2023 JOINT CAPABILITY AREA DEFINITIONS

1. **<u>Force Development and Design</u>**– The ability to establish, develop, and maintain a mission ready Joint Force and build relationships with foreign and domestic allies and partners.

   1.1. Force Integration: The ability to establish and maintain a deliberate, iterative, and continuous process of planning and development of the current and future Joint Force through concept development, assessment, and capability development.

      1.1.1. Concepts: The ability to examine challenges and opportunities of the future operational environment and identify potential alternate methods of operating and potential required capabilities.

      1.1.2. Force Configuration: The ability to translate doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTmLPF-P) requirements into programs and structure.

      1.1.3. Experimentation: The ability to conduct analytic activities derived from unbiased trials conducted under controlled conditions within a representative environment to help solve joint challenges/problems/issues.

      1.1.4. Human Capital Management: The ability to ensure and support, within the life cycle management of total force human resources, the availability of personnel equipped with skill sets required for mission success.

   1.2. Force Preparation: The ability to develop, enhance, and adapt the Joint Force, complemented by Allies and Partners for unified action.

      1.2.1. Training: The ability to instruct and apply exercises for acquiring and retaining skills, knowledge, and abilities required to perform specific tasks.

      1.2.2. Exercising: The ability to conduct military maneuver or simulate wartime operations involving planning, preparation, and execution that is carried out for the purpose of training and evaluation

      1.2.3. Education: The ability to convey general bodies of knowledge and develop habits of mind applicable to a broad spectrum of endeavors to foster breadth of view, diverse perspectives, critical analysis, and abstract reasoning.

      1.2.4. Doctrine: The ability to provide fundamental principles that guide the employment of military forces in coordinated action toward a common objective and serves to make US policy and strategy effective in the application of military power.

      1.2.5. Lessons Learned: The ability to identify, collect, analyze, validate, disseminate, and operationalize a lesson that contributes to improved performance or increased capability through documentation of lessons and best practices across DOTmLPF-P.

   1.3. Building Partnerships: The ability to conduct activities and engage with foreign and domestic ally and partner leaders, security and other government institutions, nongovernmental organizations, and relevant populations to build defense relationships through formal and informal agreements to achieve shared objectives.

1.3.1. Engage Allies and Partners: The ability to integrate and synchronize interactions with foreign and domestic governments and institutions to facilitate the development of formal or informal partnerships.

1.3.2. Manage Alliance and Partnership Agreements: The ability to develop, maintain, and disestablish partnerships.

1.3.3. Security Cooperation Activities: The ability to assess, monitor, evaluate, sustain, develop, and leverage the military, security, or other capabilities and capacities of allies and partners.

1.3.4. Civil-Military Operations: The ability to establish and maintain relations between military forces, indigenous populations, and institutions by directly support the attainment of objectives relating to stability within a region or host nation.

2. **Battlespace Awareness (BA)** – The ability to sense, understand, and orchestrate observables that impacting the operational environment to enable national and military decision making.

   2.1. **Planning and Direction:** The ability to synchronize resources and integrate the activities of gathering, extraction, and dissemination to satisfy all joint functional information requirements.

      2.1.1. **Defining and Prioritizing Requirements:** The ability to translate national, operational, and tactical objectives into time dominant and content dominant information requirements.

         2.1.1.1. **Defining Time Dominant Information Requirements:** The ability to identify, document, and communicate the minimum amount of information required along with the associated attributes necessary to accomplish a time-sensitive, mission essential task.

         2.1.1.2. **Defining Content Dominant Information Requirements:** The ability to identify, document, and communicate the minimum amount of information required to accomplish a mission essential task.

         2.1.1.3. **Prioritizing Information Tradeoffs:** The ability to identify, understand, weigh, and prioritize tradeoffs between time dominant information requirements and content dominant information requirements.

      2.1.2. **Developing Data Orchestration Plans and Strategies**: The ability to determine the best approach for aligning resources to gather, extract, and disseminate information to satisfy all time and content dominant information requirements.

         2.1.2.1. **Human-Machine Teaming:** The ability to create systems that can be trusted to understand human intent while collaborating to perform physical and cognitive tasks.

         2.1.2.2. **Machine Learning Operations:** The ability to design, build, and manage reproducible, testable, and evolvable Machine Learning-powered software.

         2.1.2.3. **DEVSECOPS:** The ability to integrate security, software development, and information technology operations to shorten systems development lifecycles and provide continuous delivery of software.

      2.1.3. **Monitoring and Tasking Resources:** The ability to proactively track information gathering activities and associated resources, then adjust gathering activities based on new information to satisfy all joint functional information requirements.

      2.1.4. **Partner Integration**: The ability to collaborate with mission partners to satisfy all joint functional information requirements.

   2.2. **Gathering:** The ability to gather information from all-sources to satisfy all joint functional information requirements aligned to Data Orchestration Plans and Strategies.

      2.2.1. **Sensing and Collection:** The ability to observe, investigate, measure, and capture information about objects and phenomena within the operational environment.

2.2.1.1. Signals Collection: The ability to gather information based on the interception of electromagnetic impulses.

2.2.1.1.1. Communications: The ability to intercept and derive information from voice and data communications.

2.2.1.1.2. Electronic Emissions: The ability to intercept and derive information from non-communication transmissions.

2.2.1.1.3. Foreign Instrumentation: The ability to intercept data from foreign equipment and control systems.

2.2.1.1.4. Cyberspace Networks: The ability to access and gather data from automated information systems, networks, and databases.

2.2.1.2. Imagery Collection: The ability to obtain a visual presentation or likeness of any natural or man-made feature, object, or activity at rest or in motion.

2.2.1.2.1. Electro-Optical: The ability to obtain a visual presentation of any natural or man-made feature, object, or activity derived from the ultraviolet through far infrared electromagnetic spectrum.

2.2.1.2.2. Light Detection and Ranging: The ability to obtain a visual presentation produced by recording pulsed laser light reflected from a given object.

2.2.1.2.3. Radar: The ability to obtain a visual presentation produced by recording radar waves from any natural or man-made feature, object, or activity.

2.2.1.2.4. Sonar: The ability to measure and characterize surfaces, natural or man-made objects, and layers of the maritime and littoral features.

2.2.1.2.5. Physical Environment: The ability to sense or acquire meteorological, oceanographic, and space environmental data through measurement, monitoring, and sensor observations.

2.2.1.3. Measurement and Signature Collection: The ability to gather parameters and distinctive characteristics of natural or man-made phenomena, equipment, or objects.

2.2.1.3.1. Electro-Optical: The ability to obtain information on phenomena that emit, absorb, or reflect electromagnetic energy in the ultraviolet through infrared spectrum.

2.2.1.3.2. The ability to actively or passively obtain energy reflected from any natural or man-made feature, object, or activity.

2.2.1.3.3. Geophysical: The ability to detect phenomena and gather information transmitted through the geophysical area of the earth, oceans, and surrounding atmosphere, including man-made objects.

2.2.1.3.4. Radio-Frequency: The ability to obtain information from radiation transmissions and electromagnetic pulses.

2.2.1.3.5. Materials: The ability to gather information from chemical and biological agents, objects, and activities.

2.2.1.3.6. Nuclear Radiation: The ability to obtain information derived from nuclear radiation and other physical phenomena associated with nuclear weapons, reactors, devices, facilities, and fissile materials.

2.2.1.3.7. Sonar: The ability to measure and characterize surfaces, natural or man-made objects, and layers of the maritime and littoral environment.

2.2.1.3.8. Physical Environment: The ability to sense or acquire meteorological, oceanographic, and space environmental data through measurement, monitoring, and sensor observations.

2.2.1.3.9. Biometrics Data: The ability to gather measurable anatomical, physiological, and behavioral characteristics of an individual.

2.2.1.4. Human-Based Collection: The ability to gather information from human resources, human-derived data, or human reconnaissance and surveillance assets.

2.2.1.4.1. Human Intelligence: The ability to gather information for intelligence purposes from human sources.

2.2.1.4.2. Counterintelligence Collection and Investigations: The ability to gather information to identify and investigate threats posed by foreign governments, organizations, and non-state actors to include international terrorists.

2.2.1.4.3. Observation: The ability to use human resources to obtain, by visual observation and other detection methods, information about the physical environment and surrounding activities.

2.2.1.4.4. Documents, Media, and Materiel: The ability to gather documents, electronic media, and foreign materiel through battlefield seizure or other means.

2.2.1.4.5. Social-Cultural Data: The ability of human resources applying their knowledge of a language, culture, or region to gather social or cultural information about the operational environment from the individual to the national level.

2.2.1.5. Open-Source Collection: The ability to gather information from publicly available documents and electronic media.

2.2.1.5.1. Publicly Available and Open-Source Information: The ability to gather information available throughout the public domain through acquisition or other means.

2.2.1.5.2. Commercially Available Information: The ability to gather commercially sourced information through procurement or other means.

2.2.1.6. Other Gather Methods: The ability to gather information relevant to inform understanding of the operational environment through other means, methods, and modalities.

2.3. Extraction: The ability to discover information, finished intelligence, or analytical insights that provide additional knowledge or context to an event, person, or object across all joint warfighting functions.

2.3.1. Processing and Computation: The ability to convert data into forms suitable for use by humans and machines.

2.3.1.1. Cloud Processing: The ability to process and compute data by using cloud solutions.

2.3.1.2. On Premise and Device Processing: The ability to process and compute data by using on-premise and device solutions.

2.3.1.3. Storing: The ability to store information using cloud or on-premise solutions such as data stores, warehouses, lakes, and other databases.

2.3.2. Analysis: The ability to evaluate and interpret information from all available sources to develop new insights on factors that may influence the current and/or future state of the operational environment.

2.3.2.1. Analytic Tools: The ability to provide users the right tools necessary to generate and/or enhance analytical insights.

2.3.2.2. Analytic Tradecraft: The ability to provide users with the right skills to generate analytical insights and develop new methods of analysis.

2.3.2.3. Modeling and Simulation: The ability to create physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process and methods for implementing those representations over time, to include the testing, evaluation, verification, and validation of these models and simulations.

2.3.3. Exploitation: The ability to use and benefit from analytical insights.

2.3.3.1. Exploitation Tools: The ability to provide users the right tools necessary to exploit analytical insights.

2.3.3.2. Exploitation Tradecraft: The ability to provide users the right skills to exploit information and develop new methods for obtaining analytical insights.

2.3.4. Contextualization: The ability to provide new information and context about an event, person, or an object to close an existing knowledge gap.

2.3.5. Other Extraction Methods: The ability to extract information relevant from all sources to inform understanding of the operational environment through other means, methods, and modalities.

2.3.5.1. Prediction: The ability to use information such as historical trends, models, simulations, and assessments to predict the future state of the operational environment.

2.4. Dissemination: The ability to transmit, distribute, present, or make available data, information, or intelligence products.

2.4.1. Product Generation: The ability to capture, document, and articulate information in text, graphic, and other forms.

2.4.2. Data-as-a-Service: The ability to disseminate actionable information intuitively and securely via optimal methods of transport to move the right data, to the right user, at the right time.

2.4.2.1. Automated and Prioritized Data Transport: The ability to leverage automation and advanced technologies to support transport of time dominant information requirements.

2.4.3. Other Dissemination Methods: The ability to disseminate the right data, to the right user, at the right time through other dissemination methods.

2.5. Counterintelligence: The ability to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign powers, organizations, or persons, or by international terrorist organizations or activities.

2.5.1. Offensive Counterintelligence: The ability to develop information on and provide information, materials, or equipment to a Foreign Intelligence Entity (FIE) for the purpose of penetrating the FIE, or exploiting, disrupting, or manipulating the FIE target.

2.5.2. Counterintelligence Investigations: The ability to determine whether a person is acting on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts.

2.6. Digitally Literate Workforce: The ability to identify, develop, and leverage the talent, skills, and competencies required to implement Data Orchestration Plans and Strategy.

2.6.1. Talent, Skills, and Competencies: The ability to identify the types of skillsets and competencies through testing, experimentation, and other means.

2.6.2. Recruitment: The ability to incentivize and acquire talent who possess and/or are postured to learn relevant skills and competencies.

2.6.3. Training and Education: The ability to develop skills and competencies through training, education, and other means.

2.6.4. Placement: The ability to understand, organize, and deploy talent in positions/roles which complement their skillsets and maximize return on investment of newly acquired skills.

2.6.5. Retention: The ability to incentivize the workforce to maximize retention and minimize turnover.

3. **Force Application** – The ability to integrate maneuver and kinetic, electromagnetic, and informational fires to gain a position of advantage and/or create lethal or nonlethal effects on designated targets.

3.1. Maneuver: The ability to move to a position of advantage.

3.1.1. Air: The ability to move to a position of advantage in the air domain.

3.1.2. Space: The ability to move to a position of advantage in the space domain.

3.1.3. Land: The ability to move to a position of advantage in the land domain.

3.1.4. Maritime: The ability to move to a position of advantage in the maritime domain, excluding the air space above the maritime domain.

3.2. Fires: The ability to create lethal and/or nonlethal effects on designated targets.

3.2.1. Kinetic: The ability to create lethal or nonlethal effects on designated targets in the air, land, space, and maritime domains.

4. **Logistics And Sustainment**– The ability to project and sustain the Joint Force.

4.1. Deployment And Distribution: The ability to move forces and sustainment strategically and operationally in support of military operations.

4.1.1. Force Deployment: The ability to transport units, equipment, and initial sustainment from the point of origin to the point of need.

4.1.2. Force Sustainment: The ability to deliver supplies, equipment, and personnel replacements to the joint force.

4.2. Supply: The ability to identify and select supply sources, schedule deliveries, receive, verify, and transfer product and authorize supplier payments. This includes the ability to see and manage inventory levels, capital assets, domestic business rules, supplier networks and agreements (to include import requirements) as well as assessment of supplier performance.

4.2.1. Supplies and Equipment Management: The ability to maintain accountability, store, preserve, and set stockage levels of materiel and equipment.

4.2.2. Inventory Management: The ability to receive materiel in the right quality and quantity and to enable precise distribution and transfer of materiel to the customer while integrating and optimizing the links or business processes between supply nodes, maintenance, and distribution providers.

4.2.3. Global Supplier Networks Management: The ability to source routine and surge requirements from the U.S. industrial base, ensure global supply availability and the capacity to support operations involving U.S., IA, PVO, and MN partners engaged in ever changing military activities around the globe.

4.3. Maintenance (Depot & Field): The ability to manufacture and retain materiel in a serviceable condition or restore materiel to a serviceable condition.

4.3.1. Inspect: The ability to determine faults or verify repairs or determine condition of an item of equipment based on established equipment maintenance and serviceability standards.

4.3.2. Test: The ability to evaluate the operational condition of an end item or subsystem thereof against an established standard or performance parameter.

4.3.3. Service: The ability to conduct preventive maintenance checks and scheduled maintenance to detect, correct or prevent minor faults before these faults cause serious damage, failure, or injury.

4.3.4. Repair: The ability to restore an item to serviceable condition through correction of a specific failure or condition.

4.3.5. Rebuild: The ability to recapitalize an item to a standard as nearly as possible to its original condition in appearance, performance, and life expectancy.

4.3.6. Calibrate: The ability to compare an instrument with an unverified accuracy to an instrument of known or greater accuracy to detect and correct any discrepancy in the accuracy of the unverified instrument.

4.3.7. Reclaim: The ability to retain and/or demilitarize authorized end items, assemblies, and sub-assemblies prior to disposal.

4.4. Logistics Services: The ability to provide services and functions essential to the technical management and support of the joint force.

4.4.1. Food Services: The ability to plan, synchronize and manage subsistence support to the joint force to include dining facility management, subsistence procurement and storage, food preparation, field feeding and nutrition awareness.

4.4.2. Water and Ice Services: The ability to produce, test, store and distribute bulk, packaged and frozen water in a contingency environment.

4.4.3. Contingency Base Services: The ability to provide shelter, billeting, waste management and common user life support management in a contingency environment.

4.4.4. Hygiene Services: The ability to provide laundry, shower, textile, and fabric repair support.

4.4.5. Mortuary Affairs: The ability to conduct contingency fatality operations and conduct mortuary operations for the remains of persons and personal effects for whom DoD Components are responsible by policy and statute.

4.5. Operational Contract Support: The ability to plan for and obtain supplies, services, and construction from commercial sources in support of joint operations along with the associated contract support, integration, contracting support, and management functions.

4.5.1. Contract Support Integration: The ability to provide coordinated and synchronized contracted support being executed in a designated operational area in support of the Joint Force.

4.5.2. Contracting Support: The ability to coordinate and execute contracting authorities to legally bind contractors in support of military operations.

4.5.3. Contractor Management: The ability to oversee and integrate contractor personnel and associated equipment providing support to the Joint Force in a designated operational area.

4.6. Engineering: The ability to execute and integrate combat, general, and geospatial engineering to meet national and JFC requirements to assure mobility, provide infrastructure to position, project, protect, and sustain the joint force, and enhance visualization of the operational area, across the full spectrum of military operations.

4.6.1. General Engineering: The ability to employ engineering capabilities and activities, other than combat engineering, that provide infrastructure and modify, maintain, or protect the physical environment. Examples include: the construction, repair, maintenance, and operation of infrastructure, facilities, lines of communication and bases; terrain modification and repair; and selected explosive hazard activities.

4.6.1.1. Gap Crossing: The ability to enable joint forces and equipment to overcome breaks or openings in terrain (dry or wet, natural, or manmade) by providing a system of temporary and permanent crossing techniques and equipment.

4.6.1.2. Develop and Maintain Facilities: The ability to develop, rehabilitate, and maintain facilities and infrastructure by providing design, real estate, construction, and environmental services which extend through final disposition.

4.6.1.3. Establish Lines of Communication: the ability to assess, construct, repair, and improve routes, railroads, intermodal facilities, and supporting infrastructure to allow the speedy flow of personnel, supplies, and equipment into theater and forward to tactical units.

4.6.1.4. Global Access Engineering: The ability to enable theater access by determining and documenting infrastructure capacities, in- situ soils, hydrology, and environmental conditions, and forecast and mitigate limitations to enable deployment and improve throughput capacities.

4.6.1.5. Repair and Restore Infrastructure: The ability to rehabilitate critical infrastructure. This capability includes repairing or demolishing damaged buildings, restoring utilities such as electrical power, and bringing critical facilities such as hospitals, water treatment plants and waste management facilities online.

4.6.1.6. Harden Key Infrastructure and Facilities: The ability to apply site- and threat-adaptable plans and designs, advanced construction techniques and materials to enhance the prevention or mitigation of hostile actions against materiel resources, facilities, and infrastructure.

4.6.1.7. Master Facility Design: The ability to integrate land use, bills of material and forecasts, and construction requirements that facilitate project execution and developing infrastructure and facilities.

4.6.2. Combat Engineering: The ability to employ engineering capabilities and activities that support the maneuver of land combat forces and that require close support to those forces. Combat engineering consists of three types of capabilities and activities: mobility, counter-mobility, and survivability.

4.6.2.1. Defeat Explosive Hazards: The ability to locate and neutralize the full range of enemy and friendly explosive hazards that may impede routine operations, decrease mobility, or present a threat to force protection. It includes the capability to locate, avoid, and neutralize hazards in concert with mounted or dismounted maneuver (breach) or as part of tactical/operational movement (route clearance).

4.6.2.2. Enhance Mobility: The ability to enable both mounted and dismounted movement and maneuver where and when desired without interruption or delay through complex terrain (ranging from littoral to mountainous areas), built up areas (cities, towns, and villages to include subterranean structures), and complex manmade and natural obstacles to achieve the commander's intent without loss of speed or flexibility.

4.6.2.3. Deny Movement and Maneuver: The ability to enable the Joint Force Commander to quickly dominate terrain and modify the physical environment to

isolate forces, deny key terrain and impede, deny, or canalize movement via lethal and nonlethal means.

4.6.2.4. Enhance Survivability: The ability to provide coordinated and synchronized engineer support (including camouflage techniques) and construction to increase force protection and conserve the Joint Force's fighting capabilities and freedom of action.

4.6.3. Geospatial Engineering: The ability to portray and refine data pertaining to the geographic location and characteristics of natural or constructed features and boundaries to provide engineer services. Examples include terrain analyses, terrain visualization, digitized terrain products, nonstandard tailored map products, facility support, and force bed-down analysis.

4.6.3.1. Utilize Geospatial Data: The ability to provide the Joint Force Commander with the foundation layer of the operational environment for use with collaborative decision-support, and terrain analysis tools.

4.6.3.2. Provide Mobility Assessments: The ability to understand a planned area of operations through the development of assessments on aerial and seaports, transportation networks, cross country mobility, and mobility corridors.

4.7. Base and Installation Support: The ability to provide enduring bases and installations with the assets, programs, and services necessary to support US military forces.

4.7.1. Real Property Life Cycle Management: The ability to acquire, operate, sustain, recapitalize, realign, and dispose of real property assets to meet the requirements of the force.

4.7.2. Installation Services: The ability to deliver selected services not related to real property or personnel services to meet the requirements of the installation population and mission, to include emergency services, installation safety, base support vehicles and equipment, housing services, airfield management, port services, range management, launch support services, and installation feeding.

4.8. Health Services: The ability to perform, provide, or arrange the promotion, improvement, conservation, or restoration of human mental and physical well-being via face-to-face or virtual modes.

4.8.1. Operational Medicine: The ability to sustain and protect the health and effectiveness of the Joint Force and provide safe and effective movement of ill and injured personnel to higher levels of care within and outside the Joint Operational Area. This includes the ability to provide for a healthy, fit, and protected force; engage in health surveillance; and manage casualties in a Joint Operational area; and safeguard the health of detained personnel.

4.8.2. Health Services Delivery: The ability to provide acute or long- term primary or specialty care to the Joint Force outside of Joint Operational Areas in either the direct or contracted care system and build healthy communities by managing and delivering the health benefit. This ability includes clinical preventive medicine, clinical diagnostics, treatment, rehabilitation, and regeneration.

5. **Command and Control** – The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.

   5.1. Organize: The ability to align or synchronize interdependent and disparate entities, including their associated processes and capabilities to achieve unity of effort.

      5.1.1. Establish and Maintain Unity of Effort with Mission Partners: The ability to foster and maintain cooperative relations with mission partners.

      5.1.2. Structure Organization to Mission: The ability to dynamically organize elements and define roles, responsibilities, missions, and authorities. This includes assignment, allocation, apportionment, and assessment of joint forces.

      5.1.3. Foster Organizational Collaboration: The ability to establish internal structures and processes and external interfaces that facilitate interaction and coordination.

   5.2. Understand: The ability to comprehend the implications of the character, nature, or subtleties of information (individually and collectively) about the operational environment and situation.

      5.2.1. Organize Information: The ability to discover, select, and distill information within an established context.

      5.2.2. Develop Knowledge and Situational Awareness: The ability to apply context, experience, and intuition to data and information to derive meaning and value.

      5.2.3. Share Knowledge and Situational Awareness: The ability to communicate synthesized information and context.

   5.3. Plan: The ability to establish a framework to employ resources to achieve a desired outcome or effect.

      5.3.1. Initiate Planning: The ability to review and examine all available information and guidance to determine necessary actions.

      5.3.2. Conduct Mission Analysis: The ability to use synthesized information and awareness applicable to a given situation or environment to further understand the problem.

      5.3.3. Develop Courses of Action: The ability to determine and refine sequences of activities to achieve a desired outcome or effect.

      5.3.4. Analyze Courses of Action: The ability to evaluate potential solutions to determine likelihood of success within acceptable resourcing and risk.

      5.3.5. Select Courses of Action: the ability to evaluate and recommend or select the COA with the highest probability of accomplishing the mission within acceptable parameters.

      5.3.6. Prepare and Issue Plan or Order: The ability to express clearly and concisely what is to be done and how it is to be done using available resources.

5.4. Decide: The ability to select a course of action informed and influenced by the understanding of the environment or a given situation.

5.4.1. Manage Risk: The ability to recognize and balance the likelihood and consequences of undesired effects with the desired outcomes/effects.

5.4.2. Select Actions: The ability to choose a prudent idea or set of ideas that leads to a desired outcome or end-state within a defined set of constraints.

5.4.3. Establish Rule Sets: The ability to construct directives that delineate circumstances and limitations for actions.

5.4.4. Establish Intent and Guidance: The ability to formulate a concise expression of purpose, methods, acceptable risk, and desired end-state.

5.5. Direct: The ability to employ resources to achieve an objective.

5.5.1. Communicate Intent and Guidance: The ability to promulgate a concise expression of the operational purpose, assessment of acceptable operational risk, and guidance to achieve the desired end-state.

5.5.2. Task: The ability to direct actions and resources.

5.5.3. Establish Metrics: The ability to establish objective criteria to assess performance and results.

5.6. Monitor: The ability to adequately observe and assess events/effects of a decision.

5.6.1. Assess Compliance with Guidance: The ability to determine if performance adheres to established parameters and expectations.

5.6.2. Assess Effects: The ability to analyze, track, and measure the results of actions taken.

5.6.3. Assess Achievement of Objectives: The ability to determine when the desired end-state has been reached.

5.6.4. Assess Guidance: The ability to determine if direction is achieving the desired end-state and is appropriate for the situation.

6. **Joint Information -** The ability to share and protect information across DoD and with mission partners coupled with the ability to generate, project, preserve, or deny access to information to improve understanding, decision making, and communication and to affect the perceptions, attitudes, decision making, and behavior of relevant actors.

   6.1. **Information Transport**: The ability to transport information and services via assured end-to-end connectivity.

      6.1.1. **Wired Transmission**: The ability to transfer data or information with an electrical/optical conductor.

      6.1.2. **Wireless Transmission**: The ability to transfer data or information without an electrical/optical conductor.

      6.1.3. **Switching and Routing**: The ability to move data and information end-to-end across multiple transmission media.

   6.2. **Network Management**: The ability to configure and re-configure networks, services and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services.

      6.2.1. **Optimized Network Functions and Resources**: The ability to provide DoD with responsive network functionality and dynamically configurable resources, to include allocation of required bandwidth, computing, and storage.

      6.2.2. **Deployable, Scalable, and Modular Networks**: The ability to design, assemble, transport, and establish mission-scaled networks from adaptable components network modules.

      6.2.3. **Spectrum Management**: The ability to synchronize, coordinate, and manage all elements of the electromagnetic spectrum through engineering and administrative tools and procedures.

      6.2.4. **Cyberspace Survivability**: The ability to mitigate effects of malicious cyberspace activity and resulting system degradation by preserving critical functions performance at threshold levels during a cyberspace threat incident, and then after a cyberspace threat incident recover full functionality within a specified mission-relevant timeframe. Systems include, but are not limited to, enterprise and organizational networks, weapons systems, and critical infrastructures.

   6.3. **Enterprise Services**: The ability to provide to all authorized users awareness of and access to all DoD information and DoD-wide information services.

      6.3.1. **Information Sharing**: The ability to make information visible, accessible, understandable, trusted, and interoperable via secure physical and virtual access to hosted information and data centers across the enterprise and with mission partners based on established data standards.

      6.3.2. **Computing Services**: The ability to process data and provide physical and virtual access to hosted information and data centers across the enterprise based on established data standards.

6.3.3. Common Enterprise Services: The ability to provide awareness of, access to and delivery of information on the DODIN via a set of registered services.

6.3.4. Positioning, Navigation, and Timing: The ability to determine accurate and precise location, orientation, time, and course corrections anywhere in the battlespace and to provide timely and assured PNT services across the DoD enterprise.

6.4. Generation: The ability to gain and maintain access to the information environment; build awareness of information-based threats, vulnerabilities, and opportunities; hold systems at risk; and create the necessary information to plan and conduct operations.

6.4.1. Electromagnetic Spectrum Operations: The ability to coordinate and synchronize EMS to support situational awareness, coordination, and prioritization of actions across the Electromagnetic Environment and Information Environment.

6.4.2. Defensive Cyberspace Operations (Internal Defensive Measures): The ability to defeat on-going or imminent threats to defend DoD cyberspace capabilities through systems actions internal to the DODIN.

6.4.2.1. Cyberspace Defense: The ability to provide defense to data, assets, applications, and services, including internal and boundary networks.

6.4.3. Offensive Cyberspace Operations & Tools: The ability to manipulate or degrade, disrupt, or destroy designated targets in and through cyberspace, external to the DODIN.

6.5. Preservation: The ability to protect and ensure the observations, perceptions, attitudes, decisions, and behaviors of the Joint Force, its allies, and its partners.

6.5.1. Cybersecurity: The ability to identify, protect against, detect, respond to, and recover from vulnerabilities and threats to information and induration systems, including information technology and operational technology

6.5.2. Information Exchange: The ability to secure dynamic information flow within and across domains.

6.5.3. Networks Protection: The ability to anticipate and prevent successful cyberspace threat incidents on networks.

6.5.4. Data Protection: The ability to prevent theft, accidental loss, or corruption of data across applications, networks, and databases.

6.5.5. Identity Management: The ability to authenticate an identity to grant or deny access to information based on associated authorizations.

6.5.6. Access Control: The ability to control access to data, assets, applications, and services, including information technology and operational technology.

6.5.7. Application Security: The ability to secure an application by preventing exceptions to the application's security policy or the underlying information system.

6.5.8. Cyberspace Survivability: The ability to mitigate effects of malicious cyberspace activity and resulting system degradation by preserving critical functions performance at threshold levels during a cyberspace threat incident, and then after a cyberspace threat incident recover full functionality within a specified mission-relevant timeframe. Systems include, but are not limited to, enterprise and organizational networks, weapons systems, and critical infrastructures.

6.5.9. Electromagnetic Spectrum Management: The ability to exploit, attack, protect, and manage the electromagnetic environment (EME) to achieve the commander's objectives by protecting spectrum-dependent systems, networks, and operations; tactically sensing the operational environment (OE); and attacking where necessary, at a time and place of choice.

6.5.10. Electromagnetic Support: The ability to search for, intercept, identify, and locate or localize sources of intentional and unintentional EM radiation for the purpose of immediate threat recognition, threat avoidance, homing, targeting, planning, and conduct of future operations.

6.6. Denial: The ability to affect denial or compulsion in spaces and places available to all but owned by none.

6.6.1. Operational Security (OPSEC): The ability to deny the adversary the information needed to correctly assess friendly capabilities and intentions, by identifying, controlling, and protecting critical information and indicators associated with specific military operations and activities.

6.6.2. Electromagnetic: the ability to apply electromagnetic or directed energy to control the electromagnetic spectrum, to deny the use of the spectrum to the opponent and to counter-act spectrum-based actions.

6.6.2.1. Electromagnetic Attack: The ability to use electromagnetic energy, including directed energy or antiradiation weapons, to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

6.6.3. Defensive Cyberspace Operations: The ability to execute missions to defend the DODIN, or other cyberspace which DOD cyberspace forces have been ordered to defend, from active threats in cyberspace.

6.6.4. Offensive Cyberspace Operations: The ability to execute missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR or national objectives.

6.7. Operations in the Information Environment: The integrated ability to employ required forces and capabilities from across the Joint Force to sustain or change perceptions, attitudes, and other elements to affect drivers of behaviors of relevant actors.

6.7.1. Inform: The ability to communicate accurate information to domestic, international, and internal audiences.

6.7.2. Influence: The ability to affect the factors that drive the behavior of foreign individuals, groups, and populations.

6.7.3. Offensive Cyberspace Operations and Tools: The ability to manipulate or degrade, disrupt, or destroy designated targets in and through cyberspace, external to the DODIN.

6.7.3.1. Electromagnetic/Directed Energy: The ability to use electromagnetic energy, including directed energy or antiradiation weapons, to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

6.8. Human Aspects of Military Operations HAMO: The ability to prepare the force to consider human aspects of military planning and Command and Control (C2).

6.9. Military Information Support Operations MISO: The ability to execute planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments.

7. **Protection -** The ability to protect and preserve the Joint Force's fighting potential by applying active defense, passive defense, and survivability measures.

7.1. Active Defense: The ability to protect the Joint Force fighting potential, information, bases, infrastructure, lines of communication, and operational environment.

7.1.1. Counter-Air/Counter-Missile: [Air] The ability to direct defensive actions to destroy, nullify, or reduce the effectiveness of hostile air threats against friendly forces and assets, including use of aircraft, air and missile defense weapons, multiple sensors, EW and other available weapons. [Missile] The ability to direct defensive actions to destroy, nullify, or reduce the effectiveness of hostile missile threats against friendly forces and assets, including use of aircraft, air and missile defense weapons, multiple sensors, EW, and other available weapons.

7.1.1.1. Security: The ability to protect by physical measures combat and logistics forces, bases, joint security areas, and lines of communication by identifying and reducing friendly vulnerability to hostile acts, influence, or surprise.

7.1.1.2. Defensive Counter Air (DCA): The ability to degrade, neutralize, or defeat enemy air and missile attacks attempting to penetrate friendly airspace during operations. DCA may also ensure access and freedom of action in international airspace. These operations may use aircraft, surface-to-surface missiles, surface-to-air missiles, artillery, ground forces, special operations, cyberspace attack, and electromagnetic attack.

7.1.1.3. Global Missile Defense: The ability to conduct operations that affect more than one CCMD through synchronization among the affected commands to coordinate effective allocation, deployment, and employment of capabilities necessary to deter and prevent attacks, destroy enemy missiles, or nullify or reduce the effectiveness of an attack.

7.1.1.4. DODIN: The ability to conduct secure operations of DOD cyberspace, including global terrestrial networks, satellite communications, tactical wireless networks, information technology embedded in weapon systems, and critical infrastructure, and standalone systems. This security is established based upon national and DOD cybersecurity policies and incorporates integrated layers of technology, training, and personnel actions that make the DODIN less vulnerable to threats in cyberspace, including insider threats.

7.1.2. Counter-Uncrewed: The ability to direct defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile unmanned threats against friendly forces and assets, in all domains and crossing domains, including use of kinetic, directed energy, electromagnetic spectrum interference, multiple sensors, connective system-of-systems command and control, and post-engagement forensics.

7.1.2.1. Detection: The ability to detect emitting and non-emitting uncrewed systems in any/all domains using active detection methods such as radar.

7.1.2.2. Identification and Tracking: The ability to identify and detect uncrewed and track into/within/near area of responsibility.

7.1.2.3. Engagement: The ability to engage kinetically, by directed energy, and by electromagnetic interference capabilities to overtake, disable, or destroy threat of uncrewed systems.

7.1.2.4. Command and Control: The ability to manage, track data, tip, and cue (sensor to shooter) within uncrewed system of systems.

7.1.2.5. Forensic Analysis: The ability to analyze adversary uncrewed and signals data, collect and assemble gathered data, and apply modeling and simulation schemas for near-real-time updates to uncrewed capabilities.

7.1.3. Mine Counter-Measures (MCM): The ability to prevent or reduce damage or danger from mines.

7.1.3.1. Littoral MCM: The ability to conduct multi-sensor MCM search, detection, classification, localization, and neutralization of threat mines 300' to surface depth.

7.1.3.2. Deep Water MCM: The ability to conduct multi-sensor MCM search, detection, classification, localization, and neutralization of threat mines 2000' to 300' depth.

7.1.4. Countering Weapons of Mass Destruction (CWMD): The ability to curtail the conceptualization, development, possession, proliferation, and use of Weapons of Mass Destruction (WMD), related expertise, materials, technologies, and means of delivery.

7.1.4.1. WMD Pathway Defeat: The ability to dissuade, deter, delay, disrupt, destroy, deny, and assure to complicate conceptualization, development, production, and proliferation of WMD.

7.1.4.2. WMD Defeat: The ability to control, defeat, disable, dispose of extant WMD and the ability to stockpile, transfer, or employ WMD.

7.1.4.3. CBRN Response: The ability to counter WMD, to attribute responsibility for an event, minimize effects, sustain operations, and support follow on actions.

7.1.5. Physical Security: The ability to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

7.1.6. Anti-Terrorism: The ability to protect Service members, high-risk personnel, civilian employees, family members, DOD facilities, information, and equipment. Includes employment of dedicated guard forces and use of individual protective equipment, hardened vehicles, hardened facilities, and duress alarms.

7.1.7. Electromagnetic Protection: The ability to protect personnel, facilities, and equipment from any effects of friendly, neutral, adversary, or enemy use of the EMS, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability.

7.2. Passive Defense: The ability to make the Joint Force's personnel and capabilities difficult to locate, strike, and destroy by reducing the probability of hits by the threat and minimizing the effects of damage caused by hostile actions.

7.2.1. Detection: The ability that enables the perception of objects and/or events of possible impact on the Joint Force.

7.2.2. Warning: The ability to urgently communicate and acknowledge time-critical information essential to the well-being and/or preservation of the Joint Force. This includes the relaying of an imminent attack or hostile activities by the threat on friendly forces.

7.2.2.1. Early Warning: The ability to provide early notification of launch and/or approach of hostile operations.

7.2.2.2. Warning Reporting: The ability to detect and report time-sensitive information to forewarn of hostile actions against the Joint Force.

7.2.2.3. Warning Order: The ability to initiate the development and evaluation of military courses of action by commanders.

7.2.3. Deception Activities: The ability to execute activities, including those in support of perception management or influence operations, conducted by a DOD Component to deliberately mislead an adversary or potential adversary decision makers, or to conceal from foreign intelligence entity collection, and creating conditions for the adversary to take or reject specific actions, for the purpose of accomplishing the friendly mission.

7.2.3.1. Camouflage: The ability to conduct friendly activities to blend in with surroundings.

7.2.3.2. Concealment: The ability to conduct friendly activities and make them unobservable or unrecognizable to the enemy.

7.2.3.3. Decoys: The ability to conduct activities in conjunction with other military deception activities to mislead adversary intelligence collection and direct the adversary's attention away from actual forces.

7.2.4. Chemical Biological Radiological (CBRN) Defense: The ability to minimize or negate the vulnerabilities to, and/or effects of, a chemical, biological, radiological, or nuclear hazard or incident.

7.2.4.1. Understand: The ability to detect, identify, and diagnose CBRN threats, warn and report the presence of those hazards, and support operational decisions.

7.2.4.2. Protect: The ability to shield the Joint Force from CBRN hazards or their effects through individual and collective protection, as well as medical countermeasures prior to exposure.

7.2.4.3. Mitigate: The ability to mitigate exposure to CBRN threats and manage physical contamination of personnel, equipment, and/or terrain and treat/counter the physiological effects of exposure to those threats.

7.2.5. Assess Vulnerabilities: The ability to identify vulnerabilities of the Joint Force's personnel and capabilities to better safeguard personnel, prevent unauthorized access, protect against espionage, theft, enemy actions, and damage.

7.3. Survivability: The ability to strengthen the survivability of Joint Force personnel capabilities, facilities, information, and infrastructure.

7.3.1. Risk Reduction: The ability to assess risk to the Joint Force's personnel, bases, capabilities, and lines of communication and apply measures to address and mitigate exposure to threat activities and other harmful effects prior to occurrence.

7.3.2. Emergency Response: The ability to urgently undertake activities as a result of hostile or harmful actions against the Joint Force's personnel, bases, capabilities, and lines of communication and provide immediate mitigation and remedy measures to restore force well-being and effectiveness.

7.3.3. Force Resilience: The ability to strengthen the Joint Force's personnel, assets, capabilities to include the warfighting and supporting systems against threat and non-threat actions.

7.3.4. Cyber Survivability: The ability to prevent, mitigate, and recover from adverse cyber-events that impact mission related functions by applying risk managed approach.

7.3.4.1. Prevent: The ability to control access, reduce system's detectability, communications, protect system, partition, and ensure critical functions, and minimize and hard attack surfaces.

7.3.4.2. Mitigate: The ability to monitor and detect anomalies and manage system's performance when degraded.

7.3.4.3. Recover: The ability to recover system capabilities and counter vulnerabilities at tactically relevant speeds.

7.3.4.4. Adapt: The ability to manage a system's configurations to achieve and maintain operationally relevant cyber survivability risk posture.

7.3.5. EMS Survivability: The ability to prevent, mitigate, and recover from operations in congested and contested EMS by applying a risk managed approach to protect the Joint Force's personnel, assets, and capabilities from threat EMS.

7.3.6. Space Survivability: The ability to protect the Joint Force's capabilities operating in space and/or contributing to space mission in support of operations.

7.3.7. Hardening of Critical Assets: The ability to harden the Joint Force's critical assets to increase survivability against threat actions.

7.3.8. Protection of Civilians: The ability to protect persons not engaged in hostilities with protected status under law of war.

7.3.9. Personnel Recovery: The ability to prepare for and execute the recovery and reintegration of isolated personnel.