Joint Information Environment

White Paper

22 January 2013

"To fight and conquer in all battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."
-Sun Tzu

"Some people think design means how it looks. But of course, if you dig deeper, it's really how it works."
-Steve Jobs

MARTIN E. DEMPSEY
General, U.S. Army
Chairman of the Joint Chiefs of Staff

18

Joint Information Environment

22 January 2013

Foreword

On 28 September 2012, I issued the *Capstone Concept for Joint Operations (CCJO): Joint Force 2020*. It presents a vision for how the Joint Force of the future can effectively address security challenges going forward. Central to this vision is the idea of globally integrated operations, increasing the overall adaptability of the force to cope with uncertainty, complexity, and rapid change.

There is no better example of the challenge ahead than that of the information environment. From moving supplies in the wake of a hurricane disaster to ordering troops to the Pacific, or addressing the ever-changing cyber threat, the global dependence on information and networks in everyday activities demands our attention now. The approach to addressing this nexus of dependence and threat for Joint Force (JF) 2020 is the Joint Information Environment, or JIE. What follows is my vision for the JIE and its relevance for operations within the context of my vision for Joint Force 2020 and beyond.

1. Introduction

The Joint Information Environment (JIE) will be among the first concrete changes along the path to constructing Joint Force 2020. First and foremost, JIE will improve mission effectiveness. It is intended to enable and empower our military's decisive edge – our people. It will do this by providing warfighters and our mission partners a shared IT infrastructure with a common set of enterprise services, under a single security architecture. Over time, the JIE framework will produce IT efficiencies.

The JIE will be an important evolution in our information environment. It will change the way we assemble, configure, and use new and legacy information technologies. It will consist of networked operations centers, a consolidated set of core data centers, and a global identity management system with cloud-based applications and services. The JIE framework will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches coherently across the system as a whole.

JIE Enabling Characteristics:

- **Transition from Network Centric to Data Centric solutions**
- **Rapid delivery and use of integrated cloud services accessible by all means from anywhere**
- **Interdependent information environment providing real time cyber situational awareness**
- **Scalable platform allowing flexibility and mission partnering**
- **Secure where it needs to be, resilient throughout, and appropriately consolidated**

The ultimate beneficiary of the JIE will be the commander in the field and forces at the tactical edge. JIE will allow better integration of information technologies, operations, and cyber security at a tempo that supports today's fast-paced operational conditions. The operational capabilities delivered through the JIE will enable commanders to blend the art of command with the science of control, enabling JF 2020 to address emerging military challenges through the flexible integration of warfighting functions as required.

2. Why Adapt the Way We Approach Our Information Environment?

Globally integrated operations demands a far greater capacity to see, understand, operate in and defend cyberspace.[1] Our ability to do this is undermined by a lack of interoperability, cyber vulnerabilities, and the pace of technological change and associated costs. Together, these factors limit our ability to integrate an information environment within dynamic joint force operations. Currently, DoD Information Technology (IT) comprises thousands of operational systems, hundreds of globally unconnected data centers, and more than seven million computers and IT devices. In order to create an IT environment that enables mission command, JF 2020 requires us to adapt how we approach information technology, including the structure and function of our information systems, and also how we use them. We must move past our vision of IT as an array of business systems that function like a utility, and begin to assemble, train, and operate them as a core warfighting capability.

Mission Command is the conduct of military operations through decentralized execution based upon mission-type orders. Successful mission command demands that subordinate leaders at all echelons exercise disciplined initiative and act aggressively and independently to accomplish the mission.

Joint Publication 3-0 "Joint Operations"
11 Aug 2011

Our transition to JIE constitutes a new level of jointness in IT, akin to the higher levels of jointness we have achieved in areas like fires. Driving jointness deeper and sooner is at the heart of our move to JF 2020. A decade of war has plainly illustrated the need to share information beyond what our current IT infrastructure allows. The JIE will be the trusted IT framework that will enable us to share information when needed, with any mission partner, regardless of location, device, or service provider.

Lack of Interoperability

Varying degrees of interoperability within our information environment means that the Joint Force cannot share information and collaborate across the Services, mission areas, military domains, and organizations to the extent required for globally integrated operations. We currently rely on hundreds of data centers, each of which requires an inordinate amount of resources to operate, configure, and maintain. These data centers often only connect with one another with difficulty. This inefficient duplication of computing and network-based services hinders our ability to take advantage of new commercial technologies and capabilities at the enterprise level. Limitations in our hardware and network centric view of the information environment impact our ability to flexibly establish joint and coalition forces where and when needed. The JIE will provide the framework to accrue the military advantage across multiple functional areas through the integration, innovation, and consolidation of our IT systems while at the same time improve our security posture.

[1] The elements of globally integrated operations limited by our current network structures are mission command, global agility, leverage participation of partners, flexibility in establishing joint forces, and cross-domain synergy.

Cyber Security Vulnerabilities

Cyber security vulnerabilities can endanger mission success. The current network centric architecture hinders our ability to operate and protect the information environment, where adversaries seek to degrade, disrupt, or interdict data. This limits the ability of commanders to understand the situation, to communicate intent clearly to subordinates and, most importantly, to build and maintain the mutual trust required of mission command. If networks are compromised and we cannot trust the data and information, the Joint Force would be unable to achieve globally integrated operations. Lack of confidence in our connections would also mean that we cannot build trusted relationships with willing partners. Our current information environment gives us neither the depth nor breadth of operational data about movements and activities – including the potential for hostile penetration of our networks within cyberspace. The JIE will contribute to a decisive Joint Force by providing end to end visibility of our network and operational security, thus ensuring warfighter access to information even in the face of disruption or damage.

Pace of Change and Associated Costs

The Joint Force faces a shrinking technological lead and growing vulnerability in a variety of systems, most notably in information technology. Our adversaries are increasingly focused on disrupting our command and control systems. The Joint Force is challenged by the expanding geographic reach of our opponents into all warfighting domains, including cyberspace itself. Meanwhile, innovation and modernization within commercial information technologies are rapidly outpacing military system development, especially in powerful smart phones, tablets, and other mobile computing devices. The rate at which innovation in IT occurs challenges our ability to build an integrated computing environment. The proliferation of disparate IT capabilities over the last several decades has ultimately yielded a less coherent and sometimes incompatible set of systems across the force. We are left with an information technology and computing enterprise that is often unwieldy, vulnerable, incompatible, and expensive to operate and maintain. Furthermore, this suite of IT systems and capabilities is not aligned with the needs of the Joint Force commander.

3. The Joint Information Environment

In *Strategic Direction to the Joint Force*, I describe the need for a joint force that is responsive, versatile, and decisive in nature – all while remaining affordable to the Nation. JIE is critically important to realizing this vision by increasing interoperability across the force to be more responsive to the Commander, facilitating capabilities to address threats and challenges to increase security, and encouraging flexibility and resilience in our information environment that is appropriately consolidated, producing economic benefits over time.

Enabling Mission Command: The Warfighter's JIE will be the secure information framework from which the Joint Force Commander delivers responsive, versatile and decisive actions on any device, anytime, from anywhere on the globe.

Improving Warfighter Effectiveness through the Core Data Centers and JIE Cloud

Warfighter effectiveness is supported through a shared IT infrastructure that delivers more responsive outcomes. Today, we have a large number of diverse and distributed data centers around the world, all dedicated to a specific Service. The JIE will be built on Core Data Centers (CDC) and Enterprise Operations Centers (EOCs) that will link the operational environment in the Joint Force Commander's Joint Cyber Center to vital cyber reinforcement capabilities and information support resources. These Core Data Centers (CDCs) will replace Service-specific data warehouses and consolidate our IT infrastructure and be connected by a secure, interoperable common architecture, and focused on the sharing, accessing, and connecting of authorized users to the information they need in order to operate effectively. The CDCs will be the focal points for joint force elements and any mission partner, including interagency and nongovernmental partners to connect, access resources, and share information to include services such as DoD Enterprise Email.

CDCs are the foundation upon which we will begin to offer true cloud-based capabilities to DoD users, supporting posts, camps and stations in an integrated manner. Today cloud computing is used by millions of commercial network users for mobile applications. The JIE cloud will leverage the best of these approaches to develop innovative software applications and better share information across the Joint Force to include Secure Mobile Communications. From the classified to unclassified domains, the warfighter will have the power to connect to the information resources needed from any device, at anytime from anywhere in the world. Furthermore, as individuals transit into and out of a Joint Task Force, their movement within the information environment will be virtually seamless and allow them to operate from any device immediately. CDCs will allow these transitions to occur quickly and fluidly with minimum disruption or delay to JTF operations, allowing commanders, troops and our mission partners on the ground to download their mission 'app' at the pace of the problem and with the agility needed to support any mission, from counter-terrorism operations in the heart of Africa to any disaster around the globe. A cloud computing approach to the JIE is a key enabler for developing an agile and responsive JF 2020.

The Imperative of Cyber Defense

Commanders require a detailed understanding of the environment and IT systems to develop the insight and foresight about a situation and make effective decisions about how, when, and where to apply scarce military resources. The JIE drives development of a responsive Joint Force by increasing its capacity for situational awareness and its ability to share and relate this information to operations though Enterprise Operations Centers (EOCs).

Cyber security must be integral to everything we do. With JIE, shared EOCs around the world will monitor the information environment and provide cyber situational awareness down to the "desktop" level of resolution. The ability to operate, monitor, and defend the Department's information environment while adjusting cyber posture across networks in real-time will enable forces to better contribute to mission success. These EOCs are central to the JIE's ability to better operate and defend

the Joint Force's data, information, and overall mission capability through cyberspace. A Global Enterprise Operations Center will orient our overall cyber posture based on global conditions and specific events through a single security architecture and common operational picture for cyberspace. The EOCs will work with the Global Enterprise Operations Center to oversee the operations of the JIE and more effectively support the operational requirements of our military forces around the world.

Through JIE, EOCs and CDCs will allow commanders to better understand the whole network posture, and more importantly, take coherent action to respond to operational conditions much more quickly and efficiently than today, increasing the overall tempo of global operations.

Driving Innovative IT Investments

As described in the *Capstone Concept for Joint Operations (CCJO): Joint Force 2020*, I believe that 80 percent of the future joint force is either programmed or already exists. Our task is to ensure that the 20 percent to be developed over the next 8 years is suited to likely future challenges. Our JIE is clearly part of that 20 percent that will drive us toward Joint Force 2020 by selectively investing in novel data and information exchange processes. Additionally, JIE is also especially important because it will revolutionize how we are able to use existing capability, by assembling a shared and optimizing IT enterprise infrastructure to enable the Joint Force to more flexibly employ its legacy capabilities in innovative ways. Our JIE will serve as the platform by which we realize, innovate, and employ new capabilities to surprise and confound our adversaries.

4. Way Forward for the Joint Information Environment

Over the next year, we will begin to physically implement a JIE capable of supporting the needs of Joint Force 2020. Beginning in European and Africa Commands, followed by an incremental global rollout to the rest of the Joint Force, Joint Warfighters will have access to a common, protected information infrastructure with which to plan and fight together with our mission partners.

The first indication of this change that those at the warfighting edge will notice will be a significant increase in the tempo at which network or IT administrative functions are accomplished. Next, users will begin to notice an ability to move across individual computers in such a manner that their data and permissions are intact wherever they are required to log in. Later, commanders at all levels will have a much deeper understanding of their cyber posture and capacity to adapt their posture to conditions as the EOCs are established and working relationships with the combatant commands developed and codified. Finally, we will have set the conditions for next generation capabilities, fully leveraging the power and versatility of commercial information technology and evolving from a brittle, network-centric understanding of our information environment to a flexible data-centric environment enabling access to information at the point of need.

I ask all Joint Force commanders and Service Chiefs to take notice of the implementation of JIE in the European theater, and leverage the lessons learned and JIE framework to accelerate world-wide implementation and apply those tactics, techniques and procedures in your areas of responsibility.

Conclusion

The JIE is essential to globally integrated operations and enabling mission command. It is a technical capability that supports our human capital by bringing to bear the power of the Enterprise across the strategic, operational, and tactical levels. Not only must the JIE be responsive to operational needs and unified action, but we must ensure that every joint warrior thinks about our information technology systems differently than we have in the past. Our IT systems do not simply allow us to e-mail one another, chat online, and access the web for our administrative tasks. They are the backbone we use to interconnect operations across multiple domains and deliver mission success around the globe.

The JIE will enable a versatile, responsive and decisive Joint Force and will provide a critical advantage relative to our adversaries. The Joint Force must see JIE as an operational capability that evolves, shifts, adapts and responds dynamically to enable mission command, and ultimately, mission success.