REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15-04-2013	Master of Military Studies Research Paper	September 2009 - April 2010

4. TITLE AND SUBTITLE
The Use of Personal Information Technology in Military Area of Operations

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Major Michael H. Scott

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
The recent mobile personal information technology (PIT) advancements in streamlined communications, decision making tools, and the speed of information to the tactical level of warfare has brought about a reconceptualization in the operational level of war. The potential of this reconceptualization could force the U.S. military to reconsider its overall military strategy in that there may not be an operational level of war anymore. As more information is available to the warfighter on the battlefield, the need to conceptualize an operational level of war appears to be diminishing. There remains a need for an operational level of war for joint operations. However, the implementation of the PIT devices brings about the benefit of having strategic level decision making linked to tactical action like never before. As the operational art fades in this respect, a more streamlined process may emerge.

15. SUBJECT TERMS
Personal Information Technology
Iphone, Ipad, Tablet, Operational Art, Operational Level of War, Strategic

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass	UU	37	19b. TELEPONE NUMBER (*Include area code*) (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

The Use of Personal Information Technology in Military Area of Operations

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF MILITARY STUDIES

Major Michael H. Scott

AY 12-13

Mentor and Oral Defense Committee Member: Dr. Matthew Flynn

Approved: Matthew Flynn

Date: 4/29/13

Oral Defense Committee Member: J.W. Gordon

Approved:

Date: 4/19/13

P.M. Melchior

EXECUTIVE SUMMARY

Title: The Use of Personal Information Technology in Military Area of Operations

Author: Major Michael H. Scott, United States Air Force National Guard

Thesis: The recent mobile personal information technology (PIT) advancements in streamlined communications, decision-making tools, and the speed of information to the tactical level of warfare have brought about a reconceptualization in the operational level of war. The potential of this reconceptualization could force the U.S. military to reconsider its overall military strategy in that there may not be an operational level of war anymore.

Discussion: The "mobility" revolution has greatly shaped the modern era of computing. Desktops are beginning to fade in prominence as laptops, netbooks, ultrabooks, and other portable computers take over. For the first time, this aspect of the technology is taking a prominent role in military defense. Although mobile devices are the new and popular devices in today's commercial market, the military's strategy for the use of technology is not simply about embracing the newest technology. It is about keeping the Department of Defense (DoD) workforce relevant in an era of information and cyberspace playing a critical role in mission success. Computing technology is more mobile than ever, and the evolution from large mainframes to handheld mobile devices offers unprecedented opportunities to advance the operational effectiveness of the DoD. Through faster access to information and computing power from any location, warfighter functions can be quicker and more responsive to address the requirements in military operations. The continued improvements in communication and data exchange capability are ultimately decreasing the fog of war. The recent mobile personal information technology (PIT) advancements to the tactical level of warfare have brought about a reconceptualization in the operational level of war. The potential of this reconceptualization could force the U.S. military to reconsider its overall military strategy in that there may not be an operational level of war anymore. With a greater degree of communication and information capability from the strategic to the tactical levels, the U.S. military will see a lifting of the fog of war.

Conclusion: As more information is available to the warfighter on the battlefield, the need to conceptualize an operational level of war appears to be diminishing. There remains a need for an operational level of war for joint operations. However, the implementation of the PIT devices brings about the benefit of having strategic level decision-making linked to tactical action like never before. As the operational art fades in this respect, a more streamlined process may emerge.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Preface

The origins of this research paper begin with a culmination of my education, experiences, and interests. I have an associate degree in Information Systems and an MBA in Management Information Systems. I have also had the pleasure of working in the United States Air Force National Guard as a Communications Plans and Programmer and in a civilian world as a Business Systems Analyst. I have a strong interest in technology and believe in its ability to revolutionize society and tasks of everyday life.

I want to thank my mentor, Dr. Matthew Flynn, for his guidance and input into the paper and helping me to complete this project.

Additionally, I would like to express my deepest appreciation and gratitude to my family and loved ones for their patience, understanding, and encouragement. I want to especially thank my daughters for the time they gave up to allow me to be here in this class and ultimately write this paper.

INTRODUCTION

The "mobility" revolution has greatly shaped the modern era of computing. Desktops are beginning to fade in prominence as laptops, netbooks, ultrabooks, and other portable computers take over.[1] For the first time, this aspect of the technology is taking a prominent role in military defense. Defense Information Systems Agency (DISA) Director, U.S. Air Force Lt. Gen. Ronnie Hawkins, Jr., announced that mobility would be one of his eight initial efforts for his agency.[2] DISA's Strategic Plan describes how it supports the agency's mobility initiatives as they "promote rapid delivery, scaling, and utilization of secure mobile capability leveraging commercial mobile technology to enable an agile deployment environment for new and innovative applications to support evolving warfighter requirements."[3]

Although mobile devices are the new and popular devices in today's commercial market, the military's strategy for the use of technology is not simply about embracing the newest technology. It is about keeping the Department of Defense (DoD) workforce relevant in an era of information and cyberspace playing a critical role in mission success.[4] Computing technology is more mobile than ever, and the evolution from large mainframes to handheld mobile devices offers unprecedented opportunities to advance the operational effectiveness of the DoD.[5]

Through faster access to information and computing power from any location, field units can maneuver in unfamiliar environments with real time mapping and data overlay capabilities; soldiers can identify friendly forces; engineers can take pictures of mechanical parts for immediate identification and replacement ordering; and military healthcare providers can diagnose injuries and remotely access lab results while away from hospital premises.[6] Use of iPhones in medical settings means military medical professionals can now enhance triage efficacy by checking vital signs including pulse and body temperature.[7] By enabling real time

access to critical information and productivity tools such as these, as well as email and collaboration, warfighter functions can be quicker and more responsive to address the requirements in military operations.[8]

These technological advances are also finding themselves incorporated into the thinking of those contemplating how to fight and conduct wars in the years to come. There is a tantalizing payoff here, perhaps one not understood by those looking to capitalize on the technology. The continued improvements in communication and data exchange capability are ultimately decreasing the fog of war. The recent mobile personal information technology (PIT) advancements in streamlined communications, decision-making tools, and the speed of information to the tactical level of warfare have brought about a reconceptualization in the operational level of war. The potential of this reconceptualization could force the U.S. military to reconsider its overall military strategy in that there may not be an operational level of war anymore.

LITERATURE

Due to the fast paced and the continuous evolution of technology, some of the best writing on the PIT subject is in recent articles, some of them more traditional than others, with a variety of perspectives on the matter. U.S. Army journals and other military periodicals have published articles covering topics relating to opportunities to vulnerabilities. Information technology professionals and journalists reporting in mainstream media outlets have authored some of the writings that discuss how each service envisions utilizing this new technology. A common theme in the various writings of the current uses of PIT is how military organizations are embracing it as they attempt to incorporate it into their processes, and how it will continue to be used in future warfighting methods.

There is an abundance of quality current writings available on PIT, how the military currently uses it, and the military's vision on the use of this technology in tactical procedures, but the writings generally lack the big picture of the operational level of war in the military. For example, Brad Reed, a reporter for *Network World*, argues application developers are working to create military applications that soldiers can use to gather intelligence and map out dangerous areas in hostile territory. He echoes that soldiers can use these apps to gather intelligence, map out dangerous areas in hostile territory, and upload data into a central database to analyze parameters that military personnel can roam freely versus where they should proceed with extreme caution.[9] Another voice, Anna Mulrine, a staff writer for the *Christian Science Monitor*, weighs in and says a smart phone pilot program for the Army points to a culture shift that puts new streams of intelligence into soldiers' hands in the field, as well as gives them the chance to evaluate that data. This is essentially blurring the lines between officers and those they command.[10] These are all good assessments, but as mentioned, the writings neglect to consider the impact on the operational art of war.

This paper takes this important step and does so by following the U.S. military's current doctrinal views of PIT. Most famously, the DOD published a *Mobile Device Strategy* in May of 2012 that laid out some of the broadest strategic goals in the use of mobile technology in the branches of military service such as advancing and evolving the DoD Information Enterprise Infrastructure to support mobile devices, to institute mobile device policy and standards, and promoting and developing use of the DoD and Web-enabled applications.[11] However, as previously stated, there is tangential discussion at best regarding PIT and the impact on operational art.

Again, the issue is whether advances in cyber communication eliminate the practice of the operational art. Others have suggested this is happening anyway, even if not for reasons related to cyber developments. For example, William Owen says the operational level of war is a fallacy built on a failure to understand historical teaching on strategy and tactics.[12] Huba Wass de Czege, a retired U.S. Army brigadier general, adds that operational art is not a level of war or the art of generalship. It is what goes on in the explorer's mind, the mediating and balancing interaction between his strategic and tactical reasoning.[13] These authors contend that operational art does not exist, as there is only strategy and tactics. The role of cyber technology furthers their argument as it continues to close that perceived gap between the strategic and tactical levels. Because of these contentions, it is essential to discuss the incorporation of the cyber realm into the future of operational art.

CURRENT USES of PIT IN THE MILITARY

The U.S. military is exploring these technologies in all branches from top leadership to the tactical warfighter on the battlefield. The Chairman of the Joint Chief of Staff, U.S. Army General Martin Dempsey, uses an iPad to read his daily Commander Critical Information Requirements (CCIRs) classified intelligence briefings. An initiative in 2011 authorized leadership to use tablets to replace the standard, bulky briefing books prepared each day for them to read. The use of the tablets in this area alone has saved countless person-hours and costs in reproducing and printing thousands of document pages. General Dempsey also says he is interested in what the military has learned in pushing (technological) capability to the edge and empowering junior leaders with information required to maintain situational awareness. He says the iPad is "probably the tactical outpost of the future because of the generated power and the data management power of these devices in the future, where ever the commander is if he and his

staff have one of these devices it can be your tactical operations center. Every bit of information you need at one point will be available to you" in the tablet.[14]

In an online article from Popular Science, The U.S. Air Force's Air Mobility Command indicated it planned to buy up to 18,000 iPad 2 tablets or equivalent devices to replace pilots' heavy flight bags used to stow their charts and other flight materials. These devices were destined to be on the C-5 Galaxy and C-17 Globemaster. The article mentions the Air Force Special Ops Command is also planning to purchase 2,861 iPad 2s for its crews. Maj. Gen. Rick Martin, the Director of Operations for the Air Mobility Command states that transitioning "from a paper based to an electronically based flight publication system will not only enhance operational effectiveness, it can also save the Department of Defense time and money."[15] The military considers it a primary issue of weight and simplicity. The Mobility Command's flight charts are updated every 28 days, equating to 70 pounds of paper per aircraft is sorted and updated; a time-consuming process to wade through. The added weight can be a problem, even on airplanes designed to carry enormously heavy cargo. Cockpits have limited amounts of space and each crew has to manage an inordinate amount of paper. This can quickly become controlled chaos.[16] The U.S. Air Force purchased the iPads for the program "Electronic Flight Bags" early in 2012. This essentially eliminated the printed versions of manuals, maps, and charts carried in the pilot flight bags. With the aid of the iPad, the program implemented a process that eliminates $1.77 million in printing costs of the Flight Bag manual, plus an additional $3.28 million per year for printing of maps and charts, 22,000 man-hours, and $770 thousand per year in fuel. The ultimate objective of pilots possessing mobile devices is to significantly reduce paper in one's operation and improve efficiency of information management. The improved processes will continue to save money year after year, even

considering updates, repairs, or replacements to the devices.[17] This example clearly demonstrates how the Air Force supports providing PIT devices to members in the operational environment.

An article in *Bloomberg* in March 2012 printed that the U.S. Air Force purchased 63 iPad 2s from Executive Technology Inc., a Phoenix-based computer services company. The company scheduled the devices for delivery, and the Air Force was to conduct testing to ensure security measures and network connectivity concerns were within acceptable standards. The Air Force was also awarded a $9.36 million contract to buy as many as 18,000 Apple Inc. iPad 2s. This purchase is one of the military's largest orders of computer tablets as of the March 2012 date.[18] The U.S. Air Force is also acquiring smart phone devices for Air Force members. According to the defense contractor, General Dynamics, the U.S. Air Force senior leaders received 300 Sectéra Edge Smartphones in June 2011 offering access to the classified email system known as SIPRnet.[19]

In the Marine Corps, the iPad successfully implemented a navigation system in the early 1990s era AH-1W Cobra attack helicopter to aid in close air support (CAS) of ground troops. An enterprising Captain developed an application to electronically digitize and stitch map sheets together so a pilot could view them on an iPad. With the iPad's embedded GPS, the Cobra now has a portable moving map, which the early 1990's era helicopter lacks. A single tablet also contains every conceivable map in an incredibly light and easily accessible touchscreen. A simple download makes updates to the local geography and existing products. This provided the aging aircraft with a navigational system as advanced as any available in the civilian world. This leap in capability cost less than $1000 per aircraft.[20]

According to Lockheed Martin, their organization has begun making a portable signals device to enable deployed Marines to create a 4G cellular network anywhere in the world.[21] The Marine Corps began purchasing these devices in November 2011.[22] This would enable troops to have the connectivity and bandwidth required to utilize PIT devices such as the smartphone and tablets in the combat zone.

The U.S. Marine Corps Chief Information Officer (CIO), Marine Brigadier General Kevin Nally, authorized two groups—forward air controllers (Marines calling in airstrikes or air support) and pilots in Afghanistan—to utilize tablets in their operations. This was conditional with the adherence to what General Nally called the TTPs. The TTPs are tactics, techniques, and procedures. They disabled the tablets so there is no network connection. Members cannot download and store Secret material on these tablets because no data is at rest and no encryption is available for the data. Additionally, The Marine Corps G6, Marine Communications IT personnel were forward operating with these two groups of Marines and provided oversight for operation of the tablets. Currently, this is the extent of authorized utilization of the tablets within the Marine Corps. As for other uses for the mobile devices like the iPhones, Androids, tablets, etc., General Nally advised they must wait on NSA's approval to certify these through the STIGs (Security Technical Implementation Guides). The NSA's authorization will permit the use of additional devices for the Marines. Authorized Marines utilized android devices in Humanitarian Aid and Disaster Recovery (HADR) instances like with the earthquake and tsunami in Japan in 2011. They used map devices to locate people needing help, document the details, and communicate the specifics via the phone. That was a huge benefit, more effective than previous methods, and all on an unclassified level in helping with humanitarian assistance.

Marines developed apps to track the logistics of getting water, food, and medical aid to the Japanese people. [23]

These devices were a significant asset, but not hooked up into the Marine Corps computer network. General Nally says the other issue with cell phone, smartphone, and tablet devices is if used in a tactical environment, the "back end" still requires a buildup (i.e. cell phone towers, servers, etc.). Unlike in the United States where one can find a cell tower on average every 1.5 miles, in Afghanistan, the U.S. military and State Department helped construct a cellular telephone network for the Afghans. The Taliban and Al Qaeda have a tendency to turn the towers off at certain hours of the day so if the back end is built out, it must be protected it too. Building the cellular network for the tactical environment is challenging. General Nally would like to see a handheld device that acts, feels, and works like a smartphone, with the apps on it, that connects to a tactical radio that already has embedded crypto on it. Then the build out is not required on the back end. Manufacturers are working to create this type of device also.[24]

The U.S. Army is aggressively pursuing smartphone technology as a key component of its ground combat systems to allow troops to track friendly forces or view overhead surveillance images to help identify targets. The Army's chief scientist, Scott Fish, said the U.S. Army might consider scaling back its requirements for classifying sensitive information to allow more information to flow on smartphone-based systems. For example, the Army could downgrade selected classified battalion-level information to allow troops to access and exchange it on hand-held systems.[25] This year the Army is issuing smartphone-like devices to eight brigade combat teams for use in communicating with and tracking friendly troops.[26]

The Army seeks to integrate Apple Inc. products into operations for a variety of reasons. They are durable, easy to use in the field, tough to hack into, and readily available in the market

(unlike many specialized computer hardware items). Soldiers have used Apple's iPod Touche in the Middle East as simple translation tools to communicate with coalition forces and the local population.[27]

In April 2011, the Navy tested a smartphone system on the carrier George H.W. Bush that tracks the location of individual sailors aboard ship and can send alerts via text or email to personnel in specified areas of the vessel.[28] The Navy's Southeast Regional Maintenance Center (SERMC) uses an iPad type tablet to conduct a pilot-testing program that assesses a ship's state of readiness for deployment. SERMC pre-loads the ship's configuration data onto the REDI tablet system to enable the conduct of maintenance research, update documentation, and generate maintenance work orders efficiently and in a coordinated manner. All the ship's technical manuals are also loaded onto the tablets, so all relevant reference resources were immediately available on the spot. They put open jobs details and job history from the past six months into the system. The assessment process decreased dramatically from eight or more hours to 20 minutes for assessment and distribution. The new system eliminates prior paperwork and gets the job done quickly. With the use of the tablets, the inspectors can now walk around the ship and assess a discrepancy on-site. They can input everything into the discrepancy forms, obtain needed information on a broken part, retrieve all the information on fixing it, and immediately have it approved. This process could ultimately eliminate all the paperwork for the Navy's assessment program.[29] The mobile devices employed in the Navy brought about a simplification in the work procedures and made it a streamlined and efficient process overall.

The Next Generation Enterprise Network (NGEN) is the latest advancement of the Department of the Navy's enterprise networks. According to the Navy's requirements document, "NGEN will provide a secure and reliable enterprise-wide voice, video, and data networking

environment that meets the warfighter's needs, enabling command and control (C2) in conjunction with Consolidated Afloat Networks and Enterprise Services (CANES), and will provide a capability to access data, services, and applications anywhere worldwide." The network will also have the ability to interface with secure mobile devices and disseminate information to these devices via secure voice, text, and paging services.[30]

FederalNewsRadio.com reports in August of 2011 that the Coast Guard was the first military service to "ok" the iPhone and Android on a military network. It says the Coast Guard was the first military service to adopt Apple and Android-based smartphones for its workforce. The Navy was to begin phasing out the service's current inventory of Windows Mobile 6.x phones in favor of iPhones and various models running the Google-developed Android platform. The Navy was to issue these as the other plans expired and became due for replacement. The Coast Guard workforce will use smart phone devices for official email and other office productivity tools. Because the Navy has a primary mobility role, sailors can now access personal sites like personal social media and banking sites. This limited use of the devices for personal business would be unauthorized otherwise on a government-owned piece of technology and is possible because the handsets will run software, developed by Good Technology, which creates a secure, encrypted sandbox capable of walling-off government data from other areas of the phone. The devices will not directly access the Coast Guard's dot-mil network. This is exactly what the Coast Guard does want, to make these devices more capable and enable Coast Guard members to access the network. The Defense department is testing Android and iOS devices with CAC card capabilities to allow the secure use of the device on DoD networks. A pilot project for iPhones and iPads, led by the Defense Information Systems Agency, is currently underway. The Coast Guard is new to incorporating these devices in operations, but there is

clearly lots of potential to go around.[31] Each military branch is proactively seeking ways to employ the mobile devices to bring about new ways of doing old things. These new ways enable cost savings, less effort, and better communications.[32]

THE U.S. MILITARY'S VISION

At the strategic level, the connected devices provide immediate communications to anywhere on the battlefield and equip forces with capabilities not existing today. These communications now extend the warfighters' capability range beyond normal line of sight and other human sensing techniques.

The U.S. Army has predicted for some time that smartphones will play an important role in combat, but it is still working to understand just how smart devices like the iPhones and Androids might eventually supplement or replace current combat net radio voice architecture. In future military conflicts, Army officials say soldiers at the lowest echelons without these devices would not have even company-level communications access. Now smartphones and tablet computers will connect them to brigade-level networks. In Army terminology, this provides soldiers with "reach-back" capabilities to access critical battlefield intelligence. The U.S. Army's former chief information officer, retired Army Lt. Gen. Jeffrey Sorenson says a state-of-the-art tactical network would give field commanders a huge advantage over any adversary. In the past, only division and brigade-level commanders required access to the latest intelligence. Now even the lowest levels soldiers must have accurate information at all times.[33] The current and emerging smart phone technologies provide means to perform these intelligence communication functions without extended amounts of user training. They have now become a staple in public society and users are well educated in manipulating them. With the general society's and especially the younger generation's familiarity with these devices, the training to

learn how to use them would be minimal. The availability of having information readily available will provide a familiarity and a situational awareness enabling the best decision making possible in potential life threatening situations.

Most experts agree the lack of information is what creates the fog of war and this problem leads to bad decisions, such as dropping bombs on innocent civilians. General Sorenson said, "If (troops) have the wrong information…the consequences become front-page news."[34] A modern network would allow commanders from four-star generals to platoon leaders to track their troops' location and the position of the enemy in unprecedented fashion, thereby, conceivably, eliminating these mistakes.[35]

Sorenson draws a parallel between the combat advantages that information provides with that of night-vision technology. The Army's mantra years ago was to "own the night," he said. Advances in night-vision sensors paid off for the U.S. military, and the information and communications side need that same competitive edge.[36]

High-speed mobile broadband is a holy grail in today's military operations. FM radios no longer suffice. Soldiers want the ability to communicate and exploit the capabilities of the latest smartphones. Troops want the same technology powering high-speed commercial cellular networks to send photos and video, and keep track of their unit's location. The military is working toward that vision, but some hurdles remain in achieving it.[37] Among these hurdles, the military needs understanding of the technology implications on the operational art of war.

The U.S. Military wants to provide front line troops with relevant decision-making data about situational awareness issues, intelligence, and information operations to enable them to be better able to complete the mission. Ideally, the mobility of tablets and smartphones should empower the troops with enough information to coordinate their job and mission essential

tasking. A marine on the ground performing humanitarian assistance and disaster relief (HADR) in Haiti after an earthquake should be able to obtain the information required to coordinate survivors to relief supplies and have the functionality to communicate via smart technology to advise his fellow comrades that the displaced civilians are in route to their location. The United States is accustomed to spending large amounts of money on specialized hardware for troops. It has determined it can get some of the same results from the smartphone technology at a less expense. Despite the advantages of cost, there are some concerns. One of the main concerns is security of the network and encryption specialists are already hard at work to strengthen it.[38] There is an implementation gap in being able to deploy the devices due to concerns of information security and connectivity. The military is working hard to address these concerns. Ultimately, the military has a good vision, but they are not there because of these issues.

VULNERABILITIES AND CONCERNS

As many opportunities as PIT presents for the military, there are remaining bugs to work out and back up plans to develop in the application and execution of the devices and systems. IPads are certainly lighter and sleeker than a binder full of charts and graphs, but are by no means perfect. A number of technical problems could arise, such as the device home screen could freeze. The tablet could run out of battery if someone forgot to charge the device. Unless the device functionality is limited to only that of the job, pilots could become distracted from their intended mission. The application/system could close without warning, difficulty returning, show a menu one cannot get rid of; devices could perform unintended functions, etc. These are annoying issues to the users, but definitely not something one should have to manage during a wartime crisis.[39]

The use of iPads or tablets in the Secret Classified information realms is a bit trickier than unclassified arenas. Currently, regulations prohibit use of such devices on the Secure Internet (SIPRnet). The military is not at a secured point to be able to have secret information sitting out on the cloud technology to allow access to it wirelessly. Due to concerns of viruses and worms, the devices must have physical alteration, only used in a standalone mode, and locked down to minimize the risk of exposure of classified information.[40]

Some critics highlight a few significant risks associated with this functional concept's implementation. The most prominent of these risks are data compromise, connectivity, and limited battery life. While there are risks involved, the device implementation benefits far outweigh the potential risks. Technology now has provided ways to mitigate the associated risks involved. The military can remotely erase devices falling into enemy hands. A programmed, self-erasing feature could periodically delete data to prevent an abundance of information in the device memory and prevent potential compromise of mission essential information. This minimizes classified information falling into the enemy's possession.

One of the major concerns in implementing the use of smart PIT in the area of operations is connectivity and the acute shortage of network bandwidth for deployed troops. As device connectivity has expanded in more remote locations, there is now continuous carrier cell coverage.[41] Devices can connect via satellite if a cell coverage tower is unavailable in an operational area.[42] Another connectivity option if cell towers are unavailable is to utilize mobile relays or hubs, which essentially extend digital signals to maintain device connections.[43] The military must find a way to bridge the bandwidth deficiency gap existing currently in today's combat zones. Commanders contend the contrasts between the connectivity soldiers are accustomed to at home and that provided when deployed is unacceptable. [44]

External batteries, data hubs worn outside of clothing, and small field grade chargers are available to boost the devices in remote field locations.[45] These latest developments in technology now present capabilities to secure, connect, and power the PIT devices.

Cyber security is another major concern that has hindered adoption of smartphones in the area of operations. The National Security Agency increasingly is finding new ways to protect data and devices.[46] The use of wireless devices carries the risk of exposing classified information or making the DoD's information grid vulnerable to cyber-attacks.[47] Given the risk of phones getting lost or stolen, military technology experts want to be able to confirm users' identities, similar to the way a Common Access Card authorizes use on desktop computers.[48]

Another item of concern as the military attempts to move into the PIT realm is who is making the devices and who is programming the applications for it. According to an article in Forbes, companies located in China manufacture the iPad. Currently, there are no measures in place to specify any special security and vigilance requirements for the manufacturer of iPads the military would purchase. In addition to the devices themselves, there must be consideration given to the development of the software. In one particular case, the U.S. Air Force was considering purchasing 18,000 iPads with a GoodReader software application installed. A Russian firm makes the GoodReader software. As Chinese companies make the iPad and a Russian firm develops the GoodReader software, the U.S. Air Force gave it some additional consideration and cancelled the planned acquisition due to security concerns.[49] The place of manufacturing and the home of a developing firm must be a consideration in the acquisition of these types of products and in how the United States military uses them in operations. Accommodate with alternate methodologies while considering security measures prior to implementation.

Apple does electronic security differently for their products than a Windows based device. The change from the Windows-based tablets encountered significant internal resistance and after considering all variables many units find an iPad product to be a better choice. In the U.S. Air Force's fight for the paperless "Flight Bag", the military's biggest hurdle in getting Apple technology approved was overcoming outdated military policy. The U.S. Air Force's Air Mobility Command (AMC) fought for changes to policies they believed did not address the commercial technology existing today. [50]

Capt. Steven Simon, director of the U.S. Naval Academy's Center for Cyber Security Studies, says the pace of innovation is exciting, but every time a new technological innovation emerges, there is a new set of holes in their network.[51] This reality means as technology evolves, the United States must reassess threats and vulnerabilities. Due to the demand from the military and capabilities of the devices, the U.S. military is heading in this direction regardless of continual efforts to mitigate risks. Given the holes, this would mean operational art would remain a reality regardless of the impact of PIT.

IMPLICATIONS, FOG AND FRICTION

Some of the threats and challenges faced by mobile device users include the loss of device, data recovery, collection over the air, vulnerability applications, malware, and tracking. As with any military program, especially when technology is involved there is always the anxiety of spiraling costs and requirements. Any device that will log and display the locations of an entire combat squad needs to have the network carrying that data as protected as possible. Security measures for smartphone networks are a concern for those in combat situations and for officials at the U.S. DoD who often communicate potentially sensitive information to those in the field.[52]

The huge memory capacities of some of the new smart devices, users' general lack of knowledge about how smartphones and tablets work, and the potential of having devices compromised are also concerns of the DoD.[53] The different operating systems available on the market today for mobile devices push out patches and updates to change each device. Users must weigh the risk associated of this vulnerability.[54] The process of uploading of pictures instantly provides digital footprints displaying the geographic location of the devices to others on the net and potentially compromising the location of the troops and the mission. Other concerns question if the data on the device is at risk; should communications personnel encrypt a device prior to working on it? What measures to employ if a device is physically lost? The apps utilized on these devices must be safe and secure.[55]

The ubiquity and affordability of cell phones in the hands of hackers and adversaries create a considerable threat.[56] An iPhone or iPad can trigger an improvised explosive device simply by knowing the mobile identity number.[57] With the connectivity and security concerns addressed, the U.S. military should be able to utilize the mobile devises as intended. Even as these devices integrate into operations, the U.S. military does not speak to the impact on the fog of war and how it relates to operational art.

The military is moving forward with smartphone platforms and its usage began rapidly in the year 2011. It remains unclear whether to zero in on one particular smartphone, either a pre-existing commercial model or a modified military version, for use across the force.[58] According to the U.S. 3rd BCT Army battalion commander, Colonel Sam Whitehurst, the capabilities placed in his battalion tactical operations center while in Iraq in 2009 are now being put down at the soldier level.[59] New digitized and networked technologies collapse distance, merge fact and fiction, and generate virtual worlds.[60]

Additional time is required for the military leadership at the Pentagon to thoroughly assess and understand the smart phone and tablet devices along with the gains and associated flaws that come along with them. Charlie Miller is a cybersecurity specialist and a researcher for the computer security firm Accuvant Labs. He is the first person to hijack both an iPhone and an Android phone. He worked with Apple and Google to identify and advise of security holes discovered. He indicated there are many other security holes in addition to the ones he exposed. He also expresses that probably a million people have looked at the code currently used to hijack the iPhone and Android and hackers know it works. Miller suggests, "If the new technology lets you do your job better, there's a tradeoff where you have to weigh the risk against doing the job better."[61] The U.S. military will have to determine the threshold on what is the line between security, desire to become more efficient, and acceptable risk.

Military members continuously pursue adequate and relevant information about their operational environment. Commanders depend on having the right information at the right time to be mission effective and save the lives of frontline troops. Friction relates to the physical impediments to military actions inherent in military operations. The Joint Vision 2020 lists the following as sources or components of friction: 1. effects of danger and exertion, 2. existence of uncertainty and chance, 3. unpredictable actions of other actors, 4. frailties of machines and information, and 5. humans.[62]

These concerns are not new. Carl von Clausewitz describes what some have called the fog of war, which is the confusion arising from absent, misleading or contradictory intelligence. The elimination of that fog provides a clearer and more useful understanding of friction Clausewitz's describes. It helps to remove the uncertainty and the intangible stresses of military command to their rightful centrality in war.[63] Participants in military operations experience the

effects of the fog of war, culminating into a lack of situational awareness that causes less than desirable outcomes.[64] This is especially true for troops assessing Intelligence and Information Operations (IO) details because of traditional approaches to gathering and processing data.[65] Networked PIT devices provide front line troops with relevant decision-making data about situational awareness issues, intelligence, and information operations. Even though troops accessing intelligence and information operations details may experience the fog of war, PIT devices will help these individuals gain situational awareness. In each case and across the military spectrum, the fog of war is inevitable. The side that can reduce that fog the most will benefit militarily. This pursuit of curbing friction makes the operational art of war a difficult challenge.

Major General Michael Basla, in his article, "*The Cyber Domain: How it is Changing the Warfighter?,"* talks of a young U.S. soldier preferring to leave his M-16 rifle in the barracks than enter into battle without his information sources. This is alluding to the fact the soldier wants to remain connected and be informationally aware on the battlefield to ensure his safety and keep him and his peers alive. This change in attitude reflects the new genre of warfighter and the importance of information to the survival of soldiers on the battlefield. Information means a greater chance of success by reducing the "fog of war" for the commander and the private on the front line. Trusted information can provide a significantly clearer picture of enemy strength, position, and threat to friendly forces. Warfighters require adequate and trusted information to maintain confidence and ensure no hesitation in taking action when required. By seizing advantage of the new PIT devices and the entrepreneurial spirit of the tech savvy warriors, the U.S. military has the best opportunity to gain a form of battlefield superiority in the

area of operations.[66] This gain stems mainly from the chance to eliminate the fog of war from the battlefield to an unprecedented degree.

The age of digital revolution has emerged and the United States military must acclimate and adopt information technology to remain the strongest military in the world. The U.S. military is in a continuous cyber war mode and must take the necessary steps, and precautions, to capitalize on this cyber reality. The examples in this paper prove how the military is in a computerized world and incorporating mobile technology to remain an effective, resilient force. While the military is working hard to embrace technology and further utilize these mobile devices in each service's operations, there will always be the fog and friction in war, the chief reason to adopt the technology.

Some U.S. military officers grapple with how the United States might fight future wars and suggest that foreseeable advances in surveillance and information technologies will sufficiently lift the fog of war to enable future American commanders to "see and understand everything on a battlefield."[67] These military officers are not alone in this belief. During a 6-month assessment conducted by a Washington policy center on the prospects for a "military technical revolution" (MTR), participants concluded, "the MTR promises, more than precision attacks or laser beams. It promises to imbue the information loop with near-perfect clarity and accuracy, to reduce its operation to a matter of minutes or seconds, and perhaps most important of all—to deny it in its entirety to the enemy."[68]

Effective exploitation of the advances in technologies and information systems has the potential to eliminate the fog of war to an unprecedented degree while simultaneously confining one's opponent behind a wall of ignorance. This view suggests that the presumption is that technological advances will allow one to know everything happening in the battlespace. .[69]

These thinkers probably overstate things, at least at present. Still, the implications are important to consider. With a secure environment for the mobile devices to operate in, the U.S. military will have products that will provide a 360 degree situational awareness level of the pertinent and adequate information that assists the warfighter when they require it the most.

With a greater degree of communication and information capability from the strategic to the tactical levels, the U.S. military will see a lifting of the fog of war. This raises the key question of this MMS. As more information is readily available to the warfighter on the battlefield, the need to conceptualize an operational level of war appears to be diminishing. There remains a need for an operational level of war involving joint (interagency, coalition, etc.) operations across domains. However, the fact is, implementation of PIT devices brings about the benefit of having strategic level decision making linked to tactical action like never before. As the operational art fades in this respect, a more streamlined process may emerge which could become a mainstay of military action.

The operational level of warfare will soon flow through mobile devices designed to communicate strategic plans and to ensure tactical implementation leading to mission success. Although the PIT devices bring about some levels of risk in the security and connectivity arenas, they provide a level of information to the warfighter that the military was incapable of providing in previous times. The rewards far outweigh the risks of deploying PIT devices into the area of operations. Cyber reality and the mobility technological revolution have arrived. One must adapt to it or be at serious disadvantages in the next war. The unprecedented communications allowing the warfighter to gain situational awareness is moving in a forward direction in preparing U.S. troops for the next war. A revolution in the operational art of war is not far behind.

ENDNOTES

---

[1] Army, "Mobile Device Management," *Signal.army.mil*, Summer 2012, http://www.signal.army.mil/ArmyCommunicator/2012/Vol37/No2/Mobile_Device_Management.pdf (accessed January 13, 2013).

[2] Army, "Evaluating mobile technology for warfighter use challenging," *Army.mil*, October 31, 2012, http://www.army.mil/article/90298/Evaluating_mobile_technology_ for_warfighter_use_ challenging/ (accessed January 13, 2013).

[3] Army, "Evaluating mobile technology for warfighter use challenging."

[4] Department of Defense, "defense.gov," May 2012, http://www.defense.gov/news/dodmobilitystrategy.pdf (accessed December 29, 2012), Page i.

[5] Department of Defense, "defense.gov," Page i.

[6] Department of Defense, "defense.gov," Page i.

[7] Department of Defense, "Cyber Pro Discusses Mobile Network Security Challenges," *defense.gov*, December 5, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118715 (accessed January 2, 2013).

[8] Department of Defense, "defense.gov," Page i.

[9] Brad Reed, "Military apps putting iPhone in the battlefield," *Network World*, April 14, 2011, http://www.networkworld.com/news/2011/041411-military-iphone-apps.html (accessed March 1, 2013).

[10] Anna Mulrine, "How an iPhone revolution could turn the Army upside-down," *The Christian Science Monitor*, November 15, 2011, http://www.csmonitor.com/USA/Military/2011/1115/ How-an-iPhone-revolution-could-turn-the-Army-upside-down (accessed March 1, 2013).

[11] Department of Defense, "defense.gov," Page ii.

[12] William F. Owen, "The Operational Level of War Does Not Exist," *Military Operations*, 2012: 17-20.

[13] Huba Wass de Czege, "Thinking and Acting Like an Early Explorer: Operational Art is Not a Level of War," *Small Wars Journal*, 2011**,** pg 4.

[14] Barbara Starr, "The highest ranking iPad in the military," *CNN Security Clearance Blog.* October 7, 2011, http://security.blogs.cnn.com/2011/10/07/the-highest-ranking-ipad-in-the-military/ (accessed January 19, 2013).

[15] Rebecca Boyle, "The Air Force is Buying iPads To Replace Pilots' Books and Maps," *POPSCI,* February 9, 2012, http://www.popsci.com/technology/article/2012-02/air-force-buying-ipads-replace-flight-bags (accessed January 19, 2013).

[16] Boyle, "The Air Force is Buying iPads To Replace Pilots' Books and Maps."

[17] Lory, "Thanks to the iPad, The Air Force is Saving More Than $5 Million Per Year," *Padgadget.com,* September 28, 2012, http://www.padgadget.com/2012/09/28/thanks-to-the-ipad-the-air-force-is-saving-more-than-5-million-per-year/ (accessed January 20, 2013).

[18] Brendan McGarry, "Air Force Gives $9 Million Award for as Many as 18,000 IPads," Bloomberg.com, March 2, 2012, http://www.bloomberg.com/news/2012-03-02/air-force-grants-9-million-award-for-as-many-as-18-000-ipad2s.html (accessed January 20, 2013).

[19] Andrew Tilghman, "iPhone, Android to be OK'd for official use," *Marine Times,* December 1, 2011, http://www.marinecorpstimes.com/news/2011/12/military-iphone-android-to-be-okd-for-official-use-120111w/ (accessed January 19, 2013).

[20] Ben Kohlmann, "Disruptive Thinking and How the iPad Changed Close Air Support in Afghanistan," *Disruptive Thinkers,* May 14, 2012, http://disruptivethinkers.blogspot.com /2012/05/lessons-in-how-ipad-changed-close-air.html (accessed January 19, 2013).

[21] Tilghman. "iPhone, Android to be OK'd for official use."

[22] Tilghman. "iPhone, Android to be OK'd for official use."

[23] Colin Kelly, "FedTech Interview: Marine Corps CIO Brig. Gen. Kevin Nally," *FedTech,* August 7, 2012. http://www.fedtechmagazine.com/article/2012/08/fedtech-interview-marine-corps-cio-brig-gen-kevin-nally (accessed January 20, 2013).

[24] Colin Kelly, "FedTech Interview: Marine Corps CIO Brig. Gen. Kevin Nally.**"**

[25] Tilghman. "iPhone, Android to be OK'd for official use."

[26] Tilghman. "iPhone, Android to be OK'd for official use."

[27] Dan Nosowitz, "U.S. Army Visits Apple HQ to Discuss Uses for the iPad (Other Than Saving the Publishing Industry)," *Fast Company,* March 25, 2010. http://www.fastcompany.com/

1596878/us-army-visits-apple-hq-discuss-uses-ipad-other-saving-publishing-industry (accessed January 20, 2013).

[28] Tilghman, "iPhone, Android to be OK'd for official use."

[29] "Navy Uses iPad-type tablet to Conduct a Ship's Readiness Assessment," *Business and Mobile.com,* August 14, 2012, http://www.businessandmobile.com/navy-uses-ipad-type-tablet-to-conduct-a-ships-readiness-assessment/ (accessed January 20, 2013).

[30] DACS, *Use of Mobile Technology for Information Collection and Dissemination,* A DACS Technology Assessment Report, Utica, NY: Prepared for the Defense Technical Information Center, 2012.

[31] Jared Serbu, "Exclusive: Coast Guard first to OK iPhone, Android on network," *Federal News Radio.com,* August 10, 2011, http://www.federalnewsradio.com/239/2490957/Exclusive-Coast-Guard-first-to-OK-iPhone-Android-on-network (accessed January 20, 2013).

[32] It is interesting to note that the DoD has started to integrate chemical and biological sensors into mobile devices. Researchers from the University of California, San Diego have developed a miniature chemical sensor that can detect harmful gas in the air and automatically send the information regarding the type and transmitting range of the gas. The chemical sensor is a silicon chip with hundreds of independent miniature sensors. These can identify the molecule of specific toxic gas and report on it. DACS, *Use of Mobile Technology for Information Collection and Dissemination*.

[33] Eric Beidel, Sandra I. Erwin and Stew Magnuson, "10 Technologies the U.S. Military Will Need For the Next War," *NDIA's Business and Technology Magazine,* November 2011, http://www.nationaldefensemagazine.org/archive/2011/November/Pages/10TechnologiestheUSMilitaryWillNeedFortheNextWar.aspx (accessed January 19, 2013).

[34] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies.**"**

[35] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies.**"**

[36] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies.**"**

[37] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies.**"**

[38] Ned Potter, "Army's New Secret Weapon: the iPad," *ABC News,* September 27, 2011, http://abcnews.go.com/Technology/smartphones-military-pentagon-tests-apps-androids-iphones-ipads/story?id=14615595 (accessed January 19, 2013).

[39] Boyle, "The Air Force is Buying iPads To Replace Pilots' Books and Maps."

[40] Barbara Starr, "The highest ranking iPad in the military," *CNN Security Clearance Blog*, October 7, 2011, http://security.blogs.cnn.com/2011/10/07/the-highest-ranking-ipad-in-the-military/ (accessed January 19, 2013).

[41] Verizon, *Verizon Global Services Coverage Map*, 2013, http://verizon.p0b.cellmaps.com/1.2/tiles/1.0.0/intl_verizon_all/5/14/14.png (accessed February 23, 2013).

[42] "Boost for Smartphone and Tablet Connectivity on board as Vizada XChange goes mobile," *Astrium*, September 4, 2012, http://www.vizada.com/1896_1&page_id=9916 (accessed February 23, 2013); *Thuraya XT-DUAL Satellite / GSM Phone.* n.d. http://www.sattransusa.com/thu-pho-xtdu.html (accessed February 23, 2013).

[43] "PM WIN-T," *U.S. Army PEOC3T.* n.d. http://peoc3t.army.mil/wint/inc3.php (accessed February 23, 2013).

[44] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies."

[45] Greg Crowe, *Army Puts Lightweight Battery Chargers Into The Field*, December 3, 2012, http://gcn.com/blogs/mobile/2012/12/army-lightweight-battery-chargers.aspx (accessed February 24, 2013); Paul McCloskey, *For Soldiers, A Wearable Data Hub Managed Via Smart Phone*, February 13, 2013, http://gcn.com/articles/2013/02/13/wearable-data-hub-managed-via-smart-phone-for-soldiers.aspx?sc_lang=en (accessed February 24, 2013); Paul Mah, "Recharge Your Smartphone, Tablet on the Go With These 3 Battery Packs," *CIO.* September 26, 2012, http://blogs.cio.com/peripherals/17431/recharge-your-smartphone-tablet-go-these-3-battery-packs (accessed February 24, 2013).

[46] Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies.**"**

[47] Tilghman, "iPhone, Android to be OK'd for official use."

[48] Andrew Tilghman, "Troops can't use personal smartphones for work, Pentagon says, " USA Today, Tech, September 28, 2012, http://www.usatoday.com/story/tech/2012/09/28/troops-cant-use-personal-smartphones-for-work-pentagon-says/1601335/ (accessed January 20, 2013).

[49] Nigam Arora, "Thank Goodness Air Force Dropped iPad Purchase," Forbes.com, March 1, 2012, http://www.forbes.com/sites/greatspeculations/2012/03/01/thank-goodness-air-force-dropped-ipad-purchase/ (accessed January 20, 2013).

[50] Lory, "Thanks to the iPad, The Air Force is Saving More Than $5 Million Per Year," *Padgadget.com,* September 28, 2012, http://www.padgadget.com/2012/09/28/thanks-to-the-ipad-the-air-force-is-saving-more-than-5-million-per-year/ (accessed January 20, 2013).

[51] Chris Carroll, "iPads, iPhones and other top mobile devices still banned from DOD networks," *Stars and Stripes.com,* October 5, 2011, http://www.stripes.com/news/ipads-iphones-and-other-top-mobile-devices-still-banned-from-dod-networks-1.156997 (accessed January 20, 2013).

[52] Net Resources International, "Battlefield Smartphones Receive a Ringing Endorsement," *Army-Technology.com,* July 31, 2012, http://www.army-technology.com/features /featurebattlefield-smartphones-endorsement-technology (accessed January 1, 2013).

[53] Defense.gov, "DOD Works to Boost Smartphone Security," *U.S. Department of Defense.* August 29, 2011, http://www.defense.gov/news/newsarticle.aspx?id=65182 (accessed January 2, 2013).

[54] Defense.gov, "DOD Works to Boost Smartphone Security."

[55] Defense.gov, "DOD Works to Boost Smartphone Security."

[56] Department of Defense, "Cyber Pro Discusses Mobile Network Security Challenges," *defense.gov,* December 5, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118715 (accessed January 2, 2013).

[57] Department of Defense, "Cyber Pro Discusses Mobile Network Security Challenges."

[58] Tilghman. "iPhone, Android to be OK'd for official use."

[59] Claire Heininger, "Army Rolls Out New Network Approach," *Military Information Technology,* December 2012, http://www.military-training-technology.com/mit-home/460-mit-2012-volume-16-issue-11-december/6272-army-rolls-out-new-network-approach.html (accessed January 18, 2013).

[60] James Der Derian, "Information Technology, War, and Peace Project," *Watson Institute for International Studies, Brown University,* n.d. http://www.watsoninstitute.org/project_ detail.cfm?id=1 (accessed January 19, 2013).

[61] Chris Carroll, "iPads, iPhones and other top mobile devices still banned from DOD networks."

[62] United States Department of Defense, *Joint Vision 2020,* U.S. Government Report, Washington, DC: U.S. Government Printing Office, 2000.

[63] Eugenia C. Kiesling, "On War Without the Fog," *Military Review*, 2001: p. 85.

[64] Fog of war, January 25, 2013, http://en.wikipedia.org/wiki/Fog_of_war#cite_ref-2 (accessed March 13, 2013).

[65] Victor M. Rosello, "Clausewitz's Contempt for Intelligence," *DTIC.MIL.* 1991, p 112 http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527999, (accessed March 19, 2013).

[66] Major General Michael J. Basla, "The Cyber Domain: How is it Changing the Warfigher?" *Rusi Defense Systems*, 2009: 67-70.

[67] Barry D. Watts, "Clausewitzian Friction and Future War," Clausewitz.com, August 2004, http://www.clausewitz.com/readings/Watts-Friction3.pdf#zoom=100 (accessed January 20, 2013), Pg 2, para 2.

[68] Watts, "Clausewitzian Friction and Future War."

[69] Watts, "Clausewitzian Friction and Future War."

BIBLIOGRAPHY

Army. "Evaluating mobile technology for warfighter use challenging." *Army.mil.* October 31, 2012. http://www.army.mil/article/90298/Evaluating_mobile_technology_for_warfighter_use_challenging/ (accessed January 13, 2013).

Army. "Mobile Device Management." *Signal.army.mil.* Summer 2012. http://www.signal.army.mil/ArmyCommunicator/2012/Vol37/No2/Mobile_Device_Management.pdf (accessed January 13, 2013).

Arora, Nigam. "Thank Goodness Air Force Dropped iPad Purchase." Forbes.com. March 1, 2012. http://www.forbes.com/sites/greatspeculations/2012/03/01/thank-goodness-air-force-dropped-ipad-purchase/ (accessed January 20, 2013).

Basla, Major General Michael J. "The Cyber Domain: How is it Changing the Warfigher?" *Rusi Defense Systems*, 2009: 67-70.

Eric Beidel, Sandra I. Erwin and Stew Magnuson. "10 Technologies the U.S. Military Will Need For the Next War." *NDIA's Business and Technology Magazine.* November 2011. http://www.nationaldefensemagazine.org/archive/2011/November/Pages/10TechnologiestheUSMilitaryWillNeedFortheNextWar.aspx (accessed January 19, 2013).

Boyle, Rebecca. "The Air Force is Buying iPads To Replace Pilots' Books and Maps." *POPSCI.* February 9, 2012. http://www.popsci.com/technology/article/2012-02/air-force-buying-ipads-replace-flight-bags (accessed January 19, 2013).

Carroll, Chris. "iPads, iPhones and other top mobile devices still banned from DOD networks." *Stars and Stripes.com.* October 5, 2011. http://www.stripes.com/news/ipads-iphones-and-other-top-mobile-devices-still-banned-from-dod-networks-1.156997 (accessed January 20, 2013).

Caudle, Daryl L. "Decision-Making Uncertainty and the use of Force in Cyberspace: A Phenomenological Study of Military Officers." D.M., University of Phoenix, 2010.

Corbin, Kenneth. "CIO." *Iran Is a More Volatile Cyber Threat to U.S. than China or Russia.* March 21, 2013. http://www.cio.com/article/730589/Iran_Is_a_More_Volatile_Cyber_Threat_to_U.S._than_China_or_Russia (accessed March 22, 2013).

Czege, Huba Wass de. "Thinking and Acting Like an Early Explorer: Operational Art is Not a Level of War." *Small Wars Journal*, 2011.

DACS. *Use of Mobile Technology for Information Collection and Dissemination.* A DACS Technology Assessment Report, Utica, NY: Prepared for the Defense Technical Information Center, 2012.

Defense Systems. " The future of military comms on the battlefield." *Defense Systems* . January 13, 2013. http://defensesystems.com/articles/2012/02/08/cover-story-military-communications-technologies.aspx (accessed January 14, 2013).

Department of Defense. "defense.gov." May 2012. http://www.defense.gov/news/dodmobilitystrategy.pdf (accessed December 29, 2012).

Derian, James Der. "Information Technology, War, and Peace Project." *Watson Institute for International Studies, Brown University.* n.d. http://www.watsoninstitute.org/project_ detail.cfm?id=1 (accessed January 19, 2013).

Erwin, Sandra I. "Army Under Pressure to Bring Broadband to the Battlefield." National Defense 95, no. 682 (Sep 2010): 40-44.

Fischer, Carl E. "The Impact of Automated Cognitive Assistants on Situational Awareness in the Brigade Combat Team." Ed.D., University of Kansas, 2010.

Fox, Wesley. "Switch on the Digitised Battlespace." Armada International 35, no. 5 (Oct/Nov 2011): 1-4,6,8,10,12,14,16,18,20.

George, Larry. "Issues in the Non-Integration of Information Operations in Military Decision Making." D.Sc., Robert Morris University, 2008.

Heininger, Claire. "Army Rolls Out New Network Approach." *Military Information Technology.* December 2012. http://www.military-training-technology.com/mit-home/460-mit-2012-volume-16-issue-11-december/6272-army-rolls-out-new-network-approach.html (accessed January 18, 2013).

Howard, Courtney E. "Achieving the Information Advantage." Military & Aerospace Electronics 21, no. 7 (Jul 2010): 24-32.

"Portable Flash Drives Likely to Return to the Battlefield." Military & Aerospace Electronics 20, no. 12 (Dec 2009): 11-12.

Huhtinen, Aki-Mauri. 2010. The Way of Warfare in Three Possible Worlds - from Art of War to Information Warfare. , http://search.proquest.com/docview/869506985?accountid=14746.

Keller, John. "Data Dissemination and Validation on the Battlefield." Military & Aerospace Electronics 22, no. 9 (Sep 2011): 28-36.

Kelly, Colin. "FedTech Interview: Marine Corps CIO Brig. Gen. Kevin Nally." *FedTech.* August 7, 2012. http://www.fedtechmagazine.com/article/2012/08/fedtech-interview-marine-corps-cio-brig-gen-kevin-nally (accessed January 20, 2013).

Kiesling, Eugenia C. "On War Without the Fog." *Military Review*, 2001: 85-87.

Kohlmann, Ben. "Disruptive Thinking and How the iPad Changed Close Air Support in Afghanistan." *Disruptive Thinkers.* May 14, 2012. http://disruptivethinkers.blogspot.com/2012/05/lessons-in-how-ipad-changed-close-air.html (accessed January 19, 2013).

Lawlor, Maryann. "Cell Phones on the Front Lines." Signal 64, no. 3 (Nov 2009): 19-22.

Lory. "Thanks to the iPad, The Air Force is Saving More Than $5 Million Per Year." *Padgadget.com.* September 28, 2012. http://www.padgadget.com/2012/09/28/thanks-to-the-ipad-the-air-force-is-saving-more-than-5-million-per-year/ (accessed January 20, 2013).

McGarry, Brendan. "Air Force Gives $9 Million Award for as Many as 18,000 IPads." *Bloomberg.com.* March 2, 2012. http://www.bloomberg.com/news/2012-03-02/air-force-grants-9-million-award-for-as-many-as-18-000-ipad2s.html (accessed January 20, 2013)

Moellinger, Terry. "To Think Different: The Unexpected Consequences of Personal Computer and Internet use." Ph.D., The University of Oklahoma, 2010.

Mulrine, Anna. "How an iPhone revolution could turn the Army upside-down." *The Christian Science Monitor.* November 15, 2011. http://www.csmonitor.com/USA/Military/2011/1115/How-an-iPhone-revolution-could-turn-the-Army-upside-down (accessed March 1, 2013).

"Navy Uses iPad-type tablet to Conduct a Ship's Readiness Assessment." *Business and Mobile.com.* August 14, 2012. http://www.businessandmobile.com/navy-uses-ipad-type-tablet-to-conduct-a-ships-readiness-assessment/ (accessed January 20, 2013).

Nosowitz, Dan. "U.S. Army Visits Apple HQ to Discuss Uses for the iPad (Other Than Saving the Publishing Industry)." *Fast Company.* March 25, 2010. http://www.fastcompany.com/1596878/us-army-visits-apple-hq-discuss-uses-ipad-other-saving-publishing-industry (accessed January 20, 2013).

Owen, William F. "The Operational Level of War Does Not Exist." *Military Operations*, 2012: 17-20.

Peterson, Patrick. "Harris Corp.'s ' Falcon Fighter Gives Troops Digital Technology." Florida Today, Mar 27, 2011. http://search.proquest.com/docview/858714625?accountid=14746.

Potter, Ned. "Army's New Secret Weapon: the iPad." *ABC News.* September 27, 2011. http://abcnews.go.com/Technology/smartphones-military-pentagon-tests-apps-androids-iphones-ipads/story?id=14615595 (accessed January 19, 2013).

Reed, Brad. "Military apps putting iPhone in the battlefield." *Network World.* April 14, 2011. http://www.networkworld.com/news/2011/041411-military-iphone-apps.html (accessed March 1, 2013).

Schwartz, Mathew J. "Uncertain State Of Cyber War." Information Week (Government). January 21, 2013. http://www.informationweek.com/government/security/uncertain-state-of-cyber-war/240146543 (accessed January 22, 2013).

Smith, David J. "Russian Cyber Operations." *Potomac Institute.* July 2012. http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf (accessed March 22, 2013).

Starr, Barbara. "The highest ranking iPad in the military." *CNN Security Clearance Blog.* October 7, 2011. http://security.blogs.cnn.com/2011/10/07/the-highest-ranking-ipad-in-the-military/ (accessed January 19, 2013).

Strickland, Jonathan. "Is Cyber Warfare Coming." How Stuff Works. n.d. http://computer.howstuffworks.com/cyberwar1.htm (accessed January 20, 2013).

Tilghman, Andrew. "iPhone, Android to be OK'd for official use." *Marine Times.* December 1, 2011. http://www.marinecorpstimes.com/news/2011/12/military-iphone-android-to-be-okd-for-official-use-120111w/ (accessed January 19, 2013).

Tilghman, Andrew. "Troops can't use personal smartphones for work, Pentagon says." USA Today, Tech. September 28, 2012. http://www.usatoday.com/story/tech/2012/09/28/troops-cant-use-personal-smartphones-for-work-pentagon-says/1601335/ (accessed January 20, 2013).

Tsirlis, Christopher S. "Networking Communicates the Kill." United States Naval Institute. Proceedings 135, no. 7 (Jul 2009): 76-78.

U.S. Government. "Digital Government." *Whitehouse.gov.* n.d. http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html (accessed January 12, 2013)

Windrem, Robert. "Expert: U.S. in Cyberwar Arms Race with China, Russia." *NBC News.com.* February 20, 2013. http://openchannel.nbcnews.com/_news/2013/02/20/17022378-expert-us-in-cyberwar-arms-race-with-china-russia?lite (accessed March 22, 2013).

Zieniewicz, Matthew J., and Eric Goodman. "Battlefield Information Concepts for the Highly Mobile Warrior." Army AL & T (Mar/Apr 2003): 23-25.