WHY HAS THE US ARMY BEEN SLOW TO ADOPT MODERN HANDHELD TECHNOLOGY?

A Monograph

by

MAJ Justin T. Agostine
US 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

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

1. REPORT DATE *(DD-MM-YYYY)* 23-05-2013	**2. REPORT TYPE** SAMS Monograph	**3. DATES COVERED** *(From - To)* JUL 2012 – MAY 2013

4. TITLE AND SUBTITLE

WHY HAS THE US ARMY BEEN SLOW TO ADOPT MODERN HANDHELD TECHNOLOGY?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Justin T. Agostine

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

Despite the significant popularity of handheld devices in the civilian sector, the US Army has taken eight years to adopt handheld devices for field use. Why has the US Army been slow to adopt handheld devices? This monograph considers three possible explanations for the US Army's delay in adopting handheld devices. First, it is possible the handheld device architecture does not lend itself to practical military application. Secondly, the Department of Defense's need for secure communications may delay the assimilation of handheld technologies in field operations. Third, it is possible that the Department of Defense acquisitions process cannot evaluate and purchase handheld devices before an upgraded device replaces the technology. *Continued in Abstract.*

15. SUBJECT TERMS

US Army, handheld device, military application, security, field operations, acquisitions, smartphone, technology, network.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Justin Agostine
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UU	47	**19b. TELEPHONE NUMBER** *(include area code)* 209-401-7829

MONOGRAPH APPROVAL PAGE

Name of Candidate: MAJ Justin T. Agostine

Monograph Title: Why Has the US Army Been Slow to Adopt Modern Handheld Technology?

Approved by:

____, Monograph Director
William J. Gregor, Ph.D.

____, Seminar Leader
James E. Barren, 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

WHY HAS THE US ARMY BEEN SLOW TO ADOPT MODERN HANDHELD TECHNOLOGY?, by MAJ Justin T. Agostine, 43 pages.

Despite the significant popularity of handheld devices in the civilian sector, the US Army has taken eight years to adopt handheld devices for field use. Why has the US Army been slow to adopt handheld devices? This monograph considers three possible explanations for the US Army's delay in adopting handheld devices. First, it is possible the handheld device architecture does not lend itself to practical military application. Secondly, the Department of Defense's need for secure communications may delay the assimilation of handheld technologies in field operations. Third, it is possible that the Department of Defense acquisitions process cannot evaluate and purchase handheld devices before an upgraded device replaces the technology.

Data obtained from Army Field Manuals, white papers, informational briefs, institutional reports as well as statements made by senior Army and directorate leadership indicated not only an active interest in employing handheld devices but also a wide variety of applications suitable for military operations. Test results from the US Army Brigade Modernization Test Directorate and the Connecting Soldiers to Digital Applications made clear that meeting the security requirements was a significant challenge. However, technological advances and changes in network security methods will soon make possible secure communications using handheld devices. Analysis of the acquisitions process showed that it has been an obstacle to adoption of commercial handheld technology because the process usually cannot be completed before the technology had been updated or replaced.

The Army has a strong interest in handheld technology. The development of military applications has been slow but there are many promising applications. Concern for security did limit adoption of handheld technology for a time but advances in technology now make secure use of handheld devices possible. There are some efforts to define new procurement procedures to permit timely acquisition of handheld devices, but until those efforts bear fruit, the Army will remain slow to use those devices.

TABLE OF CONTENTS

ACRONYMS

SPOT	Situation, Position, Observation & Task

ILLUSTRATIONS

TABLES

INTRODUCTION

In 2005, the Personal Data Assistant became available for commercial purchase and use. The Personal Data Assistant sought to augment individual productivity and efficiency. Yet the Personal Data Assistant simply provided the foundation for the modern handheld device. In January 2007, the Apple Corporation released the iPhone and began handheld device popularization. Since then the Apple Corporation has sold over 84 million iPhones. Over one million applications are available for Apple devices alone. Companies such as Google and Microsoft have released handheld devices as well. The Google Corporation claims over 400 million Android based devices have been activated. Clearly, handheld devices have become globally popular.

Despite the popularity of handheld devices in the civilian sector, the US Army has taken eight years to adopt handheld devices for field use. Why has the US Army been slow to adopt handheld devices into field applications? Research revealed three possible explanations for the US Army's delay in adopting handheld devices. First, it is possible the handheld device architecture does not lend itself to practical military application. Secondly, the Department of Defense's need for secure communications coupled with strict security requirements may cause a delay in utilizing commercial off the shelf technologies in field operations. Third, it is possible that the Department of Defense acquisitions process cannot evaluate and purchase handheld devices before an upgraded device replaces the technology. Nevertheless, US Army leadership has stated an interest in handheld devices for military use and the US Army has introduced handheld devices into its inventory on a limited basis.

In efforts to exploit the smartphone phenomenon, the US Army issued Blackberry phones to senior leaders[1] and created an app-marketplace. The US Army has sought through its app-marketplace to expand the soldier's use of handheld technologies. However, searching the Apple Corporation's app-center using the term, "US Army" shows less than 20 apps created for, or by, the US Army. [2] Most US Army apps in Apple's search database offer references intended to help potential and Delayed Entry Plan recruits gain familiarity with the US Army. For example, one app quizzes a recruit on ranks by name and appearance. One app helps track Army Physical Fitness Plan scores as well as physical fitness training regimens for soldier and civilian alike. Another app offers popular quotes from well-known military leaders, such as General Patton or General Colin Powell. The most commonly downloaded app provides official US Army webpage access. The Army app-marketplace is clearly not a site of technological innovation. Innovation and experimentation is provided elsewhere. The Brigade Modernization Command located at Fort Bliss, TX conducts tactical field tests and develops security solutions for the US Army as it seeks to adopt popular handheld technologies for field use. Current US Army efforts, such as US Army app-center initiatives, reveal a desire to maximize modern technology. Yet field-units have not yet operationally utilized handheld devices.

If handheld devices offer operational applications, an impediment to handheld technology in the US Army may result from Department of Defense information technology requirements. Clearly, many US Army operations require secured communications. In response to that need, the Department of Defense created the Certificate of Networthiness. Manufacturers and developers must earn a Certificate of Networthiness before equipment or software may gain access to any

[1] Sandra I. Erwin, "Smartphones-for-soldiers Campaign Hits Wall as Army Experiences Growing Pains," *National Defense Magazine*, June 2011, http://www.nationaldefensemagazine.org/archive/2011/June/Pages/Smartphones-for-SoldiersCampaignHitsWallasArmyExperiencesGrowingPains.aspx (accessed December 20, 2012).

[2] Searches conducted on December 1, 2012 and January 1, 2013, respectively.

military network. The Certificate of Networthiness confirms that the software or device meets the standards of the security triad. Three elements comprise the security triad concept - confidentiality, integrity and accessibility. Confidentiality refers to an ability to prevent unauthorized disclosure. Integrity refers to the ability to operate independent of outside support when necessary. Accessibility refers to the ability to connect with the network in a secure medium. The certificate is both a precursor and an integral acquisitions process component. After a device earns the Certificate of Networthiness, it moves through the formalized acquisitions process before purchase and entry into the US Army equipment inventory.

The acquisitions process features four distinct phases. The acquisitions phases consist of concept and technology development, system development and demonstration, production and deployment, and the final phase is sustainment and disposal. The four phased acquisitions process is sequential. The Department of Defense acquisitions process is ideal for large and enduring equipment types, such as vehicles and weapons. Yet unlike weapons or vehicles, handheld devices are not readily upgraded or repaired. In addition, before acquiring handheld devices, the US Army must determine whether handheld devices will augment current US Army capabilities.

Research revealed that handheld devices do offer numerous field applications. Initial data in support of handheld applications came from senior US Army leaders. Senior US Army leaders stated their consistent belief in the military utility of handheld devices. Periodicals and statements from sister federal agency representatives provided data on successful and unsuccessful uses of handheld technology in the public sector. The US Army can use sister agency handheld device findings as blueprints for handheld application. Yet the most significant data came from field tests, white papers and briefings prepared by the US

Army Brigade Modernization Command. Brigade Modernization Command field tests prove military applications exist for handheld devices in field environments.

After investigating whether or not military applications exist for handheld devices, data revealed security restrictions are partially responsible for the US Army's delay in adopting handheld technology. Research revealed the security triad concept and the Certificate of Networthiness requirement present challenges for defense contractors. The research examined the LandWarNet network system. The US Army is currently developing that system in order to maximize communications and to overcome security restrictions. The data shows security restrictions are only partially responsible for the US Army's delay in adopting handheld technology.

After researching security requirements, the third research section investigated the four-phased acquisitions process and displayed how handheld devices fit into current acquisitions architecture. Commercial off the shelf devices have undergone testing against ruggedized devices in field environments. Handheld devices do not require ruggedization. Investigation into procurement processes revealed that military equipment types that are best served by the current acquisitions process do not resemble handheld devices, which is why current acquisitions procedures may not be ideal for modern handheld devices. US Army acquisitions publications reveal the acquisitions process favors larger, longer lasting equipment such as vehicles and equipment. After overcoming purchase restrictions through the new Agile Acquisitions initiative, handheld devices received appropriate purchase processes. Therefore, the traditional acquisitions process has been the primary factor in the US Army's delay in adopting handheld devices for field use.

The most current information determined the US Army has actively sought uses for handheld devices. Field-testing proves numerous applications exist for handheld devices in operational environments. Evidence revealed security requirements are only a minor obstacle and are responsible for only a fraction of the US Army's delay in adopting handheld devices. Security constraints have limited handheld devices to a reference tool and rudimentary public affairs medium. The major obstacle in the Army effort to exploit handheld devices is the acquisitions process. The acquisitions process is ill suited for rapid purchase of commercial off-the-shelf devices and cannot keep pace with commercial upgrades to handheld technology. Although field-testing proved handheld devices offer numerous practical applications in field environments, security requirements coupled with a traditional acquisitions process are delaying the adoption of handheld technology.

MILITARY APPLICATIONS

Since their introduction in 2007, Smartphones have found great acceptance in the commercial marketplace. In 2010, Lieutenant General Michael A. Vane, director of the Army Capabilities Integration Center, displayed great interest in smartphones for all soldiers. Lieutenant General Vane stated the US Army would issue smartphones to soldiers, "like any other piece of equipment." General Vane knows there are 1.3 million regular, reserve and National Guard soldiers in service. The simple math suggests purchasing a $200 smartphone for every soldier would cost over $2 billion. To mitigate this cost, Lieutenant General Vane considered an additional stipend for soldiers who might use their own smartphones for military purposes. The stipend option would allow soldiers to use their own smartphones thus, saving the US Army money. The smartphone stipend would offset the cost of data minutes and apps the soldier might purchase to accomplish his mission using his smartphone.[3] The consideration of a smartphone stipend displays the US Army belief in the utility of smartphones for field use. The stipend proposal also shows that the US Army is seriously seeking solutions to enable military use of smartphone capabilities.

The Army Learning Concept of 2015, states an interest in utilizing handheld technologies for training. The Army Learning Concept of 2015 states modern technologies offer unique capabilities for the US Army to utilize in the future. General Martin Dempsey, US Army Chief of Staff, writes:

> "The Army Learning Concept 2015 does not focus on any particular technology, but rather focuses on the opportunities presented by dynamic virtual environments, by on-line gaming, and by mobile learning. The Army Learning Concept of 2015 mentions how technologies can be used to blend physical and virtual collaborative environments as well as learning outcomes." [4]

Not only did General Dempsey visualize the potential uses for technology in training, Major General Steven Smith, Director of the US Army Cyber Directorate stated, "I have a dream, and the Army has this dream of operating in a mobile environment."[5] The statements by General Dempsey and Major General Smith show how US Army leadership see mobile technology playing a significant role in training and operations.

In 2010, the US Army began an initiative for adopting handheld devices, referred to as Connecting Soldiers to Digital Applications. The Connecting Soldiers to Digital Applications initiative coordinates with the US Army test directorate. The Connecting Soldiers to Digital Applications initiative grew from statements by Major General Smith and

[3] Gary Mortimer, "Army Sees Smartphones Playing an Important Role," sUAS News, December 2010, http://www.suasnews.com/2010/12/3004/army-sees-smart-phones-playing-important-role/ (accessed December 22, 2012).

[4] Department of the Army, TRADOC PAM 525-8-2: *The US Army Learning Concept for 2015*, 20 January 2011, i.

[5] Joe Gould and Lauren Biron, "Security Concerns Hobble US Army's Mobile Learning," Defense News, http://www.defensenews.com/article/20120620/TSJ01/306200004/Security-Concerns-Hobble-U-S-Army-8217-s-Mobile-Learning (accessed September 18, 2012).

General Dempsey. Since the release of the 2011 US Army Learning Concept, Connecting Soldiers to Digital applications allowed for explicit experimentation and funding for mobile devices. The US Army Test Directorate is located at Fort Bliss, Texas and White Sands Missile Range in New Mexico and acts as the proponent for handheld device field-testing. Mike McCarthy, mission command deputy at Fort Bliss' Future Force Integration Directorate stated, "We're looking at everything from iPads to Kindles to Nook readers to mini-projectors."[6] Mike McCarthy's statement highlights US Army efforts to adopt current commercial technologies for military use. It is evident that the US Army not only wants to use handheld devices, the Army has conducted tests to determine if handheld devices are truly feasible for military use.

The US Army has put great time and effort into determining if military applications exist for smartphones. As of January 2013, White Sands Missile Range has hosted three Network Integration Exercises. The fourth Network Evaluation Exercise will begin in summer 2014. As an example of how seriously the US Army is taking mobile device testing, the 2011 Network Integration Exercise cost the US Army over 60 million dollars.[7] Results from the 2011 Network Integration Exercise will assist in making equipment and determining tactics, techniques and procedures, TTP, decisions for 2nd Brigade, 1st Armored Division's 2013 deployment to Afghanistan. The US Army found handheld devices significantly augment the commander's ability to locate soldiers on the battlefield. Colonel Daniel Pinnell, 2nd Brigade, 1st Armored Division Commander, states, "Before this point I had to grab a hand

[6] Mortimer, "Army Sees Smartphones Playing Important Role"

[7] "Battlefield Smartphones Receive a Ringing Endorsement," Army-Technology, http://www.army-technology.com/features/featurebattlefield-smartphones-endorsement-technology (accessed September 30, 2012).

mic and ask 30 people to describe to me as best they can on what piece of dirt they're on and what condition they're in".[8] With a smartphone, soldier and unit locations are automatically updated and available. The ability to update soldier and troop locations is money well spent as it allows the commander to make better decisions in less time.

Field-testing also confirms the utility of handheld device applications in military operations. At the US Army's White Sands Missile Range in New Mexico, soldiers test commercial handheld devices. The tests, named Network Integration Exercises, test emerging technologies.[9] The 2011 Network Integration Exercise demonstrated smartphones can definitively improve the situational awareness of a commander on the battlefield. Colonel Daniel Pinnell, Commander of the 2nd Brigade of the 1st Armored Division noted a 40% increase in situational awareness. Colonel Pinnell noted a 40% increase in SPOT Reports.[10] Furthermore, SPOT reports were even more useful because the smartphone gave the soldiers a simple means to send a photograph or video, along with the report. The smartphones camera is a standard part of its design and fit well with military requirements. Meanwhile, contractors realized smartphones possess untapped capabilities.[11]

The smartphones potential to augment command and control capabilities caught the attention of defense contractors. The 2011 Network Evaluation Exercise tested apps that

[8] Ibid.

[9] "Inspecting Gadgets," AUSA, Association of the United States Army, http://www.ausa.org/publications/ausanews/specialreports/2011/8/Pages/Inspectinggadgets.aspx (accessed January 05, 2013).

[10] A SPOT report is a basic field intelligence report. SPOT stands for, situation, position, observation and task. Any soldier can submit a SPOT report and commanders use them to assist in gaining timely information on the location of enemy movements in specified location.

[11] "Smart Phones - and Their Apps - Go to War," Defense Systems, http://defensesystems.com/microsites/2012/snapshot-c4isr/02-smartphones-apps-for-soldiers-warfighters.aspx (accessed January 03, 2013).

allowed soldiers to report real-time data to their commanders. Another app allowed commanders to send secure messages to soldiers, thereby decreasing response times. Northrop Grumman developed a handheld device that provides text messaging, email and a full-color tracking display. Clearly, defense contractors sought to enter the military market for the handheld devices before the US Army became attached to commercial handheld devices. Furthermore, the Raytheon Corporation sought to develop secure messaging apps. These rudimentary apps demonstrate US Army efforts to utilize smartphones as well as the efforts of defense contractors to help fill the void.

The US Army is not the only government agency striving to adopt handheld mobile devices. The National Nuclear Security Administrations' 2012 Global Threat Reduction Initiative developed a project management app. The program management app can operate with any handheld device operating system. The National Nuclear Security Administration used the Global Threat Reduction Initiative app to augment their project management system. The Global Threat Reduction Initiative app augments project management information systems by giving National Nuclear Security Administration program managers the ability to manage projects and radiological materials from any location. The Global Threat Reduction Initiative app accomplishes its mission by filtering real-time, geo-spatially-linked information while integrating it "with scope, schedule, and cost and infrastructure information."[12] Not only has the Global Threat Reduction Initiative app allowed key managers to work away from their desk, it allows the National Nuclear Security Administration employees to safely increase their personal productivity.

[12] NNSA Office of Public Affairs, "NNSA's Global Threat Reduction Initiative Launches Mobile App," National Nuclear Security Agency, Office of Public Affairs, http://nnsa.energy.gov/blog/nnsa%E2%80%99s-global-threat-reduction-initiative-launches-mobile-app (accessed December 15, 2012).

Other federal agencies realize the benefits handheld devices offer. The Department of Homeland Security has sought commercial contracts in efforts to increase their productivity. On November 26, 2012, the Homeland Security Department's Customs and Border Patrol Agency announced it was seeking smart-phone accessories for Customs and Border Patrol officers.[13] The Customs and Border Patrol seeks smartphone accessories will enable its officers to easily scan documents and biometric data and send the data to a real-time database server. The database would then respond to the Customs and Border Patrol officer with data, helping the officer decide whether an individual or vehicle in question requires further searching. A military checkpoint operation is a similar common military mission The deployed US Army soldier would scan biometric data on a handheld device and receive near instantaneous feedback on a foreign national' criminal status. The Customs and Border Patrol Agency has also considered the handheld device shortcomings. The Custom and Border Patrol's request for information also specifies power consumption standards. Power consumption is a concern as a result Customs and Border Patrol officers have a steady and demanding workload and must minimize returning a mobile device to a charging or battery changing station when battery power runs low. The US Army can learn from the Border Patrol Agency's real-time database feed when developing handheld applications.

While similar to other large federal agencies, the US Army cannot always consider inter-agency actions and motivations as similar to its own. The US Army's mission is not motivated by profit. The General Services Administration, for example, shut down its apps.gov website when it found it primary users utilized the site as a price checking resource

[13] US Customs and Border Protection Targeting and Analysis Systems Program Office, Procurement Directorate, Request for Information regarding Smartphone Scanning Peripheral Devices, Washington, District of Columbia, dated November 26, 2012.

to guide personal purchases, and not for buying government merchandise.[14] From its inception in 2009 until its shut down in 2012, the General Services Administration did not realize how its apps.gov center was counterproductive. This example highlights how the US Army must remember its particular mission does not always find comparability in the federal sector when operating in the digital realm.

In addition to the smartphones commercial popularity and the US Army's desire to utilize the smartphone trend, the smartphone must show it can augment core US Army capabilities. The 2011 US Army's Strategic Planning Guidance states it will retain a technological edge by aligning new product delivery.[15] In response, the US Army sought ways that the handheld device market could augment its operational efficiency. In effect, the US Army has established an app marketplace, providing a basic, yet not popular capability. [16] The Army app marketplace is currently an empty distribution capability pipeline. Investigating existing smartphone apps with US Army needs in mind indicated that Army requirements could be met through the adoption of smartphone technology.

Examination of Army doctrinal releases reveal how US Army doctrine aligns with marketplace studies. Comparing marketplace studies with US Army doctrine helped to determine if military exploitation is feasible. One study found the most common uses for handheld devices are the internet, social media, listening to music, playing games, making

[14] Matthew Weigelt, "After 3 Years, Apps.gov to Go Dark," *Federal Computer Weekly*, http://fcw.com/articles/2012/11/30/goodbye-apps.gov.aspx (accessed December 15, 2013).

[15] HQs, Department of the Army, *US Army Strategic Planning Guidance of 2011. (*Washington, DC: Government Printing Office, 2011).

[16] Chief Information Office / G-6, US Army, "Introducing Us Army Apps Marketplace," Architecture Community, http://architecture.army.mil/technical-view/applications/applications.html (accessed September 30, 2012).

phone calls, email messaging and texting. [17] Conversely, the US Army states the two core competencies it must accomplish are, combined arms maneuver and wide area security.[18] The US Army sub- divides the two core competencies into seven enabling competencies. Thus, the core US Army Competencies can be compared with the most common smartphone uses and if the common smartphone uses meet the Army's needs then smartphones potentially offer strategic benefit to the military.

Table 1 Most Common Civilian Uses for Smartphones

Most Common Civilian Uses for Smartphones
Internet
Social Media
Music
Games
Phone Calls
Emails
Texts
Pictures

Table 2 US Army Enabling Competencies

US Army Enabling Competencies
Support security cooperation
Tailor forces for the combatant commander
Conduct entry operations
Provide flexible mission command
Support joint and US Army forces
Support domestic civil authorities
Mobilize and integrate the Reserve Components

[17] Chris Smith, "Making Calls Fifth Most Popular Use for Smartphones," Tech Radar, http://www.techradar.com/news/phone-and-communications/mobile-phones/making-calls-fifth-most-popular-use-for-smartphones-says-report-1087623 (accessed December 14, 2012).

[18] Army Doctrinal Publication 1, page 3-4, defines combined arms maneuver (CAM) as the ability to, "find, fix, close with, and destroy enemy forces on land and then exploit opportunities created by the enemy's defeat." Wide Area Security (WAS) is, "the ability of land power to secure and control populations, resources, and terrain within a joint operational area.

The following simplified descriptions of the most popular uses of smart phone technology revealed information sharing and communications are key uses for the smartphone. After categorizing software by function, it was possible to understand how the US Army might convert current software technologies for its own use. Yet first, the top civilian smartphones uses need to be described in functional terms. The descriptions are as follows; communications functions such as social media, music recordings, emails, texts and pictures are one-way communiqués and phone calls are two-way communications exchanges. Data access characterizes internet use. Commercial games utilize modeling software.[19] Consequently, the four broad descriptions applied to US Army enabling competencies are, one-way communications, two-way communications, data access and modeling capability. These descriptions are further consolidated into three categories, communications, data storage and retrieval and modeling. All seven US Army enabling competencies utilize communications. Yet the mission command competency would most benefit from the communications applications handheld devices offer. In practice, smart phones assume a role in the mission command system as a mission command enabler.[20] Therefore, if the US Army adopted smart phone technology, it would substantially augment mission command capabilities. The US Army has adopted the use of one and two-way communications formats such as email, texting, photos and social media. Most communications in the US Army occur though telephonic voice and email methods. Comparing US Army doctrine to commercial smartphone-usage studies reveal smart phones offering notable benefits to mission command capabilities. Mission command capabilities would increase due to the speed and increased communications that smartphones provide.

[19] Games operate software which apply operator input against algorhythms and display modeled imagery.

[20] Department of the Army, *Army Doctrine Publication: 6-0: Mission Command*, Washington D.C.: US Government Printing Office, may 2012, iv.

Handheld technology also offers *unexploited* data access capability that might substantially increase US Army efficiency and save money. Currently, the US Army issues at least one government owned personal computer to its leaders. The US Army has also made efforts to expand its share-drive capability. The share-drive is a storage device, typified by its ability to deliver data to a remotely located computer. Remote accessing usually occurs through a local network as though the data was located on the user's computer. Share-drive resources exist on US Army installations such as Fort Hood. Fort Hood's Network Enterprise Center encourages digital storage services for all units. Fort Hood's policies and procedures are common and enable subordinate units to establish and utilize share-drive services.[21] Ergo, handheld technology adds data access capabilities to a leader when away from his desk. The ability to work away from a desk would allow leaders to increase their productivity.

The Presidents Security Telecommunications Advisory Committee Report of May 2012 offers evidence of the newly burgeoning shift toward cloud data service.[22] The President's National Security Telecommunications Advisory Committee report offers a 240-page security controls appendix for government agencies to consider as they shift toward cloud data storage. The extensive nature of the security appendix shows reveals the federal government acknowledging the reality of mobile computing as a permanent reality. However, the onerous delays created by security requirements, act as obstacles to the US Army's implementation of handheld devices.

Colonel Chris Miller, the Director of the US Army's Data Consolidation Center provides statements regarding US Army data consolidation efforts. Colonel Miller states how the US Army

[21] Fort Hood NEC, "SAN Storage Services," Fort Hood Network Enterprise Center, http://www.hood.army.mil/NEC/EnterpriseServices/SANStorageServices.aspx (accessed December 15, 2012).

[22] US National Telecommunications Security Advisory Committee, *NSTAC Report to the President on Cloud Computing*, Washington, DC: Government Printing Office, 2012.

seeks to eliminate duplication through modernization. The US Army has identified over 500 data centers. The prior definition of the term data center was "a facility with 300 square feet or larger devoted to data processing." However, a data center is currently defined "as a closet, room, floor or building for the storage, management and dissemination of data and information." In other words, a data center used to mean a sizeable and dedicated facility dedicated to digital data storage and dissemination. Yet given the advances and reliance on digital data dissemination, a data center can exist in a single server. For reference, a typical server weighs less than 25 pounds and fits in a 24x24x6" rack space. Clearly, servers have become more numerous than in the past, and the US Army has realized it must consolidate servers in order to gain data control and cut the costs of server management. Colonel Miller observed there are over 500 Army data centers in operation and the US Army prefers to downsize and utilize approximately 185 data centers. Colonel Miller states the challenge the US Army Data Consolidation Center faces does not appear to be technical, but rather one of "culture and politics." He appears to lament the eight-year process as unnecessarily long. Data consolidation should be a "forklift operation," hampered only by logistics and movement constraints. Yet the process of consolidating data centers began in 2003, prior to the 2010 Federal Data Center Consolidation Initiative. After eight years, the US Army's data consolidation goal was only 37%, 185 of 500, complete. The logistical challenges the Data Center Consolidation Initiative faces are not atypical of the Department of Defense 'efforts to modernize its technological infrastructure. Handheld devices have proven operational merits, yet security requirements receive much more attention than the data centers, which enable the military cyber domain.[23]

[23] Rutrell Yasin, "Army Sees Big Savings in Application Modernization." *Government Computer News*, June 20, 2012, http://gcn.com/Articles/2012/06/20/Army-Data-Center-Consolidation-Application-Savings.aspx?sc_lang=en&p=1, (accessed September 20, 2013).

SECURITY

The US Army makes extensive use of computers. All computers, hardware and software must satisfy security requirements before gaining access to the military domain. The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security. The CIA triad is often referred to as the security triad. The security triad provides concepts that military and commercial programmers and managers must consider when developing hardware and software applications for sale to the US Army. The first element of the security triad is confidentiality. Confidentiality is the ability to prevent the unauthorized disclosure of information. The second security triad concept is integrity. Here, integrity means that the device possesses the ability to operate independently. The third concept in the security triad is accessibility. A handheld device is accessible when it can connect to data centers, or other devices. The greatest asset of the handheld device is its accessibility.

The handheld device is ubiquitous in the civilian sector because of its ability to access information. Yet the need to protect classified information creates a challenge for handheld devices in military operations. The security requirements diminish the operating advantage of handheld devices. Research reveals internet access and social media are the top uses for handheld devices. The US Army is no different in how its users access the internet and social media. A cell phone data access plan is required for any US Army user who is required to use the internet for referencing information or accessing social media. The US Army must consider how it will satisfy confidentiality, integrity and accessibility requirements as it implements smartphones into operations.

Connecting soldiers to the military network is a significant obstacle. Although making a digital connection is simple, retaining confidentiality adds complexity. In order to minimize reliance on the commercial cellular network and increase confidentiality, the US Army sought to build network access capabilities into brigade equipment sets. A brigade network capability would reduce the network vulnerabilities inherent to the commercial internet. Field tests reveal found brigade network sets can provide confidential network access. The mobile internet-protocol capability that will allow brigade command teams to communicate in austere environments is the WIN-T Increment 2. The previous version, WIN-T Increment 1 was a stationary network and did not allow the brigade command team to communicate more than one command level below itself. However, most tactical engagements take place at the company level. WIN-T Increment 1 did not allow company level commanders to communicate with each other or to communicate up their chain of command. A WIN-T Increment 2 addresses company-level communication oversights and allows peer-to-peer communications in the existing voice radio systems. If handheld devices gain access to the WIN-T Increment 2 system, the handheld device would then connect the soldier to the digital network. The WIN-T Increment 2 system will also improve the commander’s situational awareness.

WIN-T Increment-2 can also assist leaders in preventing fratricide. A company commander may use his or her device and its app would securely reveal a soldier’s geo-location. Automatic geo-location services would greatly assist in preventing fratricide. Soldiers could also forward short text-messages or photographs to their intelligence sections, thereby supplying real-time updates on friendly or enemy actions and whereabouts. Brigadier General Dan Hughes of the Systems Integration Directorate, states the WIN-T Increment 2 could, “change how small-unit tactics are executed.” Although impressive in its potential scope, WIN-T Increment 2 access for handheld devices is not yet a military reality. Given the progress and testing underway, it appears likely. [24]

As the US Army prepares itself for network access in austere environments, it finds risks in partially open internet networks. One example of network vulnerability lies in the public-key-

[24] Wylie Wong, “Army IT Goes Agile,” *Fed Tech*, August 2012, 22-25.

access infrastructure. Public-key-infrastructure is used to access to a device. The digital key acts as an added security checkpoint to the network and its numerous connections. The public-key-infrastructure is not without precedent. Since 2003, the Department of Energy has ceased to rely on public-key-infrastructure. The Department of Energy began using the Entelligence Messaging Server. The Entelligence Messaging Server is the most recent development in the evolution of the public-key infrastructure.[25] The Entelligence Messaging Server offers the Department of Energy the ability to utilize public-key-infrastructure to encrypt and sign messages with their servers rather than at the user-device level. This is useful, as it would solve the US Army's challenge in providing security at the user level by allowing encryption to take place with the email server. However, the Entelligence Messaging Server offers only limited security benefits, because it only helps to secure email from malicious attacks.

An agency, named IDC Government Insights, has developed a practice the US Army can learn from as it considers mobile devices. Government agencies such as the Bureau of Alcohol, Tobacco and Firearms, the Department of Veterans Affairs, and the General Services Administration utilize smartphones. These three agencies have identified that different users have different needs. For example, the Bureau of Alcohol, Tobacco and Firearms divided its user-base into four categories; senior executives, staffers, field-agents and inspector. Each separate user category required distinct capabilities from their smartphones. For instance, executives need to see progress reports by task. Conversely, a field-agent only needs to see his or her own status report, as opposed to reports of an entire directorate. A diverse set of access requirements caused the Bureau of Alcohol, Tobacco and Firearms to compartmentalize an apps interaction with hardware on the network. Although compartmentalizing created a more secure environment, it

[25] William Jackson, "Energy Adapts Its Pki to Handle Old and New Technologies," Government Computer News, http://gcn.com/articles/2012/10/01/doe-pki-edge-secure-email.aspx (accessed December 20, 2012).

acted as an obstacle for other user groups as well. In response, the Bureau of Alcohol, Tobacco and Firearms decided to relax its mobile device policy in order to allow personal devices on their network.[26]

In US Army information technology, there is a notable delay in identifying a security problem and implementing a timely and useful solution. For example, in 2012 the US Army's Communications-Electronics Research, Development and Engineering Center signed a $3.1 million contract with the Raytheon Corporation to develop the Morphing Network Assets to Restrict Adversarial Reconnaissance. The Raytheon Corporation states the Morphing Network Assets to Restrict Adversarial Reconnaissance is a "technique of dynamically modifying aspects and configurations of networks, hosts and applications in a manner that is undetectable and unpredictable by an adversary, but still manageable for network administrators." Morphing technology operates through a technique known as port hopping. Port hopping allows IP, internet protocol, addresses to remain obscure. For example, if a users device uses the Morphing Network Assets to Restrict Adversarial Reconnaissance technology, the network address would appear to an intruder as if it were on a windows operating system, when it has actually moved to another system, such as a Linux-based architecture. Although Morphing Network Assets to Restrict Adversarial Reconnaissance will not solve the US Army's network intruder threats, the Communications-Electronics Research, Development and Engineering Center expects it will offer significant security benefit to the military network. Morphing is advantageous because stationary addressing is more vulnerable to attack. It is a particular problem with handhelds because they are more numerous, they are not kept in fixed secure locations, and there signals are in the open. The

[26] John Mello, "Managing Mobility Facing the Spread of Network Endpoints, Agencies Search for the Right Fit to Meet Their Security Needs" *Fed Tech*, Winter 2012, 15-16.

Morphing Network Assets to Restrict Adversarial Reconnaissance will go into service in 2014, after a two-year delay in contract delivery.[27]

The concepts of the security triad also cause delays. The security triad concepts were rendered into the Certificate of Networthiness. The Certificate of Networthiness is the standard that must be satisfied in order to gain access to any Department of Defense information network. The Department of Defense defines Networthiness as:

> "the result of an operational assessment of IT to verify compliance with security, interoperability, supportability, sustainability, and usability regulations; guidelines, and policies as issued by Federal, Department of Defense and Combatant Command/Service/Agency Components."[28]

This statement by the Department of Defense Information Operations Chief reveals the many variables influencing the Certificate of Networthiness. In March 2012, the Macintosh Computer Operating System earned the Certificate of Networthiness from the US Army Signal Command. Earning the Certificate of Networthiness allowed the Apple Corporation's top-selling iPad and iPhone products to gain access to specific US Army information technology networks.[29] [30] The US Army clearly seeks to adopt handheld technology. Yet the Certificate of Networthiness is a necessary safeguard. Ironically, the Certificate of Networthiness is a protection as well as an obstacle.[31]

[27] Kevin McHaney, "Army's MORPHINATOR: A shape-shifting approach to network defense," Government Computer News, http://gcn.com/articles/2012/08/03/army-morphinator-cyber-maneuver-network-defense.aspx (accessed March 19, 2013).

[28] Office of the DoD Chief Information Officer, "Department of Defense Mobile Device Strategy" (memorandum for Secretaries of the Military Departments, Washington, DC, June 08, 2012) 3.

[29] Dan Spalding, "Centrify Directcontrol for Mac Os x Earns Certificate of Networthiness from Us Army Netcom," Marketwire, http://dmnnewswire.digitalmedianet.com/article/Centrify-DirectControl-for-Mac-OS-X-Earns-Certificate-of-Networthiness-From-US-Army-NETCOM--1947309 (accessed December 22, 2012).

[30] Cory Gunther, "Apple Announces Iphone 5 as Fastest Selling Phone in History," Slashgear, http://www.slashgear.com/apple-announces-iphone-5-as-fastest-selling-phone-in-history-23253373/ (accessed December 22, 2012).

[31] Henry Kenyon, "Army Makes Strides in Smart-Phone Security," Defense Systems,

The largest obstacle to the US Army's full adoption of handheld devices is the concern over classified material. Mike McCarthy, director of operations, Brigade Modernization Command, US Army Training and Doctrine Command, believes smartphones will gain the ability to handle classified information in the near future. Mr. McCarthy made this statement at the 11th Annual C4ISR Conference and Awards meeting in Arlington, Virginia. Mr. McCarthy also stated, "If you look at many of the capabilities gaps we've identified in the military the smartphone is the solution for many of those gaps." In further efforts to complete their modernization mandate, Mr. McCarthy relayed how General Peter Chiarelli, Vice Chief of Staff of the US Army told the Modernization Command that they should not, "follow the normal acquisition model" and look for acceptable risk levels, as opposed to a zero risk mindset. These statements indicate the US Army's efforts to differentiate between necessary and superfluous security requirements. [32]

ACQUISITIONS

Handheld technology must not only provide military applications and satisfy security requirements; the technology must also pass through the Department of Defense acquisitions process. The Department of Defense acquisitions process has four phases, each phase marked by a milestone denoting progress in the acquisition process. In effect, any equipment under consideration for purchase must meet the objective in each phase to advance within acquisitions system. [33] The image below denotes the four major phases in the acquisitions process as well as the formalized milestones that permit advancement to the next phase.

http://defensesystems.com/articles/2011/01/24/cyber-defense-army-smartphone-deployment.aspx (accessed December 18, 2012).

[32] Lindy Kyzer, "Classified Smartphones Will Soon Be a Reality," Clearance Jobs, http://www.clearancejobs.com/defense-news/443/classified-smartphones-will-soon-be-a-reality (accessed October 29, 2012).

[33] US Defense Acquisition University Press, Systems Management College, *Systems Engineering Fundamentals*, (Washington, DC: Government Printing Office, 2001), 12.

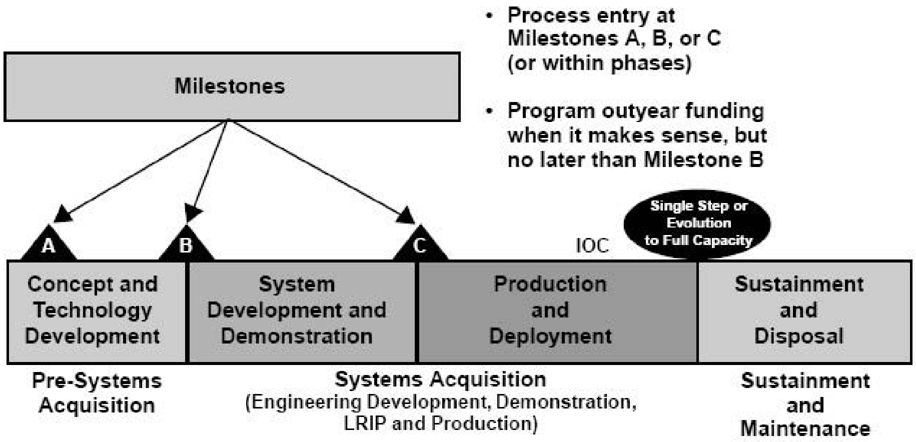
Milestones
• Process entry at Milestones A, B, or C (or within phases)
• Program outyear funding when it makes sense, but no later than Milestone B
A
B
C
IOC
Single Step or Evolution to Full Capacity
Concept and Technology Development
System Development and Demonstration
Production and Deployment
Sustainment and Disposal
Pre-Systems Acquisition
Systems Acquisition (Engineering Development, Demonstration, LRIP and Production)
Sustainment and Maintenance

Figure 1 Phases of the DoD Acquisitions Process

Source 1 Systems Engineering Fundamentals, Defense Acquisition University Press, 2001, Page 12.

The US Army acquisitions process must comply with the Department of Defense 5000 Series acquisition guidance. Certain pieces of military equipment, such as weapon systems or vehicles, rely on extensive commercial infrastructure to sustain the hardware when it is upgraded or requires repair. Yet unlike weapons or vehicle manufacturers, the handheld device community does not offer a sustainment infrastructure. Furthermore, the Department of Defense acquisition guidance categorizes information assistance supplies along with weapons. The US Army Acquisitions Procedures manual then subsequently states material purchases must be uniformly applied to:

> weapon systems; command, control, communications, and computers/information technology systems; national security systems; special access programs (unless specifically excepted per program charter); computer resources integral to those items or systems; system and nonsystem training aids, devices, simulations, and simulators; embedded training; embedded testing; instrumentation, targets, and threat simulators; and clothing and individual equipment.[34]

[34] DA Pam 70-3, *US Army Acquisition Procedures, (*Washington, DC: Government Printing Office, April 2009), 1.

Here US Army acquisitions verbiage is consistent with Department of Defense acquisitions guidance. The guidance above presents a challenge to the rapid acquisition of handheld devices because it forces the purchase of all equipment ranging from weapons to information technology systems under the same purchasing guidelines. To meet purchasing and accountability requirements, the US Army stated it would utilize commercial off the shelf purchases of smartphones because the purchase of ruggedized military smartphones would be cost prohibitive and unnecessary.[35] Handheld devices do not last as long as some pieces of military inventory, such as weapons systems. Nevertheless, handheld devices are not exempt from the four-phased acquisitions process.

The Department of Defense Acqusitions Process shown in figure 1 above sets milestones between System Development and Production and Deployment phases. Specifically, the US Army Acqusition Procedures Pamphlet states review boards at three levels must assess any equipment problems that may surface in order to determine if equipment should stop development or merely receive solutions.[36] Each review level is dependent upon successful completion of the preceding board. For this reason, the US Army Capabilities and Integration Center notes the acqusitions process takes approximately 17 years to complete.[37] Although information technology acquisitions take approximately three years to complete, the US Army Capabilities and Integration Center sponsors the Agile acquisitions process as a better solution to traditional Department of Defense acquisitions procedures.[38] Yet not all United States' governmental agencies rely on Department of Defense guidelines when purchasing equipment.

[35] Mortimer, "Army Sees Smartphones Playing Important Role"

[36] DA Pam 70-3, *US Army Acquisition Procedures*, 117.

[37] US Army Capabilities Integration Center (ARCIC), "Changing a Paradigm...forging the Future" (US Army Capabilities Integration Center brief to Massachusetts Institute of Technology at the Lincoln Laboratory Communications Conference, Cambridge, Massachusetts, March 24, 2012) 2.

[38] Ibid., 8.

Sister federal agencies such as the Department of Veterans Affairs do not rely on Department of Defense acquisitions processes. The Department of Veterans Affairs has found an internal solution for mitigating the problem created by rapid commercial technology development. The Department of Veterans Affairs solution does not focus on any one operating system, such as the Apple Corporation's internet operating system. The solution is to install a specific management system, "on every device we own that boots – laptops, tablets and smartphones." The US Army has also determined it will not rely on any single handheld software architecture.[39]

The US Army is not the only Department of Defense agency constrained by acquisitions requirements. Department of Defense purchase requirements also restrict defense contractors. The US Army requires a reliable supply chain. Supply chains create expensive requirements for defense contractors to satisfy. Furthermore, many manufacturers cannot maintain low prices when they ruggedize their product. In short, equipment ruggedization creates high priced products the US Army cannot afford to buy in large numbers. Many contractors prefer to develop equipment that can service commercial and military buyers. For instance, Gretchen Alper advises potential defense contractors:

> "commercial off the shelf products are a good solution for lower costs and quick design but are not always the most logical solution when any particular requirements are needed. Specialized companies who can ruggedize existing commercial off the shelf products and guarantee long-term delivery or who can supply military-grade commercial off the shelf products (sometimes referred to as Military Off-the-Shelf) may be better option (sic) to obtain the latest technology with a lower cost of ownership and risk".[40]

[39] Mello, "Managing Mobility Facing the Spread of Network Endpoints, Agencies Search for the Right Fit to Meet Their Security Needs", 16.

[40] Gretchen Alper, "Commercial Off-the-shelf (commercial Off the Shelf) Sounds Simple, but the Defense Industry Has Special Requirements," Beyond the Data Sheet, http://info.adimec.com/blogposts/bid/57875/Commercial-Off-the-Shelf-COMMERCIAL OFF THE SHELF-sounds-simple-but-the-defense-industry-has-special-requirements (accessed December 05, 2012).

Alper’s statement reveals the financial intimidation small commercial developers’ face when seeking military contracts. Specifically, while the US Army acquisitions process is meant to be fair and equitable for all contractors, the competitive purchase process favors financially advantaged contractors. Smaller businesses are unable to alter their products to meet military requests. The small business’ limited financial buffer is an additional variable in the US Army’s adoption of modern handheld technology.

Evidence also reveals commercial off the shelf equipment might not need ruggedization to meet military specifications. Mike McCarthy, Director of Operations and Program Manager at the US Army Brigade Modernization Command voiced a concern that handheld devices may not be durable enough to put into an operational environment. Mr. McCarthy states 18 months of testing hardware in realistic operational conditions resulted in only two broken smartphones. Mike McCarthy states one smartphone broke when it fell on a carpeted office floor and broke into three pieces. Another device broke when a soldier who was storing the device in a pouch in his armored vest took his vest off and set it on the ground; at which point the armored vest was run over and crushed by a 12-ton, mine-resistant armored vehicle. Military ruggedization would not have prevented the damage to the smartphone in either of these examples. In effect, an 18-month long field-test provided no evidence to support military ruggedization. Ergo, handheld device ruggedization probably is not necessary. Furthermore, ruggedization is expensive, $2500 per phone. In contrast, a commercial off the shelf smartphone costs approximately $200. Mike McCarthy, Deputy Director of the Brigade Modernization Command stated many companies would love to sell the government a ruggedized phone that is virtually bullet proof, but ruggedization is not necessary. The Brigade Modernization Command does not need devices that are shock resistant, hardened and expensive. Commercially available devices have proven to be more than adequate and sufficient.[41] The US Army has, therefore recommended, that commercial off the shelf technology receive implementation into academic and field environments.[42]

The US Army is required to spend its funds responsibly. To ensure the durability of its purchases, the US Army has adopted life cycle management procedures. Life Cycle Management procedures were formalized in August 2004 when the Assistant Secretary of the US Army for Acquisition, Logistics and Technology and the US Army Materiel Command, Commanding General, signed a Memorandum of Agreement, formalizing the US Army's Life Cycle Management Initiative.[43] The initiative "is intended to strategically and operationally align structure, processes, and responsibilities to enable greater synergies and improve the effectiveness and efficiency of all organizations involved in life cycle management".[44] Life cycle management goals include streamlined acquisitions and reduced aftermarket purchase costs. The 2004 US Army Life Cycle Management Initiative is evidence that the Army is altering its acquisitions processes to adapt to commercial purchasing realities.

As commercial off the shelf systems, smartphones have a supporting reliable repair and upgrade infrastructure. Field tested smartphones currently rely on theater-repair when in battle simulation conditions. Theater-repair provides for the quick return of equipment by using components that are modular and easily accessible. The quick fix solution reduces the need for additional ruggedization. The quick fix solution also reduces handheld size and weight. Mark

[41] John Edwards, "Is Military Ruggedization Going, Going, Gone?" Government Computer News, http://gcn.com/articles/2012/02/28/defense-it-1-rugged-computing.aspx (accessed December 22, 2012).

[42] US Army Brigade Modernization Command, "Crossing the Threshold" (US Army White Paper for Chief of Staff of the Army discussing the status of the Connecting Soldiers to Digital Applications (CSDA) initiative, Fort Bliss, TX, January 29, 2013) 5.

[43] US Department of the Army, *2008 Army Posture Statement; Life Cycle Management Initiative* (Washington, D.C.: Headquarters, Department of the Army, 2008)

[44] US Department of the Army, Information Paper, Life Cycle Management Initiative, http://www.army.mil/aps/08/information_papers/reset/Life_Cycle_Management_Initiative.html, (accessed December 30, 2012).

Holleran, President of Xplore technologies stated the Xplore technology ruggedized table computer, “is around five pounds, but our competitions’ is around 8 or 9 pounds.” Five pounds versus an average of eight and a half pounds is a weight loss of approximately 58%. When transporting any product, a 58% weight reduction is substantial and provides strong argument for the lighter item. The high technology theater-repair capability concept offers positive solutions that counter the current unreliable supply chain. [45]

The US Army’s $6 billion dollar information technology budget has created a problem for the smartphone supply chain system. The US Army’s Test Ground at White Sands Missile Range has pledged to open its market to technologies that are not programs of record.[46] A program of record is a system that currently exists in the US Army’s inventory and the Test Directorate at White Sands Missile Range has found itself in a difficult position due to acquisitions procedures that rely on program of record norms. For instance, through US Army Network Integration Evaluations:

> “The Army is seeking to buy digital radios, smartphones, portable 3G and 4G networking systems and other wireless technology to equip its combat brigades. The goal is to compress a process that would normally take three to five years into a few months, so technologies don’t become obsolete by the time they reach the battlefield.” [47]

As noted in Mike McCarthy’s white paper, the Ft Bliss, Texas Brigade Modernization Test Directorate finds itself challenged by a need to test the most modern equipment. Yet the Brigade Modernization Command must legally bypass unnecessary acquisitions guidance so it can quickly supply US Army field testing units with handheld technology. The field exercises, which hasten commercial off the shelf purchases while matching them with current mission sets, are

[45] Edwards, “Is Military Ruggedization Going, Going, Gone?”

[46] Sandra I. Erwin, “Army's Acquisition of Battle Network Slowed Down by Red Tape,” National Defense Magazine, March 2012, http://www.nationaldefensemagazine.org/archive/2012/March/Pages/Army%E2%80%99sAcquisitionofBattleNetworkSlowedDownbyRedTape.aspx (accessed October 29, 2012).

[47] Erwin, Army’s Acquisition of Battle Network Slowed Down by Red Tape.

known as the Network Integration Evaluation Exercises. Yet the Network Integration Evaluation is not without challenges.[48] Richard Cozby, Deputy Director of the Office of Acquisition Systems Integration Office, Technology and Logistics states, “It might take only six months for the US Army to evaluate and decide it wants to buy a particular system, but it takes 30 months to award a contract.” The lengthy contracting award process is cumbersome not only for the US Army, but also for government contractors as well. The US Army suffers from purchase delays, and the potential contractor must have the patience continue his business while awaiting a contract. Because there is a large cost associated with bringing equipment to test at White Sands, only larger contractors have the financial wherewithal to participate. It costs defense contractors millions to send equipment and support infrastructure to the Missile Range in New Mexico. Yet appearing at a US Army Network Integration Evaluation does not guarantee a contract at all. J. Michael Gilmore, Director of Weapons Testing and Evaluation, questions the need for the numerous systems the Network Integration Evaluations process considers at an exercise. Gilmore states, “The Army should be cautious about inserting too many untried, experimental systems into the Network Integration Evaluations. . . . too many systems in an event create problems with data collection.” As a result, the Network Integration Evaluation could be an obstacle, as well as a solution, to the new equipment-fielding problem facing the US Army as it considers handheld technology.

It is a challenge for the US Army to keep pace with commercial smartphone technology turnover rates. Major General Keith Walker, Commander of US Army Brigade Modernization Command in 2011, says the smartphone industry prides itself over its rapid

[48] Michael McCarthy “Connecting Soldiers to the Network” (White Paper presented to Vice Chief Staff of the Army, Fort Bliss, TX, May 30, 2012).

technology upgrades. Major General Walker describes the ideal US Army modernization pace as incremental brigade modernization. While the US Army seeks incremental change, Major General Walker states, "if you buy new technologies for the entire United States Army, by the time you get it to the last unit, it's already way out of date." [49] Clearly, incremental change is not useful if it is outdated change. Furthermore, not every piece of equipment that is tested will receive purchase approval. Major General Walker cited three systems that the Network Integration Evaluation did not approve for purchase. The three items the US Army declined to purchase were manned ground sensors, unmanned ground sensors and an unmanned aerial vehicle. Yet the Network Integration Evaluations did find utility in handheld devices for reconnaissance and surveillance tasks. In spite of the 2011 handheld field-tests, the US Army will not purchase handheld devices for soldiers in combat brigades until 2013.

On February 13, 2013 a California-based technology company, AOptix, announced a $3 million research contract with the Department of Defense. The contract stipulates AOptix would develop a peripheral device that gives smartphones the capability to use biometric identity verification data. Yet biometric technology is not new to the US Army. Currently the US Army accomplishes its eye-scanning, fingerprint and voice-recognition capabilities through stand-alone Handheld Interagency Identity Detection System devices. The contract with AOptix is distinct as it strives to incorporate Handheld Interagency Identity Detection System features in a commercial handheld mobile device. The AOptix addition wraps around the smartphone and reportedly weighs less than one pound. The AOptix Company claims it is

[49] Robert Gray, "Q & A with Maj. Gen. Keith Walker Commander, Brigade Modernization Command" El Paso News, May 02, 2011.

superior to the currently fielded Handheld Interagency Identity Detection System. Specifically, AOptix states their equipment can scan "faces up to two meters away, irises from one meter and voice from within the typical distance from a phone." [50] The auxiliary AOptix device can also scan a fingerprint by touching it to the flat of one's' finger. Furthermore, the smartphones inherent camera capabilities offer optimized use in bright sunlight. For instance, the AOptix contract acknowledges it may take two years of research before a product can be ready for delivery. Consider the following timeline: in 2006, the US Army began using biometric data. In 2009, Handheld Interagency Identity Detection System devices were common in the Iraq and Afghanistan theaters of operation. In February 2013, the Department of Defense signed a contract for the research and development of a smartphone-based biometric scanning device. The contract delivery is due in 2015. Force-wide fielding for the AOptix device is likely to occur in 2016. Assuming the commercial sector continues to develop technology faster than the military can adopt commercial technology, the Department of Defense may receive outdated technology for a potentially outdated mission requirement. The current contracting process ill suited for the US Army's plan to exploit the use of handheld devices because the procurement process cannot be completed in the time of a commercial development cycle.

In the past, the US Army could not benefit from Network Integration Evaluation Exercises. The acquisitions delay prevented the Army from benefitting from testing at White Sands Missile Range. The US Army created the Agile Process to streamline technology

[50] Liz Klimas, "Pentagon Wants to Turn Ordinary Smartphones Into Eye-Scanning, Thumbprint-Taking Super Machines," The Blaze (Government), February 13, 2013.

http://www.theblaze.com/stories/2013/02/13/pentagon-wants-to-turn-ordinary-smartphones-into-eye-scanning-thumbprint-taking-voice-recognizing-wonder-machines/ (accessed February 14, 2013).

purchases and equip personnel with cheaper and the most current equipment. The Agile Process contains seven-phases intended to overcome the difficulties attendant in the current four-stage acquisitions process. The Agile process' seven phases are: Phase 0 – Define Near Term Requirements, Phase 1 – Solicit Potential Solutions, Phase 2 – Conduct Candidate Assessments, Phase 3– Evaluation Preparation, Phase 4 – Network Integration Rehearsal, Phase 5 – Network Integration Evaluation, Phase 6 – Develop a Network Implementation Plan. The exercises in Phase-5 cannot occur until the US Army and its defense contractors have completed extensive coordination. Prior to Phase V, the US Army develops a needs-statement and presents the needs-statement to any military contractor who attends an industry-day-event in the continental United States. Regarding industry-day events, Gary Blohm, director of the US Army Architecture Integration Center at the US Army Chief Information Office/G-6 states, "The goal is to provide the most effective and efficient technology while improving cyber security and reducing costs." [51] The Industry Days are advantageous as the US Army finds opportunity to focus on its particular needs, while potential military contractors determine methods to meet contractual military realities. The Network Integration Evaluations have been successful in identifying equipment for soldier fielding. In particular, the White Sands Missile Range tests will result in the US Army equipping eight combat brigades with handheld devices.

Despite the introduction of the Agile Process, many still hold that the current acquisition architecture is ill suited for purchase of commercial off the shelf products, such as handheld technology. In a report partially sponsored by the Naval Post-graduate School, Jacques S. Gansler and William Lucyshyn state:

> In the twenty-first century, the United States will likely encounter a wide-range of threats, such as those posed by terrorists, rogue states and other non-state actors—all of whom are taking full advantage of globally available, high-tech commercial systems

[51] Wong, "Army It Goes Agile," 22.

> (e.g., from night vision devices, through secure cell phones, to satellite photos). At the same time, technology is changing more rapidly than ever before, and the Department of Defense must learn to embrace the fact that it no longer holds a monopoly on all military-relevant technology (many of the information-intensive innovations result from commercial activities).[52]

Gansler and Lucyshyn posit that the current Department of Defense acquisitions process cannot keep pace with the development of equipment necessary to defend the United States. Gansler and Lucyshyn recommend commercial off the shelf products receive special consideration under Department of Defense law. Gansler and Lucyshyn have defined the problem but not specified a solution. The Department of Defense procurement rules constrain not only the US Army, but other military services as well.

CONCLUSION

The US Army has not yet fielded handheld devices to operational units. Research initially hypothesized three potential explanations for the US Army's delay in adopting handheld technology. The explanations were that handheld technology did not offer the military any capabilities significantly different from current Army systems; that the technology could not meet Army operating and security needs; and lastly, that the Defense Department procurement system could not deliver the systems before the selected device was obsolete. However, as the research revealed, US Army has identified current and future uses for handheld devices. Those devices increase productivity and improve mission efficiency. Secondly, although initially handheld devices had difficulty meeting security requirements and protocols, recent technology advances will soon permit secure communication and data storage. The third area of concern, the US Army acquisitions process, proved to be the most significant factor delaying the US Army's handheld technology. Evidence shows the acquisitions process cannot keep pace with the rapid pace of

[52] Jacques S. Gansler and William Lucyshyn, US Naval Postgraduate School, University of Maryland with partial sponsor by the Naval Postgraduate School, *Commercial Off the Shelf, Doing it Right*, Report (College Park, MD, 2008), iv, 58-59.

commercial technology development. The longest delays in the acquisitions process stem from Department of Defense review and approval boards. Specifically, Department of Defense review and approval boards cannot approve commercial off the shelf technologies as fast as commercial upgrades are released.

The cause for delay in employing handheld devices is certainly not a paucity of applications. Senior US Army leaders believe there are applications for handheld devices in training, education and the field. The Network Evaluations Exercises at Ft Bliss provided data on verifiable uses for handheld devices, as well as the limitations inherent therein. Reports at educational forums and White Paper Briefs to Senior US Army leaders summarized the Brigade Modernization Commands' findings; non-ruggedized commercial handheld devices are ideally suited to military applications. Currently, US Army is developing the WIN-T Increment-2 network. The WIN-T Increment-2 network will allow US Army brigades to operate on their own secure network. Secure handheld devices will significantly augment the commanders' situational awareness. Smartphone technologies are useful in satisfying the Army's core mission requirements. The smartphones ability to help US Army leaders make timely and informed decisions is perhaps the greatest benefit smartphones offer. The ability to augment the mission-command competency of the US Army is significant and valuable.

Securing smartphone communications has been a significant challenge. It has been difficult for handheld devices to meet the requirement for confidentiality while also maintaining accessibility. Many of the procedures used to ensure security for fixed networks are not easily implemented using handheld devices. Thus, when security is increased, there is a decline in accessibility. However, new approaches to securing handheld devices have been devised. Brigade level mobile access networks have emplaced new security protocols and have undergone testing, evaluation and improvement cycles to push through obstacles inherent in security and accessibility nodes. The US Army has also decreased security threats to email by moving user access permissions to centralized network enterprise centers.

The Army procurement process is largely not suited for purchasing commercial handheld devices.. The four-phased acquisitions process contains acquisitions requirements best suited for long-term life cycle equipment. Most equipment is expected to exist in the Army inventory for an average of 17 years. 17 years stands in stark contrast to the 1-3 year life cycle of a handheld device. The Network Evaluations Exercises at Fort Bliss reveal the current four phased acquisitions process is too slow to keep pace with handheld technologies because handheld technology is continually improved and commercial business' cannot keep handheld devices priced low and provide the repair infrastructure the US Army requires for its traditional weapon and vehicle inventory. Tests conducted at White Sands Missile Range revealed that commercial off the shelf handheld devices can help the US Army achieve mission requirements while costing 10% less than the price of a ruggedized device.

The US Army finds that the information technology acquisitions process typically takes three to five years. Nevertheless, through the Network Integration Evaluations, the US Army is striving to complete the information technology acquisitions process in less than six months. Notable changes to the acquisitions process have developed throughout the Army ever since the Network Integrations Evaluations began. The newest process, named the Agile Process, strives to involve the commercial producer during the development of the US Army's needs statement and, thereby, speed the development of equipment that is secure and ready for testing in New Mexico. The Agile Process' suggests the US Army's solution to adopting smartphone technology lies in developing products that satisfy tactical needs and security requirements while the acquisitions community sheds unrelated purchasing constraints. The Department of Defense needs to change its methods in order to adapt to the current market environment.

In conclusion, the US Army has not deployed modern handheld technology into field operations. However, the US Army has sought to use technology popularized in the civilian sector. The reasons for the US Army's delay in adopting handheld devices are now clear. Although the operational benefits realized through handheld technology are significant, security requirements and an aging acquisitions process have delayed the US Army's adoption of handheld technologies. Soon the handheld device will meet security requirements. Once acquisitions policy has been reformed to accommodate handheld devices, those devices will propel the US Army further into the digital era through enhanced mission command capabilities.

BIBLIOGRAPHY

Ackerman, Robert. "Geospatial Intelligence Enters New Era." *Signal* 62, no. 10 (2008).

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. Washington, DC: Cforty Onesr Cooperative Research, 2003.

Alexander, Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* 5, no. 2, June 2011: 3-12.

Alper, Gretchen. "Commercial Off-the-shelf (commercial Off the Shelf) Sounds Simple, but the Defense Industry Has Special Requirements." Beyond the Data Sheet. http://info.adimec.com/blogposts/bid/57875/Commercial-Off-the-Shelf-COMMERCIAL OFF THE SHELF-sounds-simple-but-the-defense-industry-has-special-requirements (accessed December 05, 2012).

Army-Technology. "Battlefield Smartphones Receive a Ringing Endorsement." http://www.army-technology.com/features/featurebattlefield-smartphones-endorsement-technology (accessed September 30, 2012).

Association of the United States Army. "Inspecting Gadgets." Association of the United states Army. http://www.ausa.org/publications/ausanews/specialreports/2011/8/Pages/Inspectinggadgets.aspx (accessed January 05, 2013).

Association of the United States Army. "Inspecting Gadgets." http://www.ausa.org/publications/ausanews/specialreports/2011/8/Pages/Inspectinggadgets.aspx (accessed January 05, 2013).

Brigade Modernization Command Homepage, http://www.bctmod.army.mil/. (accessed December 12, 2012).

———. "Crossing the Threshold." US Army White Paper for Chief of Staff of the Army discussing the status of the Connecting Soldiers to Digital Applications (CSDA) initiative, Fort Bliss, TX, January 29, 2013.

Bristol, Michael. "Swiftlink-Bringing Broadband to the Battlefield." *Milsat Magazine* July-August 2010 (2010).

Brown, Brittney. *The Way Ahead for DoD Social Media Policy*. February 9, 2011. http://armylive.dodlive.mil/index.php/2011/02/the-way-ahead-for-dod-social-media-policy/ (accessed February 13, 2011).

Capabilities Integration Center (ARCIC), US Army. "Changing a Paradigm...forging the Future." US Army Capabilities Integration Center brief to Massachusetts Institute of Technology at the Lincoln Laboratory Communications Conference, Cambridge, Massachusetts, March 24, 2012.

Chief Information Officer, G-6, U.S. Army. “Introducing Us Army Apps Marketplace.” Architecture Community. http://architecture.army.mil/technical-view/applications/applications.html (accessed September 30, 2012).

Chief Information Officer, Office of the DoD. “Department of Defense Mobile Device Strategy.” Memorandum for Secretaries of the Military Departments, Washington, DC, June 08, 2012.

Cone, Robert W. “Shaping the Army of 2020,” *ARMY*, October 2011.

Defense Systems Incorporated. “Smart phones – and their apps – go to war.” http://defensesystems.com/microsites/2012/snapshot-c4isr/02-smartphones-apps-for-soldiers-warfighters.aspx. (accessed January 03, 2013).

Edwards, John. “Is Military Ruggedization going, going, gone?” *Government Computer News*. March 27, 2012. http://gcn.com/Articles/2012/02/28/Defense-IT-1-rugged-computing.aspx?admgarea=TC_Mobile&p=1. (accessed December 22, 2012).

Erwin, Sandra. “Army’s Acquisition of Battle Network Slowed Down by Red Tape.” March 2012, *National Defense Magazine*, Arlington, VA. http://www.nationaldefensemagazine.org/archive/2012/March/Pages/Army%E2%80%99sAcquisitionofBattleNetworkSlowedDownbyRedTape.aspx. (accessed October 29, 2012).

Erwin, Sandra I. “Smartphones-for-soldiers Campaign Hits Wall as Army Experiences Growing Pains.” *National Defense Magazine*. http://www.nationaldefensemagazine.org/archive/2011/June/Pages/Smartphones-for-SoldiersCampaignHitsWallasArmyExperiencesGrowingPains.aspx (accessed December 20, 2012).

Gansler, Jaques and Lucyshyn, William. U.S. Naval Postgraduate School. University of Maryland with partial sponsor by the the Naval Postgraduate School. *Commercial Off the Shelf, Doing it Right*, Abstract. College Park, MD, 2008.

Gould, Joe, and Lauren Biron. “Security Concerns Hobble U.S. Army’s Mobile Learning.” *Defense News*. http://www.defensenews.com/article/20120620/TSJ01/306200004/Security-Concerns-Hobble-U-S-Army-8217-s-Mobile-Learning (accessed September 18, 2012).

Gray, Robert. “Q & A with Maj. Gen. Keith Walker Commander, Brigade Modernization Command.” *El Paso News*. May 02, 2011.

Gunther, Cory. “Apple announces iPhone 5 as fastest selling phone in history.” *SlashGear*. October 23, 2012. http://www.slashgear.com/apple-announces-iphone-5-as-fastest-selling-phone-in-history-23253373/. (accessed December 27, 2012).

Headquarters, Department of the Army, U.S. Army Doctrinal Publication (ADP), *1, Operations*. Washington, D.C.: Department of the Army, September 2012.

———. Army Doctrinal Publication (ADP) 3-0, *Unified Land Operations*. Washington D.C.: Government Printing Office, October 10, 2011.

———. Army Doctrinal Publication (ADP) 6-0. *Mission Command*. Washington, DC: Government Printing Office, 2012.

———. Field Manual (FM) 1-02, *Operational Terms and Graphics*. Washington, DC: Government Printing Office, 2004.

———. Field Manual (FM) *3-0, Operations*. Washington, D.C.: Department of the Army, 2011.

———. Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Washington, DC: Government Printing Office, 2003.

———. Field Manual, *7-0, Training Units and Developing Leaders for Full Spectrum Operations*. Washington, D.C.: Department of the Army, 2011

———. Pamphlet (Pam) 525-7-8, *Cyber Space Operations Concept Capability Plan 2016-2028*. Washington, DC: Government Printing Office, 2010.

———. Pamphlet (Pam) 525-8-2: *The Army Learning Concept of 2015*. Washington, DC: Government Printing Office, 2011.

———. Pamphlet (Pam) 70-3. *US Army Acquisition Procedures*. Washington, DC: Government Printing Office, April 2009.

———. Training Circular (TC), *7-100, Hybrid Threat*. Washington, D.C.: Department of the Army, 2010.

———. *US Army Strategic Planning Guidance of 2011*. Washington, DC: Government Printing Office, 2011.

———. *US Army Social Media Handbook*. Washington, D.C.: Headquarters, Department of the Army. August 2011.

———. *US Army Strategic Planning Guidance of 2011*. Washington, DC: Government Printing Office, 2011.

———. *2008 Army Posture Statement; Life Cycle Management Initiative*. Washington, D.C.: Headquarters, Department of the Army, 2008.

Jackson, William. "Energy Adapts its PKI to handle old and new technologies*."* *Government Computer News*, September 24, 2012. http://gcn.com/Articles/2012/10/01/DOE-PKI-edge-secure-email.aspx?p=1. (accessed December 20, 2012).

Johnson, David E. *Military Capabilities for Hybrid War Insights from the Israel Defense Forces in Lebanon and Gaza*, Santa Monica: RAND, 2010.

Kenyon, Henry. "Army makes strides in smart-phone security." *Defense Systems*, January 13, 2011. http://defensesystems.com/articles/2011/01/24/cyber-defense-army-smartphone-deployment.aspx. (accessed December 18, 2012).

Klimas, Liz. “Pentagon Wants to Turn Ordinary Smartphones into Eye-Scanning, Thumbprint-Taking Super Machines.” *The Blaze LLC*. http://www.theblaze.com/stories/2013/02/13/pentagon-wants-to-turn-ordinary-smartphones-into-eye-scanning-thumbprint-taking-voice-recognizing-wonder-machines/. (accessed February 14, 2013).

Kyzer, Lindy. “Classified Smartphones Will Soon be a Reality.” *Clearance Jobs, Dice Holdings Services.* October 27, 2011. http://www.clearancejobs.com/defense-news/443/classified-smartphones-will-soon-be-a-reality. (accessed October 29, 2012).

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* California: RAND Corporation, 2007.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010. https://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain. (accessed September 28, 2012).

Magnuson, Stew. "Eyes Wide Open: Army Wants to Make 'Every Soldier a Sensor'." *National Defense* 91, no. 642 (2007): 44(4).

McBride, Margaret. “Apps for the Army Challenge Builds 53 Apps in 75 Days.” *US Army CIO/G6*. 2012. (accessed September 30, 2012).

McCaney, Kevin. “Army’s MORPHINATOR: A shape-shifting approach to network defense.” *Government Computer News*. August 03, 2012. http://gcn.com/Articles/2012/08/03/Army-morphinator-cyber-maneuver-network-defense.aspx?p=1. (accessed December 15, 2012).

McCarthy, Michael. “Connecting Soldiers to the Network.” White Paper presented to Commanding General Brigade Modernization Command, Fort Bliss, TX, May 30, 2012.

Mello, John. “Managing Mobility: Facing the Spread of Network Endpoints, Agencies Search for the Right Fit to Meet Their Security Needs.” *Fed Tech*, Winter 2012, 15-16.

Mortimer, Gary. “Army Sees Smart Phones Playing Important Role.” sUAS News. http://www.suasnews.com/2010/12/3004/army-sees-smart-phones-playing-important-role/ (accessed December 22, 2012).

National Nuclear Security Administration, Office of Public Affairs. November 29, 2012. “Global Threat Reduction Initiative Launches Mobile App.” http://nnsa.energy.gov/blog/nnsa%E2%80%99s-global-threat-reduction-initiative-launches-mobile-app. (accessed December 15, 2012).

Network Enterprise Center (NEC), Fort Hood. “SAN Storage Services.” Fort Hood Network Enterprise Center. http://www.hood.army.mil/NEC/EnterpriseServices/SANStorageServices.aspx (accessed December 15, 2012).

Net Resources International. “Battlefield Smartphones Receive a Ringing Endorsement.” July 31, 2012. http://www.army-technology.com/features/featurebattlefield-smartphones-endorsement-technology. (accessed September 30, 2012).

National Nuclear Safety Administration Office of Public Affairs. “NNSA’s Global Threat Reduction Initiative Launches Mobile App.” National Nuclear Security Agency, Office of Public Affairs. http://nnsa.energy.gov/blog/nnsa%E2%80%99s-global-threat-reduction-initiative-launches-mobile-app (accessed December 15, 2012).

Nye, Joseph S. Jr. *The Future of Power*. New York: PublicAffairs, 2011.

Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy of the United States of America, 2011*. Washington, D.C.: The Pentagon, 2011.

Office of the Chief of Public Affairs. "Social Media Roundup/Geotagging Safety." *Official U.S. Army Slideshare Profile.* April 18, 2011. http://www.slideshare.net/USArmySocialMedia/social-media-roundupgeotagging-safety?from=ss_embed (accessed September 18, 2012).

Smith, Chris. “Making Calls Fifth Most Popular Use for Smartphones.” Tech Radar. http://www.techradar.com/news/phone-and-communications/mobile-phones/making-calls-fifth-most-popular-use-for-smartphones-says-report-1087623 (accessed December 14, 2012).

Spalding, Dan. “Centrify DirectControl for Mac Os x Earns Certificate of Networthiness from Us Army Netcom.” Marketwire. http://dmnnewswire.digitalmedianet.com/article/Centrify-DirectControl-for-Mac-OS-X-Earns-Certificate-of-Networthiness-From-US-Army-NETCOM--1947309 (accessed December 22, 2012).

Thomas, Timothy. *The Dragon’s Quantum Leap: Transforming from a Mechanized to an Informationized Force*. Fort Leavenworth: Foreign Military Studies Office, 2009.

Turabian, Kate L. *A Manual for Writers of Research Papers, Theses, and Dissertations*. 7th ed. Chicago: University of Chicago Press, 2007.

U.S. Customs and Border Protection Targeting and Analysis Systems Program Office, Procurement Directorate. “Request for Information Regarding Smartphone Scanning Peripheral Devices.” Washington, District of Columbia. November 26, 2012.

U.S. Defense Acquisition University Press. Systems Management College. *Systems Engineering Fundamentals*, by Department of Defense. Washington, DC: Government Printing Office, 2001.

U.S. National Telecommunications Security Advisory Committee. *NSTAC Report to the President on Cloud Computing*. Washington, DC: Government Printing Office, 2012.

US Department of Defense. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington D.C.: The Pentagon, 2011.

US Joint Chiefs of Staff. “Joint Vision 2020: America’s Military – Preparing for Tomorrow.” *Joint Force Quarterly* (Summer, 2000): 62, 65-66.

Ward, Jeff, “*What is a Game Engine, Game Career Guide.” UBM Technology.* April 29, 2008. http://www.gamecareerguide.com/features/529/what_is_a_game_.php. (accessed December 02, 2012).

Weigelt, Matthew. “After 3 years, Apps.gov to go dark.” 1105 Government Information Group. November 30, 2012, http://fcw.com/articles/2012/11/30/goodbye-apps.gov.aspx. (accessed December 15, 2013).

Wong, Wylie. “Army IT Goes Agile,” *Fed Tech*, August 2012, 22-25.

Yasin, Rutrell, “Army Sees Big Savings in Application Modernization.” *Government Computer News*. June 20, 2012. http://gcn.com/Articles/2012/06/20/Army-Data-Center-Consolidation-Application-Savings.aspx?sc_lang=en&p=1.(accessed September 20, 2013).