DEPARTMENT OF DEFENSE

STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT

June 2016

FOREWORD

Although the term information environment (IE) is relatively new, the concept of an "information battlefield" is not. The role of information, either provided or denied, is an important consideration in military planning and operations. In fact, throughout the history of warfare, militaries have sought advantage through actions intended to affect the perception and behavior of adversaries. Information is such a powerful tool, it is recognized as an element of U.S. national power – and as such, the Department must be prepared to synchronize information programs, plans, messages, and products as part of a whole of government effort.

With the advent of the internet, the expansion of information technology, the widespread availability of wireless communications, and the far-reaching impact of social media, today's information environment poses new and complex challenges for military operations. This networked environment has enabled both state and non-state actors to employ activities in the IE to achieve their objectives effectively. They use various capabilities to exploit, disrupt, and disable command and control systems and other critical infrastructure; to disseminate propaganda and disinformation; to foster internal dissent; to recruit and solicit financing; and to promote legitimacy for their actions while discrediting the legitimacy of others. Although we can expect potential state adversaries to offer sophisticated challenges through aggressive operations in the IE, new forms of technology and communication have lowered the barriers of entry for non-state actors. These actors, and their supporters and surrogates, can now access the IE with ease and at relatively low cost, using it to advance their objectives and influence audiences around the globe.

This *Strategy for Operations in the Information Environment* has been developed in part as a response to the requirement for an information operations strategy in the National Defense Authorization Act for FY 2014. Its purpose is not to consolidate or centralize capabilities or functions, but to serve as a cornerstone document to align Departmental actions and ensure effective integration of DoD efforts in a dynamic IE. In this information age, the Department must adapt to technological and sociological changes and adjust to support the military needs of the Joint Force Commander. This strategy describes how the Department will set conditions to achieve an advantage in the IE with particular emphasis on the tasks associated with four key lines of effort: people, programs, policies, and partnerships.

This strategy signals our commitment and resolve, and provides my guidance on important steps we must take as a Department to enhance our ability to conduct military operations.

Ash Carter

TABLE OF CONTENTS

INTRODUCTION

One of the most challenging aspects of the rapidly evolving information environment (IE) is the growing impact and proliferation of stratagems by state and non-state actors to control the narrative surrounding their operations. Often using commercial capabilities, these actors disseminate truthful, biased, and false information using digital technologies and access to global audiences to recruit, to gain support and sustainment, and to exploit, disrupt, and delegitimize U.S. and coalition operations. While conducting activities in all domains of the operational environment, today's adversaries and other actors increasingly target non-military audiences with powerful, symbolic, strategic communication in conjunction with physical effects, creating a significant depth of influence.

This strategy aims not only to set conditions for success at the operational and tactical levels of warfare, but also to guide DoD support to the whole-of-government effort. It complements, and supports, other guidance documents including the National Security Strategy, the Quadrennial Defense Review, the DoD Cyber Strategy, and the Strategy for Implementing the Joint Information Environment, which focuses on Information Technology implementation including enabling DoD Information Network operations, improving cyber security, and providing mission support.

Australian soldiers with the 7th Battalion, The Royal Australian Regiment, assigned to the U.S. Army 2nd Cavalry Regiment Task Force, patrol at Multinational Base Tirin Kot, Uruzgan province, Afghanistan, Nov. 6, 2013. (DoD photo by Cpl. Mark Doran, Australian Defense Force/Released)(CJTF-OIR) Aug. 20, 2015.

The strategy defines an operational *end-state,* and associates it with the ways to accomplish the end-state, and the *means* necessary to support the *ways.* This ends, ways, means framework is described in greater detail later in the document.

End-State: Through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations.

This document also lays out parallel efforts addressing near-, mid-, and long-term objectives with focus on outcomes. *Near-term* efforts will focus on rapid, prioritized, high-impact changes; *mid-term* efforts will focus on synchronization of maturing solutions; and *long-term* efforts will focus on institutionalized and integrated operations in the IE. These three series of efforts will run simultaneously to address near-term challenges and opportunities while aligning mid- and long-term efforts. This approach also aligns with, and leverages, Joint Staff development of the Joint Concept for Operating in the Information Environment (JCOIE) and the Joint Concept for Integrated Campaigning (JCIC). An IO Executive Steering Group[1] (ESG) will provide oversight, management, and horizontal integration within the Department.

There are two follow-on issuances to this strategy – an *Implementation Plan* and an *Investment Framework* – that will guide execution of the strategy. These documents will be synchronized with the implementation of the DoD *Cyber Strategy,* which is the authoritative reference document relevant to the development of manning, training, equipping, and integrating full spectrum cyberspace operations into DoD policy, plans, and programs.

1 *As articulated in DoD Directive 3600.01, Information Operations, dated May 2, 2013.*

KEY TERMS

The ***Information Environment (IE)*** *is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information*[2].The IE is a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. With its function as a conduit for influence on decision-making and command and control, the IE is a key component of the commander's operational environment. Characterized by ubiquitous on-demand media and interpersonal hyper-connectivity, today's IE enables collaboration and information sharing on an unprecedented scale. Within the IE, the United States can expect challenges across three interrelated dimensions: the *physical*, composed of command and control systems, and the supporting infrastructure that enables individuals and organizations to create information-related effects; the *informational,* composed of the content itself, including the manner by which it is collected, processed, stored, disseminated, and protected; and the *cognitive,* composed of the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information. Effects in the physical and informational dimensions of the IE ultimately register an impact in the human cognitive dimension, making it the central object of operations in the IE.

Cyberspace *is a global domain within the information environment consisting of the interdependent network of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*[3] Cyberspace operations targeting the physical and informational dimensions of the IE also have an impact in the human cognitive dimension.

Information-Related Capabilities (IRCs) *are tools, techniques, or activities employed within a dimension of the information environment to create effects and operationally desirable conditions.*[4] IRCs historically include, but are not limited to operations security (OPSEC), military deception (MILDEC), military information support operations (MISO), electronic warfare (EW), cyberspace operations (CO), and special technical operations (STO).

Information Operations (IO) *is the integrated employment during military operations of information-related capabilities (IRCs), in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*[5] IO integrates the application of force and the employment of information with the goal of affecting the perception and will of adversaries. The integration of IRCs for effect can be compared to fire support coordination, in which a targeting methodology synchronizes and employs various capabilities to generate desired effects. It is the *integration* and *synchronization* of IRCs that enables desired effects in and through the IE at specified times and locations.

---

2 *Joint Publication (JP) 1-02, The Department of Defense Dictionary of Military and Associated Terms*

3 *Ibid*

4 *Ibid*

5 *Department of Defense Directive 3600.01, Information Operations, May 2, 2013.*

THE STRATEGIC ENVIRONMENT AND THE IE

Although the *2015 National Security Strategy* states the U.S. military must remain dominant in every domain, assure access to shared spaces, support alternatives to extremist messaging, and lead with capable partners, key national intelligence documents and the *Defense Planning Guidance for FY 17-21* describe a complex and evolving strategic environment with extremely dangerous, ubiquitous, and elusive threats to the United States.

> The technology-enabled 21st century operational environment offers new tools for state and non-state adversaries, such as terrorists, to pursue asymmetric approaches, exploiting where we are weakest.
>
> ***--2014 Quadrennial Defense Review***

Major trends affecting military operations in the strategic environment include the increasing breadth and depth of information available through all forms of communications media, the increasing speed with which information flows from and through a population, and the proliferation of interoperable digital devices. This global hyper-connectivity is more than just a technological trend; it is a societal and cultural trend as well. An entire generation has grown up not knowing a world without the internet, and these "digital natives" interact with others within virtual environments in ways fundamentally different than in previous generations. In most parts of the world, nearly everyone and everything is connected in some manner, and the convergence of information technology with human values, attitudes, beliefs, and perceptions has created new challenges and new vulnerabilities for the United States. Individuals and organizations can leverage social media to catalyze protests in a fraction of the time it took only a few years ago. The spread of mobile technology, especially in developing nations, has dramatically increased the ability of many to access and share information rapidly, and the ubiquity of personal communications devices with cameras and full-motion video allows much of the world to observe unfolding events in real time. These same capabilities can be utilized by adversaries for operational purposes, as well as for propaganda and disinformation.

The expansion and diffusion of advanced technology has lowered the cost of entry into the IE such that non-state actors can now acquire information-related capabilities that once were available only to developed countries. Many state and non-state actors are now competing with the United States to gain advantage in the IE, and today's adversaries are focused on identifying and exploiting vulnerabilities in our infrastructure, the information that flows within it, and the decision-making processes dependent on that information. We can expect them to continue to expand their operations from the physical battleground to other contested spaces in and through the IE or through virtual environments with little regard for international law and norms. The capability advantage the U.S. once enjoyed over adversaries in this environment is rapidly narrowing.

International organizations like NATO will often be used to address confrontations short of war.

Today, as in the past, the United States is contending with international confrontations short of open war. In these situations, actors seek to advance their interests by seizing the strategic and/or operational initiative, undermining alliance cohesion, managing escalation, complicating decision making, slowing the coordination of effective response, and intensifying both uncertainty

and friction. Our principles of truth and accountability contrast with those of less scrupulous and opaque adversaries, who frequently offer misleading or false information as propaganda. In support of a broader whole-of-government effort, the Department has a role to be trained, equipped, and prepared to counter such activities in this uneasy, steady-state environment traditionally referred to as phase zero.[6] To maintain unity of effort, DoD must closely coordinate operations, actions and activities with other United States Government (USG) departments and agencies to facilitate horizontal and vertical continuity of strategic themes, messages, and actions. In steady-state and in conflict, the Department must establish policies and set the conditions for components and their staffs to identify adversarial and potential adversarial threats (including attempts to undermine U.S. Alliances and coalitions) and bring capabilities to bear in an effort to affect, undermine, and erode an adversary or potential adversary's will.

6 *Phase 0 (Zero), is described in DoD Joint Publication 5.0 as, "Joint and multinational operations – inclusive of normal and routine military activities – and various interagency activities performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends or allies."*

KEY TENETS OF THE STRATEGY

- Information operations are an important component of military operations and in all phases of an operation or campaign, including shaping activities in the steady-state. The ability to monitor, characterize, and analyze the IE, and the ability to plan and integrate IO activities in coordination with other joint operations, are critical competencies for the Joint Force.

- In some cases, Joint Force operations in the IE will require close collaboration not only within the Department, but also across the USG (through the interagency process), with our allies and international partners, and with the public and private sectors.

- Although information activities may be conducted in the steady-state and in conflict, some are more restricted in peacetime by policies, doctrine, or operational plans that will require high-level permissions for their execution. The Department has procedures in place to manage information activities appropriately across the spectrum of conflict.

- DoD seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests, in a manner consistent with U.S. and international law. To this end, DoD develops capabilities for operations in the IE, including countering those threats, and integrates them into the full array of tools the USG has at its disposal.

- Effective information operations require substantial and sustained intelligence support. Given the dynamic nature of the IE, some legacy processes and tools may not be sufficiently responsive and new methods for sensing, assessment, and command-and-control may be required.

- The Department has fixed resources in place to sustain IE operations at current levels. To elevate capability or capacity, efficiencies must be realized through informed resource prioritization or offsets. DoD provides unique approaches, capabilities, and capacity that are integral to the success of USG strategies.

- The Department must coordinate and synchronize influence activities with informing activities, primarily public affairs, which release information that becomes immediately available to all public audiences including adversaries and potential adversaries. The credibility and legitimacy of the United States must be preserved.

DESIRED OUTCOMES

In moving forward, the Department must balance near-term, mid-term, and long-term efforts with sufficient flexibility to adapt to change, as well as to take advantage of emerging opportunities. These efforts will begin immediately and will be executed in parallel.

Near-term efforts (looking 6-18 months ahead) will focus on rapid, prioritized, high-impact changes to existing policy, doctrine, and professional military education and assessment efforts. The Department will improve its ability to assess the efficacy of IO, better integrate with the capabilities and capacities of allies and partners, and incorporate lessons-learned and best practices into doctrine and policy. In the first 12 months, the Department will establish the IO ESG and publish the *Implementation Plan,* the *Investment Framework,* and the Joint Concept documents for Operations in the IE and Integrated Campaigning.

Mid-term efforts (looking 18-36 months ahead) will focus on synchronization of efforts and effects. New concepts and policies will improve agility and responsiveness, clarification of authorities will streamline and better focus operations in the IE, and enduring partnerships across the USG will facilitate effective DoD operations in the IE.

Airmen and Soldiers train for Cyber Guard 15, conducting a "red vs. blue" cyber exercise.

Long-term efforts (looking 36 months ahead and beyond) will focus on institutionalized and integrated operations in the IE. The Department will field and manage a well-trained, educated, and ready IO and total-force to meet emerging requirements. The Department will possess the ability to characterize the IE effectively. Research and development efforts will identify and develop new science and technologies, and adapt emerging ones, while ensuring the maintenance and sustainment of capabilities and capacities across the Department.

A STRATEGY FOR THE FUTURE

In today's dynamic and changing world, the Department must fully understand the dimensions of the IE to plan and master operations within it; and these efforts must nest within a broader USG understanding of how adversaries and others will seek to gain diplomatic, informational, military, and economic advantage through exploitation of the IE.

The Office of the Secretary of Defense (OSD) and the Joint Staff will develop metrics, measurements, and assessment criteria for each of the strategy's ways, means, and tasks within the forthcoming *Implementation Plan* and *Investment Framework* to map efforts and track progress toward achieving the strategy's end state.

Ends (End-state)

Through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations.

Ways

The following nine *ways* support the end state above and serve as guidance to enable effective Departmental operations in the IE. Accomplishment of these *ways* will be achieved through the four *means* (described later in the document) and related specified tasks that refine and develop the *ways* described below.

- **Improve the capability of the Department to monitor, analyze, characterize, assess, forecast, and visualize the IE.** This capability is the foundation for operations within the IE. Characterization, in particular, is a continuous process occurring from preparation of the environment to effectiveness assessments.

- **Update joint concepts to address the challenges and opportunities of the IE.** Joint concepts refine the Department's approach to military operations and, as concepts emerge and evolve, considerations for operations in the IE will be addressed. The Joint Concept for Operations in the IE, the Joint Concept for Integrated Campaigning, and the Capstone Concept for Joint Operations will be key documents that prepare the Department for successful future operations in the IE.

- **Train, educate, and prepare the Joint Force as a whole for operations in the IE.** This includes Joint Force Commanders, their supporting staffs, and components. The total force must recognize that campaign planning integrates actions in the physical dimension with actions in a contested IE. This effort includes an understanding of other-agency support to JFCs, as well as DoD support to whole-of-government efforts in the IE.

- **Train, educate, and manage IO professionals and practitioners.** These personnel provide subject matter expertise to the Department and the Joint Force Commander on the conduct of information operations and the integration of IRCs.

- **Establish policy and implement authorities, coupled with doctrine and tactics, techniques, and procedures, which maintain the agility of the joint force in the IE, including the capability to adapt as the IE changes.** The IE exists outside the context of geographic boundaries, however, the effects achieved are identifiable within one or more Combatant Commanders' areas of responsibility. To succeed in the IE will require novel approaches to provide agility, flexibility, and command-and-control for the joint force.

- **Acquire and maintain sufficient capability and capacity of resources focused on operations in the IE.** These are specific personnel and IRCs available to Joint Force Commanders to support ongoing and planned operations. Capability and capacity should be examined in analytical studies and assessments, and during joint exercises.

- **Integrate and synchronize DoD efforts for operations in the IE with other USG activities.** Regardless of DoD's supporting or supported role in the IE, the Department operates within a whole-of-government effort to support U.S. national interests and will seek innovative ways to enhance interagency collaboration and cooperation for operations, actions, and activities in the IE.

- **Foster the credibility, legitimacy, and sustainment of U.S. and coalition operations, actions, and activities.** This includes exposing adversary and potential adversary malign operations, actions, and activities, such as disinformation.

- **Establish and maintain enduring and situational partnerships.** The United States maintains strong relationships with its allies, partners, and coalition members, as well as continuing partnerships with academia, industry, and non-governmental organizations (NGOs). The Department will continue to stress military interoperability through collaborative training and shared resources.

Means

The *means,* or the tools necessary for the Department to be successful with this approach, are categorized as **people, programs, policies, and partnerships.** Each of these categories is broad in scope and is described with associated tasks in the section that follows.

PEOPLE

Our military and civilian professionals are our decisive advantage. They are the foundation of our operational excellence and our ability to successfully innovate. Therefore, we are dedicated to building creative, adaptive professionals skilled at leading organizational change while operating in complexity.

--2015 National Military Strategy of the United States

Commanders, components, and their staffs lead and manage operations in the IE. IO professionals and practitioners directly support the Department, the Joint Force, and the Joint Force Commander through training, education, planning, and the integration of IRCs to produce effects within the IE.

Task – Train, educate, and prepare commanders and their staffs, and the Joint Force as a whole, to lead, manage, and conduct operations in the IE.

- The Under Secretary of Defense for Personnel and Readiness, in conjunction with the Joint Staff, the Services, and the U.S. Special Operations Command (USSOCOM), educate and train commanders and their staffs to plan, lead, and manage operations in the IE.
- The Services and USSOCOM educate the force as a whole on operations in the IE.

Task – Train, educate, and prepare IO professionals and practitioners to enable effective operations in the IE.

- OSD, in conjunction with the Joint Staff, the Services, and Defense Agencies as appropriate, ensure an integrated approach to establish standards for Joint and Service IO personnel to address Combatant Command (CCMD) needs.
- The Joint Staff and the Services, in coordination with OSD, ensure that IO personnel, and supporting elements (e.g. intelligence support) are provided with the core competencies necessary to meet stated needs. Education, training, and knowledge/skills/abilities must comport with emerging changes in the IE.

Task – Manage IO professionals, practitioners, and organizations to meet emerging operational needs.

- The Services, in coordination with the Joint Staff, manage IO organizations and active, reserve, and civilian personnel to meet operational needs. This includes refining force structure needs for operations in the IE, including the recruitment, accession, and retention of highly skilled IO professionals.
- The Joint Staff, in coordination with OSD, identify surge capability and capacity needs not met by current assignment or allocation of forces to the CCMDs. CCMD needs vary depending on the complexity, scope, phase, and/or intensity of specific contingency operations.
- The Joint Staff, in coordination with OSD, validate the baseline Joint personnel needs for operations in the IE across the Future Years Defense Program (FYDP).
- The Joint Staff, Components, and Services, in coordination with OSD, identify and manage other supporting personnel needs (e.g. intelligence support).
- The Joint Staff, in conjunction with the CCMDs, ensure an optimized organizational structure is identified for CCMDs to provide C4I and coordination for operations in the IE.

We are conducting resource-informed planning. The U.S. military requires a sufficient level of investment in capacity, capabilities, and readiness so that when our nation calls, our military remains ready to deliver success.

--2015 National Military Strategy of the United States.

To conduct successful operations in the IE, the Department must improve the ability of commanders and their staffs to characterize and operate in the IE and assess the effectiveness of operations. The Department will promote research, development, maintenance, and sustainment of capabilities and capacities to create and sustain an operational advantage in the IE.

Task – Establish a baseline assessment of DoD's current ability to conduct operations in the IE.

- OSD, in coordination with the Joint Staff, oversee a Capabilities-Based Assessment (CBA) of DoD's ability to operate in the IE. The IO ESG will serve as the collaborative forum as planning and programming efforts are synchronized and integrated.

- Joint Staff, in coordination with the Services and OSD, conduct a DOTMLPF-P analysis of DoD operations in the IE. The IO ESG will serve as the collaborative forum for governance and oversight as sustaining efforts are synchronized and integrated.

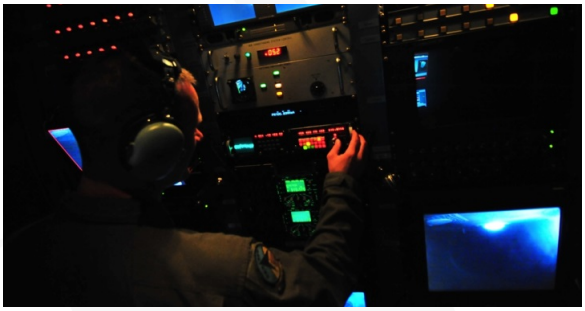
Task – Develop the ability of the Department and operating forces to engage, assess, characterize, forecast, and visualize the IE.

- OSD, in conjunction with the Defense Intelligence Enterprise (DIE), the Joint Staff, and the Services, ensure that DoD has the material and personnel capacity and tradecraft needed to meet the growing requirements for detailed characterization of the current and forecasted IE.

- OSD, in coordination with the DIE, the Joint Staff, and the Services, assess IE characterization-related intelligence manpower, training, education, and experience requirements to ensure that the DIE has the capability and capacity to meet warfighting needs for IE characterization.

- OSD, in coordination with the Joint Staff, and the Services, ensure intelligence professionals who characterize the IE are identified, educated, trained, and managed and sufficient efforts are in place to recruit, access, and retain the needed talent.

- OSD, in conjunction with the DIE, the Joint Staff, and the Services, explore the recruitment, accession, and retention of a sufficient number of IO professionals with the requisite knowledge, skills, and abilities across the broad range of activities in all dimensions of the IE; this is particularly important for the cognitive dimension of the IE and its socio-cultural characteristics.



A U.S. Air Force EC-130J Commando Solo electronic communication systems operator performs an electronic attack mission during Emerald Warrior 2013, Hurlburt Field, Fla., May 1. The primary purpose of Emerald Warrior is to exercise special operations components in urban and irregular warfare settings to support combatant commanders. Emerald Warrior leverages lessons from Operation Iraqi Freedom, Operation Enduring Freedom and other historical lessons to provide better trained and ready forces to combatant commanders. (U.S. Air Force photo by Staff Sgt. Elizabeth Rissmiller)(Released)

Task– Develop and maintain the proper capabilities and capacity to operate effectively in the IE in coordination with implementation of the DoD Cyber and JIE strategies.

- OSD, in coordination with the Services, lead efforts across DoD Component portfolios and with partner nations, as required, to acquire, modify, or develop the necessary tools to support characterization and visualization of the IE.

- OSD will facilitate and support collaborative IO planning, not only within the Department, but also with other USG departments and agencies and with allies and partners, as appropriate.

- OSD, in conjunction with the Joint Staff, support the JFCs responsibility to synchronize actions in the IE.

- OSD, in conjunction with the Joint Staff, lead efforts to synchronize programs across CCMDs in support of DoD's contribution to USG strategic guidance and direction.

- The Joint Staff, in conjunction with the Services and OSD, synchronize the development of capabilities and capacity for the commander to conduct actions and activities in the IE for the campaign plan across the range of military operations.

- OSD, in conjunction with the Joint Staff, annually assess and identify gaps in existing capabilities, identify and describe planned investments within the FYDP, evaluate needs to operate in expected contingencies and the expected IE in the future beyond the FYDP; and make recommendations regarding DoD investments.

Task – Develop and maintain the capability to assess accurately the impact of operations in the IE.

- The Joint Staff, in conjunction with OSD, the DIE, and the Services, refine existing assessment methodologies, using both qualitative and quantitative assessment techniques, to assess what success looks like in the IE across the range of military operations.

- OSD, in conjunction with the Joint Staff, the Services, and CCMDs, validate metrics, measurement, and assessment for operations in the IE.

Task –Adopt, adapt, and develop new science and technology for the Department to operate effectively in the IE.

- OSD, in conjunction with the Joint Staff, the Defense Advanced Research Projects Agency, and the Services, develop and evaluate the budgetary needs for science, technology, research, development, sustainment, and maintenance investment in support of operations in the IE.

U.S. Marine Corps Capt. Brent Molaski, right, an information operations officer assigned to Marine Expeditionary Brigade-Afghanistan, and U.S. Army Sgt. Igor Lebedev, a Tactical Psychological Operations (PSYOP) non-commissioned officer assigned to 310th PSYOP, carry a Radio In A Box (RIAB) from an MV-22 Osprey aircraft at Camp Leatherneck, Helmand province, Afghanistan, Dec. 3, 2009. The RIAB is being delivered to a forward operating base to broadcast messages. (U.S. Marine Corps photo by Sgt. Evan Barragan/Released)

POLICIES

Success will increasingly depend on how well our military instrument can support other instruments of power and enable our network of Allies and partners.

--2015 National Military Strategy of the United States.

Well-articulated and timely policy and guidance are necessary for operations in the IE. This requires not just policy, concepts, doctrine, a legal framework, and authorities, but also the agility to adapt to and adopt changes rapidly in the IE.

Task – Develop and adapt IE-related concepts, policies, and guidance.

- OSD, in conjunction with the Joint Staff, ensure that oversight and management structures, such as the IO ESG and the IO Quadrilateral Senior Steering Group, are in place to serve as deliberative bodies to inform, coordinate, and resolve IE-related policy and guidance issues.
- OSD, the Joint Staff, and the Services, conduct a biennial review of concepts, policies and guidance to ensure effective DoD operations in the IE; as required, adjust concepts, policies and guidance.
- The Joint Staff, in conjunction with OSD, the Services, and select Defense Agencies, will develop and execute the JCOIE, which will inform both the Implementation Plan and the Investment Framework.
- The Joint Staff, in conjunction with OSD and the Services, review and ensure that relevant policies and guidance reflect the findings of the JCOIE.
- CCMDs, in conjunction with their Service Components, explore innovative concepts to increase agility, effectiveness, and efficiency, e.g., command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

Task – Ensure doctrine relevant to operations in the IE remains current and responsive based on lessons learned and best practices.

- The Joint Staff, in conjunction with the Services, review and ensure that all relevant doctrine reflects IE extant capabilities, current force structure and material, and contemporary lessons-learned. This effort will include harmonizing Service, Joint, and allied doctrine in the IE.

Task – Develop, update and de-conflict authorities and permissions, as appropriate to enable effective operations in the IE.

- OSD, in coordination with the Joint Staff and the Services, conduct a biennial review of legal frameworks and authorities that impact DoD operations in the IE; as appropriate, update, develop, or propose new legal frameworks and authorities to facilitate flexible and adaptive operations, activities and actions.
- OSD, in coordination with the Joint Staff, identify authorities suitable for delegation to operational-level commanders, and as appropriate, facilitate that delegation.

PARTNERSHIPS

America's global network of allies and partners is a unique strength that provides the foundation for international security and stability. We will preserve our alliances, expand partnerships, maintain a global stabilizing presence, and conduct training, exercises, security cooperation activities, and military-to-military engagement.

--2015 National Military Strategy of the United States.

The U.S. military's capability and capacity to operate globally in the IE will be contingent on its ability to establish and maintain situational and enduring partnerships across the USG, and with academia, industry, and nongovernmental organizations. It is equally important to work with foreign and international partners, particularly those with whom the United States has common security interests.

Task – Establish and maintain partnerships among DoD and USG interagency partners to enable more effective whole-of-government operations in the IE.

- OSD, in conjunction with the Joint Staff and the Services, reinforce existing (or establish new) partnerships within DoD and across the USG.

Task – Establish and maintain appropriate interaction with non-U.S. Government entities (e.g., industry, academia, federally funded research and development centers (FFRDCs), and other organizations) to enable operations in the IE.

- OSD, in conjunction with the Joint Staff and the Services, reinforce existing (or establish new) relationships with industry, academia, FFRDCs, and others to enable better harmonized and more effective operations in the IE. Relationships may be enduring or situational.

Task – Establish and maintain collaboration between and among DoD and international partners (e.g. partner nations and NGOs) to enable more effective operations in the IE.

- OSD, in conjunction with the Joint Staff and the Services, leverage international partnerships to gain access to unique IO capabilities/capacities, language skills, cultural expertise, and/or appropriate roles of non-U.S. entities.

Task – Foster, enhance, and leverage partnership capabilities and capacities.

- OSD, in conjunction with the Joint Staff, develop appropriate policies that facilitate the reciprocal and timely sharing of information with partners to enable successful multinational operations in the IE.

- OSD, in conjunction with the Joint Staff and the Services, make Joint and Service-related IE and IO training and education opportunities available to partners, as appropriate.

CONCLUSION

The operating environment is increasingly enabled by technology, which provides the types of capabilities, once limited to major powers, to a broad range of actors. The rapidly accelerating spread of information is challenging the ability of some governments to control their populations and maintain civil order, while at the same time changing how wars are fought and aiding groups in mobilizing and organizing.

--2014 Quadrennial Defense Review

The U.S. military operates in a world evolving both technologically and socially at an ever accelerating pace, and our adversaries and others have effectively leveraged the IE as a means to advance their objectives. This strategy is one of several efforts underway to gain and sustain military advantage in the IE, and it provides a roadmap for how the Department will set conditions through nine *ways* and four major *lines of effort* involving people, programs, policies, and partnerships.

The Department will review this strategy biennially. Appropriate elements will be reflected in the Joint Concept for Operations in the IE and in the living execution documents, the *Implementation Plan,* and the *Investment Framework*. All efforts will link to, and support, other guidance documents including the National Security Strategy, the Quadrennial Defense Review, the National Military Strategy, the DoD Cyber Strategy, and the Strategy for Implementing the Joint Information Environment.

By pursuing the elements of this strategy, DoD will leverage the inherent strengths of individual IRCs, human capital, and relationships both within the USG and with our Allies and partners. Near, mid, and long-term efforts running in parallel will focus on positive changes that will lead to synchronized and institutionalized operations in the IE with the following end-state: *through operations, actions, and activities in the IE, DoD has the ability to affect the decision-making and behavior of adversaries and designated others to gain advantage across the range of military operations.*

GLOSSARY AND ACRONYMS

Cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. *(JP 1-02. Source: JP 3-12)*

Cyberspace Operations. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. *(JP 1-02. Source: JP 3-0)*

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. *(JP 1-02. Source: JP 3-13.1)*

Information Environment (IE). The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. *(JP 1-02. Source: JP 3-13)*

Information Operations (IO). The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. *(JP 1-02. Source: JP 3-13)*

Information-Related Capability (IRC). A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. *(JP 1-02. Source: JP 3-13)*

Joint Information Environment (JIE). A secure joint information environment comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. The JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs). *(DoD CIO. Source: Approved in JCS Tank in 2012)*

Military Deception (MILDEC). Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. *(JP 1-02. Source: JP 3-13.4)*

Military Information Support Operations (MISO). 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, organizations, groups, and individuals in a manner favorable to the originator's objectives. *(JP 1-02. Source: JP 3-13.2)*

Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. *(JP 1-02. Source: JP 3-13.3)*

Public Affairs (PA). Those public information, command information, and community engagement activities directed toward both the external and internal publics with interest in the Department of Defense. *(JP 1-02. Source: JP 3-61)*

Social Media. Means of interaction within the cyber domain among users in which they create, share, and exchange information and ideas in virtual communities and networks.

Strategic Communication: Focused USG efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. *(JP 1-02: Source: JP 5-0)*

Department of Defense
Official Document