THE MILITARY APPLICATIONS OF CLOUD COMPUTING TECHNOLOGIES

A Monograph

By

MAJ Dallas A. Powell, jr.
SAMS Class 13-01, U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-15-2013	Master's Thesis	July 2012 – May 2013

4. TITLE AND SUBTITLE

The Military Applications of Cloud Computing Technologies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Dallas A. Powell, jr., U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Ave.
Ft. Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Cloud computing – remotely hosting network services and data – is an emerging concept in the business world that enables the use of mobile devices, increases security, and enables more effective information sharing within organizations. Within the last year, the U.S. Department of Defense has mandated that its networks be consolidated in order to achieve the goals of efficiency, effectiveness, and security. Through cloud computing across the network as an entire enterprise, efforts such as the Joint Information Environment and Enterprise Email endeavor to achieve those goals.
The view of military networks as an enterprise blurs the existing lines between garrison and tactical. Consolidation efforts are effective in permanent, garrison networks that are connected with high-bandwidth, fiber optic cables. Furthermore, hosting mission-critical services and data in the cloud will save resources and increase cyber security in the long run. However, similar application of consolidation efforts in the temporary, tactical networks which are employed in austere environments presents unique challenges that will be more effectively overcome if mission command systems are developed for use in both environments, remaining issues of physical security are more fully addressed, and if the concepts of cyber are effectively operationalized in a more comprehensive doctrine.

15. SUBJECT TERMS
Cloud computing, Joint Information Environment, Enterprise Email, Global Network Enterprise Construct, Network Integration Exercise, Network Centric Warfare, Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified	UU	55	(913)684-3302

MONOGRAPH APPROVAL PAGE

Name of Candidate: MAJ Dallas A. Powell, jr.

Monograph Title: The Military Applications of Cloud Computing Technologies

Approved by:

_____, Monograph Director
Matthew Schmidt, Ph.D.

_____, Seminar Leader
Michael J. Lawson, COL

_____, Director, School of Advanced Military Studies
Thomas C. Graves, COL

Accepted this 23rd day of May 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE MILITARY APPLICATIONS OF CLOUD COMPUTING TECHNOLOGIES, by MAJ Dallas A. Powell, jr., 55 pages.

Cloud computing – remotely hosting network services and data – is an emerging concept in the business world that enables the use of mobile devices, increases security, and enables more effective information sharing within organizations. Within the last year, the U.S. Department of Defense has mandated that its networks be consolidated in order to achieve the goals of efficiency, effectiveness, and security. Through cloud computing across the network as an entire enterprise, efforts such as the Joint Information Environment and Enterprise Email endeavor to achieve those goals.

The view of military networks as an enterprise blurs the existing lines between garrison and tactical. Consolidation efforts are effective in permanent, garrison networks that are connected with high-bandwidth, fiber optic cables. Furthermore, hosting mission-critical services and data in the cloud will save resources and increase cyber security in the long run. However, similar application of consolidation efforts in the temporary, tactical networks which are employed in austere environments presents unique challenges that will be more effectively overcome if mission command systems are developed for use in both environments, remaining issues of physical security are more fully addressed, and if the concepts of cyber are effectively operationalized in a more comprehensive doctrine.

ACKNOWLEDGMENTS

While much of this research originated with some of the author's experiences as a U.S. Army Signal Officer, some individuals deserve special recognition for their inspiration, mentorship, and expert input. When I served as a Brigade S-6, then-Maj. Gen. Susan Lawrence (commander of NETCOM at the time) first suggested to me – much to my chagrin – that future technologies could eliminate the need for Brigades to deploy with their own network servers. This research has certainly borne out the possibilities those technologies can provide. That Brigade's commander at the time, then-Col. Joseph Harrington, also strongly urged me to write about those and other experiences. In many ways, this paper is an outgrowth of his mentorship.

Two other Army officers have contributed immeasurably to this project. Col. Claire Cuccio, who was the director of the TNOSC in Kuwait several years ago when I was an inexperienced Battalion Executive Officer, provided technical oversight and an expert pair of eyes to ensure the technical details of this research were right. Her eventual successor in that previous position, Lt. Col. Brian Vile, is a battle buddy and friend who is now the writer of the very document which currently defines the Joint Information Environment. I could not have completed this research without either of them.

TABLE OF CONTENTS

ACRONYMS

ABCS	Army Battle Command System
AKO	Army Knowledge Online
APC	Area Processing Center
ARCIC	Army Capabilities Integration Center
ARFORGEN	Army Force Generation
ARCYBER	U.S. Army Cyber Command
AUSA	Association of the U.S. Army
BCCS	Battle Command Common Services
BCSS	Battle Command Server Suite
BCT	Brigade Combat Team
BVTC	Battlefield Video Teleconference
C4I	Command, Control, Communications, and Computers
CAC	Common Access Card
CAM	Combined Arms Maneuver
CCJO	Capstone Concept for Joint Operations
CIO/G-6	Chief Information Officer/G-6
CJCS	Chairman, Joint Chiefs of Staff
COE	Common Operating Environment
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COP	Common Operational Picture
CPN	Command Post Node
CPOF	Command Post of the Future

DCO	Defensive Cyber Operations
DGO	DoD GIG Operations
DigSOP	Digital Standing Operating Procedures
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoD-CIO	Department of Defense Chief Information Officer
DSN	Defense Switched Network
EEmail	Enterprise Email
EOIP	Everything Over Internet Protocol
EXORD	Execution Order
FHRN	Fixed Regional Hub Node
FOB	Forward Operating Base
GAL	Global Address List
GAO	Government Accounting Office
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
GPS	Global Positioning System
IaaS	Infrastructure as a Service
IAADS	Installation as a Docking Station
IP	Internet Protocol
IT	Information Technology
JIE	Joint Information Environment
JNN	Joint Network Node
JTF	Joint Task Force

JWICS	Joint Worldwide Intelligence Communications System
KaaS	Knowledge as a Service
LAN	Local Area Network
LWN	LandWarNet
MBps	Megabits per second
MSps	Megasymbols per second
NCW	Network Centric Warfare
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NETOPS	Network Operations
NIE	Network Integration Evaluation
NIPRNET	Nonsecure Internet Protocol Routed Network
NIST	National Institute of Standards and Technology
NOSC	Network Operations and Security Center
NSC	Network Service Center
OCO	Offensive Cyber Operations
OPVAL	Operational Validation
OWA	Outlook Web Access
PaaS	Platform as a Service
RMA	Revolution in Military Affairs
SaaS	Software as a Service
SIPRNET	Secure Internet Protocol Routed Network
STRATCOM	U.S. Strategic Command
TACHUB	Tactical Hub Node
TBC	Tactical Battle Command

TNOSC	Theater Network Operations and Security Center
TOC	Tactical Operations Center
TTPs	Tactics, techniques, and procedures
ULO	Unified Land Operations
USAFRICOM	U.S. African Command
USCYBERCOM	U.S. Cyber Command
USEUCOM	U.S. European Command
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
WAN	Wide Area Network
WAS	Wide Area Security
WIN-T	Warfighter Information Network – Tactical

ILLUSTRATIONS

Page

INTRODUCTION

This research began with investigating the military applications of cloud computing technologies, while inferring that doing so will have a positive overall impact on military networks in terms of leveraging network and fiscal efficiencies, but that some technical challenges in the tactical networks will remain – such as security, bandwidth limitations, and reduced tactical network redundancies. The analysis of recent U.S. Army experiments revealed that bandwidth limitations and network redundancies are not as serious as originally considered. However, the analysis confirmed challenges still exist in physical security of networks, and discovered other issues. Securing networks "in the cloud" presents its own unique challenges, especially physical security limitations. Additionally, the physical limitations of bandwidth in the frequency spectrum – especially on the tactical edge of the network – will directly affect feasibility of hosting certain services in the cloud.

Through studying recent incidences of the Army's efforts to employ cloud computing, several other important points were revealed. Primarily, although current doctrines and directives take a view of military networks as a singular enterprise, clear delineations exist between the permanent networks in garrison locations and the temporary, portable networks employed in tactical environments. These demarcations reside in the infrastructure, applications, and devices developed for exclusive use in one environment or the other. Furthermore, issues abound in using tactical applications on garrison networks. In addition, the research discovered a distinct absence of a doctrinal explanation of cyberspace, outside of the Information Technology spheres of influence; incorporating cyber into the doctrinal lexicon can explain its history and relevance to current concepts as a distinct warfighting domain. While cloud computing will ultimately save money as well as increase security and interoperability between services, agencies, and coalition partners, these issues will potentially hinder its true effectiveness.

Background and Significance

The recent, rapid advance of networking technologies supporting the U.S. Armed Forces has produced an additional layer of complexity to the modern battlefield, while enabling commanders and their staffs at all levels to employ unprecedented information dominance, virtually instantaneous visualization of the battlefield, and global communications capabilities. Cloud computing – in short, remotely storing data and hosting network services that are traditionally provided locally – is a recent business practice that is employed in civilian networks to reduce overhead and manage corporate information more effectively.[1] In the last several years the U.S. military, specifically the Army, has investigated how to apply cloud computing technologies to its C4I systems in order to provide more cost-efficient, effective services to units in garrison locations around the globe as well as operational and tactical units under deployed conditions in austere environments.[2] Ostensibly, cloud computing would provide more reliable information access and security, simplicity for deploying units, increased possibilities for virtual training, and reduced costs in terms of locally-maintained hardware. However, some challenges include physical security, information assurance (in keeping networks of different classification truly separate), and the physical limitations and increased costs of satellite bandwidth. While these challenges are relatively simple to overcome in garrison networks or deployment environments (such as Afghanistan) where the networks have "matured" or become more permanent, the difficulties are compounded when employing cloud computing in more austere

---

[1]Eric Knorr and Galen Gruman, "What cloud computing really means," *InfoWorld*, http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 [accessed January 31, 2013].

[2]Command, Control, Communications, Computers, and Intelligence; see Chairman of the Joint Chiefs of Staff, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, (*Washington, DC: 15 August 2012), Appendix A.

environments. This paper will examine the military applications of cloud computing, and assess those applications' necessity, feasibility, and potential effectiveness. Some recent case studies will be analyzed in order to support these observations, while demonstrating Army efforts to utilize cloud computing on both legacy and upgraded networks. The military implementation of cloud computing technologies will have a positive overall impact on the military network in terms of leveraging network and fiscal efficiencies. Despite these benefits, some technical challenges in the tactical networks will remain, such as security, bandwidth limitations, and reduced tactical network redundancies.

Current networked, digital systems on the battlefield are supported by a wide area network (WAN) which connects tactical and operational units to the Global Information Grid (GIG), which is the military's worldwide web, phone, and video teleconferencing network. The GIG is operated and maintained by the Defense Information Systems Agency (DISA).[3] This system provides secure and unclassified voice, video, and data services to the military. The Army's portion of the GIG, known as LandWarNet (LWN), consists of all of the Army's networks at every post, camp, or station in the world – including tactical networks in combat theaters of operation.[4] Deployable satellite terminal packages under the Warfighter Information Network –

---

[3]The GIG is the strategic layer of military network services that includes major satellite and terrestrial backbone links, as well as applications used at higher echelons of command. *JP 6-0*, p. II-1, defines the GIG thus: "…the 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." In essence, the GIG is the DoD's World Wide Web, and includes "information, and information services residing on transporting infrastructures and segments." (see also FM 6-02.71, p. 1-1.)

[4]LWN is the Army's portion of the GIG, including all Army networks and services, and encompassing tactical and garrison-based networks across all classifications, and includes data, voice and video services. (See FM 6-02.43, 3-3 through 3-4.) The Army's CIO/G6 has overall responsibility for operating and defending LWN. The organizational structure of the personnel who accomplish these tasks depends on the location and environment of that particular part of the LWN. Oversight of the entire LWN is the mission of the U.S. Army Cyber Command

Tactical (WIN-T) program connect units on the WAN. This allows access to network services from almost anywhere in the world, typically through a Joint Network Node (JNN). Under current organizational configurations, approximately 210 unit headquarters, from Corps and Army Service Component Command down to Battalion, are supported by a JNN-equipped Signal Company that connects the Tactical Operations Centers (TOC) to the LandWarNet through its JNN.[5] These headquarters are equipped with a self-contained server set known as the Battle Command Server Suite (BCSS), which includes a Microsoft Windows network for the unit. The Windows network includes email, file sharing, and anti-virus servers for protection. Each BCSS package also contains databases to connect and support data from every digital, mission command system.[6] The mission command systems are collectively known as Army Battle Command Systems (ABCS), and essentially provide the commander and his or her staff with a Common Operational Picture (COP) of the battlefield. The ABCS is a "system of systems." It also provides various tools for processing, analyzing, and disseminating various data for intelligence, targeting, logistics, airspace management, medical and friendly unit locations. Most individual ABCS systems were essentially developed as stovepipe systems to perform these

---

(ARCYBER), which is directly subordinate to U.S. Cyber Command (CYBERCOM), a sub-unified command that is currently part of U.S. Strategic Command (STRATCOM). ARCYBER directs 9th Army Signal Command/Network Enterprise Technology Command (NETCOM), which oversees the various subordinate Signal Commands.

[5]Battalions connect through a smaller Command Post Node (CPN), providing less bandwidth than a JNN, which supports Brigade and higher-level units.

[6]Headquarters, Department of the Army, *Army Doctrinal Reference Publication 6-0, Mission Command*, (Washington, DC: May 2012), 1-5, defines mission command system as "…the arrangement of personnel, networks, information systems, processes and procedures, and facilities and equipment that enable commanders to conduct operations." For the purposes of this paper, "mission command system" refers to networked C4I systems designed to provide a COP view of the battlefield across all warfighting functions. See also "Army Battle Command Systems (ABCS)," http://www.dote.osd.mil/pub/reports/FY2005/pdf/army/2005abcs.pdf [accessed March 10, 2013].

specific functions, but are connected through the BCSS databases at the Division level or above in the network. The following diagram illustrates the basic WIN-T Increment 1 network, without the BCSS or ABCS systems:

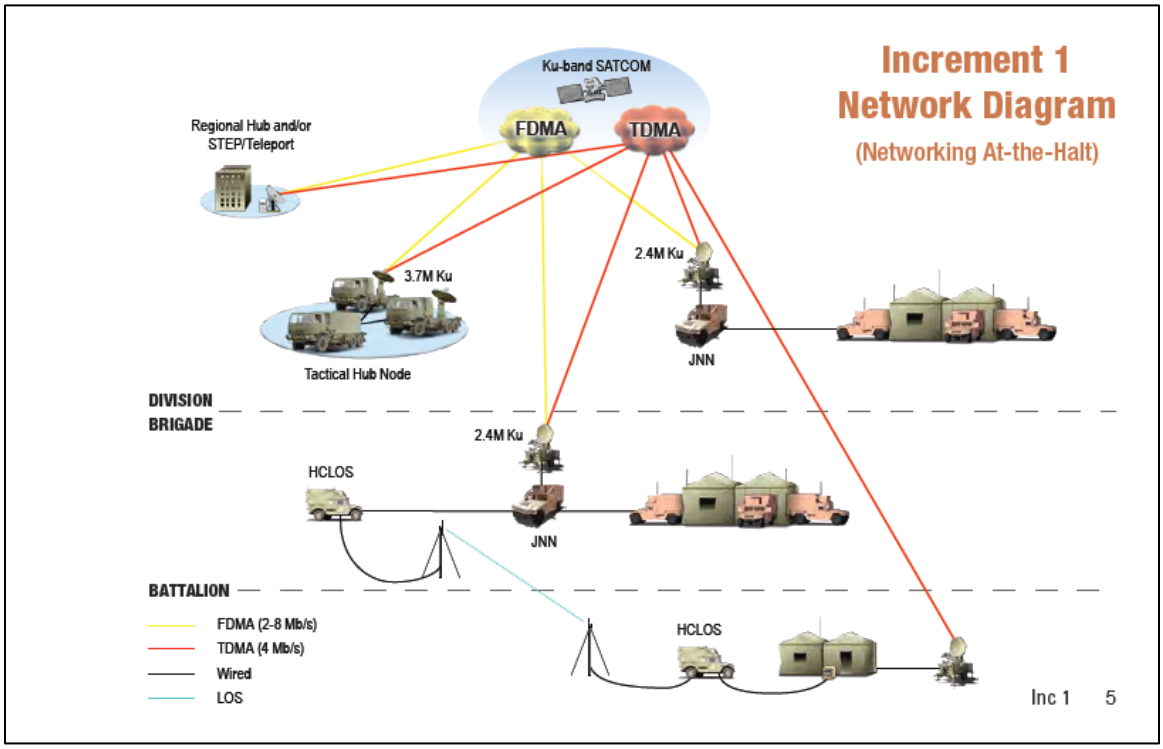

Figure 1. WIN-T Increment 1 Network Diagram.

Source: General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 5.

These networks, including domains of different classifications, are known collectively as "the enterprise," a term which implies a view of all disparate networks as one.[7] Current doctrine,

[7]A common but ill-defined term in the Signal community, "the enterprise" is essentially a federation of networks that individually serve narrow communities of users (See FM 6-02.43, *Signal Soldier's Guide*, March 2009, 6-1.) According to FM 6-02.71, the enterprise is a subset of Network Operations (NETOPS): "An 'enterprise' is described as a set of diverse, physically separated, but related, components that work together in order to achieve a functional objective. Enterprise services are those that offer collaborative, software distribution, messaging, discovery, storage, user/system assistance, and security functionality." (FM 6-02.71, *Network Operations*,

recent strategic directives, and Army initiatives reflect this model; however, separations exist which current modernization efforts will address. For the Army, LWN is synonymous with the enterprise and is a primary enabler of the Army's mission command philosophy and doctrine.[8] The present Department of Defense Chief of Information Operations (DoD-CIO) recently issued a strategy for employing cloud computing through the Joint Information Environment (JIE), which is mirrored in the recent Chairman Joint Chiefs of Staff (CJCS) execution order and white paper. These documents describe the JIE, provide details on an implementation strategy, and assign overall responsibility for implementation to DISA – however, they do not address any Service-specific plans for tactical LWN connectivity.

Since 2009, the Army has conducted experiments focused on implementing cloud technologies and other best business practices in the enterprise – especially at the tactical edge of the LWN – in order to identify and mitigate network issues in tactical units as they deploy. The Operational Validation (OPVAL) exercises, conducted in 2009 and 2010, tested the now-defunct Global Network Enterprise Construct (GNEC) concept, which sought to utilize certain cloud computing ideas to remotely backup some server data for deploying units.[9] The Army's semi-annual Network Integration Evaluation (NIE) exercises, conducted since 2012, have tested cloud-delivered services at the tactical edge of LWN, using JIE constructs.[10] These tests were conducted

---

July 2009, 1-5 through 1-6.) Administrative management of the enterprise is conducted through Active Directory, the directory service for Windows 2003 and subsequent server capabilities (and later versions). (FM 6-02.71, Appendix A.)

[8]Jeffrey A. Sorenson, "Welcome to the Enterprise," *Army* 60, No. 10 [October 2010].

[9] The JIE concept effectively replaced GNEC in 2011.

[10]William Welsh, "Network validation effort sets stage for Army's upcoming NIE 13.1," *Defense Systems*, October 4, 2012, http://defensesystems.com/articles/2012/10/04/army-validation-exercise-nie.aspx?admgarea=DS [accessed November 12, 2012].

using tactical units and network connectivity equipment, with the purpose of minimizing the differences between tactical and garrison networks. As this strategy matures, the ways in which future, deployed units connect to the LWN will change. Furthermore, these changes will revolutionize mission command systems down to the tactical edge, utilizing the very latest technologies in smart phones, tablet computers, and other hand-held devices. As the research will show, the changes wrought by cloud computing will benefit by saving money, improving information sharing, and increasing cyber security – but issues will remain in physically securing critical network nodes, using the latest technologies on both sides of the network, and operationalizing the concepts related to cyber.

Cloud Computing Defined

At its most basic, cloud computing means using a minimal computing device to access remotely-hosted data or services. This official definition is according to the National Institute of Standards and Technology (NIST):

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[11]

A cloud infrastructure is the configuration of hardware and software that enables five essential characteristics: on-demand self-service, meaning a user can connect as needed automatically; broad network access, with minimum hardware requirements; resource pooling; rapid elasticity, meaning capabilities can be automatically scaled transparent to the consumer and according to

[11] Peter Mell and Timothy Grace, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," *NIST Special Publication 800-145,* September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [accessed October 1, 2012], 2.

demand; and measured service, or a charge-per-use basis. Current military doctrine does not define cloud computing, but the DoD-CIO's guidance echoes the NIST definition and differentiates cloud computing from previous models: "While the traditional IT delivery model is focused on the development, maintenance, and operation of computing hardware and software, the cloud computing model focuses on providing IT as a service. …service providers and service consumers interact…over and Internet Protocol (IP)-based network."[12]

Conceptually, the cloud infrastructure is viewed as both the physical layer (servicing hardware such as server, storage, and network components) and the abstraction layer (software which manifests the essential cloud characteristics). Services in a cloud environment are provided via one of three service models, in which the user does not control underlying cloud infrastructure:[13]

- Software as a Service (SaaS). Consumers use the provider's applications running on a cloud infrastructure, typically through a web browser, and can only manipulate local, limited application configuration settings. An example is Google's document editing features over the Internet.
- Platform as a Service (PaaS). Consumers create or acquire applications supported by the provider, such as Apple applications being used on a user's iPad. As applied to military

[12]Department of Defense Chief Information Officer, "Cloud Computing Strategy," July 2012, http://www.disa.mil/Services/~/media/Files/DISA/Services/Cloud-Broker/dod-cloud-strategy.pdf [accessed August 1, 2012], 2.

[13]Mell and Grace., 2-3.

networks, this approach would reduce the number of stovepipe systems by simplifying and standardizing them across the board.[14]

- Infrastructure as a Service (IaaS). Devices use the infrastructure with any (ostensibly approved) operating system or software, and users control storage and applications. Virtual Private Network (VPN) services, such as those provided commercially by Verizon, enable users to connect securely to cloud services from personal devices.
- A fourth service model, Knowledge as a Service (KaaS), has also been proposed in the business world. [15] This model essentially provides tailorable data solutions to customers based on their specific needs, and is based on the recent "data finding data" concept.[16]

These services are delivered through various configurations of the cloud infrastructure, defined as four deployment models: [17]

- Private. Exclusive use by a single organization, with the infrastructure normally housed off-site and possibly operated by a third party. Example: a multinational corporation's

---

[14]Henry Kenyon, "Out With the Old, In with the New," *Signal Magazine Online*, November 10, 2011, http://www.afcea.org/content/?q=2011/11/10/14575 [accessed December 4, 2012].

[15]Jamie Dos Santos and Jill Singer, "Looking for the Right Answers in the Clouds," white paper, Armed Forces Communications and Electronics Association," September 2012, 7, http://www.afcea.org/committees/cyber/documents/LookingfortheRightAnswersintheCloudsWhitePaper.pdf [accessed October 15, 2012].

[16]Jeff Jonas and Lisa Sokol, "Data Finds Data," in *Beautiful Data, The Stories Behind Elegant Data Solutions,* by Tony Segaran and Jeff Hammerbacher (USA: O'Reilly, 2009), 105-118.

[17]DoD-CIO, "Cloud Computing Strategy," C-1.

cloud services may be operated by Amazon, but accessible only to employees of that corporation.[18]

- Public. Services are open for use by anyone in the general public, and can be owned or operated by business, academic, or government entities. Example: Google's cloud services allow limited free storage of files, accessible anywhere via the web, or more storage for a fee.[19]
- Community. Services are available for exclusive use by members of a community of shared interest and are operated by a combination of members of the community or a third party.
- Hybrid. Any combination of the above that are linked by standard technology enabling portability of data and applications. The military's implementation will likely follow this model.

The most likely cloud computing construct to be implemented by the DoD would be an IaaS/Hybrid cloud. Although this construct is not specified in any directives or plans, it is essentially providing IT as a service through this combination of the service/deployment models, and forms the backbone of the JIE. While "the cloud" can provide effective failover services in a catastrophic network outage, this paper will avoid oversimplifying "the cloud" or its military applications as some omniscient entity that will easily solve all of the military's IT problems; rather, in this sense "the cloud" is a carefully engineered set of installations, circuits, hardware,

---

[18]Quentin Hardy, "Active in Cloud, Amazon Reshapes Computing," *The New York Times*, August 27, 2012, http://www.nytimes.com/2012/08/28/technology/active-in-cloud-amazon-reshapes-computing.html?emc=eta1 [accessed August 28, 2012].

[19]"Build your business on Google Cloud Platform," https://cloud.google.com [accessed January 31, 2013].

etc., that will enable the JIE and, coupled with network governance and IT acquisitions procedures, will provide capabilities to achieve the DoD-CIO's consolidation goals.

WHY IMPLEMENT CLOUD COMPUTING?

Impetus for Change

Specialized networks and systems have been developed over the last couple of decades for specific purposes such as targeting and intelligence, with little focus on integrating them into a simpler construct. Many efforts have been taken to connect these stovepipes together in the military – and the key goal of the JIE is to do just that, enabled by cloud computing. But in the face of limited budgets after years of seemingly profligate military spending on two extended wars, how necessary is it to modernize the network? The primary reason for transformation is to save money in the current, fiscally-constrained environment. Over two years ago, IT mogul Michael Dell opined:

> The federal government spends approximately $76 billion to support its widely dispersed information technology assets. Up to 30 percent of that spending could be saved by further reducing IT overhead, consolidating data centers, eliminating redundant networks and standardizing applications.[20]

In military networks, those unnecessarily redundant expenditures also come primarily from differing governance standards in security, hardware, and software licenses between military posts in different regions of the world, as well as those belonging to different military services. Expenditures spiral even more when one considers the costs of employing redundant IT staffs – for instance, in late 2010 an interim contract was awarded to ITT Corporation to employ some

---

[20]Samuel J. Palmisano and Michael Dell, "Washington can save $1 trillion," *Politico*, October 6, 2010, http://www.politico.com/news/stories/1010/43188.html [accessed November 29, 2012.

2,000 civilian contractors to operate and maintain military networks in Southwest Asia and North Africa, for $538 million for an 18-month period ending July 2012.[21] Although this expense is necessary on its surface to support base communications for deployed forces, it might have cost significantly less if the networks had been centrally designed and managed as a true enterprise from the start.

At the outset of the recent wars in Iraq and Afghanistan, ad hoc networks between units were cobbled together with little planning for their enduring needs. Units deploying from their home stations and would bring their computers and WIN-T equipment, and in the wars' initial stages some units even deployed outdated, analog networks that were not compatible with the all-digital WIN-T network. In each theater, temporary, tactical networks were separately transformed into permanent networks with little regard for standards or costs, in favor of “getting the job done” well enough. Varying local network standards and policies between garrisons at home, staging areas, and their forward deployed locations required units to completely erase their computers at multiple stops along the way before those computers could be connected. All too frequently, users would also have to have separate login and email account at each stop as well. As a result, commanders would have to endure periods of time with limited or no network access, or rely on other units for help. According to Lt. Gen. Susan Lawrence, the current CIO/G-6 of the Army, every individual service or agency that deployed into either Iraq or Afghanistan brought their own network solutions, which ultimately caused degraded security and unnecessary confusion from disparate standards. Responding to other crises around the globe presented other challenges that became too difficult or too expensive to manage, and provided more reasons for

[21]“TAC-SWACAA 12-month Interim Contract,” https://www.fbo.gov/notices/dde704d4b7746f68fb6ad1a2867ccf5c [accessed November 29, 2102].

transformation. Furthermore, according to Lawrence, the current network in Afghanistan is modernized with all voice, video, and data services being provided digitally (known as "Everything Over Internet Protocol," or EOIP) – yet the garrison-based networks throughout the army are still obsolete.[22]

Additionally, as units in the ARFORGEN cycle train for the next deployment, the computers that soldiers use in the field cannot be connected to their garrison-based networks without significant reconfiguration. Consequently, ABCS systems are stored and often unused for months at a time between field exercises – and vital data is lost, or skills on those systems atrophy because systems are not being used in garrison. As equipment and systems were developed and fielded for deploying units, a physical and logical separation was created and still exists, which separated the tactical networks from the garrison-based networks. This means that every user has to have separate login usernames and passwords for each network, and even more confusion is caused by maintaining separate login and email accounts.[23] These needs – to eliminate unnecessary redundancies, streamline acquisition, reduce IT staffs, maintain security and establish a common, more user-friendly network – necessitate modernization. This modernization will continue to merge garrison and tactical networks into a singular enterprise. As further sections will address, the JIE will seek to solve these and other issues.

---

[22]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1," digital video, October 23, 2012, http://www.dvidshub.net/video/159082/cyber-domain-and-landwarnet-part-1#.UREpp6V9LSg [accessed December 12, 2012].

[23]John Nelson, "The Operational Impacts of the Global Network Enterprise Construct," SAMS Monograph, May 2010, 10-17, http://www.dtic.mil/dtic/tr/fulltext/u2/a523131.pdf [accessed June 25, 2012].

DoD Directives: An Operational Design Approach

In addition to standardizing networks and cutting costs, securing and defending cyberspace is a national security priority which is specifically mentioned in almost every strategic document of the current administration.[24] The President's most recent State of the Union speech highlighted the need to modernize the nation's networks in order to solve the problems of information sharing and cyber security in order to achieve and maintain dominance in cyberspace; this has also been a consistent priority of the U.S Government for several years.[25] The Department of Defense, in recognizing the need to modernize its military and supporting networks in support of that strategic purpose, takes an enterprise view in its operational approach to solving the problem. According to the DoD-CIO, problems exist in the unnecessarily complex IT networks which for years were developed to provide immediate, specific capabilities and caused reduced security, ineffectiveness in sharing relevant information across services and agencies, and needless expense. Officials and senior military leaders realized that the need existed for the desired end state of the enterprise to enhance operational efficiency and thus increase cyber security, improve effectiveness of both garrison and tactical networks in the enterprise, reduce overall costs and maintain the flexibility to utilize future emerging technologies.[26]

---

[24]Cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." See *JP 1-02*, 77. Cyberspace is commonly used in exchange with the shorter term, cyber.

[25]Barack H. Obama, State of the Union speech, February 7, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address [accessed February 13, 2013].

[26]Department of Defense Chief Information Officer, "Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap," September 6, 2011, http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf [accessed September 30, 2012], 4-5.

This desired state will be realized in consolidating a massive IT infrastructure which currently includes some 15,000 network enclaves and over seven million computing devices across hundreds of installations around the world. To achieve this end, the DoD-CIO developed twenty-six specific initiatives to support five major functional areas (or Lines of Effort): Network Services, Computing Services, Application and Data Services, End-User Services, and IT Business Practices.[27] Three major approaches were considered: consolidation of IT services either at the DoD Component level (meaning individual military services), aiming to optimize the joint environment, or at the DoD enterprise level. The DoD-CIO chose the second approach, optimizing consolidation across the joint environment, primarily because it would best support the Lines of Effort and achieve shorter-term efficiency and expenditure objectives, while enabling future consolidation efforts across the DoD (third approach).[28]

The DoD-CIO's subsequent Cloud Computing Strategy, published July 2012, outlined more specific details on how the IT Enterprise Strategy would be implemented.[29] Again, an operational design approach was taken to show the current state, desired state, problem statement, and Lines of Effort with supporting decisive points, all of which describe the strategy of implementing cloud computing in order to achieve the objective of a more secure, efficient, and adaptable network. The four concurrent LOE's used in this approach are: foster adoption of cloud computing, optimize data center consolidation, establish the DoD Enterprise cloud infrastructure, and deliver cloud services. This will be accomplished across the three major network domains: Nonsecure Internet Protocol Router Network (NIPRNET), which is for unclassified information

---

[27]Ibid., iv-v.

[28]Ibid., 1.

[29]Department of Defense Chief Information Officer, "Cloud Computing Strategy," July 2012, E-1.

only; Secure Internet Protocol Router Network (SIPRNET), which is for information classified as secret; and the Joint Worldwide Intelligence Communications System (JWICS), handling top secret information; as well as other joint and coalition network domains.[30]

These imperatives are echoed in strategies from the Chairman of the Joint Chiefs of Staff (CJCS). His recent "Capstone Concept for Joint Operations (CCJO): Joint Force 2020" highlights cloud-enabled command and control technologies as a primary implication of globally integrated operations.[31] This concept underscores the need for military networks to mature apace with the civilian sector, and the development of common digital tools for situational awareness. Coupled with the USCYBERCOM commander's realization of the need for a comprehensive view of the enterprise in order to defend it, consolidate it, and make it more efficient, these efforts have resulted in the Joint Information Environment concept.[32] A more recent CJCS white paper on the JIE emphasized that cloud computing is the critical technology behind the JIE, which "…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."[33]

As the next sections will explain, the JIE and Enterprise Email, through cloud computing technologies, will accomplish DoD consolidation efforts and achieve its goals. A monumental undertaking, the issues of performing these tasks across networks in garrison will prove to be

---

[30]Ibid., E-2 to E-3.

[31]Chairman of the Joint Chiefs of Staff, "Capstone Concept for Joint Operations (CCJO): Joint Force 2020," September 10, 2012, 9, . http://www.jfcom.mil/newslink/storyarchive/2009/CCJO_2009.pdf [accessed October 1, 2012].

[32]JIE Operations Sponsor Group, "Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS), January 25, 2013, 5.

[33]Chairman of the Joint Chiefs of Staff, "Joint Information Environment White Paper," January 22, 2013, 3.

more difficult when applied to tactical network. While these two cases show efforts on garrison networks to incorporate tactical networks into the enterprise, the next major section will show that issues remain which show that some separation between the two still exists.

IMPLEMENTATION IN GARRISON NETWORKS

In short, garrison networks provide voice, video, and data services over unclassified or classified network domains to the military's permanent installations – bases, posts, camps, and stations – in the Continental United States (CONUS) and abroad. These networks consist of a permanent, fiber optic cable backbone (with data bandwidth up to 100 MBps), linking buildings on an installation to centrally-managed server/router clusters, and those clusters to the GIG. The primary tasks of installation, operation, and maintenance of these networks on Army installations are primarily performed by civilians at all locations through local Network Enterprise Centers (NEC) and regional Network Operations and Security Centers (NOSC), which are subordinate to a military command structure.[34] At overseas bases, particularly in more established theaters such as Europe and South Korea, military leadership and NOSC oversight is provided by Theater Signal Commands and their subordinate Signal Brigades, with supporting Battalions responsible for larger regions and their subordinate companies comprising the NEC's stationed in smaller locations. CONUS-based networks are operated primarily by all-civilian NEC's with regional

[34]NEC's (formerly Director of Information Management (DOIM)) provide administrative control and install, operate, and maintain servers, routers, telephone switches, video teleconferencing equipment, etc. that serve units and activities at each location. See Headquarters, Department of the Army, *Army Regulation 25-2, Information Assurance*, (Washington, DC: October 2007), Chap. 3. NOSC's manage the network – maintaining constant situational awareness over every node, router, etc. that connect bases, and also have a cell that defends the network (monitoring and blocking viruses and cyber-attacks). See also *FM 6-02.43*, Chap. 1.

NOSC oversight, but the military leadership is provided by Signal Brigades that divide the country into two regions of responsibility (having no subordinate Battalions).

This section will examine two primary projects in support of DoD's consolidation efforts: the JIE as an emerging concept enabled by cloud computing, and the Army's ongoing implementation of Enterprise Email. These summaries will include analyses of potential benefits these efforts will provide to permanent, garrison networks, as well as issues that have been encountered.

The Joint Information Environment

Led by the Army's CIO/G-6, the JIE is the DoD's effort to consolidate IT infrastructure and accomplish the goals of improved and simplified cyber security, effectiveness, and efficiency. The recently approved "Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS)," provides this definition:

> The JIE is 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. JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).[35]

In meeting the goals outlined earlier, JIE shows a potential to be the long sought-after solution to the military's IT woes. The recent words of Lt. Gen. Rhett Hernandez, commander of the U.S. Army Cyber Command (ARCYBER), echo these themes and stress the importance of a comprehensive solution:

> Current doctrine recognizes that modern information technology makes cyberspace and the electromagnetic spectrum essential for human interaction including military

[35]JIE Operations CONOPS, 6.

> operations in a way that impacts the operational environment to make them both congested and contested during operations. …This reliance on networks in cyberspace to conduct traditional operations shows the importance of addressing the synergies between these two operational domains which requires unified land and cyber operations – a unified force with land and cyber forces under a single commander to conduct mission command and produce a combination of effects in both domains to achieve operational and tactical objectives.[36]

These comments indicate mission command systems and mission success are entirely reliant on the success of safe, effective cyber capabilities. The JIE is thus a holistic approach to achieving the DoD-CIO's consolidation goals to deliver a joint, interagency, intergovernmental, and multinational information sharing environment. Implementation will include an IaaS/Hybrid cloud computing construct as described above, but the JIE is really an "integrated compilation of programs, projects, and services" that forms a robust IT framework for network management, standardized capabilities, delivery of enterprise services, and enforcement of common architectural standards, as well as tactics, techniques, and procedures (TTPs).[37] The JIE will also encompass systems acquisitions processes. An iterative process, implementing the JIE as a solution will begin in the European theater with the U.S. European Command (USEUCOM) and U.S. Africa Command (USAFRICOM), with subsequent, incremental upgrades planned for the rest of the force.[38] This implementation will begin with garrison networks and extend to the tactical portion of LWN.

The JIE's cloud computing construct will be utilized in core data centers which will deliver enterprise services and data storage. These data centers will also be established in the

---

[36]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1."

[37]Chairman of the Joint Chiefs of Staff, "DoD Joint Information Environment (JIE) EXORD," memorandum dated December 5, 2012, 4.

[38]Chairman of the Joint Chiefs of Staff, "Joint Information Environment White Paper," January 22, 2013, 7.

network behind one centrally-managed security structure, supporting the goal of improving security posture.[39] On garrison networks, JIE will also address thorough common identity management, "hardware agnostic" solutions, and network bandwidth -- supporting the goal of improving effectiveness.[40] Server reduction and acquisition of updated technologies, supporting the goal of enabling efficiencies, are also key components of JIE. Some issues not yet fully addressed under JIE include physical security of network enclaves, and network permissions.

Until recently, many of the Army's installations each developed their own network infrastructure which was designed to meet region-specific requirements and was installed, operated, and maintained under slightly different standards than neighboring regions. Consequently, users would have one login identity (username and password) that worked at one installation, but would not work at another base in the same theater. Once Common Access Cards (CAC) became the standard for identity management and access control on NIPRNET computers across all theaters, there were still separate networks between regions within a given theater. Because Windows networks were separate at each post, before a person could possess a login identification at one post – even though all login accounts are centrally linked under Enterprise Email – he could not have a login identification on another post's network servers. Once this problem was solved within theaters, users could login at any post within a given theater by just using their CAC. However, the problem is not yet solved between theaters. A user stationed in Germany, for instance, cannot travel to a CONUS post on temporary duty and simply login on any computer at that post, unless NEC personnel create a guest account for him on the CONUS

[39]"JIE Operations CONOPS," 4-6.

[40]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1."

network. Through cloud computing, the JIE addresses this issue – not only at Army posts, but at other services' bases as well.[41]

A key conceptual goal of the JIE is IaaS or "hardware agnostic" solutions, with mobility as the main goal – basically, a user with a verified identity on the network can use almost any mobile device from a wider variety of devices to access services such as email, web portals, or documents developed in the office and stored in the cloud, from anywhere in the world with much more simplicity than is currently in place. Although this concept is relatively new in military use – with the possible exception of Blackberry devices being in use for a decade already – in seeking to solve these issues and provide these services, the military looks to current civilian business practices for potential techniques and procedures in providing the capability to use smartphones and tablets running either Windows, Apple, Android, or other operating systems. As the business world embraces increasingly capable and securable touch-screen devices, their employment as more than simply personal communication devices is becoming more widespread.

A simple example is that of the National Football League, which recently started using cloud technologies with iPads for its coaches and players to replace bulky, paper playbooks as well as for viewing game footage. As teams replace their internal wireless networks, they have also put policies into place to discourage misuse – such as $10,000 fines for Miami Dolphins players who download unapproved software or forget to bring their iPads to meetings. Customizable apps can show potential scenarios, and security – the most dominant concern – is addressed with the ability to remotely erase the devices in the case of loss, or if a player is

[41]"JIE Operations CONOPS," 7.

traded.[42] Additionally, durable devices can save on recurring printing costs. Some teams report spending as much as $100,000 annually on printing, roughly equal to enough of the latest, highest-priced iPads for the entire team and staff (around 120).[43] If those devices are replaced every three years, an estimated two-thirds costs savings will be realized. The JIE will translate similar features to "hardware agnostic" military applications, improving effectiveness and efficiency for commanders and their staffs, especially in garrison. For instance, junior leaders can use these devices to store and read technical and field manuals (more than mere playbooks), fill out and sign administrative forms, and read or send official email without being tied to an office.

Fiscal efficiencies are also being improved with the consolidation of servers across the Army. As of October 2012, the Army had closed some 61 data centers, and condensed about 7,000 IT maintenance contracts into one– potentially saving the government hundreds of millions of dollars over the next few years.[44] Another effort in 2012 was to purchase the routers, switches, and other network infrastructure upgrades to modernize some 30 installations, representing approximately 80% of the Army's entire installations. Under old acquisition contracts, the cost for accomplishing this task would have been in excess of $200 million. While partnering with IT industry allowed for open competition, the final bill was around $22 million, saving almost 90% of the original cost estimate.

---

[42]Joe Aimonetti, "The iPad has revolutionized the NFL," *CNET online*, July 18, 2012, http://reviews.cnet.com/8301-31747_7-57475063-243/the-ipad-has-revolutionized-the-nfl/ [accessed November 18, 2012].

[43]Ryan Faas, "Why Most NFL Teams Are Ditching Their Playbooks For IPads," *Cult of Mac*, September 5, 2012, http://www.cultofmac.com/188847/why-most-nfl-teams-are-ditching-their-playbooks-for-ipads-feature/ [accessed November 18, 2012].

[44]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1."

Amidst the potential of the JIE concepts, there will still be challenges in garrison network implementation. One of the areas not specifically addressed in the CONOPS or other documents is that of physical security of the network infrastructure – specifically, physical cables outside of military installations, as well as cloud server farms owned and operated by private companies. Many of the virtual circuits that DISA maintains are leased from private companies all over the world, and are carried by fiber optic networks that cross oceans as well as land masses in between countries and cities, and connect to military installations. These circuits often service all classifications of domains, virtually trunked together for transport and decrypted and separated at end points. Although it is nearly impossible to intercept or decrypt the transmissions through these cables (without the exact encryption device available, detecting intrusions of this type is instantaneous), the worldwide, physical network of fiber optic cables, particularly near military installations, is vulnerable to accidents or sabotage – both of which can cause severe interruptions in service. For instance, in March of 2008, during a severe storm a commercial ship was directed to wait for the weather to clear off the coast of Alexandria, Egypt. High seas and winds conspired to drag the ship's anchor across a bundle of fiber optic cables buried just beneath the Mediterranean Sea's floor, severing the cables. The particular bundle of fiber optic cables provided the bulk of global Internet service to the Middle East – and the ensuing outage, lasting over a week, caused the majority of U.S. forces in the region to switch to satellite-based services.[45] The difference was similar to comparing a water main pipe to a soda straw – and tens of thousands of U.S. service personnel were without vital internet services for several days. DISA network engineers were able to reroute network traffic over longer, more expensive circuit routes

[45]Camilla Hall, "Mediterranean Cables Cut, Disrupting Communications," *Bloomberg*, January 30, 2008, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWe706hsLNdY [accessed February 7, 2013].

through the Pacific Ocean, restoring service within a week. While fiber cuts are common, incidences of this magnitude are rare.[46] Nevertheless, this accident revealed an inherent susceptibility within otherwise permanent, garrison networks that could conceivably be reflected in cloud computing scenarios. As the JIE seeks to contract out cloud services, those companies could have similar vulnerabilities – and these are contingencies which should be covered when contracts are formed.

Another area not addressed is that of network permissions. In a typical garrison network, any touch labor is done by NEC personnel, not unit personnel. For instance, when a unit needs a new printer installed in an office, or a new arrival needs an email account created, the work must be done by someone who has the required certifications and access (network permissions within the Windows Active Directory servers). Certain levels of access grant more ability to perform more functions on the network. According to a January 2011 directive by the 7th Signal Command, which oversees all NEC's in CONUS, those clearly defined levels of permissions are only granted to NEC employees. Ostensibly, these strict requirements contribute to cyber security by limiting access to administrative functions on the network. However, a level of effectiveness is lost when units have to wait for work to be done. To alleviate these issues, some NEC's have developed relationships with individual units that allow certified soldiers to train with or work with NEC network administrators. While this has shown to increase effectiveness locally, the JIE should address the issue across the enterprise – but current plans do not specify how.

Given these promises and challenges, the Army has thus far led the way in developing the infrastructure to support JIE initiatives and an operational approach to reach the strategic consolidation goals of effectiveness, efficiency, and security. To those ends, the Army's CIO/G-6

---

[46]John Borland, "Analyzing the Internet Collapse," *ABC News*, February 5, 2008, http://abcnews.go.com/Technology/story?id=4244474&page=1 [accessed February 7, 2013].

has developed four lines of operation to build the JIE, while focusing on developing and delivering capabilities in the enterprise.[47] The first line of operation, build capacity, is meant to support global deployments, realistic training for all Army units, and access to information regardless of geographic location. The second line of operation, improve cyber security, includes developing the doctrine and TTP's necessary to operationalize the cyber domain, and the capability to identify and track all users and equipment. As noted above, this should include physical security considerations as well as network permissions. The third line of operation, provide network enterprise services to the tactical edge, will develop the capabilities to access the cloud from anywhere; share information with mission partners regardless of service, agency, etc.; and simplify the standard suite of IT services available (e.g., voice, video, data, mobile). As previously discussed, "hardware agnostic" mobility is the key goal of this line of operation. The fourth line of operation, enforce network standards, introduces the concept of Installation as a Docking Station (IAADS) – through the IaaS/Hybrid cloud construct, applications would allow units to train in garrison without their JNN network. This is already being accomplished on seven military installations, including Fort Bragg, North Carolina, where units' warfighting function applications are hosted in the cloud, and they can plug in and use their ABCS clients anywhere on the network. This has also been proven in forward areas such as Afghanistan.

The following diagram illustrates the conceptual end-state of the JIE, characterized by defendable and resilient architecture, federated and shared infrastructure, enterprise services, and identity and access management:

[47]U.S. Army Cyber Command (ARCYBER), "Cyberspace Operations Prevent, Shape and Win," Association of the United States Army 2012 conference slides, October 23, 2012, 15.

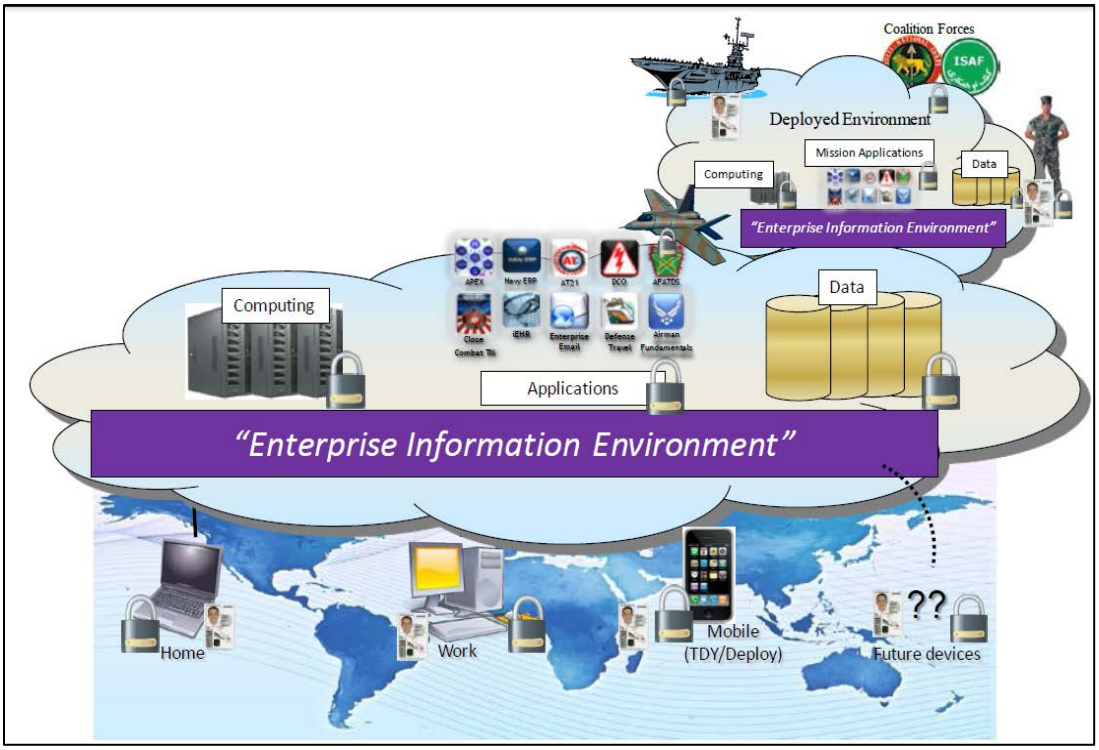

Figure 2. JIE Endstate.

Source: "JIE Operations CONOPS," 7.

In summary, cloud computing will enable the JIE to be more effective, efficient, and secure. JIE will ultimately provide a single identity for all users regardless of which classification domain, enable data access from anywhere, and minimize manning requirements to support units at the tactical edge. The next section will examine an ongoing, practical application of cloud computing technology and analyze its effects on effectiveness, efficiency, and security as well.

Enterprise Email

The first, earnest effort to utilize cloud computing technologies to consolidate IT infrastructure was DISA's Enterprise Email (EEmail) project, which began in early 2011 and is continuing as of this writing. EEmail was developed to consolidate the military's disparate email servers on the NIPRNET, create an all-encompassing Global Address List (GAL) that would

show all users, and ultimately save government money by eliminating redundant infrastructure and attendant personnel requirements. The first service to volunteer to transfer its email accounts was the Army, largely because of the efforts of the current CIO/G-6, and also because the Army has the most users at 1.4 million total on NIPRNET alone.[48]

This concept was developed from the Army's common operating environment (COE) strategy, which began in late 2010 and aims to standardize and streamline software development and delivery across the Army. The COE is being applied to five types of platforms to support the warfighter: enterprise servers, tactical servers, vehicles, desktop users, and handheld devices.[49] Because many NEC's have historically maintained their own email servers, email accounts became problematic and soldiers often have to maintain multiple email accounts across domains whether in garrison or deploying. For example, if a user stationed at Fort Sill, Oklahoma moved to Fort McPherson, Georgia, the Fort Sill NEC was required to delete the user's account before NEC personnel at Fort McPherson could create a new email account. By 2008, despite ongoing consolidation efforts at the time, the Army still had at least 18 unique networks with both NIPRNET and SIPRNET instances that caused unnecessary redundancy and high operation and maintenance costs. The confusion was compounded with Army Knowledge Online (AKO), which was developed as an information portal and provided a web-based email service in addition to the

[48]U.S. Army CIO/G-6, "Enterprise Email (EEmail)," November 10, 2011, http://ciog6.army.mil/ LinkClick.aspx?fileticket=Zx_lnaJnyLI%3d&tabid=122 [accessed November 1, 2012].

[49]Sorenson, "Welcome to the Enterprise," 178.

redundant services provided at installations around the globe. EEmail was designed to solve these issues as a cloud-based service, over an IaaS/Hybrid construct.[50]

By December 2011, after transferring approximately 300,000 users in the first several months of operation, EEmail planners were directed by Congress to pause upgrade operations, conduct a formal audit, and prepare a detailed report on their progress, which was submitted in February 2012. Original estimates showed that EEmail would save $100 million annually, but adjusted figures projected a total savings of $380 million over five years (FY 13 through FY 17). A previous, two-month pause in 2012 afforded the opportunity to improve network capacity, which increased the maximum number of migrations per business day to 7,000.[51] As the first cloud-based service to be implemented across the enterprise, EEmail planners also discovered that bandwidth was a particular issue that hindered efficiency and effectiveness. A careful analysis resulted in an upgrade plan to support EEmail across multiple installations, at a total cost increase of only $1.4 million for FY 2012, and a resulting increase of only $180,000 for FY 2013.[52] These network infrastructure upgrades were projected to be enough to support future JIE improvements. After resuming operations in March 2012, a total of some 600,000 users were migrated as of October 2012.[53] The report recalculates a base assumption of 1.6 million total

---

[50]Headquarters, Department of the Army, "Enterprise Email Army Service Acquisition: Report to Congress," February 1, 2012, 8, http://ciog6.army.mil/LinkClick.aspx?fileticket=tZ64mNUAWGk%3d&tabid=108 [accessed February 12, 2013].

[51]Ibid., 12.

[52]Ibid., 21.

[53]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1."

users, and also projects all Army email users to be migrated to EEmail by the end of March 2013.[54]

Another significant, unforeseen challenge posed by the EEmail migrations was how to address user identity management. One of the requirements of EEmail was that all users must authenticate on the network using their CAC; this certainly improved security by assigning each user a "persona" tied to a unique, 10-digit number associated with each CAC. However, emerging "dual-persona" identities were an unforeseen effect that caused a hindrance to effectiveness. As EEmail migrations began in early 2011, local NEC's discovered that many users worked as civilians (or contractors) and required regular access, but were also Reservists or had other reasons to have a second identity on the network. This problem was ultimately solved by providing alternate smart cards similar to the CAC, which then authenticated the user's secondary or tertiary identities.[55] Furthermore, for the more than 200,000 SIPRNET users that have already begun migration, EEmail utilizes additional, smart identity cards similar to CAC, and tied to the same 10-digit identification number on the user's original CAC.[56]

As the next section will show, implementing these changes on the tactical side of the enterprise will magnify these challenges, as well as reveal some that are unique to austere environments. Not every service is embracing these changes with enthusiasm. While the Air Force and Navy departments wait for the Army to work through challenges in implementing JIE and EEmail, the Marine Corps has publicly stated that it will maintain its own networks and email

---

[54]David Perera, "Army enterprise email migration saving estimates overblown," *Fierce Government IT*, April 4, 2012, http://www.fiercegovernmentit.com/story/army-enterprise-email-migration-saving-estimates-overblown/2012-04-04 [accessed January 24, 2012].

[55]"Enterprise Email Army Service Acquisition: Report to Congress," 12.

[56]Sorenson, "Welcome to the Enterprise," 180.

systems.[57] This may present future challenges to obtaining and maintaining the true joint nature of information sharing in the JIE. And as the EEmail program matures, the one topic yet to be addressed in any of the current plans is that of extending services to deployed users on a long-term basis. DISA is currently formulating plans to deploy cloud-managed EEmail servers to forward areas, but, as detailed below, bandwidth will still be an issue that may hinder effectiveness.

IMPLEMENTATION IN TACTICAL NETWORKS

The differences between garrison and tactical networks will potentially cause some unique issues when implementing the JIE. Tactical networks are temporary in nature, and are utilized by units from ASCC/Corps level and below when deploying to an austere environment, or one that does not yet have any sort of permanent network installed. As mentioned previously, when a warfighting unit either conducts field exercises or deploys, these networks are installed, operated, and maintained by JNN-enabled, Signal Corps units. In contrast to the units and agencies which are responsible for garrison networks, these units consist entirely of uniformed Soldiers. Some 210 Army BCT's and separate Brigades each are assigned one Signal Company, and most subordinate Battalion-sized units have a signal team equipped with a smaller Command Post Node (CPN) which will provide connectivity into the Brigade's or Division's networks. The tactical Signal Company works in close coordination with (and is typically under the tactical control of) the Brigade S-6, which operates and maintains its own BCSS.[58] Deployed theaters

---

[57]Rita Boland, "CIOs Argue Enterprise Email," *Signal Online*, May 9, 2012, http://www.afcea.org/content/?q=2012/05/09/17392 [accessed March 7, 2013].

[58]Tactical control (TACON): a command relationship where one entity has authority over assigned or attached forces limited to detailed direction necessary to accomplish specific missions or tasks. See *JP 1-02*, 351.

typically have a strategic NOSC-like entity set up early in enduring operations that may become somewhat permanent as in the case of Southwest Asia – for instance, the Cyber Center in Kuwait serves as NOSC for the region, and truly fuses offensive and defensive capabilities with its network management oversight as well.

For tactical networks, JIE will bring many of the same improvements over current and legacy systems and practices which have contributed to the overall issues in recent years. However, while JIE is touted as an enterprise-wide solution to meet DoD-CIO's consolidation goals, JIE does not address many issues that exist and are handled differently when units deploy. Among those issues are EEmail access, network permissions, and bandwidth. This section will examine some recent experimentation with efforts to standardize tactical networks deployed in southwest Asia, analyze their benefits in the light of these challenges, and in the case of NIE 13.1, show how more of the DoD-CIO's IT consolidation goals will be supported.

Global Network Enterprise Construct (GNEC)

The military has recognized the importance of consolidating its networks for several years. As a cloud-enabled program, the Global Network Enterprise Construct was the Army's first strategic effort to "transform LandWarNet to an enterprise activity."[59] Led by NETCOM, from 2009 to 2011 the Army conducted tactical network experiments with a couple of Brigades, using the GNEC concept to consolidate services for tactical users in deployable units using WIN-T (Increment 1) equipment.[60] The overarching goal of GNEC was to enable units to "fight on

[59]Headquarters, Department of the Army, "Global Network Enterprise Construct (GNEC): The Army's Strategic Vision for the Transformation of LandWarNet," July 10, 2010, 4.

[60] WIN-T Increment 1a, which provides network connectivity at-the-halt. See: General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," Version 1.6,

arrival," or have uninterrupted access to their mission data from the time they started training at home stations, continued through the first days of a mission deployment in a different theater. Other goals included universal email addresses and file storage for users, and standardized network tools for administrators. Under GNEC, individual theaters would have a permanent Network Service Center (NSC) consisting of the Theater NOSC (TNOSC), Fixed Regional Hub Node (FRHN), and an Area Processing Center (APC) that would provide services to units in austere environments through its satellite equipment.[61] While the unit was still in garrison, IT staff would connect their servers through their JNN via satellite to the FRHN; the unit's server data would be uploaded to the neighboring APC's servers – in reality, a copy of the unit's servers – then tested.[62] The unit would then ship their equipment and servers to the theater, leaving behind some laptops and allowing them to access their windows network and tactical email through the garrison network, so they could continue to work with units in theater. When the unit arrived in theater, it could access the data and services it needed directly through its JNN (without its Division TACHUB), in its forward staging area.[63] While the unit was moving to its final area

---

February 2011, 3, http://tactical-communicator.com/pdf/Commanders_Handbook_ v1.6.pdf [accessed March 10, 2013].

[61]An FRHN is a permanent satellite facility that provides backbone Defense Information Systems Network (DISN) services such as SIPRNET, NIPRNET, and Defense Switched Network (DSN, which is legacy phone services) to WIN-T enabled units. See General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 9.

[62]This data, up to several terabytes of information, comprises login accounts, email accounts and messages, administrative files, and vital mission application (i.e., ABCS) information that is generated daily on the unit's SIPRNET servers and computers it takes to the field.

[63]In the early versions of WIN-T Increment 1, every brigade in a division had to connect its JNN via satellite to a TACHUB to receive DISN services; Increment 1a and beyond enabled CPN's and JNN's to connect directly to a FRHN or the TACHUB, depending on the situation. See General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 5.

of operations, it could access the same data and services at the halt, within about an hour of initially setting up a CPN or JNN. Primarily, GNEC proved that through limited cloud applications, units could have a reliable backup system for its data; however, as analyzed below, some challenges remained in the areas of effectiveness and efficiency.

In terms of GNEC's viability, the OPVAL II exercise conducted with the 75th Fires Brigade, from Fort Sill, Oklahoma, showed promise. In April 2010, the Brigade TOC and staff deployed with its communications equipment to Grafenwoehr, Germany, to participate in OPVAL II and concurrently support Austere Challenge 10 (AC10), a joint and combined, command post exercise that simulated a Joint Task Force (JTF) headquarters, led by USEUCOM. For both events, the Brigade established its own WAN through its JNN and a CPN, and its local area network (LAN) connected ABCS systems to its Battle Command Common Services (BCCS) server suite.[64] Participating coalition partners communicated to the same, simulated JTF headquarters through a separate, secure coalition network. Because the Brigade TOC did not connect any of its ABCS systems on this network, it required the use of some systems provided by the exercise controllers.[65] Furthermore, network bandwidth was accessed via satellite from the FRHN located in Landstuhl, Germany.

The main goals of OPVAL II were to evaluate GNEC methods to provide deploying BCT's with: a single tactical identity for communications and access to network resources; the ability to collaborate with higher, adjacent, and subordinate units between theaters, through all phases of operations; and the capability to arrive in an austere operational area ready to

---

[64]BCCS provides a Windows-based logon network, email services, network defense services, and a database that connects all the unit's ABCS clients.

[65]Although this provided sufficient digital means to communicate with coalition partners, the JNN network can be modified to accommodate coalition circuits.

communicate and fight upon arrival. As such, a key achievement of OPVAL II was the discovery of and working through differing standards and configurations between the two CONUS and Europe TNOSC's. This exercise laid the groundwork for improving network effectiveness through JIE.

In OPVAL II, the Brigade learned it must operate its tactical systems on SIPRNET (or on a coalition network) in garrison, well in advance of a deployment. Exercise plans assumed the extensive use of tactical SIPRNET in garrison by the 75th Fires before deployment – in reality, the initial fielding of ABCS was accelerated to accommodate exercise goals. Connecting the Brigade's BCCS servers involved extensive coordination between the unit and the Fort Sill NEC, with direct NETCOM support to ensure that all the necessary accreditation paperwork was properly prepared so that the NEC could approve the required network connections. Once the unit's servers were accredited and connected, several network tests were conducted before deployment, to include: replicating BCCS server configuration data through the network to a forward APC located at Ft. Bragg, North Carolina; configuring identical, "virtual servers" at the forward APC using the Brigade's server data; turning off local servers; verifying SIPRNET services from the APC through the Fort Sill garrison network; turning off the APC servers; and turning local servers back on and verifying local services. Once this phase was successful, the entire process was repeated through the APC at Grafenwoehr, Germany. However, step six was eliminated in order to prepare the unit's servers and other systems for shipment to Germany. This resulted in a successful, remote connection to the Brigade's servers through the garrison network – albeit with significantly noticeable lag time, which can limit mission success. During transport, the Brigade successfully connected several of its ABCS systems in garrison, verifying SIPRNET services over the Tactical Battle Command (TBC)/Command Post of the Future (CPOF) systems to repositories that were now being hosted in the Grafenwoehr APC.

Most beneficially, OPVAL II validated a reliable data backup concept for BCT's. Known as Continuity of Operations (COOP), this essentially means that in the event of a catastrophic network interruption or failure, a copy of all the unit's files and server data could be restored with minimal loss, depending on how recently the backup occurred.[66] Units would ostensibly have to determine how often and when to backup their data, with the understanding that, as validated during OPVAL II, the backup process takes time and drastically reduces available bandwidth. In the clinical environment of OPVAL II, backups were conducted at night when network usage requirements were at an absolute minimum; times were eventually reduced to approximately two hours, with minimal data bring replicated. In an unpredictable, deployed environment, especially with a BCT otherwise decisively engaged, these backup procedures would be difficult to schedule in with any given unit's high operations tempo.

Despite this apparent benefit, another essential OPVAL II goal, providing a single network identity to users, achieved limited success. During AC 10, the Brigade successfully connected its ABCS systems through the JNN/CPN network over SIPRNET to the higher-level repositories at Grafenwoehr – thus, the unit did not have to re-image its computers – albeit, the exercise-specific configuration was not quite representative of a typical deployed network.[67] But since the exercise included coalition partners, much of the data passed was over a separate, secure coalition network. In order to preserve the JNN/CPN network's integrity to collect connectivity data for OPVAL II, the Brigade used externally-provided systems for its coalition traffic. Thus, users had to maintain three separate login accounts just for the classified networks. However, with the right additional equipment the tactical network can be modified to include coalition

---

[66]Department of the Army, *Army Regulation 500-3, U.S. Army Continuity of Operations Program Policy and Planning,* April 18, 2008, 7.

[67]"Network Service Center Operational Validation II: Final Reports and Findings," 10.

circuits, as long as the systems that are used on that network are properly prepared to operate on that domain.

After OPVAL II, the unit's BCCS servers were in operation in garrison to allow full-time connection to the SIPRNET without the JNN/CPN network connectivity. This theoretically allows garrison training on BCCS and ABCS, collaboration between staff and subordinate elements on the network, and development of classified products and briefings on the BCCS servers. An added benefit of this configuration is that BCCS servers and connected ABCS clients will receive software updates and security patches as they are published over the network, rather than catching up after an extended period of time. However, while this LAN is connected to the physical infrastructure of the unit's buildings, it is not connected to the Fort Sill NEC's SIPRNET servers, routers, or switches that serve its garrison SIPRNET customers. Rather, the SIPRNET services are fed through the GIG from an APC facility at Ft. Bragg, North Carolina. Consequently, none of the ABCS systems could be used in garrison, largely due to accreditation issues identified during OPVAL II.[68] Furthermore, when the Brigade's subordinate Battalions conducted field exercises away from Fort Sill, the unit's JNN was required to be set up in garrison to provide mission command system connectivity through the Battalions' CPN's. Few Army units conduct day-to-day business this way while in garrison, but future capabilities under development with JIE will enable every tactical unit to operate mission command applications on SIPRNET, full-time.

On the NIPRNET, some issues pointed to a need for help desk continuity between theaters. Users brought their laptop computers from their offices at Fort Sill, and could still use their CAC login to access the computers. However, since the email servers were located in

[68]Ibid., 23.

CONUS, on a different Windows login network, users were not able to use Microsoft Outlook as they did in their garrison offices, and had to rely on the internet-based Outlook Web Access. Consequently, the NSC help desk, established to support OPVAL II, could not provide support for these email issues. While JIE and EEmail will ultimately solve this particular problem, there were other, similar issues encountered (for instance, VTC connections and scheduling, Army Knowledge Online-SIPRNET (AKO-S) email, and specific ABCS system issues) – and if the unit had had a single point of contact to call for all its IT issues, much confusion could have been avoided.[69]

As some GNEC concepts have evolved into JIE, questions remain concerning satellite bandwidth, network permissions (touch labor), and EEmail. Despite some notable accomplishments, bandwidth proved to be a limiting factor. Using the fielded Battlefield Video Teleconferencing (BVTC) suite, the unit conducted several successful video teleconferencing sessions between its deployed TOC, the Fort Sill unit headquarters, and a subordinate battalion that was simultaneously conducting field exercises at Fort McCoy, Wisconsin.[70] Brigade TOC personnel were also able to establish critical, mission application links to the same unit, signifying the implications of controlling fires over extended distances, in much the same way CONUS-based UAV pilots control their aircraft overseas (a heretofore unrealized potential). The 75th Fires was the first unit to successfully deploy to another theater while its SIPRNET services were being hosted in a forward APC (during OPVAL I, the unit stayed at its home station).

The Increment 1 systems use the Ku-band of the frequency spectrum, which limits the available bandwidth on both the JNN (at 8 MBps, dedicated to the Brigade TOC) and CPN (at 5

---

[69]Ibid., 33.

[70]Ibid., 24-25.

MSps, shared between all CPN's on that circuit).[71] This bandwidth proved to be insufficient for COOP, and remote network connections to the deployed unit proved to be slow. When VTC's were being used, other network services had to be minimized in order to ensure VTC connectivity remained uninterrupted. Effectively, because satellite bandwidth is limited and expensive on the Ku-band, remotely hosting services with the current equipment (and essentially, removing all servers from the TOC's) would cause problems. Increasing bandwidth can be costly; effectively moving to a higher frequency spectrum may increase the amount and speed of information that can be transmitted. However, higher frequencies are more susceptible to atmospheric interference, especially larger amounts of dust (such as in desert environments) or severe weather. As many units can attest, while the weather at their field location might be clear, some services are interrupted when storm systems move on the FRHN that the unit's JNN and CPN's are connected to. When that occurs, a unit will lose satellite connectivity to the outside world temporarily, but during that outage will still have LAN connectivity to its subordinate units and have the ability to carry on its mission with ABCS, internal file sharing, and tactical email capabilities. However, if all of the unit's data services, mission applications, and email are consolidated and hosted in the virtual cloud, then the literal clouds can potentially compound already complex network issues. Essentially, removing a unit's network and data servers removes a layer of redundancy in their network – as well as decreasing access to services – and increases the potential for catastrophic failure when network outages occur.

The remaining GNEC questions directly relate to EEmail and customer service. While EEmail has improved the network identity issue in garrison networks, as noted above that program has yet to fully address access over tactical networks. Until the EEmail issues are solved,

---

[71]General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 9.

tactical users will still need to rely on their unit-owned email servers. The question of touch labor and network permissions will remain problematic in the field, as current systems are under the exclusive control of the soldiers who install, operate, and maintain them. Enterprise consolidation efforts across garrison networks have yet to determine who will be responsible for those duties in deployed units – i.e., whether forward-stationed DISA personnel will perform the touch labor in the TOC. If the Army is to continue to train its Soldiers on computer and server operation and maintenance, then utilizing those skills more effectively, and at a minimal cost, veritably mandates that those same soldiers have the ability to perform those tasks in the entire enterprise.

GNEC demonstrated that even with the limited connectivity and bulky servers provided by WIN-T Increment 1 equipment, tactical units could have reliable COOP capabilities and could, with the right preparation and training, enter the fight very soon after arriving in an austere theater without a mature network. This could significantly reduce a unit's idle time during preparations for a deployment, as well as during the first, critical days of a deployment – especially if the deployed environment is already actively hostile. Furthermore, some of the GNEC lessons learned developed into JIE concepts and goals – single network identity and access management, and effectiveness of information sharing are but two important examples demonstrated. As the Army moves forward into JIE, it is imperative that the lessons learned from GNEC are applied in the future. Ultimately, GNEC also showed that consolidation efforts evaluations must be viewed as a testing and delivery of data-centric capabilities, enabled by a robust but simple network. As the next section will show, WIN-T Increment 2 equipment is the next step in the evolution of tactical networks and consolidating the enterprise.

Network Integration Evaluation 13.1

Since 2011, the Army has taken a more holistic approach to modernizing tactical networks. Conducted at Fort Bliss, Texas, the Army Capabilities Integration Center's (ARCIC)

Network Integration Evaluation (NIE) exercises are designed to center on a designated BCT, the 2nd Brigade of the 1st Armored Division, to field and test the latest WIN-T equipment (Increment 2 fielding began in late 2012) as well as other portable computing devices for use at the tactical edge, and examine some of the challenges and benefits that the JIE will provide. [72]

WIN-T Increment 2 is a different approach from the previous JNN network model, in that it introduces a limited, wireless capability to a unit's LAN that will enable limited, on-the-move capability. Under previous WIN-T iterations, tactical units were tied to their TOC for most digital connectivity, although radio technologies have provided some limited success. The new capability set provides an ability for front-line units to report time-sensitive information (such as intelligence) back to the TOC through portable, wireless devices that are inexpensive and securable. Under this new program, the network will also be extended to the company level – previous iterations only provided connectivity to Battalion TOC's. New "self-healing" radio devices such as the AN/PRC-117G will automatically switch as needed between the frequency modulation, line-of-sight communications spectrum to satellite bandwidth, depending on the terrain. [73] Furthermore, Increment 2 (as well as Increment 1b, the interim upgrade) changes all satellite bandwidth to the Ka-band, meaning a maximum bandwidth of 30-40 MBps (more than ten times Increment 1 systems) will be available to each deployed unit – about the same as one can obtain commercially in a private residence in most American cities. The following diagram depicts the basic network using WIN-T Increment 2 equipment:

---

[72]Amy Walker, "Network serves as commander's eyes, ears," *The Bayonet*, January 9, 2013, A5.

[73]George I. Seffers, "Army Mobile Network Poised for Combat," *Signal*, July 2012, 25.

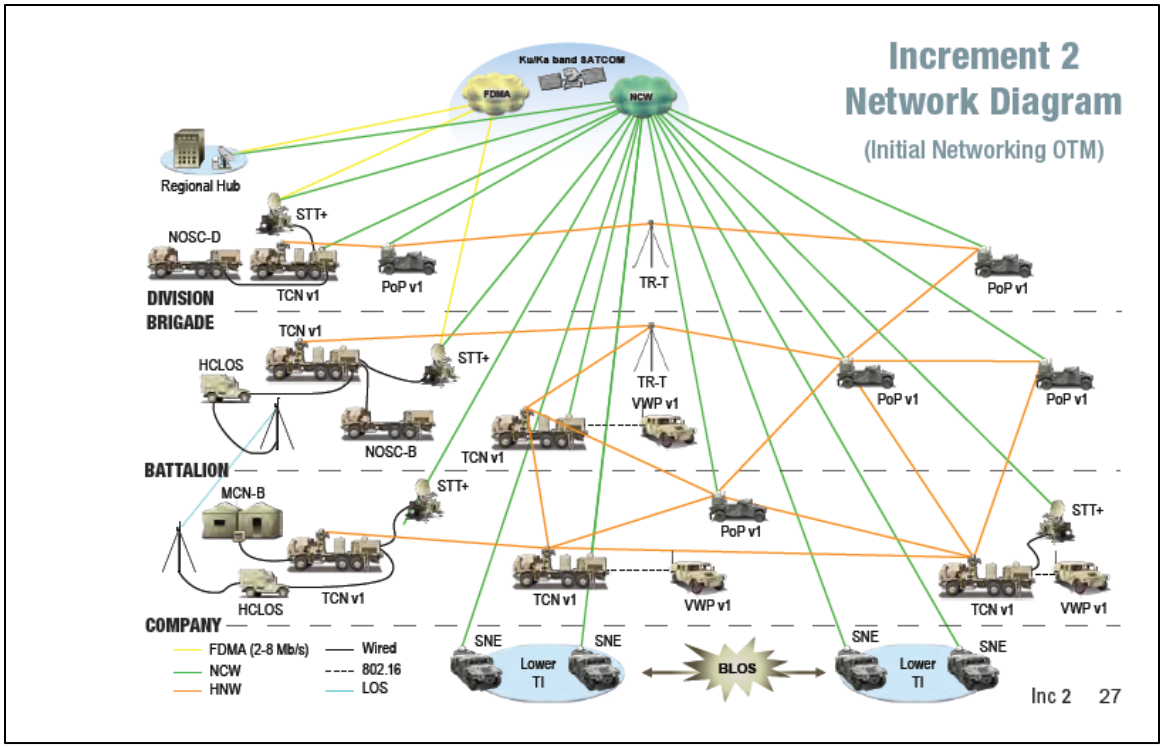

Figure 3. WIN-T Increment 2 Network Diagram.

Source: General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 27.

NIE 13.1 concluded in November 2012, and was the latest exercise to test WIN-T Increment 2 equipment. The exercise was intended to validate Capability Set 13 (CS 13), a fully-integrated package of modernized communications and computer equipment being fielded all at once to certain deploying units.[74] Besides the improvements in bandwidth, NIE and CS 13 focused on two key concepts: secure smart phone devices are fielded down to the soldier levels and integrated into the network, and commanders' vehicles are equipped with the necessary gear to connect into the new network on the move. In addition to the improved equipment, a paradigm shift of sorts has occurred in the way the Army procures and tests network equipment – instead of

[74]Seffers, 25.

developing systems and vehicles separately then delaying fielding of systems due to system redesigns, the vehicles are designed with the network in mind and both are tested and fielded together.[75]

NIE supports the Army's JIE initiatives, including cloud computing. The brigade's SIPRNET login, data, file management, and mission command application servers are located back in a garrison location, and accessed through the WIN-T network, which appears to operate effectively.[76] With the greatly improved network capabilities, commanders had the flexibility to move around the battlefield and have real-time access to the information they needed. Even company commanders worked more effectively by having the ability to remain with their units instead of traveling to higher headquarters to receive or plan for the next mission. Cloud computing also improved the COP, while subsequent JIE implementations should provide further improvements.

Certain network security management functions are handled at the enterprise level, decreasing the work load on the unit's IT staff.[77] However, the Brigade noted that this information assurance function is lost when the unit's network is disconnected from the cloud, thereby potentially degrading the unit's cyber security posture.[78] NIE 13.1 also does not appear to address certain lessons learned from GNEC – specifically, EEmail and single network identity goals. Although most of the unit's hundreds of network users ad their email accounts already migrated

---

[75]Ibid., 27.

[76]U.S. Army Capabilities Integration Center, "Brigade Modernization Command (BMC) Fiscal Year (FY) 2013 Network Integration Evaluation (NIE) Iteration One (NIE 13.1) Summary Report," December 18, 2012, 3.

[77]Specifically, the capability is the Host-Based Security System (HBSS) that was first tested during OPVAL II and subsequently fielded to BCT-level units.

[78]ARCIC, "NIE 13.1 Summary Report," 4.

to EEmail, the capability on NIPRNET is genuinely only available in their garrison offices, or over a new version of Outlook Web Access (OWA) that works very well when bandwidth is widely available in garrison or at home, but slows down considerably when used in the field and bandwidth management is a primary concern.[79] Bandwidth issues, another GNEC lesson, were greatly improved at the Brigade and Battalion levels but caused some problems at the company levels. Additionally, network redundancy, originally a concern of this research, is not an issue under WIN-T Increment 2. As Figure 3 above shows, the tactical side of the LAN is more robust. When satellite outages occur, the WIN-T Increment 2 LAN includes the same HCLOS connections as Increment 1, and adds a layer of wireless connectvitiy.[80] The recent NIE 13.1 summary report does not address single network identity issues, although it specifically mentions the need for identity and access management across the new, cloud based, mission command systems that were tested.[81]

Secure smart phones, tablets, and similar devices were tested at the soldier level with success, although unforeseen challenges such as frequency management did emerge.[82] While this capability is important at the tactical edge – inasmuch as secure smartphones, other devices, and applications are developed according to needs of warfighting forces – many of these devices should have a dual use or at least a dual-use feature that ensures the device can be easily used in any environment. If a secure device is used in the field, then it should be able to be used in garrison, on the garrison network. Similarly, applications should be designed with not only field

---

[79]OWA is a web-based email interface that is an integral part of Microsoft Office.

[80]General Dynamics, "Warfighter Information Network-Tactical Commander's Handbook," 27.

[81]Ibid., 8.

[82]Ibid.

requirements in mind, but potential uses in garrison as well – beginning with realistic training usage.

Other points noted in the report summary indicated the need for a veritable paradigm shift to occur in the military culture, specifically the way it operates within the networks, and how it educates its professional force. Units must first develop "Digital Standing Operating Procedures (DigSOP)," that take into account the increased complexity of these emerging technologies by emphasizing deliberate data management as well as information and knowledge management.[83] In effect, the designated staff officer who performs this mission would be using the IaaS service model to tailor the network to the unit's needs, thus approaching a KaaS model at the tactical edge. Commander and leaders must also be educated on these new technologies and procedures for employing them, starting with institutional leader training.[84]

While NIE 13.1 is another important evolutionary step in achieving the DoD-CIO's consolidation goals, future NIE iterations (currently conducted semi-annually) will hopefully address the unresolved issues that EEmail and GNEC presented. As the Army moves more toward a more robust, secure, effective and efficient JIE, planners and leaders should also take into account the necessary procedures in both garrison and tactical environments that will ensure these changes are enduring.

AN APPLIED SCENARIO

[83]Ibid., 5.

[84]Ibid., 8.

For most units in the Army, the vast majority of operations conducted in garrison offices is done on NIPRNET systems. And all too often, commanders and their staffs must still attend to that business while they are in the field. Tactical networks are primarily in the SIPRNET domain – hence, there is an obvious disparity between how the Army conducts business in each environment. A possible solution may be to move more daily, garrison operations to SIPRNET; a move of this kind would ensure far greater information security on the network, but would generate new requirements for more IT resources, not to mention increased clearance requirements. Perhaps some typically field-conducted operations – say, for instance, battle update briefs done over the network mission command applications – should be conducted in garrison the same way they are in the field.

Given the goals and challenges of applying cloud computing to military networks, one can consider a hypothetical scenario where these applications show their importance. Suppose a BCT deploys from CONUS to an austere theater. The brigade commander sends an advance, battalion-size task force to support the JTF, which is headquartered in the capital city of a remote country. Before the BCT's main body departs its home station, the forward battalion deploys initial, dismounted patrols in nearby villages to conduct an initial assessment of the situation, assist the host country's military in clearing insurgents, and begin to build relationships with the local populace. A small insurgent force engages an American platoon in a neighborhood several miles from the JTF's Forward Operating Base (FOB), and requests assistance. The current tactical situation might warrant changing the rest of the BCT's deployment schedule, and the commander's situational awareness and understanding are directly affected by the digital systems at his disposal.

With the current network infrastructure, mission command applications, and WIN-T Increment 1 equipment, the brigade commander in this scenario is essentially half-blind – almost all of his BCT's tactical network equipment is in transit, and he has no digital systems to maintain

his situational awareness and understanding. Late at night, he receives a call from his forward battalion commander (who has to call via an unclassified VoIP connected to his CPN, to a DSN operator at his home base, who must then transfer his call to the brigade commander's government-contracted cell phone) that an incident has happened, but details are in a classified email message. The brigade commander then has to travel to his office, log on to his SIPRNET computer (which is likely locked in a safe), and access the message over his AKO-S email account. If the commander's staff had withheld any secure laptop computers that are running current mission applications, they would be essentially useless – the JNN and CPN's necessary to connect them are in transit, likely at a port in or near the remote country awaiting the personnel to arrive and set up the tactical network. In this realistic situation, the commander's access to the common operational picture would be essentially limited to whatever PowerPoint graphics his forward-deployed elements can send to his AKO-S email account.

Under JIE, the commander's access to the common operational picture, not to mention his situational understanding, will significantly change. He would have a secure, wireless, touchpad computing device – likely maintained and operated in an interim operations center at his garrison headquarters – that would show him his forward units' locations, and instantly show him or his staff mission graphics, applications, and messages. Because the JIE is one network, the secure, mission command applications are hosted in the cloud and accessible through any device. At the tactical edge, the entry into the JIE is through WIN-T increment 2 equipment. The commander and his battalion commanders would also have secure smartphones with similar, scaled-down mission applications. These smartphones would connect to any network, and would be secured with the individual's SIPRNET smart identity card and a unique, personal code that he was issued by his local NEC. The forward battalion commander would simply use his smartphone to call the brigade commander, and could send him the information, photographs, or mission graphics the brigade commander needs to make an informed decision about how to next proceed.

The commanders could also conceivably use their touchpads to conduct an impromptu VTC to discuss the situation – and the BCT commander would use his same equipment to communicate with his division commander, whether before he deploys (as in this scenario), while he is in transit, or after he is on the ground.

DOCTRINAL IMPLICATIONS

The preceding sections shows that military applications of cloud computing will continue to improve effectiveness, efficiency, and security of the military's vital information networks. However, a cultural paradigm shift must occur for these efforts to reach their true potential. Part of this cultural shift includes understanding the JIE's relationship to the emerging concept of cyber. The recent revamping of Army doctrine leaves a noticeable gap: the absence of a comprehensive doctrine that defines and operationalizes cyberspace in ways understandable to professionals outside of the IT community. Though the holistic efforts of JIE, enabled by cloud computing, will meet the DoD's consolidation goals in the near future, there is currently no doctrine concerning its relationship to the concepts of cyber. This section presents an analysis of the recent, historical roots of cyber, and proposes a framework for understanding cyber as an additional warfighting domain – perhaps to be included in a future Army Doctrinal Publication.

Although there is not yet consensus in the military community concerning the efficacy of information technology as a *true* revolution in military affairs, there can be little doubt that automated information networks have revolutionized the conduct of war. Beginning with World War II, when miniaturization of circuitry enabled advantageous technologies such as precision munitions and wireless communications, more recent increases in networking technologies led to

greater lethality on the battlefield.[85] As the proliferation of computers and their connected networks in the military has paralleled that of society in general, the result is that modern commanders have unprecedented visibility, intelligence, and instantaneous communications capabilities across the entire spectrum of conflict from the highest generals down to the lowest riflemen. Inherently, there are some potential pitfalls in the application of this technology – namely, according to Martin van Creveld, if it is true that "...other things being equal, the simpler the environment in which war is waged the greater the advantages offered by high technology," then more complex combat environments tend to minimize those advantages.[86] Perhaps prophetically, Van Creveld further warns of the greater risk of over-reliance on electronic technology in a "guerrilla-type conflict" than in a conventional war – a valuable lesson learned in America's recent operations in Iraq and Afghanistan.[87] A truly unified network – enabled by cloud computing and employing devices and applications developed for field and garrison use – could mitigate that risk.

These risks are embodied in the concept of network-centric warfare (NCW), an idea theorized by Vice Admiral Arthur Cebrowski and summarized as the harnessing of network technologies in order to create an overwhelming advantage over an adversary on the battlefield by linking Global Positioning System (GPS)-enabled vehicles, weapons platforms, sensors such as Unmanned Aerial Systems, and commanders' staffs through a complex, integrated network. In the essence of the concept, the economic paradigm shifts wrought by rapid technological advances – somewhat ironically first developed by the DoD for military purposes – were echoed in a new

---

[85]Martin van Creveld, *Technology and War,* (New York, NY: Macmillan, Inc., 1991), 267-269.

[86]Ibid., 272.

[87]Ibid., 282.

model of fighting and winning wars.[88] By its very nature, NCW was touted as the American military's "killer app," or a new and dominant category of warfare that would net enormous profits on investment.[89] This idea of the killer app was introduced as a business strategy model in 1998 by Larry Downes and Chunka Mui, who astutely recognized that "...digital technology has become the most disruptive force in modern history."[90] Cebrowski and other NCW adherents declared that this disruptive force would create near-perfect intelligence, solve the problems of the fog and friction of war, and shift the ideal model of war from platforms to networks – thus ushering in the new RMA.[91] Having been supposedly validated by the overwhelming superiority of American forces against Iraq in Operation Desert Storm in 1991 as well as operations in the Balkans, NCW theorists generally agreed that new technologies would bring about quick, decisive victory in the next war and its adherents predicted low costs, casualties, and collateral damage resulting from pinpoint-accurate munitions delivered from anywhere in the world.

In the wake of Operation Iraqi Freedom and Operation Enduring Freedom, however, strategy commentators such as H.R. McMaster understand that NCW was based on flawed assumptions – specifically, "…that surveillance, communications, and information technologies would deliver 'dominant battlespace knowledge' and permit US forces to achieve 'full spectrum dominance' against any opponent mainly through the employment of precision-strike

---

[88]Arthur K. Cebrowski and John J. Gartska, "Network-Centric Warfare: Its Origin and Future," *Proceedings* 124, No.1, (January 1998), 139, http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future [accessed November 5, 2012].

[89]Larry Downes and Chunka Kui, *Unleashing the Killer App: Digital Strategies for Market Dominance* (Boston, MA: Harvard Business School Press, 1998), 4.

[90]Ibid., 21.

[91]P. W. Singer, *Wired for War* (New York, NY: Penguin Group, 2009), 185.

capabilities."[92] P. W. Singer argues that although the hype of NCW reached practically mythical proportions, it became evident that the focus on the network, rather than the platforms they enabled, was the most important error made in the application of NCW as a paradigm for warfare.[93] Other authors such as Andrew Bacevich similarly assert the prolonged conflicts demonstrated American over-reliance on technology as a gross detriment.[94] Perhaps these realizations inspired Gen. James Mattis, USMC, to propose a new paradigm for command and control. His idea of "command and feedback," a cybernetic approach that is enabled by networks rather than controlled by them, asserts that improper use of technology produces "digital dependence" and ultimately subverts the art of war.[95] NCW was ultimately ignored, having neither been codified in Army doctrine nor its field-grade officer education programs.

Consequently, the military continues to temper NCW's hysteria by adapting communications networks in an effort to provide an advantage over potential adversaries in the most efficient and effective ways possible – and as a result, has evolved the concept. In an attempt to dispel the myths of NCW, the emergent, conceptual model in doctrine is that of cyberspace – noted as a subset of information operations, it is the fifth domain of military

---

[92]H.R. McMaster, "On War: Lessons to be Learned," *Survival* 50, n.1 (February-March 2008), 21.

[93]P. W. Singer, *Wired for War*, 192-193.

[94]Andrew J. Bacevich, *Washington Rules* (New York, NY: Metropolitan Books, 2010), 160-167.

[95]James J. Mattis, "Military Needs New Operational Paradigm," *Signal*, October 2009, 64.

operations (after land, air, sea, and space).[96] But what is cyberspace? The Government Accountability Office (GAO) mirrors the broad, Joint definition:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[97]

Perhaps more succinctly, current Army doctrine defines the domain as an essential part of Unified Land Operations (ULO):

> *Cyber electromagnetic activities* are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.[98]

In a recent speech on cyber security, Lt. Gen. Susan Lawrence referred to an operational objective of "technological overmatch" in cyberspace.[99] If the concepts of cyberspace are operationalized so that warfighting commanders can understand its implications and utility on the battlefield beyond an enabling tool for mission command, cyber – as realized in the Joint Information Environment – could well be the killer app sought by the military.

Similarly, in a recent speech before students at Fort Leavenworth, Lt. Gen. David Perkins, Commander of the Combined Arms Center, emphasized that the Army's core competencies of combined arms maneuver (CAM) and wide area security (WAS) are

---

[96]Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0, Joint Operations*. (Washington, DC: 11 August 2011), xiv.

[97] United States Government Accountability Office (GAO), "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011, 8, http://cryptome.org/0004/gao-11-421.pdf [accessed January 31, 2013].

[98]*ADRP 6-0,* 3-6.

[99]U.S. Army Cyber Command, "Cyber Domain and LandWarNet, Part 1."

simultaneously conducted not only in the land domain but in the cyber domain as well, in order to gain a position of relative advantage over an adversary while denying relative advantage to that enemy. As a distinct domain, cyber is the milieu of the commander in the same respect as the land domain – effectively, the Signal Corps operates and defends the LWN as virtual lines of communication in the traditional sense (thereby rendering signaleers as digital logisticians), while the Military Intelligence Corps is the primary platform to conduct offensive operations on those networks.[100] This is a key principle in the current doctrine of mission command, and commanders must visualize "the Network" as a weapons system that connects and enhances human interaction networks to achieve military objectives. Understanding cyber in operational terms is imperative for modern commanders, who must synchronize employment of the network across warfighting functions and manage "bandwidth as a class of supply."[101]

Though currently not specified in military doctrine, USCYBERCOM's CONOPS outlines three lines of operations for the command: DoD GIG Operations (DGO); Defensive Cyber Operations (DCO); and Offensive Cyber Operations (OCO). DGO is a unified approach to engineering, operating and maintaining the JIE. DCO is essentially cybersecurity: it provides unity of command and unity of effort in detecting, analyzing, countering, or mitigating threats to DoD networks. OCO is basically the offensive capability of conducting cyber-attacks as part of a military mission, including hacking, intrusion, denial of service, and the various forms of electronic warfare.[102] Given this background, in order to understand the operational impacts of

---

[100]David Perkins, "Army Doctrine 2015," speech to SAMS students, November 28, 2012.

[101]Charles A. Flynn, Wayne W. Grigsby, and Jeff Witsken, "The Network in Military Operations," *Army,* May 2012.

[102]"US Cyber Command: Integrating Cyber Operations," (slide presentation) 6, http://www.afcea.org/smallbusiness/files/CommitteeMeetings/PODCAST_Cyber_Command_Brief_February_2011/USCC%20Brief_unclass_AFCEA.pdf [accessed January 31, 2013].

the JIE in the absence of a doctrinal definition, one must first understand cyber. This paper proposes that as an illustrative model, the three primary components of cyber – operating the network, defending the network, and conducting offensive operations on the network – comprise the "cyber triad" as represented by the following diagram:

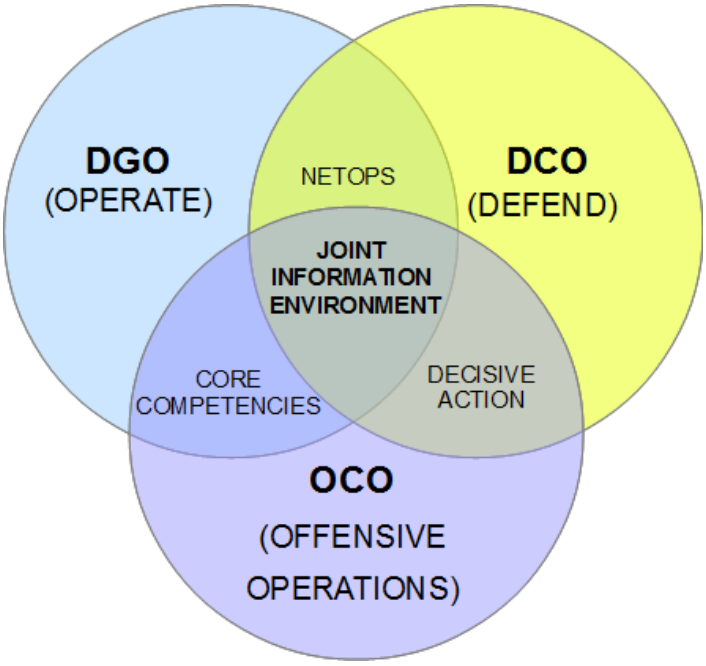

Figure 4. Cyber triad.

Source: Created by author.

According this model, where operating and defending the network intersect is the definition of network operations (NETOPS). According to *Joint Publication 6-0,* this essentially entails operating and managing networks as well as enforcing network standards.[103] Defending the network and conducting offensive operations on the network support ULO throughout offensive and defensive operations as well as stability and defense support to civil authority –

[103]*JP 6-0, Joint Communications System,* IV-1.

these define decisive action as an essential component of ULO.[104] Core competencies, summarized as the combination of CAM and WAS, effectively comprise the intersection of offensive capabilities of the network, combined with operating the network. The combination of all of these components is the essence of the Joint Information Environment. Although the concepts of how to apply ULO to the cyber domain are still being developed, particularly rules of engagement when it comes to cyber warfare itself, the development and defense of the network's infrastructure are crucial to future operations.

CONCLUSIONS

This research shows that the military applications of cloud computing technologies will have a positive overall impact on the military network by leveraging network and fiscal efficiencies, but some technical challenges on the network – such as security, bandwidth limitations, integrating emerging technologies on both sides of the network, and fully operationalizing doctrine – will remain. Viewed as an enterprise, network consolidation within JIE makes sense and saves money for garrison networks operating on a fiber optic backbone. When faced with the challenges of extending the network to austere environments, some concepts can work, but there are the unique difficulties that must be taken into account when implementing the JIE.

As shown by analysis of recent U.S. Army experiments, these challenges and others still exist. Securing networks "in the cloud" presents physical security limitations, while the bandwidth limitations will directly affect feasibility of hosting certain services in the cloud. Moreover, although an enterprise view blurs the distinction between garrison and tactical

---

[104]Army Doctrinal Publication 3-0, *Unified Land Operations*, 5-6.

networks, the infrastructure, applications, and devices developed for exclusive or primary use in one environment or the other continues to define that separation. While JIE can effectively remove the boundary, a cultural paradigm shift must occur that will solidify the security, effectiveness, and efficiency that consolidation efforts will achieve. Stewardship of public resources, cyber security, and effective sharing of information must be embedded with current operating doctrines across all military services, but that shift must start with command emphasis at every level, and effective education of all people who use any device connected to the network. Finally, the relation of cloud computing to cyber concepts, and including those concepts in doctrine, can assist commanders and their staffs to gain a more complete understanding of cyber as a fifth domain.

BIBLIOGRAPHY

"Army Battle Command Systems (ABCS)," http://www.dote.osd.mil/pub/reports/FY2005/pdf/army/2005abcs.pdf [accessed March 10, 2013].

"Build your business on Google Cloud Platform." https://cloud.google.com [accessed January 31, 2013].

"DoD Joint Information Environment (JIE) EXORD." Memorandum dated December 5, 2012.

"TAC-SWACAA 12-month Interim Contract." https://www.fbo.gov/notices/dde704d4b7746f68fb6ad1a2867ccf5c [accessed November 29, 2102].

"US Cyber Command: Integrating Cyber Operations." Slide presentation. http://www.afcea.org/smallbusiness/files/CommitteeMeetings/PODCAST_Cyber_Command_Brief_February_2011/USCC%20Brief_unclass_AFCEA.pdf [accessed January 31, 2013].

Aimonetti, Joe. "The iPad has revolutionized the NFL." *CNET online,* July 18, 2012. http://reviews.cnet.com/8301-31747_7-57475063-243/the-ipad-has-revolutionized-the-nfl/ [accessed November 18, 2012].

Bacevich, Andrew J. *Washington Rules*. New York, NY: Metropolitan Books, 2010.

Borland, John. "Analyzing the Internet Collapse." *ABC News,* February 5, 2008. http://abcnews.go.com/Technology/story?id=4244474&page=1 [accessed February 7, 2013].

Cebrowski, Arthur K., and Gartska, John J. "Network-Centric Warfare: Its Origin and Future." *Proceedings* 124, no.1 [January 1998,. http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future [accessed November 5, 2012].

Chairman of the Joint Chiefs of Staff. "Capstone Concept for Joint Operations (CCJO): Joint Force 2020." September 10, 2012. http://www.jfcom.mil/newslink/storyarchive/2009/CCJO_2009.pdf [accessed October 1, 2012].

Chairman of the Joint Chiefs of Staff. "Joint Information Environment White Paper." January 22, 2013.

Chairman of the Joint Chiefs of Staff. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: 15 August 2012.

Chairman of the Joint Chiefs of Staff. *Joint Publication 3-0, Joint Operations*. Washington, DC: 11 August 2011.

Chairman of the Joint Chiefs of Staff. *Joint Publication 6-0, Joint Communications System*. Washington, DC: 10 June 2010.

Department of Defense Chief Information Officer. “Cloud Computing Strategy.” July 2012. http://www.disa.mil/Services/~/media/Files/DISA/Services/Cloud-Broker/dod-cloud-strategy.pdf [accessed August 1, 2012].

Department of Defense Chief Information Officer. “Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap.” September 6, 2011. http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf [accessed September 30, 2012].

Dos Santos, Jamie and Singer, Jill. “Looking for the Right Answers in the Clouds.” Armed Forces Communications and Electronics Association, September 2012. http://www.afcea.org/committees/cyber/documents/LookingfortheRightAnswersintheCloudsWhitePaper.pdf [accessed October 15, 2012].

Downes, Larry and Kui, Chunka. *Unleashing the Killer App: Digital Strategies for Market Dominance*. Boston, MA: Harvard Business School Press, 1998.

Faas, Ryan. “Why Most NFL Teams Are Ditching Their Playbooks For IPads.” *Cult of Mac*, September 5, 2012. http://www.cultofmac.com/188847/why-most-nfl-teams-are-ditching-their-playbooks-for-ipads-feature/ [accessed November 18, 2012].

Flynn, Charles A., Grigsby, Wayne W., and Witsken, Jeff . “The Network in Military Operations.” *Army,* May 2012.

General Dynamics. “Warfighter Information Network-Tactical Commander’s Handbook.” Version 1.6, February 2011. http://tactical-communicator.com/pdf/Commanders_Handbook_v1.6.pdf [accessed March 10, 2013].

Hall, Camilla. “Mediterranean Cables Cut, Disrupting Communications.” *Bloomberg*, January 30, 2008. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWe706hsLNdY [accessed February 7, 2013].

Hardy, Quentin. “Active in Cloud, Amazon Reshapes Computing.” *The New York Times*, August 27, 2012. http://www.nytimes.com/2012/08/28/technology/active-in-cloud-amazon-reshapes-computing.html?emc=eta1 [accessed August 28, 2012].

Headquarters, Department of the Army. *Army Doctrinal Publication 3-0, Unified Land Operations.* Washington, DC: October 2011.

Headquarters, Department of the Army. *Army Doctrinal Reference Publication 6-0, Mission Command.* Washington, DC: May 2012.

Headquarters, Department of the Army, *Army Regulation 25-2, Information Assurance*, (Washington, DC: October 2007)Headquarters, Department of the Army. *Army Regulation 500-3, U.S. Army Continuity of Operations Program Policy and Planning* (Washington, DC: April 18, 2008).

Headquarters, Department of the Army. “Enterprise Email Army Service Acquisition: Report to Congress.” February 1, 2012. http://ciog6.army.mil/LinkClick.aspx?fileticket=tZ64mNUAWGk%3d&tabid=108 [accessed February 12, 2013].

Headquarters, Department of the Army. *Field Manual 6-02.71, Network Operations.* (Washington, DC: July 2009).

Headquarters, Department of the Army. *Field Manual 6-02.43, Signal Solder's Guide.* (Washington, DC: March 2009).

Headquarters, Department of the Army. “Global Network Enterprise Construct (GNEC): The Army’s Strategic Vision for the Transformation of LandWarNet.” memorandum of July 10, 2010.

JIE Operations Sponsor Group, “Joint Information Environment Operations Concept of Operations (JIE Operations CONOPS), January 25, 2013, 5.

Jonas, Jeff and Sokol, Lisa. “Data Finds Data,” in *Beautiful Data, The Stories Behind Elegant Data Solutions.* by Tony Segaran and Jeff Hammerbacher (USA: O’Reilly, 2009).

Kenyon, Henry. “Out With the Old, In with the New,” *Signal Magazine Online,* November 10, 2011, http://www.afcea.org/content/?q=2011/11/10/14575 [accessed December 4, 2012].

Knorr, Eric and Gruman, Galen. “What cloud computing really means.” *InfoWorld.* http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031, [accessed January 31, 2013].

Mattis, James J. “Military Needs New Operational Paradigm.” *Signal,* October 2009, 64.

McMaster, H.R. “On War: Lessons to be Learned.” *Survival* 50, no.1 (February-March 2008), 21.

Mell, Peter and Grace, Timothy. “The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology.” *NIST Special Publication 800-145,* September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [accessed October 1, 2012].

Nelson, John. “The Operational Impacts of the Global Network Enterprise Construct.” SAMS Monograph, May 2010. http://www.dtic.mil/dtic/tr/fulltext/u2/a523131.pdf [accessed June 25, 2012].

Obama, Barack H. State of the Union speech. February 7, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address [accessed February 13, 2013].

Office of the Secretary of Defense. *Report of the Defense Science Board Task Force on Cyber Security and Reliability in a Digital Cloud* (Washintgon, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013). http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf [accessed March 10, 2013].

Palmisano, Samuel J. and Dell, Michael Dell. “Washington can save $1 trillion.” *Politico*, October 6, 2010. http://www.politico.com/news/stories/1010/43188.html [accessed November 29, 2012].

Perera, David. “Army enterprise email migration saving estimates overblown.” *Fierce Government IT*, April 4, 2012. http://www.fiercegovernmentit.com/story/army-enterprise-email-migration-saving-estimates-overblown/2012-04-04 [accessed January 24, 2012].

Perkins, David. “Army Doctrine 2015.” speech to SAMS students, November 28, 2012.

Seffers, George I. “Army Mobile Network Poised for Combat.” *Signal*, July 2012.

Singer, P. W. *Wired for War.* New York, NY: Penguin Group, 2009.

Sorenson, Jeffrey A. “Welcome to the Enterprise.” *Army* 60, No. 10 [October 2010].

United States Government Accountability Office (GAO). “Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities.” May 2011. http://cryptome.org/0004/gao-11-421.pdf [accessed January 31, 2013].

U.S. Army Capabilities Integration Center. “Brigade Modernization Command (BMC) Fiscal Year (FY) 2013 Network Integration Evaluation (NIE) Iteration One (NIE 13.1) Summary Report.” December 18, 2012.

U.S. Army CIO/G-6. “Enterprise Email (EEmail).” November 10, 2011. http://ciog6.army.mil/LinkClick.aspx?fileticket=Zx_lnaJnyLI%3d&tabid=122 [accessed November 1, 2012].

U.S. Army Cyber Command. “Cyber Domain and LandWarNet, Part 1.” Digital video, October 23, 2012. http://www.dvidshub.net/video/159082/cyber-domain-and-landwarnet-part-1#.UREpp6V9LSg [accessed December 12, 2012].

U.S. Army Cyber Command. “Cyberspace Operations Prevent, Shape and Win.” Association of the United States Army 2012 conference slides, October 23, 2012. http://www.afcea.org/events/tnlf/east12/documents/CGbriefFINAL.pdf [accessed February 10, 2013].

van Creveld, Martin. *Technology and War.* New York, NY: Macmillan, Inc., 1991.

Walker, Amy. “Network serves as commander’s eyes, ears.” *The Bayonet*, January 9, 2013.

Welsh, William. “Network validation effort sets stage for Army’s upcoming NIE 13.1.” *Defense Systems*, October 4, 2012, http://defensesystems.com/articles/2012/10/04/army-validation-exercise-nie.aspx?admgarea=DS [accessed November 12, 2012].