A Zero Trust Approach to Implementing Commander's Intent for Cybersecurity

CAPT Andrew D. "Andy" Stewart, USN (Ret.)
National Security and Government Senior Strategist for Cybersecurity
Cisco

A zero-trust design strategy based on a platform-approach that constantly enforces least-privilege access from edge to hybrid multi-cloud is the operational outcome for a software-defined network that satisfies Commander's Intent for Cybersecurity and DoD Network Operations. Implementing the Commander's Intent for Cybersecurity means applying, monitoring, and enforcing network controls as operational policy—including DoD Comply-to-Connect (C2C) requirements and integrating all network controlling actions across the enterprise from users/endpoints to data and applications—no matter where they reside. By implementing Commander's Intent for Cybersecurity, operations on DoD networks can be transformed into a real-time, network operational platform capability.

Just like commander's intent is applied through controlling actions and maneuver orders to units of action (according to the unit's identity and defined capabilities), so too must effective cybersecurity policy (commander's intent) be applied to users, devices, and applications with knowledge of their status, how they are connected to the network, their allowed data, applications, and functions on the network – with verification and validation – continuously, at speed and scale. Operationalizing the DoD Network Platform with this zero trust design approach will satisfy Commander's Intent for Cybersecurity.