Role of the DoD Information Network (DODIN) in Supporting Operations

Proficiency Code: A

The DoD Information Network (DODIN) is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. The DODIN comprises all of DOD cyberspace, including the classified and unclassified global networks (e.g., NIPRNET, SIPRNET, Joint Worldwide Intelligence Communications System) and many other components, including DOD-owned smartphones, radio frequency identification tags, industrial control systems, isolated laboratory networks, and platform information technology (PIT). PIT is the hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, including weapon systems. Nearly every military and civilian employee of DOD uses the DODIN to accomplish some portion of their mission or duties.

The importance of Cyberspace Operations (CO) support to military operations grows in direct proportion to the joint force's increasing reliance on cyberspace. Issues that may need to be addressed to fully integrate CO into joint planning and execution include centralized CO planning for DODIN operations and defense and other global operations; the Joint Force Commanders (JFC's) need to integrate and synchronize all operations and fires across the entire Operating Environment (OE), including the cyberspace aspects of joint targeting; deconfliction requirements between government entities; Partner Nation (PN) relationships; and the wide variety of authorities and legal issues related to the use of cyberspace capabilities. This requires all members of the commander's staff who conduct planning, execution, and assessment of operations to understand the fundamental processes and procedures for CO, including the organization and functions of assigned or supporting cyberspace forces.

We continue to operate in a contested battlespace, where the barrier to entry is low and oftentimes unchallenged. We must recognize that mission success is defined by our ability to pre-emptively disrupt, degrade, or deny our adversaries, both internal and external, unimpeded access to the information and capabilities of the Department of Defense Information Network (DODIN). We must sustain our operations and defenses before, during, and after an attack by reducing the attack surface, continually improving defensive cyberspace operations, and effectively commanding and controlling the DODIN.

The DISA Strategic Plan for 2015 – 2020 will see the evolution towards executing synchronized DODIN command, operations, and cyber defense missions to ensure freedom of maneuver for the warfighter and mission partners. The strategic plan will establish, train, and implement cyber workforce elements; shape readiness through continuity programs; and execute synchronized operations that will offer us more visibility and response to cyber threats.