REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
29-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

Command and Control in Korea: are we prepared to operate in a communications degraded environment.

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Hooks, Jr., John, A., Major, USMC

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. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

Our communications systems and the way we train are based off of open, flat, and desert type operations. Contrary to our customs, Korea's restrictive enviornment presents complex operational challenges. The typography of this environment is very different compated to where U.S. forces have operated over the last decade. This contrasting environment limits the capabilities and types of communication systems available to use throughout the peninsula for command and control. The focus to solve this issue has been on satellite communications. However, military forces cannot rely solely on this type of technology. With the current capability that our enemy possesses to jam or interrupt frequencies of old satellites and generate levels of saturation, there is not enough bandwidth for forces; and while commanders continue to stress a need for "more" data. Another issue is the joint acquisitions process which is extremely flawed. This process is too protracted to keep up with the pace and production of technology today. The last factor that has complicated all these areas is the arrival of cyber. Cyber has added complexity to the existing C2 issues greatly. If the U.S. military intends to improve its C2 capability and capacity these issues need to be resolved. The U.S. military needs to find a way to correct these issues because the implications that follow can affect joint interoperability and joint operations if we have to operate in the Korean environment.

15. SUBJECT TERMS

Command and Control (C2), Command, Control, Communications, Computers, and Intelligence (C4I), Korea, and Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Marine Corps University/Command a
Unclass	Unclass	Unclass	UU	41	**19b. TELEPHONE 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

Command and Control in Korea: Are we prepared to operate in a communications degraded environment?

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major John A. Hooks Jr.
USMC CG 12

AY 2014-15

Mentor and Oral Defense Committee Member:
Approved: Major Flynn
Date: 4/6/15

Oral Defense Committee Member:
Approved:
Date: 4/14/2015

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER UNITED STATES GOVERNMENTAL AGENCY.

REFERENCES TO THIS STUDY SHOULD INCLUDE THE FORGOING STATEMENT.

Executive Summary

Title: Command and Control in Korea: are we prepared to operate in a communications degraded environment.

Author: Major John Hooks, United States Marine Corps

Thesis: Communications technology has improved; however, the age old command and control (C2) issues have not been cured. The government's inability to procure emerging commercial technology reduces the command and control ability of US forces in unique areas such as the Korean Peninsula. That environment degrades mobility and the ability to effectively communicate leading to possible security concerns.

Discussion: Our communication systems and the way we train are based off of open, flat, and desert type operations. Contrary to our customs, Korea's restrictive environment presents complex operational challenges. The typography of this environment is very different compared to where U.S. forces have operated over the last decade. This contrasting environment limits the capabilities and types of communication systems available to use throughout the peninsula for command and control.

Recently, the focus to solve this issue has been on satellite communications. However, military forces cannot rely solely on this type of technology. With the current capability that our enemy possesses to jam or interrupt frequencies of old satellites and generate levels of saturation, there is not enough bandwidth for forces; and while commanders continue to stress a need for "more" data. The communication systems that are organic to each U.S. service component are proprietary in nature and this limits what systems will be developed and procured. This shortcoming causes a problem with interoperability between U.S forces as well as coalition forces. There are a vast amount of commercial technologies that exist today to aid this issue. The commercial industry leverages state of the art technology versus decade old technology that the US military employs. In the services, every major end-item has to be a program of record, which slows down the procurement cycle and reduces capabilities. This means that each service desires to procure its own "unique" system, instead of making a unified effort to ensure compatibility. Another issue is the joint acquisitions process which is extremely flawed. This process is too protracted to keep up with the pace and production of technology today. As long as the military continues to conduct business this way, the military will never catch up. The last factor that has complicated all these areas is the arrival of cyber. Cyber has added complexity to the existing C2 issues greatly. If the U.S. military intends to improve its C2 capability and capacity these issues need to be resolved. The U.S. military needs to find a way to correct these issues because the implications that follow can affect joint interoperability and joint operations if we have to operate in this environment.

Table of Contents

Page

INTRODUCTION

We operate in a combined command where two languages, two military structures and two cultures work side-by-side. Fundamentally, we train "joint and combined" every day. We strengthen the ROK-US alliance as we work and train together as one team.

—General John H. Tilelli, Jr.
Commander-in-Chief, Combined Forces Command, 1996-1999

Throughout history, command and control (C2) has plagued a commander's ability to effectively control forces in mountainous and very dense and heavily vegetated environments. The bid for success within any operation rests in large part on the commander's ability to command and control his or her forces. Command and control can be defined as the means that a commander recognizes what needs to be done, and sees that the appropriate actions are taken by his or her forces. The environment of the Korean peninsula challenges this requirement in unique ways. As U.S. forces pivot to the Pacific, more forces will be deployed to South Korea and other countries within Asia in order to serve as a deterrent and to posture for any potential threat from North Korea. As a part of the National Security Strategy (NSS), the current administration's goal is to tackle the challenges of the peninsula as a unified effort with Japan and South Korea, who are important leaders in East Asia. Both countries play a critical role in maintaining global security within the region. This unified effort is also a key for the U.S. military's sustained presence in the region.

U.S. forces currently use communication platforms, like Network on the Move (NOTM), that do not operate well on the Korean Peninsula due to the restricted frequencies. Many platforms that exist in the U.S. inventory do not fully integrate with the Republic of Korea (ROK) forces. This presents the U.S. leadership with unique issues to command and control forces, with obvious serious implications if American and ROK

units cannot communicate due to a lack integrated platforms.

Communication technology has improved. Data systems have increased processing speeds, radios have been reduced in size and weight, single radios can operate multiple waveforms simultaneously, and data and radio networks can be tied together. However, command and control issues persist on the Korean Peninsula. The US government's inability to procure emerging commercial technology reduces the deployed forces' ability to command and control in unique areas such as the Korean Peninsula, where the environment degrades the ability to effectively communicate. This paper discusses the current problem and threat, the impact of technology, limitations of current systems, broken and slow acquisitions process, and potential solutions to this issue. When the bad news is considered, the way forward to overcoming this C2 issue due to terrain, and doing so via advanced communication technology, becomes clear and therefore badly needed.

BACKGROUND

It has been more than 50 years since an armistice ended the fighting in the Korean War in 1953. But Korea is still one of the countries that have yet to extinguish all the flames of the Cold War. North Korea still remains a substantial threat to South Korea since that authoritarian state possesses one of the world largest armies. North Korea's offensive posture, its development of ballistic missiles, lethal special operations forces, and weapons of mass destruction (WMD), cause the Korean peninsula to be very volatile for US forces and its allies.[1]

In the first few decades of the 2000s, the dilemma on the Korean peninsula has become more complex. The once traditional conventional threat is not the only concern.

Now that North Korea has focused more on forms of asymmetric negation, non-linear security, and its recent development of cyber-related offensive capabilities, this creates new and complex issues that have to be dealt with. The current debate that arises is whether U.S. forces are equipped with the proper command, control, communications, computers and intelligence (C4I) capabilities to operate in tandem with its sister ROK forces and rapidly respond to a North Korean invasion of South Korea. Are U.S. Forces capable of establishing information dominance that will enable the accomplishment of operational goals and objectives? Information dominance is defined as, "the operational advantage gained from fully integrating [U.S. force's] information functions, capabilities, and resources to optimize decision making and maximize warfighting effects."[2] Information dominance provides three capabilities: 1) Assured C2, 2) Battlespace Awareness, and 3) Integrated Fires. In some respect, U.S. forces could be ready to handle the unique C2 issues that Korea presents only with ample time and the ability to leverage commercial technology.

LITERATURE REVIEW

This paper looks at the C2 challenges in Korea as well as at how cyber realities are creating new C2 challenges in Korea that can potentially destabilize the peninsula by ironically, solving those very issues. Joint Publication (JP) 1, defines command as the "authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment."[3] ADP 6-0 defines control as "the regulation of forces and warfighting functions to accomplish the mission in accordance with the commander's intent."[4] There are many actions that contribute to successful command and control, which includes planning, training, and education. Planning, whether hasty or deliberate,

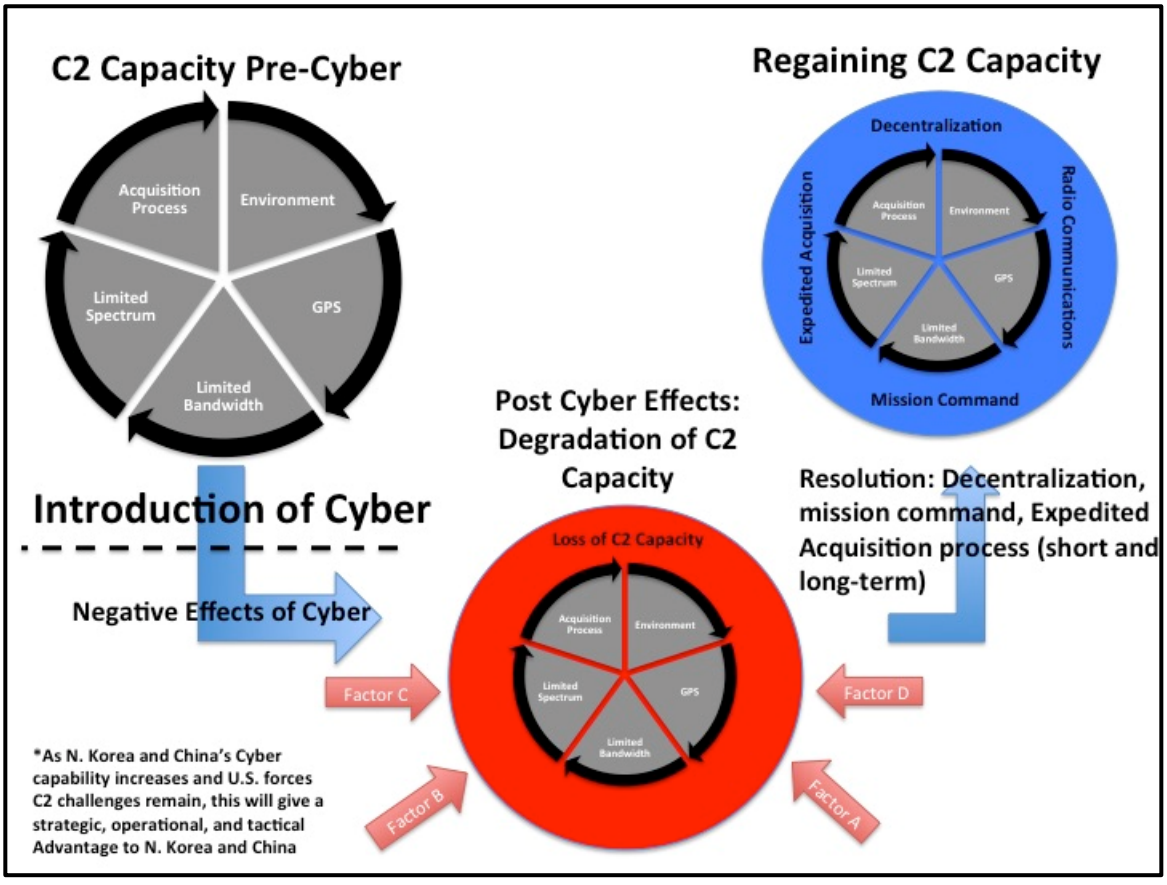
provides a foundation of shared understanding. Effective training and education, which make it more likely that subordinates will take the proper actions in combat, help ensure the success of command and control.[5] A commander bases the level of flexibility and coordination of activities and policies on an operational environment.[6]

C2 within the military is critical and utilized at all levels. These levels are divided into three categories: commanders, staff, and various entities (FDC, etc.). Everyone at each level has to be prepared to fight in event of a crisis. This can not be accomplished without C2. All of these users expect for C2 to operate so plans can be issued, direction given, and so that operational orders can be executed. The Korean language is extremely difficult and this difficultly adds to the complexity of C2. Korean officers take English growing up, however, American officers get no specialized language training prior to assuming duties on the peninsula.

Even with the vast amount of technology that exist today, challenges of C2 still exist for military forces. These challenges are further complicated in areas such as Korea. Systems are not well tied together, top to bottom. This topic has been covered throughout time. In 1986, COL (retired) John Cushman covered this topic in two studies. One of his studies was *Command and Control of Theater Forces: The Korea Command and Other Cases,* which is the sequel to his first study, *Command and Control of Theater Forces: Adequacy*. In 2004, COL Patrick T. Stackpole covered this topic in his, *Route to a Stronger Alliance: Command and Control of the Second Infantry Division*. The common theme in both studies was interoperability, language, and slow procurement processes. These two studies typify what kind of work is done when addressing C2 in Korea. They are good works, but the concept of cyber was nonexistent or at most in its infancy when

they were writing. Therefore, it is neglected. Additionally, C2 on and off the peninsula is considered in this paper, and that is another difference. In 2006, *Signals* produced a study of C2 in the Korean theater. Naturally, given its date, the focus on cyber was limited in scope. In 2008, a *RAND* study provided an additional aspect to C2. Again due to the date, this study does not take into account cyber. This MMS paper provides a needed examination of C2 and how key, military concepts relate to US forces on the peninsula in the age of cyber. The figure below depicts the evolution of C2 challenges pre-cyber and post-cyber, while looking at how to possibly resolve the gap that was created from cyber.

Figure 1



CURRENT PROBLEM

"*War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. . . . The commander must work in a medium which his eyes cannot see; which his best deductive powers cannot always fathom; and with which, because of constant changes, he can rarely become familiar*."

—Carl von Clausewitz

There is no aspect of coalition, military operations more crucial than effective communication. The sharing of critical intelligence, necessary logistical planning and real-time targeting, depend on clear and accurate communications.[7] When interruptions in communications occur, this leads to disruptions and confusion in operations. These issues occur between U.S. forces, but there are more coordination complications between the U.S. and ROK forces. Not only do both forces have to deal with C2 complications, each force has to deal with the language barrier. There are not enough linguists on either side to be efficient in combined operations, so C2 planning and coordination is vital.

There are a multitude of problems facing U.S. forces regarding C2 on the Korean peninsula. One issue is the difficulty of operating in a Global Positioning System (GPS) degraded environment. For U.S. forces, full GPS functionality is critical to enable action across the range of military operations (ROMO). GPS provides the timing that is necessary to synch C2 nodes together, to attain the accuracy that U.S. forces use for precision guided munitions and to ensure air operations. This last, key functionality is particularly problematic. In 2014 aviation advisory, the Federal Aviation Administration (FAA) reported "to all U.S. operators regarding flying in the Korean Peninsula Incheon (RKRR)...The FAA cautions operators to be prepared to use non-GPS navigation aids...[due to] reports of interference and disruption in the region."[8] The National

Business Aviation Association (NBAA)'s vice president of regulatory and international affairs stated, "We urge Member Companies that operate in this region to exercise caution and plan to use backup navigation methods in the event of GPS reliability issues."[9] The significance of the last statement from the NBAA vice president is that, all organizations that are or will operate in this AOR, need to be prepared to execute in an area that is active with offensive electronic attack. Even though this message was issued to civilian organizations, this vulnerability applied to any U.S. military unit operating in this area as well. If operations take place in a GPS degraded environment, U.S. forces need to ensure that their operational effectiveness is not affected.

Even though GPS is important to operations, U.S. forces have to able to conduct operations in a communications limited environment like Pyongyang and Yongbyon. The mountainous environment there interferes with voice and digital communications, impairing line-of-site (LOS) C2 systems. The climate in Korea has approximately the same if not more of an impact on C2 systems as does the terrain. Korea has torrential downpours, heavy winds, and severe thunderstorms during the summer monsoon season, with harsh winters that also can interrupt radio, satellite, and digital transmissions. Weather is always a concern for communications infrastructure. However, due to the harsh conditions in Korea, main systems like Support Wide Area Network (SWAN-D) (main system that pulls data) breakdown because of the sensitivity of the system.

The operational environment creates unique challenges for communications, but the severity of these challenges effect the ability to share information in an efficient and timely manner. U.S., Korean, and Allied Forces stationed in Korea use similar military equipment, but the majority of their communication equipment and encryption is

different. This creates interoperability and security issues. The difference in equipment sets and encryption can be attributed to budget constraints. The FY 2000 National Defense Authorization Act directed the Secretary of Defense to submit a report on the security situation on the Korean Peninsula. This report to Congress, stated that: "Republic of Korea (ROK) communications systems have been designed without combined interoperability in mind...Secure telephone and data encryption, interoperability of command post systems, and electronic interfaces of automated intelligence systems are all major improvements needed for interoperability in the command."[10] This speaks directly to the interoperability and encryption challenges that U.S. forces continue to face. South Korea, the country that the U.S. is partnered with and is to help protect against a North Korean invasion, fails to make the effort to fix current C2 interoperability issues.

The frequency allocation on the Korean peninsula creates additional challenges specifically for U.S. forces. Korea has restrictions on what frequency ranges are available to use and this puts limits on what C2 systems and programs can be used. The lack of dedicated frequencies also limits U.S. Forces Korea from conducting testing and fielding new and emerging equipment, which hampers the efforts to protect the Republic of Korea.[11] This also affects the interoperability between forces. The differences in the C4I equipment used among the Korean, U.S., and allied forces potentially could prohibit the expeditious exchange of vital information, causing delays in operational tempo.[12] This restriction does not affect South Korean forces due to common practices. Korean forces operate in the clear (no encryption) on a normal basis. However, this method creates an ease of access to information for North Koreans or any other potential threat.

SOLUTION

U.S. forces do not have the newest forms of technology to command and control in this environment. There is a tremendous amount of commercial off the shelf technology (COTS) that exists. However, U.S. military forces have not even scratched the surface of this new technology. For example, "A new distance record has been set in the strange world of quantum teleportation."[13] Quantum teleportation is a means to pass data at extreme speeds over fiber cables. As technology continues to improve, the U.S. military needs to seek fast and secure ways to transmit data and protect those systems. Investing in this type of technology would be a start. An example of new technology that is a government program of record (POR) is Mobile User Objective System (MUOS). MUOS is a satellite network that functions like a cellular network which uses internet protocol (IP) technology to provide secure and non-secure voice and data communications almost anywhere in the world. MUOS and its respective satellites have been in development for over 10 years. While not completely developed, launched, or fielded, early results are very promising. Another POR that would have benefitted U.S. forces is the Joint Tactical Radio System (JTRS) program. This US government program attempted to embrace some of the technology emerging in the civilian sector. It would have made communications equipment unilateral, which would increase interoperability between services and other forces. JTRS is a family of software defined radios whose software (waveform) is the same and can be ported into all radios. After approximately 15 years of development, this system was cancelled.

Systems like JTRS are cancelled primarily due to inefficiencies in the acquisitions process. The current acquisition process is broken and this broken process prevents U.S.

forces from procuring new and emerging technology in a timely and effective manner. The Defense Acquisition System exists specifically "to manage the nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces. [This system] is designed to support not only today's force, but also the next force, and future forces."[14] In July of 2012, a National Defense article reported the following about the Joint Tactical Radio System (JTRS): "The Army cancelled the JTRS Ground Mobile Radio (GMR) in October, via a kung fu smack down in the form of a letter from Frank Kendall, the undersecretary of defense for acquisitions, technology and logistics. The letter explained the technical challenges were 'not well understood due to the immaturity of technology at that time.'" It then concluded that it is unlikely that "products resulting from the JTRS GMR development program will affordably meet service requirements, and may not meet some requirements at all."[15] After 15 years of development and a bill of $6 million dollars, the program is cancelled? With a little more research, the bill due to this cancellation totaled approximately $17 billion dollars in total. How did the number come about? Forces still needed to procure radios for Iraq and Afghanistan which totaled about $11 billion dollars. This effort wasted time in research and taxpayers dollars. It ended up creating more harm than good. If the intent of the acquisition process is to be efficient and effective for the members of the Armed Forces, then there is much work that needs to be done.

WHAT HAPPENS WHEN C2 FAILS

USFK is in the process of transferring operational control (OPCON) of Combined Forces Command (CFC) to ROK. In order to do so, a robust and integrated C2 system is

needed. If C2 fails, there will be a substantial lack in situational awareness, response time, and prevention of communicating situational updates and needs on the battlefield if North Korea attacks. This translates into potential forces being overrun or not provided the necessary resources needed during conflict. Failure of C2 in this scenario would cause confusion and a lack of clarity on the battlefield. Efforts could be delayed or duplicated, which could lead to inefficiency and wasted resources. It is vital that command and control infrastructures remain intact. An efficient and effective C2 system is to also bridge the language gap. Currently there are not enough translators on either side to process the vast amount of information that will be passed. For example, during UFG ’14, USAF Staff Sgt. Jonghwan Kim stated, "Anytime something needs to be discussed with ROKAF, I jump around and translate between the military members...Anytime there are messages coming down from the exercise scenarios, or script cell, I have to translate it into Korean so ROK and U.S. are on the same page and have a mirrored understanding of the message."[16] Basic communication can be lengthy and compounded by the use of military terms. The systems that aide this process have to be as efficient as possible to ensure as much flow as possible.

THE THREAT AND WHY THE THREAT IS IMPORTANT

Today, Korea is the only place in the world where 35 million people live within the range and threat of enemy artillery. Witt almost no notice, two million soldiers could be locked in combat.

—General Thomas A. Schwartz
Commander-in-Chief, Combined Forces Command, 1999-2002

A threat has two components: intent and capability. There are a few countries that pose a direct threat to the Korean peninsula, U.S. forces, and ROK forces. These threats come primarily from North Korea and China. Each one of these potential threats is

dangerous and presents unique challenges. While Russia is not considered below, it could be added to this list as well, particularly given its very recent actions in Ukraine. However, for clarity of focus, the two most likely belligerents are addressed.

North Korean Threat

North Korea poses a significant conventional threat on the peninsula and continues to be a major exporter of ballistic missiles and associated technology. As such, North Korea poses a risk not just on the peninsula, but also throughout the region, and across the globe.

—Admiral Thomas B. Fargo
Commander, US Pacific Command

North Korea is a credible and formable threat to the U.S. and South Korean forces on the peninsula. North Korea fields the world's fifth largest military, with the third largest army, and the world's largest Special Operations Force (SOF).[17] The majority of North Korea's ground forces are strategically within striking distance of South Korea's capital, Seoul, and ready to deploy at a moments notice.

According to one estimate, the North Koreans have: "Seventy percent of their active force, to include 700,000 troops, 8,000 artillery systems, and 2,000 tanks, garrisoned within 100 miles of the Demilitarized Zone. Much of this force is protected by underground facilities, including over four thousand such facilities in the forward area alone. From their current locations, these forces can attack with minimal preparations."[18] In terms of land-based operations, North Korea has dedicated decades to prepare to invade South Korea. This threat is real and can occur with little or no indication. South Korean along with U.S. forces outnumbers the NK military. However, any attack from the North and counterattack from U.S. and South Korean forces would cause tremendous damage in South Korea, resulting in a high material and human cost.

North Korea also has a robust naval threat that includes mine laying. The majority

of U.S. forces are not stationed in the ROK. Most U.S. forces will have to travel from Okinawa, Japan via sea in order to deploy or reinforce the peninsula. That makes the sea lines of communications (SLOC) very important to both North Korean and U.S. forces. North Korea wants to use the SLOC as a means to disrupt or deny access, and U.S. forces need to utilize this as maneuver space to deploy forces. It is paramount to keep these SLOCs open.

In addition, North Korea is reported to possess between four to eight nuclear weapons as well as ballistic missiles that have been developed and tested (both short and medium range missiles; long-range missiles have not been successfully completed). It also has been developing cyber-related military capabilities, both offensive and defensive, coupled with information warfare strategies and tactics. This approach can provide it with tools that act as "force multipliers." As Michael Raska, a Research Fellow at the Institute of Defense and Strategic Studies, said, they can be viewed as new "weapons of mass effectiveness."[19] This capability gives North Korea the ability to attack from afar without the loss of lives. The effects of cyber-attacks can have a similar effect to that of nuclear weapons or ammo from a rifle or artillery gun. In order to handle a North Korean threat that can mobilize and invade the ROK, U.S. as well as Korea forces need to have effective lines of communications that enable both forces to share information that will allow minimum response times. Would this cyber threat give the North Koreans a tactical or strategic advantage over U.S. and South Korean forces? Would this capability give the North Koreans more of a reason to execute an invasion due to the illusion of an advantage? It is not clear to what the North Koreans would do with this added capability, however, with the instability that currently exists under this

regime, a cyber attack followed by a hostile act or invasion is not out of the picture. For example, in 2008, Russia combined cyber and kinetic actions to mount an offensive on Georgia. Russia used cyber as a shaping action in order to blind Georgia. This cyber (denial of service attacks) followed by operations from ground troops was a first. If this could happen then, the possibilities of occurring in the future is very likely. Cyber is a grey subject and there is no clear answer on how to respond legally to cyber attacks. The key here is the United States cannot allow North Korea to cripple or penetrate our systems. If it does, that action may lead to an attack. North Korea's increase in cyber capabilities and capacity makes for a dangerous situation.

Chinese Threat

The rise of China presents an added threat to U.S. and South Korean forces. Given historical patterns, once China achieves the ability to challenge regional order, it will seek dominance throughout the region.[20] The one area where China is improving and in which the U.S. is currently struggling is the annual defense budget. China's defense budget continues to increase which means that China can procure platforms that will make them a greater threat in the region. China's land-based ballistic and cruise missiles are a serious threat that continues to challenge the ability of the United States and its allies to operate.[21] All of the U.S. military bases are within complete range of China's missile systems. As China continues to increase capabilities, the U.S. will require continuous modernization of technology and capabilities that will allow U.S. and allied forces to operate freely. This modernization will be difficult due to defense budget constraints.

China has more often than not acted to curb some of North Korea's rash actions.

This restraint is welcomed, although its motive for doing so is not clear. It may be a desire to head off a conflict with unpredictable outcomes. Whatever this thinking may entail, China has increased its cyber threat capabilities. According to Jun Isomura, a senior fellow at the Hudson Institute, "China divides cyber into two target areas: political and military."[22] China's political cyber focus is on the White House, State Department, Energy Department and the Office of the US Trade Representative, and other parts of the US government. Its military targets include the entire US defense community, including the intelligence community. The challenge to C2 is clear. If China conducted a cyber-attack disrupting the Pentagon's unclassified Non-secure Internet Protocol Router Network (NIPRNET), this would degrade the response time of the U.S. military during a crisis. The NIPRNET is very important to the Department of Defense (DoD); it carries vital logistical, personnel and unit movement data. One target that China continues to target is the command and control nodes of the Pacific Command. Some would argue that this military system would be difficult to bring down. If China can hack into the DoD network, why would they be unable to get into the military network? Since 2013, the Obama administration passed executive orders to add additional protection of computer networks of important industries.[23] This threat is costing the U.S. hundreds of billions of dollars. The second and third order effect of this prevents the U.S. military from investing and procuring the necessary C4I equipment needed to operate efficiently. Instead of spending billions of dollars from the defense budget on C4I equipment needed on the battlefield, billions of dollars from the defense budget are being spent on network security vulnerabilities within our networks that were not done at inception.

China also presents a threat to the U.S. in space. China's development of anti-

satellite capabilities is a serious threat to U.S. forces. In 2007, China demonstrated the ability to destroy satellites orbiting at several hundred kilometers. In 2013, China also demonstrated the ability to shoot down any U.S. satellite in space. This is vital to the U.S forces for the following reasons: satellites are used for long-range communications; the guidance of fighter planes, drones, and missiles for ground surveillance.[24] The destruction of satellites can potentially paralyze the U.S. military. Even if U.S. forces are not paralyzed from this destruction, China can use this capability to interrupt or blind the United States and then begin a sequence of attacks which can further destabilize the peninsula. So again, when the impact of cyber on C2 is considered in the context of achieving security in Korea, the picture that emerges is disturbing. China, like North Korea, can use cyber, apparently a preferred means of warfare, to probe and seek out vulnerabilities of U.S. and ROK forces in Korea. These efforts, particularly given they are in the cyber domain, will impact C2 for all joint operations. On the one hand, an assumed vulnerability may well encourage China to foster North Korean recklessness. On the other hand, should no weakness be found, perhaps China will again foster North Korean recklessness as a means of disrupting the better C2 coming into focus for US and ROK forces. Frank Cilluffo, co-director of the Cyber Center for National and Economic Security at George Washington University, believes that North Korea's cyber capability constitutes "an important 'wild card' threat, not only to the United States but also to the region and broader international stability."[25] Either way, the overall security picture could well deteriorate as an adversary fear of better C2 drives their policy considerations. Given that US and ROK forces will strive to enhance its C2 in the cyber age, again, how to contain this potentially volatile situation is a critical concern.

IMPACT OF THREAT ON TECHNOLOGY

Old tactical radios were heavy and used for a single purpose: to provide secure voice communications between higher, adjacent, and lower forces. Even though it took a lot of physical effort to use these radios because they were heavy, they were reliable. Better, they could be kept functional. The ability to jam, interfere, or interrupt radio communications was not as easy then as it is today. That may be attributed to best radio practices and proper radio procedures or it could be attributed to the trust that commanders had in their subordinates and the lack of data capabilities. Either way, the old is outperforming the new.

Today, communication equipment is being developed at a rapid rate. The development of this technology can be considered revolutionary. However, with the direction that DoD is moving, greater vulnerabilities are being created at the same time. What kind of threat is being developed? Take a look at the new radio systems that are currently in inventory and what is being developed. Our radios and telephony networks are now IP based just like the data network. The method of communicating via radio is like communicating over a computer network. For example, Adaptive Networking Wideband Waveform (ANW2) and Soldier Radio Waveform (SRW) send out continuous packets looking for acknowledgment from a distant station. This radio signature continues until the radio is turned off while operating this waveform.

The new radios are taking up larger parts of the spectrum, allowing service members to share large quantities of data, video, and digital information. New technology can now provide position location information (PLI) and ISR data. These capabilities are great but when these capabilities give off a large constant radio signature once the radio

is turned on, this creates a problem. If manufactured without giving off a constant radio signature and employed with proper radio procedures, radio communications could bridge the C2 gap. Would commanders be satisfied with relying on radios and limited amounts of data? This is truly a question to consider. Commanders would lose the ability to micromanage situations (centralized command) and have to rely on principles that are so often referenced (decentralized command). One thing that is stressed in the U.S. military is decentralization. Decentralization would solve a number of C2 issues. Are leaders afraid of giving the initiative back to young leaders? Or do they want to continue to cover their six?

Technology has opened doors to a world that could eliminate entire systems at just a push of a button from a single person or very small team. The cyber world has given power to actors, state and non-state, a means to compete on the same playing field as some of the great powers. That has all changed. Take a look at Stuxnet. Stuxnet targeted an industrial control system. Labs were created to mirror its target. A Stuxnet type of attack could present a problem that could disable the entire DoD C2 system. The majority of U.S. military C2 systems are based off of software technology (rely on updates by connecting to the internet). Data, radio and switching systems all require software updates. This applies for both unclassified and classified systems. If someone used a virus employed the way that Stuxnet was employed, entire C2 networks could be disrupted or destroyed. Such a development could lead to complications in security on the US and ROK side of things. A coveted reliance on initiative in the face of the enemy, particularly given assumptions of C2 failure or complication once hostilities erupt, is being eroded in the name of better C2 thanks to cyber. Will commanders, and senior

commanders, be able to micromanage the battlefield to an unprecedented degree in Korea with better C2? Is this desirable? Is a readiness forfeited due to assumptions of an unbreakable chain of command, thereby rendering the survival skills of frontline infantry less important? This delusion that the combatant directly in the fray can be almost passive in terms of leadership directing the fight is alarming. It may not give license to US or ROK adventurism, but it may be one more indicator to the adversary that C2 has made those defending South Korea vulnerable to attack. Once again cyber has introduced a potentially destabilizing factor on the ground.

LIMITATIONS OF THE CURRENT COMMUNICATION SYSTEMS

One limitation of current communication systems is the availability of frequencies. Radios and integrated platforms that require specific frequency bands to operate become ineffective. Now, this issue does not create a problem in the United States, Iraq, or Afghanistan. However, this is a huge issue in the Pacific AOR, specifically Korea. Restrictions on frequency bands prevent U.S. forces from operating certain communication equipment. By not being able to use the available spectrum, U.S. forces lose the ability to share vast amounts of data, video, and digital information needed to carry out their missions. Another example of this limitation is ANW2. This waveform operates within certain frequency bands and these bands are restricted to Korea and other areas of the Pacific. This waveform can be seen in several different systems like NOTM. Now, these two examples are USMC specific examples, however, this applies to the other branches of the U.S. military. Even though this waveform has radio limitations that effect C2, the hub radio system still depends on satellite technology to pull data.

Satellite & Bandwidth limitations

U.S. Forces can not depend on satellite communications for command and control in the Korean AOR. Over the last decade, the focus of effort for bandwidth utilization and satellite access has been on the Middle East. There has been a lack of investment or focus in the Asia-Pacific region. With the Pivot to the Pacific, this means additional forces will flood the region, but the excess satellite communication capacity is not readily available. There are approximately 70 satellites that orbit over the Pacific. Different groups whose working relationship with the U.S. is not easy to conduct operate over half of these satellites. The issue with the other satellites is that they have fixed, wide-coverage beams focused on large land masses. This reduces the coverage areas that could support military operations. The U.S. military will be hard-pressed to find the coverage it needs to support intelligence, surveillance and reconnaissance missions in key strategic locations.

Currently, the U.S. military spends more money on commercial satellite systems. As Debra Werner says, "Worldwide, only about 20 percent of U.S. military communications travel over U.S. military satellites. For the other 80 percent, defense agencies spend $1 billion to $2 billion a year buying excess capacity on the same commercial satellites."[26] If this trend continues, the cost could rise to as high as $5 billion annually. The question that should be raised is why does the military only utilize 20 percent of military satellites? The DoD has spent decades of leasing commercial bandwidth a year at a time and continues to do so. In an attempt to change this process to extend the leasing time that would save money, Congress denied this action. The issue with this plan was that it focused on single theaters. In 2011, Northern Sky Research

estimated that, "U.S. military bandwidth demand is expected to rise 74 percent in the next 10 years."[27] There are several issues that are presented regarding satellites. The military demand for bandwidth keeps outpacing supply due largely to the adoption of intensive ISR campaigns and the proliferation of mobile devices. Werner again comments: "DoD has been unable to take advantage of these ideas due to either existing processes … or a DoD culture that appears to resist dependence on commercial providers for satellite services."[28] It takes the U.S. military 10 to 20 years to build its own satellites due to extremely high levels of bureaucracy that exist within the DoD. It takes about four years for the Defense Department to approve a detailed description of the precise job a new satellite must perform. It takes two more years to hold a competition and select the prime contractor. Then, the winner spends anywhere from seven to 14 years designing, building and testing the new satellite under the watchful eye of government officials. The commercial or private sector can design, build and fly new satellites in about three years. The satellites that are in use are old aging systems. Right now, the majority of our satellite systems use Ka band to pull data services. There is difficulty with this access.

BROKEN ACQUISITION PROCESS

The U.S. military has been under fire to streamline its slow and cumbersome acquisition process in recent years. This process has hindered the ability to procure up to date command and control systems. For that very reason, the U.S. military acquisition process needs to be reformed. Even if the entire process can not be reformed, there has to be exceptions to the current process. The U.S. military, as well as the entire DoD, needs to take a smarter approach as to how procurement is done. U.S. military as well as the DoD needs to work to identify efficiencies, to tailor the C2 acquisition model, to optimize

delivery of capabilities, and to build agility into the acquisition process.

Joint Model-DISA

One way to approach this is to purchase equipment or systems in a unified or joint process. DISA has started to implement a process that could serve as the very tool that is needed. The Joint Enterprise License Agreement (JELA) is a process that invites different branches of the Defense Department to combine their information technology (IT) buying power in order to trim expenses and boost efficiencies.[29] For example, the purchase of Microsoft and Adobe license was done so in a unified (Army, Air Force, and Defense Information System Agency (DISA)) fashion. These licenses were procured for the entire DoD. According to the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) white paper, "The multi-year, $700 million enterprise licensing agreement consolidates multiple older licensing agreements with Microsoft. As a result, military sources predict the Air Force will see $50 million in annual savings, the Army $70 million, and DISA will save 10 percent compared to its existing Microsoft contracts."[30] This unified effort saved both time and money, which should be the focus of U.S. military and DoD business. The Microsoft and Adobe contracts are examples of the type of success that can be obtained once a hard look is taken and then there is action taken to correct the acquisition process. Now, the question will be asked, how will this work for C2 systems? Are they to different? Do they have too many requirements?

SOCOM Model

The joint model unifies efforts across the DoD, however, if there was a model of a type of acquisition process to emulate, it would be that of Special Operations Command

(SOCOM). The process that SOCOM uses provides the command the ability to procure specific equipment tailored to what the command needs. Conventional U.S. forces need this type of process that would enable them to procure information technology (IT) or C2 capabilities within weeks and months versus FYs or Program Objective Memorandum (POM)s. The research and development (R&D) process is too slow to keep up with the pace that technology grows. By the time an IT or C2 product has completed the R&D process, the equipment is outdated. This process needs to be quicker and more efficient than what it currently is. Example lets look at the Joint Tactical Radio System Program (JTRS). For anyone that is not familiar with the JTRS, it is the Joint Strike Fighter of the radio world. The developers of this system attempted to build an omni-purpose communication network that can do everything but wash your windows. What did this program actually delivered after 15 years? Absolutely nothing except an invoice that totaled a little more than $6 billion. As mentioned earlier, this program was soon cancelled. The R&D process was way too long and in the end nothing was produced, time was lost, and money was wasted on a piece of technology that would have been old and outdated if fielded. The acquisition process needs to meet the demands of life cycle of equipment that is needed. SOCOM has been given the authorities to speed up their procurement process. Conventional forces should be provided this ability. Just to be clear, this type of authority should only apply to processes that have a short life cycle like IT or communication equipment.

Commercial Model

Another model that the U.S. military or DoD could emulate as it looks for ways to reduce spending and increase capabilities and infrastructure of the C2 is that of the

commercial sector. When the commercial sector buys hardware or software the job is not complete once this action is done. Questions have to be asked. What needs to be purchased and who needs it? Is the requirement being met with this purchase? Is a specific service needed, and how complex, scalable, and flexible does it need to be and what type of redundancy is available? These are some of the questions that the commercial IT sourcing department takes into account before making a decision. The system that is used to make these decisions is the IT Supply Management system. This system has four dimensions, the

> "IT Supply Strategy, with which an organization determines what services should be delivered and by how many suppliers; IT Category Management, through which an organization decides the correct approach for managing its third-party IT supply base; IT Relationship Management, through which an organization determines the governance and resources needed to manage key suppler relationships; and IT Sourcing Strategy, though which an organization determines how its key supplier relationship should evolve to meet ever changing business needs."[31]

Even though there are four steps to this system, each step is tightly tied together. One cannot operate without the other. As the DoD evaluates issues in the different areas of its acquisition process, it can benefit from the lessons learned from the experience of the commercial sector through its IT Supply Management. The key lesson learned from the commercial sector is that every decision is interconnected and no actions are isolated.

It takes the U.S. military decades to approve, build, test, and launch its own satellites, due to a slow bureaucratic process that compares unfavorably to that of the private sector. It takes about four years for the Defense Department to approve a detailed description of the precise job a new satellite must perform. It takes two more years to hold a competition and select the prime contractor. Then, the winner spends anywhere from seven to 14 years designing, building and testing the new satellite under the

watchful eye of government officials. Companies, on the other hand, can design, build and fly a new satellite in about three years. "The U.S. government is buying commercial satellite capacity the same way it buys janitorial services" on annual contracts, Osterthaler said.[32] That makes companies reluctant to invest hundreds of millions of dollars in satellites to address military demand, he added.

Foreign Military Sales

Foreign military sales (FMS) are a key factor to improving the ability of our allies. FMS is a non-appropriated program through which foreign governments can purchase defense articles, services, and training from the United States. Eligible nations can use this program to help build national security infrastructures. A limitation of this program is that the nations that require assistance are often unable to finance their needs.[33]

The sale of US military hardware to the ROK is also very helpful when it comes to interoperability. As command, control, and communication systems become more complex, it is essential that all alliance systems be able to "talk" to each other. This will ensure that military might can be brought to bear quickly and decisively as required. Not only will these systems improve today's ROK-US combat power, they will also contribute to future regional security in Northeast Asia.[34] Look at the Philippines, Canada, and Australian forces. As recent as 2015, these countries purchased tactical radios from the Harris Corporation. What this does is increase the command and control capability between the U.S. and these countries.

In the end, C2 issues could be mitigated with an efficient and effective acquisitions process. However, as it stands today, this is highly unlikely due to poor acquisitions. If things do not improve for C2, how do we assess security on the peninsula? If things

remain unchanged, will this create additional gaps that the adversary might exploit? If the DoD provides conventional forces the authority to procure IT or communications assets as referenced in the SOCOM model, change will occur more rapidly. If the DoD adopts any other model or fails to adopt anything new, change will continue to be slow and cumbersome while the ability of U.S. forces to protect and defend in this age of cyber will continue to be degraded.

RECOMMENDATIONS TO ENHANCE OPERATIONS IN A COMMUNICATIONS DEGRADED ENVIRONMENT

The following recommendations are meant to increase the ability to operate in a communications degraded environment: Develop and utilize more military or DoD owned satellites, change training and education standards, and procure new COTS technologies without having to go through the DoD's cumbersome procurement process.

The first recommendation is to develop and rely more on DoD or military grade satellite systems. Currently, the DoD spends billions of dollars a year leasing commercial bandwidth from commercial entities. The amount of control the DoD has over these systems is very limited. If the DoD put more emphasis on managing and controlling its own satellites there would be a decrease in the money spent on bandwidth per year, training opportunities would increased, and there would be a decrease in reliance on private organizations and other countries to use satellites that cover specific areas. This effort will require lots of planning regarding how many satellites would be needed, what capacity does each satellite need, and where should these satellites be placed. The end state would result in greater flexibility for the DoD operations.

The second recommendation is to change the training and education standards to execute C2. Most C2 training today stresses more data. This leads to larger data pipes and

larger, more fragile systems C2 systems. So without putting total emphasis on data networks, more emphasis needs to be put on radio training, theory, radio networks or architectures, and the interoperability of radio systems. Radio training needs to be conducted in heavy dense areas versus flat open areas that illustrate the Pacific AOR. There must be less reliance on satellite access and more on UHF, VHF, and HF capabilities and how to operate these bands efficiently.

The third recommendation is to procure more COTS communications equipment, and not just any COTS system. The DoD needs to purchase a common system that is the same across the board. This would reduce spending from each service and by purchasing the same system, increases interoperability between the services. Purchasing COTS would provide the services with newest forms of technology and do so in a timely manner. The way items are procured now takes too long to develop and deliver to the customer. This process cannot be single threaded. This must be a joint effort or U.S. forces will remain in the same position as now.

CONCLUSION

C2 is vital to all levels of warfighting. No matter what domain (air, land, sea, or cyber (if this is classified as a domain)) where operations are taking place, C2 is a must to be successful especially in a joint environment. The issue of C2 is not new. C2 issues have been addressed in the past. However, not enough emphasis have been placed on this issue. Every aspect of the warfighting functions have been at the forefront of every senior leader. As technology has improved, more capabilities where given to commanders but the underline issues have not been resolved. Is more better? Is bigger better? Not always...but how do you convey this message to those that micromanage

without even knowing they are doing such? As illustrated throughout this MMS, the Korean peninsula creates unique C2 issues for U.S. forces. If this C2 issue is not solved, there could potentially be negative impacts on joint operations, while tactical and strategic advantages could possibly shift from the U.S. over to North Korea and/or China, and commanders would have to rely on mission type orders. What about the procurement of commercial technology? Would leveraging commercial technology solve these issues? Potentially yes. However, it is unlikely that conventional forces will ever be afforded the opportunities to procure such technologies because of the slow, joint acquisitions process. The joint acquisitions process is not going to be solved in the immediate future. Therefore, timelines to purchase equipment and systems will continue to hold forces back.

The inability to provide effective C2 in a joint environment could have serious implications. There are already language barriers that have to be overcome and when C2 issues are added to the equation, additional friction is added to an already complex environment. C2 needs to be simple, effective, and efficient. The technological differences in the C4I equipment used among the Korean and U.S. forces could prohibit the expeditious exchange of vital information. This would result in delayed actions or delayed notifications of objectives and decision points. Bruce Klingner, a senior research fellow for Northeast Asia at The Heritage Foundation's Asian Studies Center, stated, "South Korean military still lacks the necessary C4ISR systems and capabilities to overcome stovepiped command structures and to enable interoperability across services. U.S. officials privately comment that at present the South Korean military is not capable of truly joint operations."[35] If this is true, U.S. and ROK have significant problems if

North Korea were to invade. Time is an important factor and the ability to stay out front of threats is dependent upon an efficient C2 system.

Cyber could also cause further C2 issues. With the advancement in cyber technology, North Korea and China could both gain a strategic advantage in this area. If either country used cyber to blind U.S. forces for a period of time to start a North Korean invasion or delay the ability to reinforce the peninsula in a timely manner, the results could be devastating to the South Koreans. Even with the development of cyber capabilities of both North Korea and China, how likely would they employ these capabilities? Or are they holding these cards as an ace in the hole? There is not a clear answer to these questions but this is something that needs to be considered during planning.

The resolutions to C2 are not new, however, and this means that commanders have to rely less on bandwidth intensive systems and depend on low bandwidth radio technology to C2 (map and pen). This means that commanders or leaders have to rely on mission type orders and trust in the concept decentralization, allowing young leaders in uniform to make decisions that they were given special trust and confidence to do. Is this a lost art? For the sake of all the future leaders, I hope not. There is no single element that is more important than C2. C2 between the U.S. and ROK, both from a technical and language perspective, will be a great challenge to overcome. The majority of these challenges need to be overcome prior to experiencing them on the battlefield. Will C2 itself destroy the enemy? Maybe not, however, C2 is essential to all military operations especially in a joint environment. C2 is a fundamental requirement for life and growth, survival, and success for any system. This keeps the status quo intact and this is best

because it introduces almost no change into a dangerous situation, one that could be made worse by the introduction of better technology making C2 more sound. One could encourage a cyber war at best, a confrontation, but one that is at least satisfactorily virtual and therefore bloodless, for now. The aim is to keep it that way. Let the adversary fish about in cyberspace for some sign of provocation to attack – that will be a reach and saddle them with starting a war. In the meantime, even in the face of changing technology, Korea remains an old fashioned battlefield in many respects, and this is a welcomed development in the age of cyber. The new is falling all about us, but some of the old must remain to stabilize things as transitions unfold. This is what Korea brings to the fight when one stresses the impact of C2 in that very unique part of the globe. While conducting this study, it is clear that cyber and C2 complications can be mitigated, but is there really a true answer or way to solve this issue?

Acronyms

AOR	Area Of Responsibility
C2	Command and Control
C4I	Command, Control, Communication, Computers and Intelligence
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance
CFC	Combined Forces Command
CMFC	Combined Marine Forces Command
COTS	Commercial Off The Shelf
CPX	Command Post Exercise
DISA	Defense Information Systems Agency
DoD	Department of Defense
DMZ	Demilitarized Zone
DPRK	Democratic People's Republic of Korea
FMS	Foreign Military Sales
GPS	Global Positioning System
GOTS	Government Off The Shelf
IP	Internet Protocol
IT	Information Technology
JELA	Joint Enterprise License Agreement
JTRS	Joint Tactical Radio System
MUOS	Mobile User Objective System
nK	North Korea
NOTM	Network on the Move
NSS	National Security Strategy
OPCON	Operational Control
OPLAN	Operations Plan
PLI	Position location information
POM	Program Objective Memorandum
POR	Program of Record
PRC	People' s Republic of China
R&D	Research and Development
ROK	Republic of Korea
SLOC	Sea Lines of Communication
SOCKOR	Special Operations Command - Korea
SOCOM	Special Operations Command
SOFA	Standard Operations Forces Agreement
SOF	Special Operations Forces
USFK	United States Forces Korea
WMD	Weapons of Mass Destruction

Endnotes

[1] John Di Genio. U.S. Forces in Korea Face Unique Challenges. October 2001. http://www.afcea.org/content/?q=node/489
[2] Naval Post Graduate School. Information Dominance Center of Excellence. July 17, 2014. http://www.nps.edu/Academics/Centers/IDCFE/InfoDominance/infodominance.html
[3] Joint Publication 1
[4] ADP 6-0
[5] MCWP 3-33.5
[6] MCWP 3-33.5
[7] Patrick T. Stackpole. Route to a Stronger Alliance: Command and Control of the Second Infantry Division. June 2004. http://web.mit.edu/ssp/publications/working_papers/wp04-2.pdf
[8] National Business Aviation Association. FAA Issues Advisory for Korean Peninsula Incheon Flight Information Region. Nov 17, 2014. http://www.nbaa.org/ops/intl/mid/20141117-faa-issues-advisory-for-korean-peninsula-incheon-flight-information-region.php
[9] National Business Aviation Association. FAA Issues Advisory for Korean Peninsula Incheon Flight Information Region. Nov 17, 2014 http://www.nbaa.org/ops/intl/mid/20141117-faa-issues-advisory-for-korean-peninsula-incheon-flight-information-region.php
[10] 2000 Report to Congress Military Situation on the Korean Peninsula. http://www.defense.gov/news/Sep2000/korea09122000.html
[11] John Di Genio. U.S. Forces in Korea Face Unique Challenges. October 2001. http://www.afcea.org/content/?q=node/489
[12] John Di Genio. U.S. Forces in Korea Face Unique Challenges. October 2001. http://www.afcea.org/content/?q=node/489
[13] Kelly Dickerson. Quantum Teleportation Reaches Farthest Distance Yet December 08, 2014. http://www.livescience.com/49028-farthest-quantum-teleportation.html
[14] Defense Procurement and Acquisition Policy. February 2015. http://www.acq.osd.mil/dpap/ccap/ap/index.html
[15] Defense Procurement and Acquisition Policy. February 2015. http://www.acq.osd.mil/dpap/ccap/ap/index.html
[16] Staff Sgt. Cody H. Ramirez, 7th Air Force Public Affairs. Ulchi Freedom Guardian: Communication is key to ROK-US relationship. August 25, 2014. http://www.pacaf.af.mil/news/story.asp?id=123422340
[17] General Thomas A. Schwartz, "U.S. Forces, Korea and UN Command / ROK-U.S. Combined Forces Command: Strength Through Friendship," in *Asia-Pacific Defense Forum*, Summer 2001, 50.
[18] Douglas J. Hine. "THE KEY TO STABILITY ON THE KOREAN PENINSULA - UNITED STATES, JAPAN AND CHINA." AIR FORCE FELLOWS PROGRAM, AIR UNIVERSITY.
[19] Michael Raska, Cyber Wars on the Korean Peninsula. April 22, 2014. http://www.aljazeera.com/indepth/opinion/2014/04/cyberwars-korean-peninsula-2014422531782925.html
[20] Ross, Robert. US Grand Strategy, the Rise of China and US National Security Strategy for East Asia. Strategic Studies Quarterly Vol. 7, No 2, 2013 http://www.isn.ethz.ch/Digital-Library/Publications/Detailots783=0c54e3b3-1e9c-be1e-2c24 a6a8c70602 33&id= 165272livepage.apple.com
[21] Matthew Hallex. China's Mighty Missile Threat: What Should America Do about It?, September 13, 2014. http://nationalinterest.org/feature/chinas-mighty-missile-threat-what-should-america-do-about-it-11271
[22] Wendell Minnick. Experts: Chinese Cyber Threat to US Is Growing, July 9, 2013. http://archive.defensenews.com/article/20130709/DEFREG03/307090009/Experts-Chinese-Cyber-Threat-US-Growing
[23] The Privacy Office and the Office for Civil Rights and Civil Liberties Department of Homeland Security Executive Order 13636 Privacy and Civil Liberties Assessment Report. April 2014. http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf
[24] Hiroyuki Akita. China ups ante in space arms race. January 6, 2015. http://missilethreat.com/china-ups-ante-space-arms-race/
[25] Mark Clayton, "In cyber arms race, North Korea emerging as a power, not a pushover," *The Christian Science Monitor*, 19 October 2013, http://www.csmonitor.com/ World/Security-Watch/2013/1019/In-

cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

[26] Debra Werner, The Military's Second Chance For a Bandwidth Fix. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR/304190013/The-Military-s-Second-Chance-Bandwidth-Fix

[27] Debra Werner, The Military's Second Chance For a Bandwidth Fix. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR/304190013/The-Military-s-Second-Chance-Bandwidth-Fix

[28] Debra Werner, The Military's Second Chance For a Bandwidth Fix. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR/304190013/The-Military-s-Second-Chance-Bandwidth-Fix

[29] Whitepaper JELA

[30] Whitepaper JELA

[31] Jeff Sorenson. IT Sourcing: It's not just an isolated procurement activity. September 7, 2014. http://www.c4isrnet.com/article/20140911/C4ISRNET18/309110001/IT-Sourcing-s-not-just-an-isolated-procurement-activity?odyssey=nav%7Chead

[32] Debra Werner, The Military's Second Chance For a Bandwidth Fix. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR/304190013/The-Military-s-Second-Chance-Bandwidth-Fix

[33] Foreign Internal Defense, Joint Publication 3-22. 12 July 2010. http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf

[34] Schwartz, Senate Armed Forces Committee statement, 17.

[35] Debra Werner, The Military's Second Chance For a Bandwidth Fix. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR/304190013/The-Military-s-Second-Chance-Bandwidth-Fix

Bibliography

"2000 Report to Congress on the Military Situation on the Korean Peninsula." 2000 Report to Congress on the Military Situation on the Korean Peninsula. September 12, 2000. http://www.defense.gov/news/Sep2000/korea09122000.html.

“Acquisition Policy.” Defense Procurement and Acquisition Policy. February 2015. http://www.acq.osd.mil/dpap/ccap/ap/index.html

Akita, Hiroyuki. "China Ups Ante in Space Arms Race - Missile Threat." Missile Threat. January 6, 2015. http://missilethreat.com/china-ups-ante-space-arms-race/.

Asmus, Ronald D. *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan, 2010.

Blanke, III, Col. Harry H. "Korea Theater Command And Control Enhancements Support Decisive Actions." SIGNAL Magazine. October 25, 2006. http://www.afcea.org/content/?q=korea-theater-command-and-control-enhancements-support-decisive-actions.

Clayton, Mark. "In Cyber Arms Race, North Korea Emerging as a Power, Not a Pushover." The Christian Science Monitor. October 19, 2013. http://www.csmonitor.com/ World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

Cushman, John H. Command and Control of Theater Forces: Adequacy. Program on Information Resources Policy, April 1983. International Press, Washington, D.C.

Cushman, John H. Command and Control of Theater Forces: The Korea Command and Other Cases. Cambridge, Massachusetts: Program on Information Resource Policy, 1986. http://www.pirp.harvard.edu/pubs_pdf/cushman/cushman-p86-2.pdf

Denmark, Abraham M and Hosford, Zachary M. Securing South Korea, A Strategic Alliance for the 21st Century. Washington, DC: Center for a New American Security 2010. http://http://www.cnas.org/files/documents/publicationsCNAS_SoutKorea_DenmarkHosford.pdf

Dickerson, Kelly. "Quantum Teleportation Reaches Farthest Distance Yet." LiveScience. December 8, 2014. http://www.livescience.com/49028-farthest-quantum-teleportation.html.

Genio, John Di. “U.S. Forces in Korea Face Unique Challenges.” SIGNAL Magazine. October 22, 2004. http://www.afcea.org/content/?q=node/489

Hallex, Matthew. "China's Mighty Missile Threat: What Should America Do about It?" The National Interest. September 13, 2014.http://nationalinterest.org/feature /chinas-mighty-missile-threat-what-should-america-do-about-it-11271.

Headquarters, U.S. Army, Mission Command, ADP 6-0. Washington, DC: Headquarters Department of the Army, May 2012

Headquarters U.S Marine Corps, Warfighting, MCDP-1. Washington, DC: Headquarters U.S. Marine Corps, June 20, 1997.

Headquarters U.S. Marine Corps, Command and Control, MCDP-6. Washington, DC: Headquarters U.S. Marine Corps, October 4, 1996.

Headquarter, U.S. Marine Corps, Counterinsurgency Operations, MCWP 3-33.5. Washington, DC: Headquarters U.S. Marine Corps, October 2004.

Hine, Douglas J. "THE KEY TO STABILITY ON THE KOREAN PENINSULA – UNITED STATES, JAPAN AND CHINA." AIR FORCE FELLOWS PROGRAM, AIR UNIVERSITY.

Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011. (10)

Joint Chiefs of Staff. Doctrine for the Armed Forces of the United States, Joint Publication 1. March 25, 2013.

Joint Chiefs of Staffs, Joint Publication 3-22, Foreign Internal Defense, July 12, 2010. http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf

Manyin, Mark E, et. al. Pivot to the Pacific? The Obama Administration's "Rebalancing" Toward Asia. Washington, DC: Congressional Research Service, 2012. http://fas.org/sgp/crs/natsec/R42448.pdf.

Minnick, Wendell. "Experts: Chinese Cyber Threat to US Is Growing." Defense News. July 9, 2013.http://archive.defensenews.com/article/20130709/DEFREG03 /307090009/Experts-Chinese-Cyber-Threat-US-Growing.

National Business Aviation Association. "Region VII: Middle East/Asia (MID)." FAA Issues Advisory for Korean Peninsula Incheon Flight Information Region. November 17, 2014. http://www.nbaa.org/ops/intl/mid/20141117-faa-issues-advisory-for-korean-peninsula-incheon-flight-information-region.php.

"Naval Postgraduate School - Information Dominance." Naval Postgraduate School – Information Dominance. http://www.nps.edu/Academics/Centers/IDCFE/ InfoDominance/infodominance.html

Ramirez, Cody, H, 7th Air Force Public Affairs. "Ulchi Freedom Guardian: Communication Is Key to ROK-US Relationship." Ulchi Freedom Guardian: Communication Is Key to ROK-US Relationship. August 25, 2014. http://www.pacaf.af.mil/news/story.asp?id=123422340.

Raska, Michael. "Cyberwars on the Korean Peninsula." - Al Jazeera English. April 22, 2014. http://www.aljazeera.com/indepth/opinion/2014/04/cyberwars-korean-peninsula-2014422531782925.html.

Ross, Robert. US Grand Strategy, the Rise of China and US National Security Strategy for East Asia. Strategic Studies Quarterly Vol. 7, No 2, 2013 http://www.isn.ethz.ch/Digital-Library/Publications/Detail/ots783=0c54e3b3-1e9c-be1e-2c24 a6a8c70602 33&id= 165272livepage.apple.com

Schwartz, Thomas A., "U.S. Forces, Korea and UN Command / ROK-U.S. Combined Forces Command: Strength Through Friendship," in *Asia-Pacific Defense Forum*, Summer 2001, 50.

Sorenson, Jeff. "IT Sourcing: It's Not Just an Isolated Procurement Activity." C4ISR & Networks. September 9, 2014. http://www.c4isrnet.com/article/20140911 /C4ISRNET18/309110001/IT-Sourcing-s-not-just-an-isolated-procurement-activity?odyssey=nav%7Chead.

Stackpole, Patrick T. "Route to a Stronger Alliance: Command and Control of the Second Infantry Division." June 1, 2004. http://web.mit.edu/ssp/publications/working papers/wp04-2.pdf.

The White House. National Security Strategy. Washington, DC: The White House, 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy .pdf

U.S. Department of Homeland Security. "Executive Order 13636 Privacy and Civil Liberties Assessment Report. The Privacy Office and the Office for Civil Rights and Civil Liberties Department of Homeland Security. April 2014. http://www. dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf

Werner, Debra. "The Military's Second Chance For a Bandwidth Fix." Defense News. April 19, 2013. http://archive.defensenews.com/article/20130419/C4ISR /304190013/The-Military-s-Second-Chance-Bandwidth-Fix.

Winnefeld, James A., and Dana J. Johnson. "Command and Control of Joint Air Operations." Some Lessons Learned from Four Case Studies of an Enduring Issues. January 1, 1991. http://www.rand.org/content/dam/rand/pubs/reports /2008/R4045.pdf

Yoon, Jong-Han. 2011. The Effect of US Foreign Policy on the Relationship between South and North Korea: Time Series Analysis of the Post-Cold War Era. Journal of East Asian Studies 11 (2): 255-287,336. http://search.proquest.com/docview/1501427975?accountid=14746.