic spectrum and cyber domain to defend our country and its allies across all warfighting domains.

The cyberspace domain in which we operate requires that we constantly stay ahead of the adversary. It takes the entire Navy team to assure access to cyberspace and the integrity of command and control. This will be enhanced as we leverage our strengths in the converged electromagnetic and cyber domains and continue to deliver on SIGINT, IO, EW, and space missions. The fundamental impact of cyber on the maritime operational level of war is clear and will only grow.
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. TENTH Fleet (C10F) 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 Meade, 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.


2 “The cyber mission force, which is being built over a period of three years, is designed to accomplish three separate mission areas: national mission teams to defend the nation by seeing foreign adversary cyber activity, blocking attacks, and maneuvering to defeat them; combat mission teams to support combatant commander priorities and missions; and cyber protection teams to defend DOD information networks and improve network security...” - “Cyber Flag Exercise Highlights Teamwork, Training,” U.S. Cyber Command News Release, November 19, 2013: http://www.defense.gov/news/newsarticle.aspx?id=121179.


5 See “Retirement Ceremony for General Keith Alexander as delivered by Secretary of Defense Chuck Hagel, Fort Meade, MD, MD, Friday, March 28, 2014.”


Material contained herein is made available for the purpose of peer review and discussion, and does not necessarily reflect the views of the Department of the Navy or the Department of Defense.