

THE FUTURE FIGHT: CYBER ENABLING DECISION ADVANTAGE

How joint and combined cyber forces can achieve
greater agility, speed, scale, and effectiveness



The speed and complexity of U.S. full-spectrum cyber operations have grown exponentially since 2016 when it took months to coordinate Operation Glowing Symphony—U.S. Cyber Command’s first large-scale cyberattack to take down the global networks of ISIS. This initial use of CYBERCOM’s authorities, capabilities, and processes for offensive cyber operations set the stage for today’s persistent engagement with adversaries. But deterring or winning future conflicts requires greater agility, speed, and scale, as well as integration of full-spectrum cyber capabilities with other elements of national power and with joint and combined capabilities.

The decisive advantage in future conflict will go to the side that can sense, understand, decide, act, and assess faster and more effectively than adversaries. This is a clear lesson learned from multiple cyber and non-cyber operations conducted since 2001 and reinforced most recently during the Russia-Ukraine War.

U.S. and partner forces must synchronize and integrate kinetic and non-kinetic capabilities at all levels to generate concurrent effects across all domains faster and more effectively than the enemy. This is what the U.S. Army calls “convergence,” and achieving it will be a critical differentiator for US and allied forces in future conflict. It will enable the joint force to maintain information and decision advantage; preserve command, control, and communications systems; and ensure critical detection and targeting operations. Full-spectrum cyber forces will play a vital role in achieving convergence.

In any future competition, crisis, or conflict, the importance of the joint/combined force’s ability to integrate and synchronize special operations forces (SOF), space, and cyber capabilities across all warfighting domains cannot be overstated. More specifically, DOD’s ability to deliver the effects of the SOF-Space-Cyber triad in permissive to

denied environments will become critical for national efforts to project power, compete, and deter adversaries while remaining under the threshold of armed conflict.

The 2023 DOD Cyber Strategy describes how the department envisions wielding the nation’s military cyberspace capabilities. Since 2018, DOD cyberspace forces, in conjunction with interagency, foreign, and commercial partners, have executed a strategy of persistent engagement; full-spectrum cyberspace operations defending forward, actively disrupting malicious cyber activity before it can affect the U.S. homeland; and, as required, attacking adversaries in and through cyberspace.

To outpace adversaries in all domains the joint/combined force must be able to see itself, see the adversary, and see all other relevant actors, actions, and activities in the operations and information environments—and then act—all at mission-relevant speed and scale. The ability of DOD to deliver the operational capabilities mandated in the DOD Cyber Strategy depends on building a robust full-spectrum capable force enabled by secure and resilient networks, valid data, unique cyber weapons systems and infrastructure, realistic training, and effectively integrating cyber with all other warfighting domains.

National security increasingly depends on effective full-spectrum cyber operations. Cyber forces need to uphold national defense, disrupt and dismantle emerging threats, and collaborate with international partners. DOD and the industrial base have an unprecedented opportunity to build a truly integrated weapons platform that is agile, scalable, interoperable, and resilient. Realistic training and operations with mission partners will ensure cyber forces can effectively apply their talent and technological capabilities to enable decision advantage. Meeting these needs today will position the joint force to meet the operational needs of the nation.

The [new DOD Cyber Strategy specifies](#) that DOD’s Cyberspace Forces, in concert with partners, must:

- **Defend the Nation.** The Department will campaign in and through cyberspace to generate insights about malicious cyber actors, as well as defend forward to disrupt and degrade these actors’ capabilities and supporting ecosystems. Additionally, DOD will work with its interagency partners to leverage all available authorities to enable the cyber resilience of U.S. critical infrastructure and to counter threats to military readiness.
- **Prepare to Fight and Win the Nation’s Wars.** The Department will ensure the cybersecurity of the DOD Information Network and will further invest in the Joint Force’s cyber resilience. Additionally, the Department will use cyberspace operations to generate asymmetric advantages in support of the Joint Force’s plans and operations.
- **Protect the Cyber Domain with Allies and Partners.** The Department will assist U.S. Allies and partners in building their cyber capacity and capability, as well as expand avenues of potential cyber cooperation. DOD will continue to conduct hunt forward operations to build cyber resiliency and will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.
- **Build Enduring Advantages in Cyberspace.** The Department will optimize the organizing, training, and equipping of the Cyber Operations Forces and Service-retained cyber forces. Furthermore, DOD will invest in the enablers of cyberspace operations, including intelligence, science and technology, cybersecurity, and culture.

**EMPOWER PEOPLE TO
CHANGE THE WORLD®**

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the WorldSM.