Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)
Concept of Operations (CONOPS)

Mission

JFHQ-DODIN exercises command and control of DODIN Operations (DODIN Ops)[1] and Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)[2] globally in order to synchronize actions to project and protect DOD Component capabilities and activities that enable power projection and freedom of action across all warfighting domains.

Concept of Operations

Intent The DODIN is contested battlespace. It is constantly reconnoitered and probed; it has been infiltrated and even attacked. Adversaries have demonstrated a willingness and ability to deny our critical capabilities and infrastructure[3] by attacking the information systems, networks, and data that reside on the DODIN. The DODIN enables virtually all DOD activities from the Services' "man, train, and equip" functions to business functions to full spectrum warfighting operations. Information and data on the DODIN encompass routine communications, personally identifiable information (PII), mission critical data, and the DOD's most sensitive information. In short, the DODIN enables all functions executed by the DOD that give the United States an operational advantage over any adversary. For this reason, the DODIN will continue to be targeted by our enemies.

My intent is to fight and win on the DODIN. There is a continuous struggle to establish and maintain the initiative in this battlespace, inability to do so could lead to mission failure for DoD Components. Our objectives are clearly defined in Concept Plan (CONPLAN) 8039, Operation GLADIATOR PHOENIX (OGP), and Operation GLADIATOR SHIELD (OGS), as part of the "Secure, Operate, and Defend the DODIN" mission. In steady-state, we will conduct DODIN Ops and DCO-IDM at the operational level to: provide access to and protect the information that resides on the DODIN; project the DODIN into joint operational areas to support Combatant Command (CCMD) operational requirements; and preserve DOD functions and traditional warfighting capabilities. JFHQ-DODIN is uniquely postured and empowered to ensure we fight as a unified

[1] DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions which address the entire DODIN, including configuration control and patching, IA measures and user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data. Although many DODIN operations activities are regularly scheduled events, they should not be considered routine or unimportant, since their aggregate effect establishes the security framework on which all DOD missions ultimately depend.

[2] DCO includes outmaneuvering adversaries taking or about to take offensive actions against defended networks, or otherwise responding to internal and external cyberspace threats. Most DCO occurs within the defended network. Internal defensive measures include mission assurance actions to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks to ensure sufficient cyberspace access for JFC forces. (JP 3-12).

[3] Critical Infrastructure refers to those assets on the DODIN under both the Defense Critical Infrastructure Program (DCIP) and DHS Critical Infrastructure and Key Resources (CI/KR) National Infrastructure Protection Plan.

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)
Concept of Operations (CONOPS)

Joint Force to provide, project, secure, and actively defend the DODIN. If measured by doctrinal phases of the Joint Campaign, JFHQ-DODIN operates in Phase 3, "Dominate," to defeat attempts that restrict our maneuver and the full-utilization of the DODIN to enable DOD capabilities.

Focus Areas

1. Support DOD Mission Essential Tasks and Functions Enabled by the DODIN. In steady-state and contingency operations, JFHQ-DODIN works alongside a supported command or agency to collectively develop situational understanding of how the DODIN supports their mission. We will analyze the supported commander's or director's mission and mission essential tasks to identify DODIN dependencies. Once identified, the supported command or agency will conduct DODIN Ops and DCO-IDM within their authority, capabilities, and capacity to secure and actively defend DODIN-enabled mission critical tasks and functions. As part of DODIN Ops, JFHQ-DODIN must assure the mission by adding redundancy, resiliency, and survivability to those DODIN-enabled mission critical tasks and functions. JFHQ-DODIN will direct actions to provide and project the DODIN in support of operational requirements and to secure and actively defend any DODIN dependencies *outside* the supported commander's or director's authority, capabilities, and capacity.

2. Integrate Planning and Execution. JFHQ-DODIN integrates DODIN Ops and DCO-IDM planning and execution into Combatant Command, Service, Agency, and Field Activity (CC/S/A/FA) operations as a supported and supporting command.

   JFHQ-DODIN conducts planning in accordance with U.S. Strategic Command (USSTRATCOM) and U.S. Cyber Command (USCYBERCOM) roles as supported commands. JFHQ-DODIN will publish an operation order for the global "Secure, Operate, and Defend the DODIN" mission under OGS and within context of the full-spectrum cyberspace operation order, Operation GLADIATOR ARMOR. As a supporting command, JFHQ-DODIN will plan to integrate DODIN Ops and DCO-IDM in support of CC/S/A/FA plans and operations. JFHQ-DODIN and regional DODIN Commands, if established, will build DODIN Ops and DCO-IDM actions and activities into CCMD plans from the ground up.

   In execution, JFHQ-DODIN serves simultaneously as a supported and supporting command. JFHQ-DODIN serves as a supported command for the "Secure, Operate, and Defend the DODIN" mission to synchronize and deconflict DODIN Ops and DCO-IDM actions and activities globally. As a supporting command, JFHQ-DODIN directs DODIN Ops and DCO-IDM actions and activities that are outside the scope of the supported CC/S/A/FA authority and ability to influence. At the operational level of war, JFHQ-DODIN seeks to support and to reinforce, not to replace CC/S/A/FA DODIN Ops and DCO-IDM efforts. To be successful in both roles, JHFQ-DODIN must ensure the following:

a. Global (enterprise-wide) overwatch – DODIN Ops and DCO-IDM actions and activities are in accordance with the DODIN's defensive posture and how we fight as a Joint Force.
b. Interdependent actions between DoD Components are coordinated and synchronized in time and space to meet operational requirements.
c. DODIN Ops and DCO-IDM are integrated into the supported command/agency plans and operations - providing greater understanding of effects (good and bad) on mission assurance.
d. DODIN Ops and DCO-IDM supporting tasks are identified and assigned to those DOD Component forces best postured to execute those tasks.

3. Synchronize and Deconflict Global, Regional, and Functional DODIN Ops and DCO-IDM. The "Secure, Operate and Defend the DODIN" mission requires Commander, JFHQ-DODIN (CDRJFHQ-DODIN) to act simultaneously as both a supported and supporting commander. ***Global and functional operational requirements for DODIN Ops and DCO-IDM are steady-state and continuous, they are global in nature, enterprise-wide, and inextricably linked to DOD activities.*** In accordance with CDRUSSTRATCOM Unified Command Plan (UCP)-assigned responsibility and CDRUSCYBERCOM authority and direction, CDRJFHQ-DODIN serves as a supported commander to meet these global and functional operational requirements for all DOD Components. Concurrently, as tasked by CDRUSCYBERCOM, CDRJFHQ-DODIN serves as a supporting commander to designated DOD Component commanders or directors to meet regional and functional operational requirements. To do so, JFHQ-DODIN reconciles global, regional, and functional priorities by synchronizing and deconflicting DODIN Ops and DCO-IDM actions and activities. As forward extensions of JFHQ-DODIN, regional DODIN Commands synchronize and deconflict regional DODIN Ops and DCO-IDM actions and activities under the tactical control (TACON) of the geographic combatant commander. JFHQ-DODIN uses a mission-based, threat-focused operational approach that seeks to project and protect the DODIN to meet supported commands/ agencies operational needs by combining the capabilities of defensive cyberspace forces (e.g., Cyber Protection Forces, Incident Response Teams (IRT), Computer Emergency Response Teams (CERT), Red Teams, Computer Network Defense Service Providers (CNDSP) and DODIN Ops elements) in ways that are complementary, mutually reinforcing, and aligned to support DOD Component missions. Through its command relationships, JFHQ-DODIN furthers an agile, unified, and responsive defense in depth. As with other operational domains, JFHQ-DODIN escalates those competing priorities that cannot be resolved at the operational-level.

4. Direct and Assess the Defensive Posture of the DODIN. As directed by USCYBERCOM, JFHQ-DODIN directs and verifies the defensive posture of the DODIN to achieve a high state of cybersecurity readiness consistent across the whole of the DODIN. The defensive posture is

dynamic, responsive to mission needs, evolving threats, and the operating characteristics[4] of a man-made domain. Assessments complement the DODIN's defensive posture by verifying a high state of cybersecurity readiness that is mission-based and threat-focused. Mission-based, threat-focused cybersecurity readiness changes the focus of CC/S/A/FA assessments from measuring strictly compliance to gauging operational risk as a function of mission-impact, threat, and vulnerability. Cybersecurity readiness assesses compliance as it relates to the information systems, networks, and data on which organizational missions depend.

5. Produce and Disseminate Intelligence Tailored for DODIN Ops and DCO IDM. The JFHQ-DODIN will collect and analyze operationally relevant information on the DODIN. This is battlefield or combat information[5] gleaned from the DODIN (blue space); it is fused with intelligence reports about threats to and vulnerabilities in the DODIN to provide a more accurate picture of the operating environment and support predictive intelligence to inform the DODIN's defensive posture, DODIN Ops, and active and passive DCO-IDM. These information and intelligence feeds are continuously aggregated, analyzed, and correlated to provide a current picture of the operating environment, produce intelligence products, and refine the Joint Intelligence Preparation of the Operating Environment (JIPOE). These products characterize the threat and the operating environment, and they are disseminated to support DoD component DODIN Ops and DCO-IDM. In this fashion, intelligence drives operations, while operations produce information that yields greater intelligence.

Purpose To plan, direct, and synchronize global, regional, and functional DODIN Operations and DCO-IDM in support of DOD Component missions.

Method JFHQ-DODIN will establish a command relationship with all DOD Components that conduct DODIN Ops and DCO-IDM to achieve unity of command and promote unity of action. In compliance with direction from USCYBERCOM, JFHQ-DODIN will operate simultaneously as a supported and supporting command to meet global, regional, and functional requirements. To exercise its command and control functions, JFHQ-DODIN synchronizes and deconflicts DODIN Ops and DCO-IDM actions and activities globally that provide, project, secure, and actively defend the DODIN. Regional DODIN Commands serve as a forward extension of JFHQ-DODIN under TACON of the geographic Combatant Commander to synchronize and deconflict regional DODIN Ops and DCO-IDM. JFHQ-DODIN directs the movement and maneuver of organic cyberspace forces. When best postured, uniquely qualified, and as directed by higher

[4] Those military characteristics that pertain primarily to the functions to be performed by equipment, either alone or in conjunction with other equipment; e.g., for electronic equipment, operational characteristics include such items as frequency coverage, channeling, type of modulation, and character of emission. JP 5-0.

[5] Time sensitive information is treated as "combat information" defined in JP 2-01 as "unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements."

headquarters, JFHQ-DODIN exercises TACON of USCYBERCOM Service Component Headquarters; a supported/supporting relationship with combatant commands; an adjacent command relationship with designated organizations operating enclaves on the DODIN based on unique authorities, roles, and missions; and Directive Authority for Cyberspace Operations (DACO) over all other DoD Components. JFHQ-DODIN conducts intelligence operations that collect and analyze battlefield (or combat) operational information, aggregate information and intelligence reports, and produce and disseminate operational intelligence relative to the mission, threat, and operating environment.

Endstate Successful implementation of this CONOPS is described as follows: JFHQ-DODIN achieves unity of command and promotes unified action by DOD Components conducting DODIN Ops and DCO-IDM on the DODIN as it currently exists - in a federated, tiered state, comprised of Service and Agency systems, networks, and data in a military operational domain; JFHQ-DODIN and regional DODIN Commands are postured to project and protect the DODIN in Joint Operational Areas (JOA); defensive cyberspace forces' actions and activities are synchronized to actively defend DOD Components' missions, tasks, and functions that depend on access to and effective operations on the DODIN; friendly cyberspace is secured and defended in depth from boundary to host levels by integrating cyberspace DCO-IDM forces, sensors, and systems in an appropriate defensive posture; and known or likely threats to the DODIN and their impact to military operations are identified and mitigated to enable power projection and freedom of action across all warfighting domains.

Operational Approach In steady-state operations, JFHQ-DODIN conducts DODIN Ops and DCO-IDM at the operational level of war in support of all DOD Components. While DODIN Ops and DCO-IDM may be treated as distinct lines of operations/effort, they are mutually reinforcing and require a commander to synchronize and deconflict actions and activities globally. As a subordinate command to USCYBERCOM, JFHQ-DODIN will accomplish objectives and assigned tasks associated with CONPLAN 8039 "Secure, Operate, and Defend the DODIN," by employing a mission-based, threat-focused operational approach that uses engagement criteria and groups DOD Components by authorities, roles, and missions. This approach combines complementary DODIN Ops and DCO-IDM actions and activities to protect DOD component missions, tasks, and functions enabled by the DODIN against known and likely threats. JFHQ-DODIN leverages CDRUSSTRATCOM UCP-assigned mission authorities delegated through USCYBERCOM to execute joint functions Command and Control (C2); Movement and Maneuver; and Intelligence to promote unified action across the DODIN and to support DOD Component mission assurance.

Engagement Criteria When the Secretary of Defense (SECDEF) directed CDRUSCYBERCOM to establish JFHQ-DODIN, it completed a larger C2 Framework that provided operational and tactical level oversight for full-spectrum cyberspace operations (Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and DODIN Operations (DODIN

Ops). JFHQ-DODIN was delegated authority for operational and tactical level planning, execution, and oversight for global DODIN Ops and DCO-IDM.

The span of control associated with JFHQ-DODIN authority exceeds 50 organizations (CC/S/A/FA). An optimal span of control is between five and seven organizations. To make the span of control feasible, JFHQ-DODIN uses engagement criteria to determine how best to exercise command through the authorities vested in CDRJFHQ-DODIN for the "Secure, Operate, and Defend the DODIN" mission. The engagement criteria bound JFHQ-DODIN DODIN Ops and DCO-IDM and preserve capabilities and capacity in order to apply them at the decisive time and place. It is best expressed as three questions in which an affirmative response to any one question meets the JFHQ-DODIN engagement criteria to conduct DODIN Ops and DCO-IDM actions and activities.

1) Is JFHQ-DODIN uniquely postured and empowered (authorized) to perform them?
2) Are they more effectively executed across the whole of the DODIN (enterprise-wide) through JFHQ-DODIN engagement?
3) Has higher headquarters (CDRUSCYBERCOM) directed them?

Grouping DOD Components by Common Roles, Missions, and Authorities JFHQ-DODIN groups DOD Components (CC/S/A/FA) into groups or "bins" based on authorities, roles, and missions. Along with the engagement criteria described above, these bins create a feasible span of control by enabling CDRJFHQ-DODIN to tailor C2 functions to the common authorities, roles, and missions of each bin. With this understanding, CDRJFHQ-DODIN establishes a C2 relationship with each CC/S/A/FA to exercise operational level C2. There is no change to CC/S/A/FA authorities to execute DODIN Ops and DCO-IDM actions and activities - to secure, operate, and defend their respective cyberspace on the DODIN. Each organization brings unique skills, expertise, and capabilities that cannot be replicated and sustained at JFHQ-DODIN. In accordance with the engagement criteria, JFHQ-DODIN exercises TACON of USCYBERCOM Service Component Headquarters; a supported/supporting relationship with combatant commands; an adjacent command relationship with designated organizations operating enclaves on the DODIN based on unique authorities, roles, and missions; and Directive Authority for Cyberspace Operations (DACO) over all other DoD Components. JFHQ-DODIN exercises these authorities to synchronize, deconflict, and direct DODIN Operations and DCO-IDM for those actions and activities that are DODIN-wide; beyond the scope, authority, and capability of any one CC/S/A/FA; and directed by CDRUSCYBERCOM.

Key Tasks

1. Exercise operational level C2 of DOD Components to achieve unity of command for global DODIN Ops and DCO-IDM.

2. Provide and project the DODIN and secure and actively defend DODIN-dependencies in support of DoD Components' mission essential tasks and functions to contribute to mission assurance.

3. Produce and disseminate intelligence on threats and DODIN vulnerabilities to secure and defend critical information, Cyber Key Terrain (C-KT), Defense Critical Infrastructure Program (DCIP) assets, and Critical Infrastructure/Key Resources (CI/KR) on the DODIN.

4. Synchronize DODIN defense in depth (from DODIN boundary to individual systems) to clear adversary and unauthorized activities on the DODIN and to assure operational forces the ability to freely maneuver and project power.

5. Integrate DODIN operations and DCO-IDM in global, regional, and functional plans and operations in order to establish cyberspace superiority.

Command and Control

The JFHQ-DODIN mission mandates a command relationship with all DoD Components to include those not assigned to CDRUSSTRATCOM. JFHQ-DODIN exercises its C2 functions as an operational level headquarters on the DODIN - as it exists today, while prepared to modify this CONOPS in support of changes to the DODIN and as the DOD progresses toward the Joint Information Environment (JIE) endstate. The DODIN enables daily mission-critical tasks and functions for the entire DOD. Accordingly, JFHQ-DODIN's OGS steady-state operations as a supported and supporting command are in Phase 3 of the Joint Campaign, "Dominate."

JFHQ-DODIN will plan, execute, direct, coordinate, and assess the execution of global DODIN Ops and DCO-IDM in coordination with all DOD components (CC/S/A/FA). This includes support to the larger DOD C2 framework integrating all Enterprise Operations Centers (EOC) - when established - and global EOC (GEOC) functions and activities; sensor and Computer Network Defense (CND) tools programs; and CNDSP efforts. In this role, JFHQ-DODIN fills a critical gap in the DOD's operational command structure for full-spectrum cyberspace operations (CO). JFHQ-DODIN's role as an operational level headquarters, balancing global, regional, and functional priorities for DODIN Ops and DCO-IDM, enables more effective C2 across the three lines of CO (OCO, DCO, and DODIN Ops).

Based on the scope, scale, and complexity of the DODIN, JFHQ-DODIN exercises operational level C2 authorities to synchronize DODIN Ops and DCO-IDM to enable Commanders/Directors mission essential tasks and functions. DOD Components possess individuals and cyberspace forces with the knowledge, skills, and abilities to identify their unique DODIN-enabled mission dependencies. For this reason, DOD Components conduct DODIN Ops and DCO-IDM for the respective systems, networks, and data within their cyberspace on the DODIN. It would be infeasible for JFHQ-DODIN to replicate this expertise.

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)
Concept of Operations (CONOPS)

The DODIN is currently a multi-tiered, federated, and interconnected network of networks in which one DOD Component's authority and infrastructure rely upon another DOD Component's authority and infrastructure and so on. The scope, scale, and complexity increase multifold when the DODIN is projected into a Joint, Interagency, Intergovernmental, and Multinational (JIIM) operational area to support a Mission Partner Environment (MPE). As part of DODIN Ops, JFHQ-DODIN synchronizes actions and activities across these seams in authority and infrastructure to empower Commanders to fully employ the DODIN in support of military operations. Implied in this task is the requirement to concurrently secure and proactively defend the DODIN through DCO-IDM.

JFHQ-DODIN's subordinate regional DODIN Commands are a forward extension of JFHQ-DODIN and serve two primary purposes; (1) to enable JFHQ-DODIN to exercise a C2 framework that simultaneously meets global and regional commander's priorities, and (2) to participate in the supported commander's battle rhythm to fully integrate DODIN Ops and DCO-IDM into plans and operations. In this capacity, regional DODIN Commands provide subject matter expertise on DODIN Ops and DCO-IDM that fall within the supported commander's authority, as well as reachback to JFHQ-DODIN to synchronize those supporting actions and activities that fall outside the supported commander's authority.

Two key questions must be answered when projecting the DODIN into an area of operations; (1) what mission threads (Service, Joint, Coalition, IC, Interagency, etc.) does the commander need to accomplish the mission; and (2) what classification are the networks containing those threads?

The Afghan Mission Network, predecessor to the Mission Partner Environment (MPE) contained eight mission threads. They were classified up to Mission SECRET to provide the Combined Joint Force Commander the ability to fight with all coalition forces across the joint functions - C2, Intelligence, Fires, Maneuver, Force Protection, and Sustainment.

Regional DODIN Commands further mitigate risk to mission for CDRJFHQ-DODIN whose span of control exceeds 50 DOD components (CC/S/A/FA). As an operational level headquarters, JFHQ-DODIN must maintain effective situational awareness (SA). Geographic CCMDs pose the greatest risk to SA due to dispersed basing, operating locations, and joint operational areas that reside within the CCMDs AOR. Establishing regional DODIN Commands as forward extensions of JFHQ-DODIN, under the Combatant Commander's TACON authority, and embedded in the battle rhythm, improves CDRJFHQ-DODIN situational understanding and mitigates risk to mission. Further, regional DODIN Commands forward presence facilitates a close working relationship with the Defense Information Systems Agency (DISA) field commands, Service forces and elements, and Agency personnel who are also positioned forward. The regional DODIN Commands' Area of Support (AOS) corresponds to the supported commanders' Area of Responsibility (AOR) and their line of communication with JFHQ-DODIN strengthens the ability to simultaneously meet global, regional, and functional priorities.

Movement and Maneuver

As a man-made operational domain, cyberspace is unique in the movement and maneuver of forces. In traditional operational domains – sea, air, land, and space, the Joint Force operates within the existing domain. Cyberspace terrain can be created. In fact, it must be created to support our ability to project the military instrument of national power in response to requirements for military operations (JP 3-0). This is a critical aspect of DODIN Ops, specifically the ability to project the DODIN in a secure, defensible manner to support the movement and maneuver of cyberspace forces that actively defend the warfighting capabilities of the Joint Force.

JFHQ-DODIN synchronizes and deconflicts the movement and maneuver of cyberspace forces both physically and logically to conduct DODIN Ops and DCO-IDM. As part of DODIN Ops, JFHQ-DODIN supports the Joint Force's operational reach by providing DODIN-enabled capabilities and projecting the DODIN into operational areas. At the operational level of war, cyberspace forces are tasked to control operationally significant areas of the DODIN and conduct DCO-IDM and operational assessments. Additional supporting and command-linked tactical tasks for DODIN Ops and DCO-IDM may be assigned based on mission analysis. The secure configuration of the DODIN and its active defense are continuous security measures; they remain an implied task for DODIN Ops and DCO-IDM actions and activities. As a supported or supporting command, JFHQ-DODIN also directs the movement and maneuver of its own organic cyberspace forces to meet global, regional, and functional operational requirements.

Mission, enemy, and cyberspace terrain considerations are combined with the availability, readiness, and capability of cyberspace forces as well as mission timelines to outline CDRJFHQ-DODIN's situational understanding and to drive decisions as to the movement and maneuver of cyberspace forces (ref METT-T). Mission-based movement and maneuver for DODIN Ops and DCO-IDM is directed to project, secure, and actively defend those information systems, networks, and data that provide critical capabilities to accomplish mission-essential tasks and joint functions. When DODIN Ops project the DODIN into a Joint Operations Area (JOA), movement and maneuver planning considerations must include those Joint Forces needed to successfully extend the DODIN in a secure and defensible manner. In support of CC/S/A/FA Phase 0 operations, mission-based movement and maneuver focuses on how best to position cyberspace defensive forces to provide, secure, and actively defend a command or agency's Joint Mission Essential Task List/Agency Mission Essential Task List (JMETL/AMETL) in support of their steady-state activities, such as a combatant commands Theater Campaign Plan (TCP) or an agency's daily support activities. Enemy-focused movement and maneuver on the DODIN is conducted to achieve a positional (or temporal) advantage over a threat in order to defeat attacks along known or likely attack vectors. Movement and maneuver oriented on cyberspace terrain is driven by those DODIN assets deemed key (C-KT) or critical (DCIP assets and CI/KR on the DODIN). It is aimed at defending or controlling these operationally significant areas of the DODIN. When terrain-focused, cyberspace defensive forces contribute to mission assurance by identifying vulnerabilities and hardening assets against attack.

Intelligence

The greatest source of intelligence for DODIN Ops and DCO-IDM is derived from the operational information resident on the DODIN. JFHQ-DODIN collects and exploits this information for operations and to produce and disseminate intelligence. Time-sensitive information that requires immediate reporting and action to secure and defend the DODIN is triaged on collection as part of JFHQ-DODIN's information management. This is a requirement for all organizations that operate on the DODIN as codified in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B. In conjunction with its responsibilities to integrate the JIE CONOPS, tools programs, and CNDSP efforts into a single C2 Framework, JFHQ-DODIN aggregates and analyzes cyber incident reporting and traffic analysis to identify risks to the DODIN; direct forces and systems in incident response; direct, assess, and verify the defensive posture of the DODIN; and identify enterprise-wide capability gaps.

Intelligence for DODIN Ops and DCO-IDM requires a collaborative environment in which information and intelligence is shared between DOD Components. JFHQ-DODIN adheres to the axiom "intelligence drives operations," as well as its corollary, "operations yield intelligence" to fuse all sources of information and intelligence. JFHQ-DODIN leverages its command relationships in a deliberate and consistent process to aggregate and examine information from all sources and across intelligence disciplines to assess the operational environment. This approach relies on an all-source approach for collection and analysis and draws on the complementary strengths of intelligence disciplines to provide an accurate and comprehensive picture of threat activity and the DODIN. USCYBERCOM has direct liaison authority (DIRLAUTH) with all United States Government (USG) departments and agencies and has established a liaison exchange with selected Intelligence Community (IC) partners. In addition, IC organizations have formed the Joint Interagency Coordination Group (JIACG) for cyberspace. JFHQ-DODIN will partner with USCYBERCOM in these relationships to create a collaborative environment that facilitates regular communications, information and intelligence sharing, and operational coordination and deconfliction for the purpose of the "Secure, Operate, and Defend the DODIN" mission.

Fires, Sustainment, and Force Protection

While JFHQ-DODIN's JMETL is derived from the previous joint functions, the remaining joint functions - Fires, Sustainment, and Force Protection - play important roles in JFHQ-DODIN planning and execution.

JFHQ-DODIN can support fires delivered in and through cyberspace by providing technical target intelligence to develop and select aimpoints in support of advanced target development. JFHQ-DODIN can also support the fires process through operational risk assessments and the combat assessment process by providing potential or actual battle damage assessment (BDA) against the DODIN. While fires are not delivered on the DODIN, an active defense may achieve the same effects (e.g., deny, manipulate) through defensive counter-infiltration (hunt) and countermeasures. These actions are planned, scheduled,

executed, and assessed using the same processes for requesting and scheduling deliberate and dynamic fires through the cyberspace tasking cycle (CTC).

Sustainment of DODIN Ops and DCO-IDM deals with provisioning the resources needed to maintain and prolong operations until mission accomplishment. Resources for DODIN Ops and DCO-IDM include the forces, materiel, and capabilities needed for the mission. JFHQ-DODIN applies organic resources and coordinates additional resources as directed to ensure sustainment. As a subordinate headquarters to USCYBERCOM, JFHQ-DODIN participates in the Cyber Requirements Investment Board (CRIB) process through the Integrated Capabilities Requirements Working Group (ICRWG) and Integrated Priority List (IPL) submissions to identify and champion operational needs for resourcing the Joint Force to conduct DODIN Ops and DCO-IDM. JFHQ-DODIN's close working relationship with DISA ensures capability-based requirements remain in the fore for developmental test and evaluation. As required, JFHQ-DODIN seeks the authority to use capabilities (tools) to support operational requirements and to access sensitive information systems, networks, and data.

DODIN Ops and DCO-IDM inherently support force protection by projecting and protecting DODIN-enabled capabilities and activities that encompass operational (warfighting) capabilities, "man, train, and equip" Service functions, and business activities involving DOD and the defense industrial base (DIB). Like all security measures, cybersecurity is continuous and integral to DODIN Ops and DCO-IDM. Cybersecurity protects and preserves the force by preventing exploitation of the information, intelligence, and data that provide operational and technological advantage. JFHQ-DODIN mission encompasses force protection and the necessary actions and activities that protect the availability, integrity, authentication, confidentiality and nonrepudiation of DOD systems, networks, and data against external (natural and man-made) and internal (insider) threats.