


Readiness: Strengthen Posture & Decrease Risk

Command Vision & Strategy FY22 **FY23** FY24

Postured for Today's Competition & Ready for Tomorrow's Fight

2nd Edition, February 2023




Joint Force Headquarters-
Department of Defense
Information Network

Commander's Message

Joint Force Headquarters-Department of Defense Information Network's top priority is enabling mission assurance, and this requires laser-focused attention to readiness. That is, readiness of the DODIN, readiness of forces and reducing risk to the DODIN.

As we enter the second year of our three-year strategic plan, we have refined our approach to strengthen the posture of the 45 DODIN areas of operation (DAO), and thus decrease risk to DoD. Our fundamental critical success factors continue to be agility, resiliency, velocity of action, boldness and accessibility to the DODIN.

We know America's security demands that we remain postured for today's competition while being ready for tomorrow's fight. Progress requires us to find ways to enable and empower the DAO commanders and directors, capitalize on innovative technologies and operational maneuverability, and leverage partnerships and our workforce to address critical challenges.

I am excited about the future and the opportunities it brings for JFHQ-DODIN to drive the Department to unparalleled heights.

Respectfully,
Robert J. Skinner
Lieutenant General, USAF
Commander, JFHQ-DODIN

Vision

Postured for today's competition and ready for tomorrow's fight.

Mission

JFHQ-DODIN effectively executes command and control by integrating, synchronizing and directing DODIN operations, security and defensive maneuvers to enable power projection and freedom of action across all warfighting domains.

Guiding Principles

Create Agility & Velocity

Operating as a unified force in steady-state competition against adversaries leads to economies of scale for DODIN cyberspace forces and enables them to thrive during times of uncertainty and crisis. This unified construct creates time and space for innovation to bolster decision-making with velocity, precision and inherent agility.

Understand Threat Environment

Understanding adversaries' intent, capabilities and campaigns underpins the ability to prioritize resources and actions protecting critical DoD data, DODIN infrastructure and DODIN-enabled capabilities.

Secure & Advocate

DoD cyberspace is best protected when all elements of the DODIN and the diverse DODIN-enabled capabilities are engineered and maintained for security throughout the design, development and operations lifecycle. Advocating for and supporting all DAOs and Sectors reinforces the importance of addressing priority needs as a unified force for developmental initiatives, policy, process changes and resources.

Embrace & Manage Risk

Real-time situational understanding of the cyber operational and threat environments gives commanders and directors decision-quality information to make risk-informed choices to improve their organization's posture.

Seamlessly Integrate

Critical thinking and integrating diversity of thought and experiences from the headquarters workforce, DODIN areas of operation and partners enhance mission success.

The DODIN & Cyberspace Environment

Cyberspace is a precarious environment and the DODIN, DoD's cyber operational battlespace underpinning all DoD missions, is dynamic and ever-changing within the greater cyber landscape.

Adversaries operate at an advanced level in scope, scale and sophistication through both opportunistic and long-term malicious campaigns. They relentlessly aim to infiltrate the DODIN and supply chains to damage, disrupt, and manipulate information, missions, operations, weapons systems and partner relationships. As a result, the cyber environment is ubiquitously contested at all times, from the garrison to the combat zone.

Readiness of the DODIN and readiness of DODIN cyberspace forces (DCF) require cultural change across DoD to give the operational perspective priority for training, technology and resource decisions. DCF include Cyberspace Operational Forces (COF) and other forces such as red teams, Mission Defense Teams and other DoD units that conduct network operations, security and on-DODIN defensive activities.

As part of engaging with adversaries, JFHQ-DODIN leverages information exchanges with partners while it directs, synchronizes and validates actions made by the DAOs to reduce and harden attack surfaces.

These efforts are integral to U.S. Cyber Command's (USCYBERCOM's) persistent engagement approach with the concepts of anticipatory resilience, defend forward and contest actions for full-spectrum cyberspace operations.

The goal is to create a seamless transition between on-DODIN and off-DODIN activities through continually strengthening the agility and resiliency of the infrastructure and processes.

Where We Need To Be

The future DODIN architecture and operations must be based on joint and coalition perspectives for mission assurance supported by the deliberate convergence of command and control processes, technology development and employment, and human action in the operational environment. The purpose is to directly support integrated deterrence operations, and enable readiness and dynamic employment of a lethal force.

Enabling Integrated Deterrence

Adaptable and defendable networks enable:

- Decisions that spark rapid response to cyber incidents
- Actions that create resiliency in technology and processes
- Understanding of the dynamic cyber terrain and the internal DoD and coalition interdependencies necessary in multi-domain operations
- Understanding adversary interests and targets
- Imposing costs to adversaries
- Layered security and defense
- Aligning forces to essential missions with understanding of the relationship between readiness of the forces, cyber terrain and mission essential tasks

Necessary conditions include:

- A secure data-centric, zero-trust environment
- Common understanding of the operational risk—who is taking risk and who is responsible for the outcome
- Deconflicted statutes, policies and doctrine
- An operational mindset toward outcomes and capabilities oriented toward mission assurance, resourcing, operational decisions and priorities

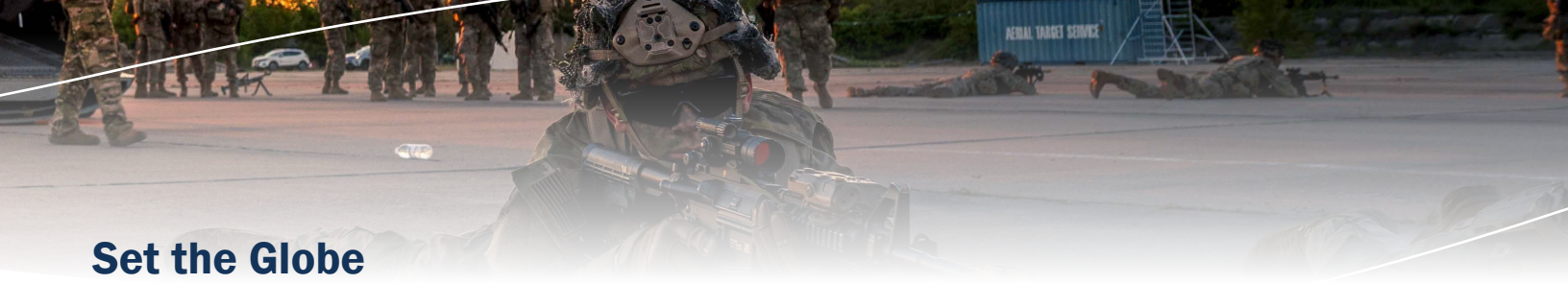
Enabling Dynamic Operations

Threat and operationally informed decisions about network operations, security and defense of the DODIN enable:

- The capability to fully support the warfighter's transition to crisis contingency with near-peer competitors at little to no notice
- Integration with partner networks and capabilities, at notice, to rapidly respond to missions where partner involvement is optimal
- The network architecture, DODIN-enabled capabilities and processes designed to rapidly support the movement of forces for priority operations

Necessary conditions include:

- Network operations, security and defensive priorities based on operational needs and requirements
- Common understanding of DCF alignment, readiness and force posture
- Decisions about policy, funding, resources, technology and priority actions informed by threat conditions
- Integration of risk management and network operations, security and defensive actions enabling operational outcomes
- A combat development function for full-spectrum cyberspace operations
- Processes and tools for continuous holistic assessment, tracking, reporting and aligning readiness of cyber terrain and assigned forces to operationally prioritized mission essential tasks across the four DoD core functions of warfighting, Services man/train/equip, DoD intelligence activities and business operations



Set the Globe

This Command Vision & Strategy, with the FY23 strategic and operational theme "Readiness: Strengthen Posture & Decrease Risk," reflects the global responsibility to fortify the DODIN security posture through continually calibrating standards, risk and operations to improve the performance of all DAOs and Sector missions. Our campaign approach with enduring pursuits and near-term and current planning objectives drive those areas we directly influence, and help shape those areas of interest where other entities have lead. The five lines of effort are critical aspects of full-spectrum cyberspace operations and include tasks for the headquarters and for the DODIN areas of operations and Sectors. They reinforce unity of command to compel action, enable accountability, optimize technology and shape cultural change across DoD.

Battlespace

The DODIN areas of operations are the center of gravity for the secure, operate and defend the DODIN mission area. Their role is critical to managing cyber risk to DoD missions. This factor reinforces the command-centric operational framework (CCOF) empowering and enabling commanders and directors to achieve unity of command and action to direct all DODIN cyberspace forces that conduct network operations, network security, and network defense for their area of responsibility. It enables DAO commanders and directors to support DODIN-wide requirements, Sector mission requirements and establish priorities for their own mission assurance. This common DoD framework provides the authoritative lineage from the Unified Command Plan (UCP) to the forces that conduct the mission. It is foundational to operational effectiveness and enables U.S. Cyber Command to fulfill its UCP responsibility for the DODIN mission area through JFHQ-DODIN. We will continually examine how we execute our supported and supporting roles with all DAOs and Sectors.

Overview of Scope & Activities:

- Organize the DODIN, ensuring all terrain and forces are assigned to the appropriate DAO commander or director
- Establish standardized functions, roles and responsibilities for network operations, security operations and on-DODIN defensive operations
- Institute, through DoD cyber academic programs, a common understanding about DODIN operations, security and defense mission area concept of operations to promulgate understanding of the command-centric operational framework for cyber
- Influence individual and collective multi-echelon preparedness through standards for COF training and certification, and integrating realistic cyberspace operations into joint exercises
- Establish readiness expectations and assessment standards for the DODIN terrain and DODIN cyberspace forces, as well as certification of DAOs

Defend

Actively defending the DODIN involves effectively and rapidly maneuvering forces and shaping or manipulating the terrain to obtain operational advantage. These actions are designed to impose cost to adversaries through a proactive unified force approach to on-DODIN operations. These activities are crucial to USCYBERCOM's full-spectrum cyberspace operations by creating a seamless transition between on-DODIN and off-DODIN activities. JFHQ-DODIN leverages unity of action across DAOs to direct daily operational activities and defensive actions to reduce and harden the attack surface, conduct countermeasures, mitigate vulnerabilities, remediate adversary attacks, manage a sensoring strategy, and leverage the cyber protection teams managed by various DoD organizations. These approaches are intended to make attempting to attack the DODIN unattractive to adversaries because it increases their

cost of resources and time, thus outweighing their perceived benefits and return on investment. We will coordinate across the DODIN to identify, aggregate and analyze risk factors, as well as facilitate information exchange and take operational lead for potential and actual adversary activity on networks for those incidents that involve more than one DAO or have potentially broad impact.

Overview of scope and activities:

- Conduct and coordinate maneuver defensive operations and coordinate actions with other USCYBERCOM components for full-spectrum cyberspace operations
- Manage incident response on the DODIN when best-postured to do so and/or when an incident impacts more than one DAO

Partnerships

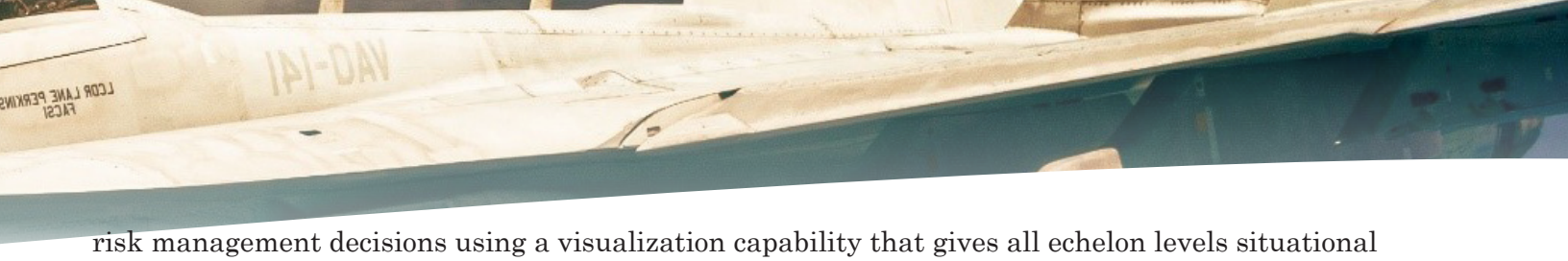
The global strategic competition environment requires partnerships acknowledging shared risks, expressing shared goals and seeking shared solutions. We prioritize partnership development to enhance awareness and interoperability for synergistic and integrated operations. Our internal-DoD partnerships press for changes in doctrine and policy to accurately reflect the secure, operate and defend the DODIN mission area responsibilities. These internal relationships center on developing common understanding to ensure technology and capability development, resource planning and support activities align with operational requirements. Our broad external reach focuses on strengthening relationships with U.S. federal agencies, allies, coalition, international partners, academia, Defense Industrial Base, and the commercial defense and technology sectors. We actively participate in USCYBERCOM's Academic Engagement Network by working closely with West Virginia University and Marshall University on curricula and special research projects that support the Command's mission. These efforts elicit partners to join the Command in protecting vital warfighting systems which defend the nation while promoting STEM careers within the DoD. Critical elements of these partnerships involve information exchange about operations, threat environment, vulnerabilities, technical expertise, capabilities and capacity, processes and practices, and talent development. We will continue to enhance relationships to identify and leverage partner authorities, responsibilities, and capabilities for network operations and protecting the DODIN.

Overview of scope and activities:

- Drive revisions of existing and establish needed new doctrine and policy to accurately reflect cyberspace operations and DODIN network, security and defense operations
- Increase operational perspective in decision-making about what operates on the DODIN
- Enhance partnerships with DoD organizations, intelligence and law enforcement communities, National Security Agency Cyber Security Directorate, CIO community and others on priority operational requirements for the mission area
- Explore information exchange opportunities and standards with international and coalition partners to strengthen operational dynamics and resiliency
- Build and expand relationships with external entities in academic and industry sectors to pursue collaborative training and education

Resiliency

Resiliency refers to having strong networks and processes that can fully and quickly recover from an adversary's presence or attack. Speed of action is the driving force to ensure continuity of network, cyber security and defensive operations. JFHQ-DODIN proactively engages across DoD to identify cyber requirements for the mission area, optimize current capabilities and capacity to the fullest potential, and operationalize modernization efforts and new technology solutions and processes across three horizons—existing, emerging and future. The priority centers on having timely information supporting



risk management decisions using a visualization capability that gives all echelon levels situational understanding of the cyber environment. The visualization allows USCYBERCOM, JFHQ-DODIN, and Sector and DAO commanders and directors to make informed decisions based in-part on assessments, mission and terrain mapping, operational sensors and threat conditions. The Nuclear Command, Control & Communication Sector and Classified and Special Networks will continue to have priority attention. We will continue to advocate for DAOs, Sectors and other DoD entities to identify and integrate enterprise level technical capabilities designed to improve velocity of action, precision and agility.

Overview of scope and activities:

- Develop and establish mechanisms and processes that create shared understanding across DoD of risks associated with network operations, security operations and on-DODIN defensive operations
- Synchronize Zero Trust principles in DODIN operations
- Establish a continuous holistic assessment framework for DAOs that includes assessment of the DODIN terrain and force posture and readiness
- Develop and leverage multi-echelon visibility and visualization efforts such as Joint All-Domain Command and Control and Joint Cyber Warfighting Architecture

Workforce

Workforce competency and organizational culture significantly influence DoD mission assurance. They are essential factors to ensuring the necessary operational perspective guides decision-making about emerging technologies and resources. We will advocate for all decisions about the DODIN to be made with this operational perspective as the priority and we will operate with a culture of velocity, critical thinking, accountability, responsiveness and communication with components, partners and our workforce. A part of this effort involves working with DoD entities to establish a knowledge base about the secure, operate and defend the DODIN mission area. With this, we will look across the talent pool to ensure we have the right diversity of thought, education, subject matter expertise and competencies. Attracting and retaining high-end talent are important elements of our talent management approach that encompasses active duty, civilian, contract and reserve personnel.

Overview of scope and activities:

- Implement a JFHQ-DODIN comprehensive human capital strategy
- Pursue resources to optimize DODIN-wide technical and joint operational capabilities and human competencies across DAOs
- Identify and refine governance, processes and practices

Way Ahead

This command vision outlines a bold strategic path to fulfilling our command and control mission as USCYBERCOM's operational arm protecting the DODIN. The efforts support the critical need for ongoing situational understanding of the cyberspace operating environment informing risk-to-mission decisions on a daily basis. We recognize the way ahead will continue to be dynamic and our lines of efforts are the guides that will keep us focused on the future.

The scope and activities listed are our priority targets for FY23. Collectively, they reflect critical themes for the headquarters and the mission area: promulgating and institutionalizing the command-centric operational framework across the cyberspace operational warfighting domain; establishing standards for forces and terrain, enhancing technology and automation, and leveraging continuous assessments and accountability that will shape cultural change across DoD. Progress in each of the lines of effort and key activities will be measured by multiple factors and will drive our battle rhythm to enable timely adjustments.




JFHQ-DODIN

Postured For Today's Competition. Ready for Tomorrow's Fight.

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) drives unified actions to improve DODIN agility and resiliency to preserve mission assurance and increase DoD's competitive advantage. Our mission addresses complex issues 24 hours a day, 7 days a week and 365 days a year. As a component command of U.S. Cyber Command, JFHQ-DODIN's global command and control responsibility establishes a postured unified force approach to network operations, security and defense that enables active maneuver and rapid response across all DODIN areas of operations (DAOs). With each DAO commander and director responsible and accountable for their organization's DODIN terrain, JFHQ-DODIN integrates, synchronizes and directs priority actions to actively manage cyberspace risk to DoD core functions, missions and Sectors.