Strategy Research Project

Strategic Leadership Challenges with the Joint Information Environment

by

Lieutenant Colonel Stephen Edward Dawson
United States Army

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* xx-03-2013	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Strategic Leadership Challenges with the Joint Information Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Stephen Edward Dawson
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Mr. Brian A. Gouker
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,852

14. ABSTRACT

In the face of growing cyber attacks against Department of Defense (DoD) networks and numerous, varied, and complex information sharing challenges within the DoD Global Information Grid (GIG), the DoD has established a strategic vision to deliver a Joint Information Environment (JIE) that will enable the DoD and its mission partners to securely access information and services they require when they need it, from where they need it, and on the DoD approved device of their choice. The envisioned strategic end-state of this strategy is to enhance mission effectiveness, increase security, and to improve information technology efficiencies through the consolidation of costly network resources and infrastructure throughout the DoD. The JIE will be the key enabler of globally integrated security operations with the DoD's mission partners during the twenty first century. The DoD is faced with three strategic challenges to achieving the desired JIE end state; (1) There is a need for inspirational strategic leadership as an agent for change to champion the JIE effort. (2) Inter-service rivalries and parochialism must be overcome. (3) JIE funding must be a top priority for the DoD during an era of fiscal constraint in the name of national security.

15. SUBJECT TERMS
Cyberspace, Cyber, Networks, Security, Architecture, Technology, USCYBERCOM

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	34	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Strategic Leadership Challenges with the Joint Information Environment

by

Lieutenant Colonel Stephen Edward Dawson
United States Army

Mr. Brian A. Gouker
Department of Military Strategy, Planning, and Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Strategic Leadership Challenges with the Joint Information Environment
Report Date:	March 2013
Page Count:	34
Word Count:	6,852
Key Terms:	Cyberspace, Cyber, Networks, Security, Architecture, Technology, USCYBERCOM
Classification:	Unclassified

In the face of growing cyber attacks against Department of Defense (DoD) networks and numerous, varied, and complex information sharing challenges within the DoD Global Information Grid (GIG), the DoD has established a strategic vision to deliver a Joint Information Environment (JIE) that will enable the DoD and its mission partners to securely access information and services they require when they need it, from where they need it, and on the DoD approved device of their choice. The envisioned strategic end-state of this strategy is to enhance mission effectiveness, increase security, and to improve information technology efficiencies through the consolidation of costly network resources and infrastructure throughout the DoD. The JIE will be the key enabler of globally integrated security operations with the DoD's mission partners during the twenty first century. The DoD is faced with three strategic challenges to achieving the desired JIE end state; (1) There is a need for inspirational strategic leadership as an agent for change to champion the JIE effort. (2) Inter-service rivalries and parochialism must be overcome. (3) JIE funding must be a top priority for the DoD during an era of fiscal constraint in the name of national security.

Strategic Leadership Challenges with the Joint Information Environment

Today, the Department of Defense (DoD) communicates across a Global Information Grid (GIG) which provides a “globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes government owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems”[1]. Data is segregated in the GIG between one of two enclaves based on classification, the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). In its current operational status, the DoD’s GIG lacks interoperability between services and agencies which greatly inhibits efficient information sharing. It also employs a network-centric architecture that is inherently plagued with security vulnerabilities that render it practically indefensible. As a result of the proliferation of disparate and incompatible information technology (IT) capabilities over the last decade, the GIG has become an IT enterprise that is unwieldy, vulnerable to attack, and economically unsustainable. To address this technological quagmire, the DoD has approved the establishment of the Joint Information Environment (JIE) which will be comprised of shared IT infrastructure, enterprise services, and a single security architecture that will enable full spectrum superiority, improve mission command, realize IT efficiencies, and increase cyber security. In order to achieve this end state, the DoD will require; (1) inspirational strategic leadership as an agent for change to champion the JIE effort, (2) Inter-service rivalries and parochialism will have to be overcome, and (3) JIE funding must be a top priority for the DoD during an era of fiscal constraint in the name of national security.

The Global Information Grid is a DoD Center of Gravity

The DoD's extreme dependency upon the GIG as a mission critical enabling capability has likely been identified as a strategic and operational Center of Gravity (COG) by potential adversaries as indicated by the alarmingly increasing rate at which DoD networks are subjected to cyber attacks or exploitation. According to Joint Publication 5-0, "A Center of Gravity (COG) is a source of power that provides moral or physical strength, freedom of action, or will to act."[2] Carl Von Clausewitz states in his book "On War" that the enemy's COG is "the hub of all power and movement, on which everything depends…the point at which all our energies should be directed."[3] Arguably, access to the GIG, its networks and data, has been a DoD Center of Gravity (COG) during military operations over the past decade and the DoD will become increasingly dependent upon the GIG during the remainder of the twenty first century.

Joint Publication 5-0 further states that "critical capabilities are those that are considered crucial enablers for a COG to function as such, and are essential to the accomplishment of the adversary's (or friendly's) assumed objective(s)"[4]. Further analysis of the GIG within the context of crucial enablers reveals the DoD's overwhelming dependency upon access to the GIG at the strategic, operational and tactical levels. Consequently, all GIG systems and subsystems are essential to the DoD's data requirements that enable mission command and the global interconnectivity that enables our network centric weapon systems to function as designed. Any deliberate disruption of the GIG's systems or subsystems would certainly inhibit mission command and would likely render useless many of the network centric weapons that the

DoD employs in the operational environment. Additionally, an adversary’s successful breach of any particular GIG subsystem generally results in access to other, sometimes more critical, subsystems.

Joint Publication 5-0 also defines critical requirements as “the conditions, resources, and means that enable a critical capability to become fully operational”[5]. Analysis of the GIG’s critical requirements within the constructs of doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMIL-PF) reveals that communications units, hardware, software, firmware, data links, facilities, and a professional IT workforce are all critical capabilities required to operate the GIG. If any of these critical requirements are left unprotected, they become vulnerabilities that can be exploited and defeated by adversaries, ultimately destroying or at least debilitating the DoD’s COG.

Joint Publication 5-0 defines critical vulnerabilities as “those aspects or components of critical requirements that are deficient or vulnerable to direct or indirect attack in a manner achieving decisive or significant results”[6]. Security of the GIG is a critical vulnerability that is both deficient and vulnerable. Today the DoD operates a GIG consisting of numerous, disparate and uncoordinated security architectures that have rendered it virtually indefensible from a comprehensive, DoD level cyber defense perspective. This current security posture has been recently acknowledged as a critical vulnerability by strategic leaders, to include, the last two Secretaries of Defense’ (SECDEF), the Chairman of the Joint Chiefs of Staff (CJCS), and the Commander of the United States Cyber Command (USCYBERCOM).

The Quadrennial Defense Review (QDR) Report published in February 2010 states that “there is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field.”[7] It further identifies Operating in Cyberspace as one of the key lines of effort to rebalancing the force. It states that

> A Department-wide comprehensive approach to DoD operations in cyberspace will help build an environment in which cyber security and the ability to operate effectively in cyberspace are viewed as priorities for DoD. Strategies and policies to improve cyber defense in depth, resiliency of networks, and surety of data and communication will allow DoD to continue to have confidence in its cyberspace operations.[8]

Since the 2010 QDR was published, the DoD has taken comprehensive and unprecedented steps to address cyber security and the vulnerabilities that exist in the DoD’s COG.

Establishment of the United States Cyber Command

The Secretary of Defense directed the Commander of U.S. Strategic Command to establish The United States Cyber Command (USCYBERCOM) the on June 23, 2009. The command is charged with consolidating existing cyberspace resources, creating synergy that did not previously exist and synchronizing war-fighting effects to defend the information security environment. USCYBERCOM is responsible for “planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries”[9]. Unfortunately, the disparate and uncoordinated security architecture that is employed in today’s GIG makes it impossible for the USCYBERCOM Commander to virtually “see” the entire DoD network and effectively defend it from national and international cyber threats. This alarming condition was recently highlighted by the USSYBERCOM Chief of Operations, Brigadier General George Franz, when he stated in an address to the students of the United States Army War College in December 2012 that "we can only see about 10 percent of the entire dot mil domain which we are responsible for defending"[10]. This grave security condition is the resulting legacy of each DoD service and agency configuring and operating stove-piped networks that are separated by layers of firewalls and incompatible security protocols that make it impossible to operate a seamless DoD GIG. Consequently, this legacy also prevents USCYBERCOM from establishing a cyber Common Operating Picture (COP) where they can virtually see the entire dot mil domain down to the workstation level across the entire GIG.

To highlight the current insecurity condition of the GIG is not to suggest that any DoD service or agency built network capacity on the GIG in an intentionally reckless manner to circumvent security protocols, ignore standards, or purposefully stovepipe their networks, nor is it an attempt to lay blame. A reasonable assessment of what likely transpired over time is the services and agencies rapidly deployed IT capability in support of mission requirements without the benefit of a clearly articulated and coordinated DoD level IT architecture strategy. This was combined with unprecedented requirements for access to data and exponential network growth fueled by over a decade of war in OIF and OEF. The existing GIG and the IT enclaves operated by DoD services and agencies were not engineered with the Joint Force Commander, federal agencies, or coalition partners in mind. GIG enclaves operated by services and agencies were engineered hastily to meet urgent and unique mission requirements.

Consequently, security vulnerabilities have been inadvertently induced into the GIG over time and identified as critical vulnerabilities of the DoD's Center of Gravity by potential adversaries. The current well-intended but uncoordinated GIG security architecture sometimes complicates legitimate access to mission critical information by DoD personnel and often results in unintentional, yet exploitable, cyber vulnerabilities that inhibit defense of the DoD's GIG

The uncoordinated security protocols that prevent USCYBERCOM from virtually seeing the entire GIG also induces severe constraints on access to information during coalition and joint operations during Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF). For instance, obtaining GIG access in Iraq with a DoD computer was a time consuming and overly complicated process bogged down by local policies and procedures. A typical DoD computer hard drive would have to be erased and reconfigured for use on the NIPRNet or SIPRNet of the deployed base (a 24 to 48 hour process). Moving the computer to a different base would result in duplicating this process to regain network access. The network centric security architecture that inhibited access to data in Iraq continues to inhibit access to data in Afghanistan today. Unfortunately, this condition will remain unchanged until OEF officially ends, due to the unacceptable risk associated with making drastic network configuration changes during ongoing combat operations required to achieve a ubiquitous information environment.

Sharing information among DoD agencies, services, federal agencies and coalition partners has also proved to be extremely frustrating and challenging as a result of the DoD's uncoordinated security architecture. The DoD has had to operate as many as a dozen different networks in each CJTF Headquarters in order to effectively share information among the DoD, federal agencies and coalition partners in both the unclassified and classified domains. The burden of installing and operating so many disparate networks and duplicating effort in a single CJTF headquarters in order to accommodate information sharing among mission partners has been accomplished but at great fiscal expense, excessive infrastructure, and exceedingly complex information systems management requirements.

Future Security Environment Implications for the GIG

The security environment of the twenty first century calls for a national security strategy that relies heavily on building partner capacity to address regional security challenges. A theme of partnership and security cooperation is heavily emphasized and nested throughout the National Security Strategy of 2010, National Defense Strategy of 2008, and the National Military Strategy of 2011. More recently, the President of the United States signed and published guidance in a document called Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, which states that "the United States will continue to lead global efforts with capable allies and partners to assure access to and use of the global commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities"[11]. Information sharing is essential to achieving the President's vision of partner and coalition interoperability in support of international security. Partnership requires a seamless and ubiquitous IT architecture with a single, standard security protocol, identity management and access control. This would facilitate timely access to information during future data centric operations. Conversely, the last decade of war has painfully illustrated that the need to share information with federal agencies, allies, and nation partners has surpassed what our current IT enterprise is capable of supporting. This legacy demonstrates that the DoD must invest in a IT enterprise that enables secure sharing of information with any mission partner from approved devices from any location in the world.

Cyber security challenges of the GIG are further exacerbated by several other factors. Currently, DoD Combatant Commands and Services operate numerous data and operation centers that lack a common operating picture (COP) and inefficiently duplicate costly infrastructure. The lack of a COP can result in unilateral decisions or execution of uncoordinated cyber operations that inadvertently compromise USCYBERCOM's mission, the strategic level organization mandated with the mission of operating and defending the GIG. Additionally, a culture of service rivalry and parochialism has resulted in the enduring legacy of the non-optimal GIG. Each service has maintained their own network because control of their apportionment of the GIG translates to funding, personnel, resources and relevance. Additionally, Title 10 of U.S. Code provides the legal basis for the roles, missions and organization of each of the services which is interpreted by each service to mean that they are required by law to organize, train, and equip which gets translated to building and maintaining their own networks. Each service also perceives the existence of service unique IT requirements, which has justified the perpetual operation of service centric networks that are not seamlessly interoperable with the entire GIG. The net result is fierce competition for finite DoD IT resources, competition which will likely become more competitive during the foreseeable fiscally constrained budget era.

For the sake of argument, there isn't anything fundamentally different about the packets of data flowing through Army networks versus, Navy, Air Force or Marine

Networks. Every member of the DoD uses the GIG for the same fundamental reason which is to gain access to information in support of mission command and to enable our network and data centric weapon systems. Accept this premise and the following quote from LTG Susan Lawrence, the Army Chief Information Officer (CIO), could have easily been stated by the CIO of the DoD or any Service or Agency CIOs regarding their own network;

> Every facet of the expeditionary Army's operations, garrison to the tactical edge, depends on the network. It must accommodate the functional needs of the entire Army, from infantryman, to logistician, to doctor, to aviator, to engineer, to resource manager. The challenge, then, is to build a network that always keeps Soldiers, commanders and civilians connected, informed, empowered. The network must be global, seamless, always available and always trusted.[12]

It is imperative for the sake of national security in the twenty first century that Service CIOs abandon their service oriented lexicon that describes Army networks, Navy networks or Air Force networks, and instead embrace language that shows support for a network that is defendable and guaranties assured accesses to mission critical information by all DoD personnel, anywhere, anytime, and from any approved device.

Current Magnitude of the Department of Defense Cyber Footprint

In Fiscal Year 2013, the DoD IT user base had approximately 1.4 million active duty users, 750,000 civilians, 1.1 million Nation Guard and Reserve, and 5.5 million family members and retirees spread over 146 countries. The DoD operated over 10,000 operational systems, 800 data centers, 65,000 servers, 7 million computers, and 250,000 mobile devices (i.e. Blackberry). All of this IT capability represented an investment of $37 Billion in the Fiscal Year 13 DoD budget which is 7% of the total DoD Budget[13]. This figure includes $20.8 billion in IT infrastructure and $3.4 billion for cyber security[14]. A general consensus exists among many service and agency IT providers that the $37 Billion which DoD attributes to IT investment does not accurately account for the full DoD investment because much of the DoD's IT capability is often buried deep within non-IT programs of record.

Furthermore, the DoD's 800 data centers are distributed around the world and mostly dedicated to meeting service specific IT requirements. This duplication of effort results in ineffective utilization of scare resources. By design, data centers require enormous investment in redundant cooling and power systems along with expensive fire suppression systems and remote monitoring capabilities to ensure high availability and survivability. Replicating costly infrastructure across 800 non-optimal data centers is an enormous drain on precious IT funds.

The Most Dangerous Course of Action: A Cyber 9/11 Attack

The magnitude of unnecessary duplication of effort and the disparity of the non-standardized security architecture of the DoD GIG and its infrastructure is fiscally unsustainable. The indefensible condition of the DoD GIG, combined with the exponential growth in cyber attacks against DoD IT systems make the possibility of a crippling cyber attack, or what some have coined as a "cyber 9/11", possible. On October 12, 2012, Mr. Leon Panetta, the Secretary of Defense, addressed the Business Executives for National Security in New York City and stated that "a cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation." [15] As a matter of national security and readiness, the DoD must do its part to safeguard its mission critical IT systems from cyber attacks so they can be prepared to defend the nation during a potential cyber Pearl Harbor. We cannot achieve this end state if the DoD's mission command systems continue to operate in their current indefensible state.

The Awakening

Senior DoD leaders have acknowledged the strategic threat posed by increased cyber attacks against the GIG, the existence of security vulnerabilities, and unbridled IT spending. As a result, a sense of urgency regarding cyber security has gained momentum at senior levels of the DoD. In August 2010, Secretary of Defense Robert Gates announced a major DoD efficiency initiative to consolidate IT infrastructure and generate savings in the way the Department manages its IT enterprise. He stated in a Pentagon speech that

> The problem is that too many parts of the department, especially in the information technology arena, cling to separate infrastructure and processes. All of our bases, operational headquarters and Defense agencies have their own IT infrastructures, processes and application ware. This decentralization approach results in large cumulative costs and a patchwork of capabilities that create cyber vulnerabilities and limit our ability to capitalize on the promise of information technology. Therefore, I am directing an effort to consolidate these assets …. This action will allow the increased use by the department of common functions and improve our ability to defend defense networks against growing cyber threats.[16]

In October of 2010, Secretary Gates provided direction to consolidate IT infrastructure and to optimize the enterprise for the joint environment. In August of 2011, Admiral Michael Mullen, Chairman of the Joint Chiefs of Staff (CJCS), tasked the Joint Staff J-6 to work with Teresa Takai, the DoD Chief Information Officer (CIO), to lead an effort to "Evolve the Future Mission Network (FMN)", and address warfighter information sharing and security concerns when operating with coalition partners. In October 2011, the Deputy Secretary of Defense (DEPSECDEF) approved a strategy for delivering a information environment by signing the DoD IT Enterprise Strategy & Roadmap.

Coincidentally, in November of 2011, General Alexander, the USCYBERCOM Commander, briefed the JCS on the risk associated with the inability to “see” the entire DoD network in order to protect and defend it, and made recommendations to consolidate IT infrastructure to improve effectiveness. In response to General Alexander’s briefing, the JCS directed the Joint Staff J-6 and USCYBERCOM to work with the DoD CIO to develop a Joint Information Environment (JIE). A strategic vision finally emerged with a mandate from the SECDEF and CJCS to build a network that enables the DoD and partners to securely access the information and services they need at the time, place and on the approved secure device. This vision for a JIE is a unifying initiative that has the potential to accomplish a historical transformation of the DoD GIG which will deliver effective and efficient information and service sharing across the entire DoD enterprise.

What the Joint Information Environment is Not

Before describing what the JIE is, it would be useful to negate what the JIE is not intended to be. The JIE is a top down driven concept that started in 2010 as a strategic vision of Secretary Gates. But it is not an attempt by the “department” to take over the services’ networks by establishing a single service provider for all DoD who owns, operates and maintains the entire GIG from data centers to workstations, from the Pentagon to the tactical edge of the battlefield. Nor is it an attempt to give the Pentagon unilateral authority and ability to make decisions and or conduct uncoordinated cyber operations on the service’s IT assets. There is not a plan to consolidate service IT budgets and resources in order to establish the JIE as a program of record managed by the Joint Program Office. In fact, each service will be required to configure their apportionment of GIG based on JIE standards and architecture principals that are established by the DoD CIO and each service will continue to maintain control of their services' network.

What the Joint Information Environment is

In August 2012, the Chairman of the Joint Chiefs of Staff approved the JIE definition as:

> A secure joint information environment comprised of shared information technology 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).

The objective of the JIE is to provide a single, secure, reliable, timely, effective, and agile enterprise information environment that enables mission command of Joint Force Commanders and partnership with non-DoD partners across the full spectrum of operations, at all echelons, and in all operational environments. The JIE will support the full range of military operations from military engagement, security cooperation and deterrence activities to defense of the DoD GIG against kinetic and non-kinetic attacks, while at the same time supporting business and intelligence operations of the entire Department. To further institutionalize this transformational effort, the SECDEF signed the JIE Transformation Execution Order (EXORD) in November 2012, with the intent to direct the DoD JIE transformation planning, coordination, and execution.

Understanding of the JIE's envisioned strategic end state can be gained by applying some critical thinking to the JIE attributes that must be achieved so that the DoD's investment in this new IT architecture can enable future joint and combined operations with federal agencies and our international mission partners, improve cyber security, and realize cost savings efficiencies.

Mission Effectiveness

An absolute imperative of the JIE future mission network is that it must shift the architectural paradigm from network centricity to data centricity. If there is one thing the DoD achieved over the last decade of war, it was extending the network to just about every echelon or entity that required it, but not always resulting in access to required data. With the proliferation of highly portable commercial satellite terminals and innovative bandwidth on demand schema, the DoD achieved great success in pushing the network to the tactical edge at a reasonably affordable cost. But the DoD's future JIE must be a data centric network in order to overcome the shortfalls of today's GIG and ensure integration of all joint forces, federal agencies, coalition partners, allies, NGOs, and even industrial partners. A data centric JIE must also address requirements for intergovernmental relationships at the federal, state and local level in support of integrated homeland defense. Not only must the JIE be configured to enable data centricity, but network policy must also evolve along with the material solution in order to provide appropriate permissions to connect to an IT system that will facilitate sharing of information with any mission partner. Network policy today does not support extension of the DoD's NIPRNet and SIPRNet to anyone outside of the DoD because it is not currently technically feasible to control access to data based simply on identity credentials and permissions management. To that end, the JIE must provide an identity management solution along with an associated access control solution.

The bottom line for JIE mission effectiveness is that it must provide users the flexibility to access, store, and disseminate the data, applications and other computing services they require, at the time they require it, from any network location, and using any DoD approved network device. The device operating system should not have to be wiped clean and reloaded with a different system configuration just to accommodate local network policies every time you relocate to another JIE point of presence (base, post, camp or station). The JIE must be a data centric information enterprise that is ubiquitous throughout the DoD (the dot mil domain) and it should look, feel, and behave the same way no matter where you plug in. This is not the case with the network centric GIG that the DoD operates today.

Additionally, the JIE must enable cyberspace operations in support of mission commanders within and across all warfighting domains. Cyber operations is a rapidly growing mission area that future (and current) joint force commanders must be able to leverage in order to mitigate cyber vulnerabilities, defeat cyber threats, and ensure data integrity in support of mission command. Trust, one of the cornerstones of mission command, will be compromised if a commander loses confidence in the integrity of the data that is accessible and available within the JIE. Allowing DoD data to be exploited as a result of poor cyber security or unauthorized access affects everyone from the joint forces commander to the soldier at the tactical edge of the battlefield. Insecurity and loss of data integrity limits the ability of commanders to understand the situation and to communicate intent clearly to subordinates, which would ultimately erode the mutual trust necessary for mission command. Additionally, lack of confidence in the data that we share with mission partners would also erode the trust and confidence they would have in the U.S. to lead a coalition.

Security

The DoD's current network-centric architecture is not conducive to the operation of a data centric environment, nor is it adequate in protecting a DoD information environment that is increasingly under cyber attack. One of the most important aspects of the envisioned end state of the JIE is that of improved security, based on a single security architecture, that is implemented across the GIG by all DoD services and agencies, using the same technical standards and protocols. This design aspect is essential to the goal of establishing regional Enterprise Operation Centers (EOCs) that will replicate their common operational picture (COP) to the USCYBERCOM's Global Enterprise Operations Center (GEOC) in real time. If the JIE can achieve this critical end state, USCYBERCOM would actually be empowered to accomplish the planning, coordinating, integrating, synchronizing, and directing of activities to operate and defend the Department of Defense information networks. Finally, the DoD would be able to know who is operating on their networks with the highest degree of confidence and deny adversaries freedom of maneuver within the JIE through anomaly detection and active defense. At the end of the day, security is about maintaining information superiority by protecting our DoD's center of gravity, the GIG. Information superiority is the critical enabling capability of globally integrated joint operations within the construct of the CJCS vision for Joint Force 2020.

Efficiencies

The DoD cannot afford to continue operating the legacy GIG that was described earlier. The unnecessary duplication of facility infrastructure, inefficient use of network transports, too numerous service providers, and unbridled investments in hardware and software licensing is an unsustainable model that the JIE intends to address.

First, the JIE must consolidate the estimated 800 data centers and network operation centers operated by services in agencies by at least 50 percent over the next decade in order to improve centralized asset visibility and control and reduce duplication of effort. This will translate to reduced investments in operational and maintenance cost associated with expensive hardened facilities and associated support systems (cooling, uninterruptable power supplies, monitors, fire suppression systems) that are typically poorly designed and not operationally optimized. A strategy of consolidation also happens to be a trend in commercial industry with companies like Facebook, Amazon, and Google building energy efficient and environmentally friendly, high density data centers and leasing capacity to smaller companies as well as offering cloud storage to individual consumers for a nominal fee. Figure 1 depicts the potential results on operations center consolidation alone based on the strategic end state envisioned by the JIE concept[17].

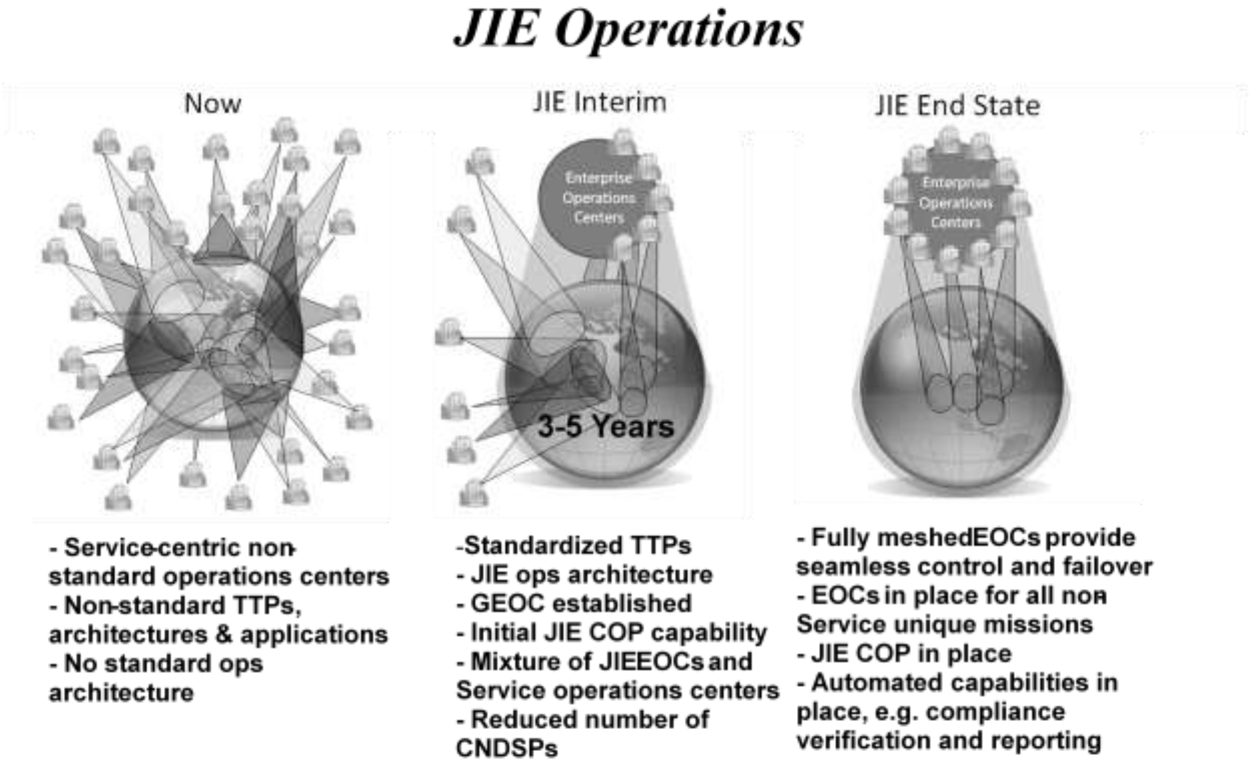
JIE Operations
Now
JIE Interim
JIE End State
Enterprise Operations Centers
3-5 Years
Enterprise Operations Centers
- Service-centric non-standard operations centers
- Non-standard TTPs, architectures & applications
- No standard ops architecture
-Standardized TTPs
- JIE ops architecture
- GEOC established
- Initial JIE COP capability
- Mixture of JIEEOCs and Service operations centers
- Reduced number of CNDSPs
- Fully meshedEOCs provide seamless control and failover
- EOCs in place for all non-Service unique missions
- JIE COP in place
- Automated capabilities in place, e.g. compliance verification and reporting

Figure 1. JIE Operations Center Consolidation

Second, the JIE must make increased use of enterprise level cloud based services such as e-mail, office productivity, business intelligence, chat, video conferencing, web collaboration, and data storage in order to realize increased mission effectiveness and operational efficiencies. In July 2012, the DoD Chief Information Officer (CIO), Teresa Takai, approved the DoD Cloud Computing Strategy which will "Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device."[18] Currently, the most widely recognized and understood achievement by the DoD in support of this cloud strategy is the proliferation of enterprise e-mail. Although this is a clear step in the right direction, enterprise e-mail is only the first incremental step in what will be at least a decade of transition. A change in mindset is required for DoD personnel who are accustomed to having applications and data located on their computer's hard drive. Instead, personnel will learn to access applications and data that reside in a secure data center (cloud) which they can't see, touch, or feel. A cloud strategy which leverages applications and data that reside in the cloud greatly reduces the risk of DoD employees accidently loosing laptop computers containing sensitive defense data such as happened in the past by the Las Alamos National Lab employees. The DoD Cloud Computing Strategy also intends to evaluate the use of commercial cloud services as an overall component to the Department's multi-provider enterprise cloud environment. By way of example, the United States Army War College (USAWC) recently gained authorization from the U.S. Army CIO G6 to utilize commercial cloud collaboration services from www.box.com for the sharing and collaboration of unclassified academic information. Based on the DoD Cloud Computing Strategy for leveraging commercial cloud services, DoD users can expect to see more authorizations for use of commercially available services similar to the USAWC example.

Strategic Challenges and Recommendations for the Road Ahead

The three most significant challenges associated with achieving the envisioned end state of the Joint Information Environment strategy will be the need for strong senior DoD leadership, the ability to influence service culture, and the ability to fund the JIE during a period of fiscal uncertainty. Although there are numerous other challenges and technical hurdles that must be overcome, the JIE can be systematically achieved over time with inspirational leadership at the DoD and service level, if a culture of service parochialism can be overcome, and if JIE funding can be made a high priority by the DoD.

Strategic Leadership

If there is one constant truism to successful outcomes in organizations, it is that strong leadership at all levels is absolutely essential to leading organizations to the desired strategic end state. The role of the strategic leader as an agent of change cannot be understated. The successful implementation of the JIE will weigh heavily on inspirational leadership at the DoD, service and agency level. Where past consolidation efforts by the services achieved marginal results or failed to meet their end state, the vision of the JIE probably has a better chance of success than any other consolidation effort of the last two decades. What makes the JIE initiative different is that the strategic vision was conceived by Secretary Gates in August of 2010 and it is being driven from the top down. With all the attention that has been given to the cyber threats to our national security, senior leaders such as Secretary Gates and Secretary Panetta have championed efforts to address the vulnerabilities that exist in our GIG. General

Dempsey, the current Chairman of the Joints Chief of Staff, also possesses an acute awareness of the vulnerabilities of the DoD's information enterprise as indicated in his January 2013 white paper on the Joint Information Environment. The mandate from the Chairman is clear. "The JIE is essential to globally integrated operations and enabling mission command", "The Joint Force must see the JIE as an operational capability that evolves, shifts, adapts and responds dynamically to enable mission command, and ultimately, mission success."[19]

Secretary Gates announced his appointment of Teri Takai as the Department of Defense Chief Information Officer (DoD CIO) in October 2010 where she serves as the principal advisor to the Secretary of Defense for Information Management/Information Technology and Information Assurance. This move further strengthened the Secretary's oversight of a defense network that is in dire need of recalibration. In her capacity as the DoD CIO, Ms. Takai provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology based capabilities required to support the broad set of Department missions. She published a Management Construct for the JIE on November 9, 2012 giving strategic momentum towards moving the entire DoD towards the JIE strategic end state. She has provided her vision for a framework which defines roles and responsibilities, established activities, and specifies processes for implementing, governing, and administering the DoD JIE strategy. Most importantly, she has established a framework for identifying compliance issues and enforcement measure to hold the DoD, services and agencies accountable for implementing the JIE.

The Army Chief Information Officer and G6, LTG Susan Lawrence, has made Army support of the JIE support clear beyond a reasonable doubt in her strategic messaging. She stated that “the Army is all in” and that “the Army is in synch with the CJCS’s vision and we are moving out aggressively”. While she cautions that while “it is not going to be quick” (seven year glide path for the Army) and “it is not going to be cheap” ($8.1 billion), “it is essential”.[20]

Influencing Service Culture

To achieve the strategic end state of the JIE, all barriers to consolidation and transition must be addressed without delay. Service parochialisms, rivalries and protection of rice bowls must be set aside in order to address a cyber threat of grave concern not only to the DoD but to the national security interest of the United States. The JIE is not about Army networks, or Navy networks, or Air Force networks, it is about enabling globally integrated joint operations with the DoD’s mission partners by readily sharing information on a data centric network that is secure and trusted. Overcoming service parochialism will require senior leaders such as the DoD CIO and each of the services’ CIOs to constantly and consistently communicate the higher purpose of the JIE and the importance of getting on board for the sake of national security. Championing the JIE is about service CIOs getting buy in, inspiring their organizations, and building unstoppable momentum towards the end state. A good example is the CJCS publishing his own JIE white paper.

Mr. W. James McNerney, Chairman, President and Chief Executive Officer of Boeing Corporation (a company of 170,000 employees located in 70 countries) addressed the U.S. Army War College in August of 2012. He explained how he changed the overall culture and subcultures within Boeing and overcame intramural rivalry and parochialism. When presented with a question regarding how he communicated his vision and changed culture, he stated that he focused his efforts on leadership development at all levels and communicated his vision to his company one conference room at a time[21]. This example of leadership in a global company highlights the importance of strategic leaders addressing the issue of parochialism head on, in person, and with conviction. This is the approach the DoD needs from the CJCS, Service Chiefs, and service CIOs.

From a parochialism perspective, the JIE will result in appointment of a single IT provider on each base, post, camp or station, to provide local infrastructure, end user device support, maintenance, and host local applications. A good example would be Joint Base Lewis-McChord in Washington State where either the Army or the Air Force will provide JIE network support to every organization located on the joint base, regardless of which parent service they belong to.

Fiscal Reality

According to the Army CIO, LTG Susan Lawrence, the looming DoD budget cuts and fiscal constraints are more of an opportunity than a threat because "we cannot afford to continue doing business the way we have been doing business."[22] She sees fiscal constraint as a driving force to push the DoD and the Army towards the goals of the JIE by consolidating network infrastructure, improving security, and improving mission effectiveness. And if there is any doubt as to where the JIE ranks in terms of other high priority investments for the DoD or the services, General Dempsey states in his JIE white paper that

> I believe that 80 percent of the future joint force is either programmed or already exists. Our task is to ensure that the20 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.[23]

The sense of urgency to fund the JIE cannot stop with the CJCS. It must reverberate throughout all services and agencies of the DoD. The enthusiasm garnered for achieving the desired end state of the JIE through the messaging and themes of our strategic leaders must be matched with actual investments when difficult fiscal decisions about national security priorities and risk mitigation are made. General Ray Odierno, the Chief of Staff of the Army, expressed his view of the JIE when he stated the following during an Army Live Blog in August 2012.

> The Army has global responsibilities that require large technological advantages to prevail decisively in combat – "technological overmatch," if you will… As I reflect upon the pace of technological change in today's modern world and the impact of rapid, global information exchange upon our overall security environment, I am both inspired and encouraged by the Army's approach to building a network able to connect our forces at all echelons. This remains our number one modernization priority.[24]

Deeds must now be matched with words. Does the JIE's initial momentum have the political inertia to come out of lengthy budget deliberations with the funding that is required to address the DoD's center of gravity and critical vulnerability? This is a question that will be answered after "sequestration "related budget cuts are sorted out by the DoD and only after the U.S. Congress pass a federal budget into law. With the current Continuing Resolution Authority (CRA) expiring on 27 March 2013, anything less than an authorizations and appropriations signed into law by congress would likely delay new investment into the JIE and cripple progress.

Conclusion

The DoD is approaching a critical crossroad where very difficult strategic decisions will be made by a military that is coming out of a decade of war. Services will be downsizing as a result of Budget Control Act of 2011 and sequestration at the same time that the DoD is attempting to grow cyber capability and improve cyber defense. The loss of conventional twentieth century military capability resulting from budget cuts will have to be balanced with investment in cyber capability order to address the twenty-first century risk that cyber threats pose to the U.S. national Security. To further offset the loss of conventional military capability, the U.S. is hedging its own conventional military capability on partner capacity and a whole of government approach to dealing with global security challenges as opposed to pure military solutions. The leveraging of partner capacity and whole of government approaches should also be included in the calculus of countering cyber threats where the DoD would use the JIE to share information regarding cyber threats with its agency, federal, commercial, and international partners.

Every strategic document to include the National Security Strategy, National Defense Strategy, National Military Strategy, and Quadrennial Defense Review, raises the issue of cyber threats to national security. The President of the United States remarked during the 2013 State of the Union Address that "America must face the rapidly growing threat from cyber-attacks.… we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[25] Pre 9/11 conditions exist in cyber space now. The DoD does not need a national commission appointed by congress to conduct forensics and investigations after a nationally devastating cyber attack to expose how the DoD did nothing in the face of real threats to national security. To that end, the JIE must be championed by strategic leaders throughout the DoD now. Parochialism and inter-service rivalries must be overcome, and funding of the JIE must be made a top priority in order to deliver the most innovative, efficient, and secure information and IT services in support of Joint Force 2020's mission, anywhere, anytime, on any authorized device.

Endnotes

[1] DoD Directive (DoDD) 8000.01, *"Management of the Department of Defense Information Enterprise*", February 10, 2009, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf, 10 (accessed February 15, 2013).

.

[2] Joint Publication 5-0, *Joint Operations Planning*, August 11, 2011, p III-22, pp e.(1).

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 595-596.

[4] Joint Publication 5-0, *Joint Operations Planning*, August 11, 2011, p III-24, e.(5).

[5] Ibid.

[6] Ibid.

[7] *Quadrennial Defense Review Report*, Department of Defense, February 2010.

[8]Ibid., 38.

[9] U.S. Cyber Command Mission, http://www.stratcom.mil/factsheets/Cyber_Command, (accessed January 29, 2013).

[10] BG George Franz, USCYBERCOM Lecture, U.S. Army War College, Carlisle Barracks, PA, December 14, 2012, cited with permission of BG Franz.

[11] President Barack Obama, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, 3.

[12] LTG Susan S Lawrence, Chief Information Officer/ G-6, Enabling Mission Command Workshop, September 5, 2012.

[13] The Department of Defense Information Technology Budget Exhibit, Fiscal Year 2012 President's Budget Request, March 2012, https://snap.pae.osd.mil/snapit/budgetdocs2013.aspx, (accessed January 29, 2013).

[14] Ibid.

[15] Remarks by Secretary Leon Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012,

http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136, (accessed January 29, 2013).

[16] Remarks by Secretary Robert M. Gates during a Pentagon News Briefing, August 9, 2010, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4669, (accessed February 26, 2013).

[17] *Joint Information Environment Operations Concept of Operations* (JIE Operations CONOPS), January 25, 2013, 10.

[18] *Department of Defense Cloud Computing Strategy*, July 2012, http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf (accessed February 28, 2013).

[19] General Martin Dempsey, Chairmen of the Joint Chiefs of Staff, *Joint Information Environment White Paper,* January 22, 2013, http://www.jcs.mil//content/files/2013-03/031813153411_JIE_-_CJCS_White_Paper.pdf (accessed February 28, 2013).

[20] LTG Susan Lawrence, Army CIO/G6, telephone interview by author, February 14, 2013.

[21] Mr. W. James McNerney, Chairman, President and Chief Executive Officer of Boeing Corporation, Changing Culture Lecture, U.S. Army War College, Carlisle Barracks, PA., August 2012, cited with permission of Mr. McNerney.

[22] Ibid.

[23] General Martin Dempsey, Chairmen of the Joint Chiefs of Staff, *Joint Information Environment White Paper*, January 22, 2013, 7.

[24] General Raymond Odierno, Chief of Staff of the Army, *Army Investment and Equipment Modernization: Maintaining the Decisive Edge*, August 7, 2012, http://armylive.dodlive.mil/index.php/2012/08/army-modernization/ (accessed February 28, 2013).

[25] Remarks by the President Obama, *State of the Union Address*, February 12, 1013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address (accessed February 28, 2013).