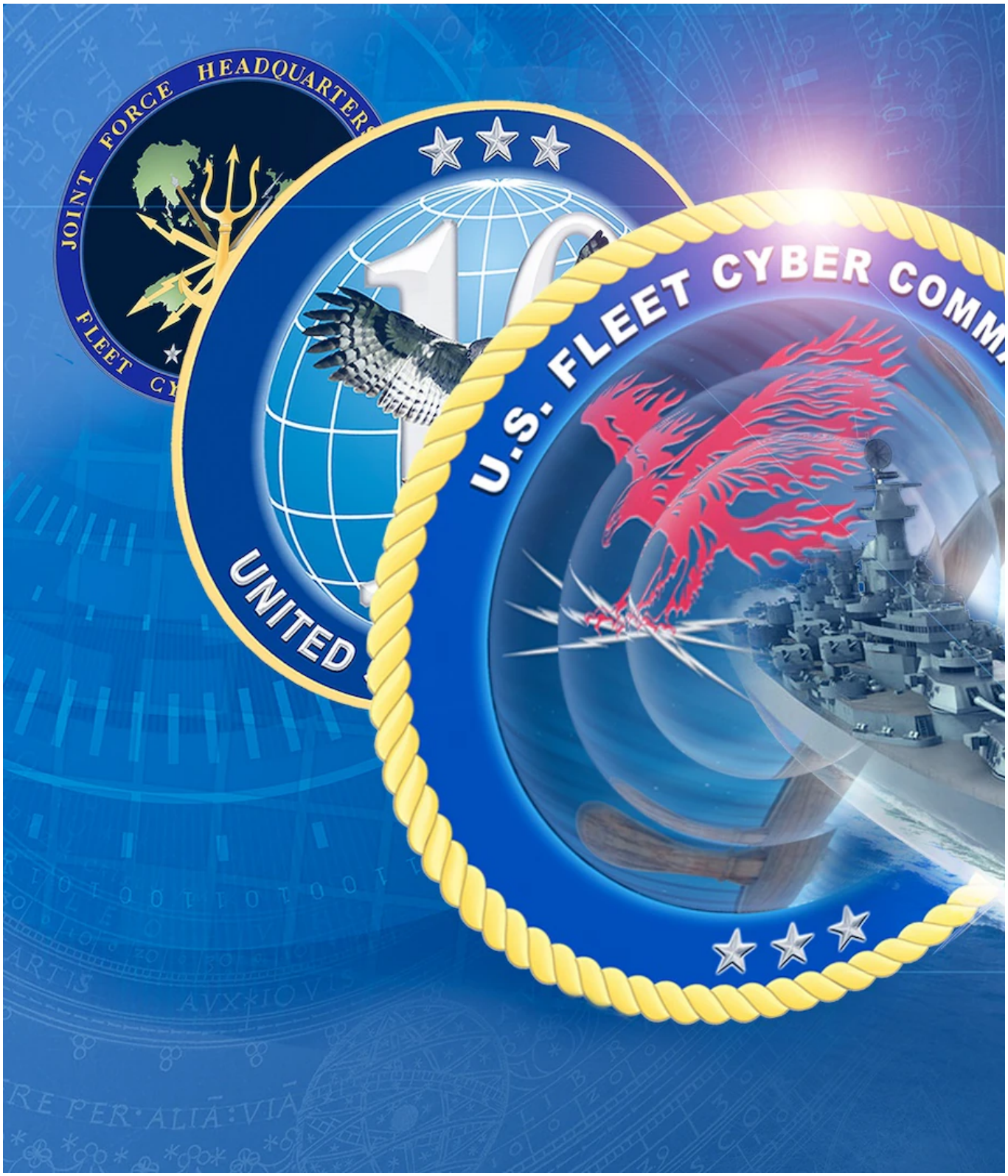
Joint Cyber Operations Strengthen DoD Networks



U.S. Fleet Cyber Command Logos
Graphic highlighting the mission of the U.S. Navy Fleet Cyber Command (U.S. Navy graphic by Oliver Elijah Wood/Released)
By U.S. Fleet Cyber Command / U.S. 10th Fleet / Published Oct. 19, 2023
FORT GEORGE G. MEADE, Md.,

Cyber Protection Teams from Fleet Cyber Command, 16th Air Force (Air Forces Cyber) and Army Threat Systems Management Office strengthened computer networks during a joint Hunt Operation on Department of Defense systems in Hawaii, Aug. 4-12, 2023.

U.S. Strategic Command, as a part of its mission to carry out global strategic operations, ran a series of network-strengthening and defense exercises that pitted the teams against a simulated adversary across multiple networks.

Hunt Operations involve teams of service members evaluating DoD networks for vulnerabilities; the Navy and Air Force defensive teams were also responding to simulated attacks carried out by a DoD-certified Army Cyber Red Team, which is specifically trained and tasked with emulating adversary forces.

“Hunt Operations are absolutely critical to ensuring our networks are robustly defended,” said U.S. Air Force Maj. Gen. John Nichols, U.S. Strategic Command’s director of global operations. “As a part of our ongoing self-assessment, operations like this help us stress-test our systems and ensure they are not just available, but resilient if attacked and ready to function in a contested environment.”

In line with the DoD’s 2023 cyber strategy, teams gained an operational advantage over a destructive cyberattack from malicious cyber actors against the DoD Information Network and more than 4 million DoD computers.

The responsibility to protect DoDIN falls to Joint Forces Headquarters-DoDIN, a component of the U.S. Cyber Command. JFHQ-DoDIN uses a unified force approach to network operations, security and defense across the DoDIN.

JFHQ-DoDIN and the services support Defensive Cyberspace Operations by globally integrating, synchronizing and directing priority actions across 45 DoDIN areas of operation that include all combatant commands, services, DoD agencies and field activities.

Defensive Cyberspace Operations consist of proactive, threat-informed steps to reduce cyber risk and respond to attacks against the DoDIN, ensuring that network operations remain agile and resilient. These operations are carried out across DoD networks daily.

Through these interactions with the service components and partners, JFHQ-DoDIN further enables the sharing of operational information and intelligence to enhance the resiliency and reliability of vital DoD networks and systems.

This particular Hunt Operation was somewhat unusual with teams coming from multiple services to not only work together, but also to look at each other’s networks. These activities further validated the status of directed network security action and provided a key defensive cyberspace priority designed to protect the totality of the DoDIN.

“Working together with teams from multiple services only increases our capabilities,” said the Navy lieutenant serving as cyber protection team leader. “We each bring our own service culture and unique capabilities, and through events like this we learn from one another.”