# Cyber Compendium

## Professional Continuing Education Course Papers

Vol 2 Issue 1 / Spring 2015

**Air Force Institute of Technology**
**Center for Cyberspace Research**
**Professional Continuing Education**

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **27 APR 2015** | | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Cyber PCE Compendium: Cyber 300 Professional Continuing Education. Volume 2 Issue 1, 2015** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| **Robert Mills; Joseph Wingo; Preston Iverson** | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| **Air Force Institute of Technology Center for Cyberspace Research,2950 Hobson Way ,WPAFB,OH,45433-7765** | **CCR-TR-2015-VOL-2-NO-1** |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT

**Approved for public release; distribution unlimited.**

13. SUPPLEMENTARY NOTES

**The original document contains color images.**

14. ABSTRACT

**This compendium represents a select collection of deliberate thoughts, strong opinions, and conscientious commentaries from students attending the Cyber 300 course at the Air Force Institute of Technology. The range of topics covers a myriad of technical and non-technical issues that are often compounded by the cyber domain, address challenges and potential solutions experienced by leaders across the enterprise. The contributing authors represent a broad pedigree of professionals across the enterprise that includes all military departments (active duty, guard, and reserve components), officers, civil service, enlisted personnel, and allied partners (Great Britain). The position papers will in some cases be rather controversial and provoke thought. In the end, the intent is to make these contributions a basis for encouraging discussion and actions, leading to the development of techniques, tactics, and procedures that advance topics relevant to cyberspace.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | | **175** | |

# Contents

# DIRECTOR'S WELCOME

Welcome to the 2015 issue of the *Cyber PCE Compendium*, a publication by cyberspace professionals for the growing community of professionals interested in cyberspace, particularly the cyberspace domain relative to military operations.

On 19 June 2008, the Secretary and Chief of Staff of the Air Force designated the Air Force Institute of Technology and the Center for Cyberspace Research as the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE). The AF CyTCoE is chartered to be a unifying and synergistic body for promoting cyberspace education, training, research, and technology development. The AF CyTCoE facilitates development of Air Force education and training in support of cyberspace operations as well as identifies and provides subject matter experts who understand doctrine, techniques, and technology to ensure dominance in cyberspace.

Based on the SECAF and CSAF directed mission and the research, education, and technical credentials of the AF CyTCoE, the Center was tasked to develop educational courses that enable cyberspace operators, regardless of specialty, to adapt to the quickly changing cyberspace environment. To this end, the AF established the Cyberspace 200 and 300 courses. Since their inception, both courses have undergone considerable revision, institutional review, and have been granted Joint certification and Allied approval.

Cyber 300 is a course for cyberspace professionals transitioning from intermediate to higher-level responsibilities. Cyber 300 students are provided a broad background in cyber concepts, including capabilities, limitations, vulnerabilities, and the associated application and employment of cyberspace options in joint military operations. A fundamental component of the educational process is to encourage critical thinking and provoke thought that will push knowledge barriers beyond the edges that collectively contain the current art of the possible.

This compendium represents a select collection of deliberate thoughts, strong opinions, and conscientious commentaries from students attending the Cyber 300 course. The range of topics cover a myriad of technical and non-technical issues that are often compounded by the cyber domain, address challenges and potential solutions experienced by leaders across the enterprise.

Please enjoy our newest issue of the cyber compendium!

ROBERT F. MILLS, PhD
Director, Air Force Cyberspace
Technical Center of Excellence
Center for Cyberspace Research

# OVERVIEW

This compendium provides a select collection of position papers generated by students attending the Cyber 300 Professional Development Course hosted by the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) at the Air Force Institute of Technology (AFIT). The position-paper construct aptly enables discussion on emerging cyber topics without the rigor of experimentation and original research normally required for publication in an academic publication. The now familiar and recognized rapid momentum in the cyber domain makes it prudent to capture and distribute emerging philosophy and opinions related to cyber warfare specific to military operations.

This compendium provides a reference source and living repository on a wide variety of cyber topics that address the unique applications of the military professional. This compendium will be refreshed semi-annually to preserve the content and resist staleness. Furthermore, the publication will maintain a persistence presence online through the services offered by the Defense Technical Information Center (DTIC).

The contributing author's represent a broad pedigree of professionals across the enterprise that includes all military departments (active duty, guard, and reserve components), officers, civil service, enlisted personnel, and allied partners (Great Britain, Australia, and Canada). The position papers will in some cases be rather controversial and provoke thought. In the end, the intent is to make these contributions a basis for encouraging discussion and actions, leading to the development of techniques, tactics, and procedures that advance topics relevant to cyberspace.

# TOPIC COVERAGE

We live in a world of technological innovation and discovery. Technology forecasting is an important element of managing information technology risks. Any organization dependent on information technology realizes that managing risk associated with technology is a difficult endeavor. The connectivity of Department of Defense (DOD) information systems and information technology-dependent warfighting platforms to DOD networks and the Internet offers exploitation opportunities and continues to present a serious risk.

The topic selection process is guided by 27 specific questions generated by the senior leadership at Headquarters Air Force in collaboration with other DOD agencies. The students attending the professional continuing education course are presented with these questions during a brain storming session and provided the time and opportunity to formulate a thoughtful response and present it as a position paper. The aggregation of those responses are captured in this volume and provided to the reader for consideration of their merits. The position papers are clustered under a single theme that represents the core topic being discussed. The themes are designed to allow them to change over time in order to mimic the rapidly changing landscape of cyberspace. It is our sincere hope that this collaborative effort will incite further discussion and expedite forethought in strategy development from the next generation of cyberspace leaders.

# THE CENTER FOR CYBERSPACE RESEARCH AND THE AIR FORCE CYBERSPACE TECHNICAL CENTER OF EXCELLENCE

In the mid-1990s, Department of Electrical and Computer Engineering (ENG) faculty at the Air Force Institute of Technology (AFIT) began developing and teaching courses in computer networks and information operations. These courses allowed students to gain expertise in emerging technology areas highly relevant to the mission of the United States Air Force. The computer network courses covered the theory and technologies behind the evolution of the infrastructure we now call the Department of Defense Information Network (DODIN). The information operations sequence covered emerging threats associated with the use of information in a computer age. This included how malicious software can be developed and deployed to exploit inherent vulnerabilities associated with systems used within the DOD.

In 2001, AFIT applied for recognition as a National Center of Academic Excellence in Information Assurance Education (CAE-IAE), sponsored by the DOD and administered by the National Security Agency (NSA). AFIT was designated a CAE-IAE in March 2002. At the time of this designation, only 12 schools across the country held this status. As a result of this designation, AFIT began to participate in the Information Assurance Scholarship Program (IASP) operated by the DOD and administered by the NSA to place military and DOD civilian students into school to gain Information Assurance-related degrees. In the spring of 2002, the AFIT Center for Information Security Education and Research (CISER) was founded. At its' inception, three ENG faculty members (Dr. Raines, Dr. Baldwin, and Dr. Gunsch) formed the core of CISER. These faculty members began to grow and expand AFIT's role in this area of education and research. As part of this expansion and growth, a Distinguished Review Board (DRB) was established to help oversee the progress on the CISER.

In 2004, AFIT approved a Master of Science degree program in Information Assurance resulting from the growth in the area and increased interest in information-security related education. In 2005, AFIT was re-designated as a CAE-IAE for 3 years and also received a grant from the National Science Foundation (NSF) to fund Scholarship for Service fellowships for five students to pursue information assurance-related degrees and then work for the US Federal Government upon completion of their programs.

In 2006, a 12-month Master's Degree program in Cyber Warfare was established as an Intermediate Development Education program for field-grade officers. The first cadre of 12 students arrived in June 2007.

In April 2007, as a result of input from Headquarters Air Force, the CISER changed its name to the Center for Cyberspace Research (CCR) to more closely align with the Air Force mission in cyberspace. Also in 2007, and as a result of direction from the center's Distinguished Review Board and operational Air Force input, the Master's Degree program in Information Assurance underwent a name change to Master of Science (Cyber Operations).

Since 2005, the CCR has worked closely with Headquarters Air Force Space Command and 24th Air Force (AFCYBER) to move towards the force development of personnel with technical skill sets required to operate in the cyberspace warfighting domain. This close working relationship CCR fostered has required an expanded role for the CCR beyond its traditional graduate education and research mission. For example, the CCR was tasked to assist Air University with the integration of cyberspace techniques and concepts into the Professional Military Education programs.

As a result of CCR initiatives, research and close interactions across the Air Force, in June 2008, the Secretary of the Air Force designated AFIT and the CCR as the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE). The charter of the AF CyTCoE is to bring a level of understanding to the Air Force on "who is doing what in cyberspace." This charter includes education, graduate research, and outreach initiatives to ensure efficiency of operations and to promote partnerships between government, industry, and academia. During this period, Dr. (then Colonel) Arata joined the AF CyTCoE as a founding member and a Cyberspace Education Board of Advisors (BOA) was established to oversee the progress of the AF CyTCoE. Also in 2008, AFIT and the CCR were re-designated as a CAE-IAE. In late 2008, the CCR was tasked by Headquarters Air Force to lead the cyberspace Professional Continuing Education development efforts based on demonstrated leadership and technical capabilities.

In 2009, the CCR received a new designation from NSA-DHS as a CAE-IAE-R. This recognizes CCR's research role in the cyberspace domain. At the time of designation, only 22 academic institutions from across the country held a similar designation. At the present time, the CCR has over 20 active faculty members and annually conducts 40-50 research efforts. The CCR has eight active research laboratories spanning critical infrastructure, computer network exploitation and attack, wireless networking and security, malicious code analysis, and software assurance/protection. With the research generated within CCR, the Air Force-level Center is able to proudly produce the Air Force's new cyber operators.

## HISTORY OF CYBER 200/300

The Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) was stood up at the Air Force Institute of Technology (AFIT) under the leadership of AFIT's Center for Cyberspace Research (CCR) in June 2008 by the Secretary of the Air Force (SECAF) and the Chief of Staff of the Air Force (CSAF) to "develop and maintain a cadre of professionals who can fight offensively and defensively in cyberspace" and to "develop relationships with and maintain awareness about the activities of various cyber-related research, education, and training communities within the Air Force, our service partners in the DOD, various federal agencies, and civilian academic and commercial research organizations across the globe."

CCR was specifically selected because it had been doing just that since 2002. In addition to the SECAF and CSAF designation in 2008, the CCR has been competitively selected for several honors and "Center of Excellence" designations, including:

- NSA/DHS Research Center of Excellence
- NSA/DHS Center of Academic Excellence in Information Assurance Education
- National Science Foundation designated Center
- Placed first in 8 of the last 10 years in annual NSA-sponsored Cyber Defense Exercise
- 1st place DOD Cyber Crime Center Digital Forensics Challenge, 2007 and 2009

Other Center honors and awards include:

- 2008 and 2010 Air Force Science/Engineering Educator Year Award
- 2008 Air Force Junior Scientist of the Year Award
- 2010 IEEE National Outstanding Elec/Computer Eng Teacher Award
- 2010 Ralph J. Mastrandrea Research Contributions Award
- 2011 Government Information Security Leadership Award (Workforce Improvement)
- 2011 AETC Info Dominance (Cyber Ops) Award
- 2011 Fellow of the Information Systems Security Association
- 2011 Fellow, National Board of Information Security Examiners
- 2012 Government Information Security Leadership Award Finalist
- 2012 AETC National Public Service Award
- 2012 AF STEM Senior Military Engineer Year Award
- 2012 Ohio Governors "Distinguished Hispanic Ohioan Award" for Research Excellence and STEM Community Outreach
- 2013 AF Research and Development Year Award
- 2013 AETC STEM Senior Military Engineer Year Award
- 2013 AETC Outstanding Scientist-Mid Career Military Year Award
- 2013 AETC Outstanding Engineer Team Year Award
- 013 AETC Research Management Year Award
- 2013 AETC General Wilma Vaught Visionary Leadership Award
- 2013 AETC Info Dominance Outstanding Cyberspace Systems SNCO
- 2013 AETC Info Dominance Outstanding Information Assurance Element

Based on these credentials and the SECAF-directed mission, SAF/CIO A6 formally tasked the AF CyTCoE to develop educational courses that would enable the cyber workforce, regardless of specialty, to adapt to the quickly changing environment. Soon after, Air Education and Training Command, under the leadership of General Stephen Lorenz, directed the AF CyTCoE to host and execute the courses by October 2010 (FY11). Air University (under Lt Gen Allen Peck), as the education arm of AETC, recommended the AF CyTCoE at AFIT as the permanent location on 12 March 2010 based on several factors, such as proximity to AF cyber research (AFRL), acquisition (AFMC/AFLCMC), intelligence (NASIC), and combat communications units, low travel and per diem costs, and existing cyber educational facilities. On 2 April 2010, AETC formally announced AFIT as the permanent location for the Cyber 200 and Cyber 300 courses. Furthermore, the SECAF, in April 2008, and most recently the VCSAF in August 2010, called out Cyber 200/300 as a formal requirement for the Air Force via the Air Force Roadmap for Development of cyberspace Professionals. The Quadrennial Defense Review also called for DOD to grow a cadre of cyber experts to protect and defend information networks in Feb 2010.


## COMPENDIUM CONTRIBUTORS

- Dr. Robbert Mills
- Lt Col Joseph Wingo
- Maj Stacie Rembold
- Maj Cully Patch
- Capt Scott Anderson
- Capt Preston Iverson, Senior Editor
- Capt Jeremy Solmonson
- CW4 Elbert Peak
- Mr. Thomas Asojo
- Mr. Juan Lopez, Editor
- Mr. Paul Simon, Editor
- Mr. James Murphy
- Ms. Carrie Solberg

# SECTION 1: CYBER WORKFORCE

Operationalizing the 17D Workforce
Major Matthew T. Hyland, US Air Force, Air Force Space Command

**ABSTRACT**
Over the next decade, mid-level cyberspace operations leaders need to focus on developing a cadre of officers with deep operational expertise and experience in cyberspace operations. The 2008 decision to re-brand all communications and information officers as cyberspace operations officers has watered down the definition of what it means to be an operator, and caused all cyberspace operations officers to lose credibility with the operational community in the Air Force. Existing strengths in technical aptitude and education should be strengthened, but training and experience in traditional communications and information roles should be divested into another career field. Additional training and experience in the culture of operations and the processes and lexicon used by the rest of the Air Force's operational community should be required for all new and existing cyberspace operators, and the assignment process should be carefully monitored and adjusted to allow the development of deep operational experience without limiting career progression.

**PROBLEM STATEMENT**
1. In 2008, Senior Air Force leaders made a decision to operationalize cyberspace in the Air Force and to transform the communications and information officer career field (represented by the 33S Air Force Specialty Code, or AFSC) into a cyberspace operations officer career field (represented by the 17D AFSC).[1] While the motivation behind this transformation (completed in 2010) was to increase the focus on operating in the cyberspace domain and shift the mindset from mission support to operations,[2] the decision to wholesale convert all 33S officers into 17D officers, with no corresponding revision of their duties and responsibilities, limits their depth of operational experience and causes confusion.

The new operations career field was formed to encompass all functions to conduct or directly support cyberspace operations. In order to achieve this objective, cyberspace operations officers face different educational requirements and the expectation to see their job as operational and not strictly one of mission support.[3] Complicating this operational transition, however, is the fact that the cyberspace operations functional area inherited several non-cyberspace related duties from the communications and information era, such as postal operations, Freedom of Information Act oversight, knowledge management, records management, and others.[4] This dilution of operational responsibilities with mission support functions is not lost on junior cyberspace operations officers, and is perceived as dysfunction.[5]

When the transformation from 33S to 17D was executed, the educational requirements for award of the 33S Air Force specialty code were carried over to the new 17D career field. While the stated requirement calls for a Bachelor of Science (or graduate academic degree) in computer science, cyberspace security, electrical, computer or systems engineering, physics, mathematics, information systems, or information security/assurance, it also bears an exception to allow any candidate with 24 credit hours of general science courses.[6] This exception has the net effect of allowing nearly all candidates with a Bachelor of Science degree to enter the cyberspace operation career field as long as they've had 6 general science courses, a requirement met by every single graduate of the U.S. Air Force Academy. While the general sciences exception provides the widest possible pool of cyberspace operations candidates, it requires that computer and networking

fundamentals be taught in Undergraduate Cyber Training, consuming valuable and expensive training time that could otherwise be focused on the operational skills, mindset and lexicon that can make cyberspace operations more relevant to the rest of the Air Force operational community.

Over the past 15 years, the total number of active duty 17D officers (33S prior to 2010) as a percentage of overall officer end strength has dropped by 35%,[7] even as the mission area grows in scope and importance.[8] In the coming year, 17D end strength will be further reduced by 9.5% as a result of fiscal year 2014 force management decisions,[9] while operational requirements are simultaneously increasing by 5% due to the growth of U.S. Cyber Command Cyber Mission Forces. Further details on the relative and absolute size of the 33S / 17D career fields can be seen in Table 1 and Figure 1 in the Appendix. These seemingly senseless reductions can be partly attributed to an underestimation of the criticality of cyberspace operations to current and future Air Force and Joint operations among the Air Force's operational community and senior decision makers. Responsibilities of the cyberspace operations officer career field are defined by the Air Force include execution of cyberspace operations and information operations functions and activities, and specifically to plan, organize and direct cyberspace operations across the spectrum of mission areas within the cyberspace domain.[10] While the Air Force's formal description of the 17D officers' responsibilities excludes those non-operational functions, Air Force senior leaders and operators continue to see base communications squadrons and A6 organizations focus on these functions, contributing to a perception of the mission area as support versus operations.[11] Dilution of the operational nature of the mission area with non-operational functions inherited from the Communications and Information era are a direct contributor to this misperception.

2. The second challenge that needs to be overcome is the mixing of network operations with offensive and defensive cyberspace operations within a single Air Force specialty. The desire to increase breadth of experience for all 17D officers contradicts the need to develop cyberspace leaders with deep experience in cyberspace operations. Formal Air Force plans for the development of cyberspace professionals recognizes the distinction between various cyberspace roles: cyberspace operators plan, direct and execute full-spectrum operations in and through cyberspace, and cyberspace specialists provision, sustain and protect friendly portions of cyberspace.[12] In the enlisted force, we've created separate Air Force specialties for operators (1BXXX) and specialists (3DXXX), yet cyberspace officers are treated as virtually interchangeable with only an Air Force specialty suffix to differentiate.

While specialized training has been created for 17DXA offensive and defensive cyberspace operators (formally cyberspace defense) in the form of Intermediate Network Warfare Training, the 17D officer assignment team at Air Force Personnel Center reports that their assignment business rules limit "A-shreds" to 1-2 assignments in that operational area before rotating back to a "B-shred" (cyberspace control) cyber specialist position.[13] The stated rational for these business rules is to ensure all 17D officers "have an opportunity" to get some experience in offensive and defensive cyberspace operations. The Air Force cannot cultivate a war-fighting culture in cyberspace operations if officers in the mission area are treated like a first-grade soccer team where "everybody needs an opportunity" to play.[14] While there's a need to develop that war-fighting culture in all three cyberspace mission areas (offensive, defensive and network operations), the differences in required education, training and experience suggest they should be managed as such. The career path of an Air Force fighter or bomber pilot who spends most of his or her career in

positions dealing with combat air forces, or an Air Force tanker or airlift pilot who focuses primarily on mobility air forces, are instructive examples for how the Air Force should manage cyberspace operators. While there are certainly examples of aviators who transition far outside the community where they start their career, these cases should be the exception rather than the rule, and only considered once there's a sufficient pool of capable operational experts in each cyberspace operations mission area to meet operational requirements. In short, operational need should drive force management with "fairness" as a secondary consideration.

**RECOMMENDATION**

1. The Air Force should revise the academic requirements necessary to enter the cyberspace operations career field to require a more rigorous technical academic background, preferably in computer science, electrical/computer engineering, or information systems security. Rather than spend limited Air Force resources to develop and maintain general technical course material, the Air Force should leverage the capacity and ingenuity of the nation's academic institutions to provide that technical foundation. Much like Air Force pilot candidates attend an Initial Flight Screening course to provide non-military specific fundamentals of airmanship prior to entering Undergraduate Pilot Training,[15] the Air Force should leverage the civilian educational base to provide the fundamentals of cyberspace. With a common foundation of technical fundamentals across all students, Undergraduate Cyber Training can focus on the military-specific aspects of cyberspace operations.

2. Part of the training time freed up by requiring a more rigorous civilian technical education should be allocated to the same type of general operations training received all Air Force operators. General operational knowledge such as operational planning, Air Force and Joint doctrine, and a general-level understanding of how all Air Force operations are executed should be included. If possible, a common general operations curriculum could be shared amongst entry-level officer training courses for all rated and non-rated Air Force operations career fields to foster a common understanding and lexicon amongst all Air Force operators.

3. The existing 17D career field should be split into cyberspace warfare operations (17S) and network operations (17D) Air Force specialties. Much like the pilot career field is separated into bomber (11B), experimental (11E), fighter (11F), rescue (11H), trainer (11K), mobility (11M), reconnaissance (11R), special operations (11S), and remotely piloted aircraft (11U),[16] so should the cyberspace career field be smartly partitioned to optimize operational expertise (depth of experience) with leadership development (breadth of experience). A suggested alignment is for the cyberspace warfare operations Air Force specialty to focus on offensive and defensive cyberspace operations, U.S. Cyber Command Cyber Mission Forces, and the various staff and leadership positions directly related to those functions. The network operations Air Force specialty should focus on DoD Information Network Operations, the Joint Information Environment, and the various staff and leadership positions directly related to those functions. Mission support functions not aligned to either of those mission areas should be divested to another functional area such as the Mission Support Air Force specialty.[17] Alternative alignments could also be considered, but lack of a mission support mission area that is a "good fit" should not be an excuse to continue to saddle an operations functional area with mission support functions.

4. Current assignment policies should be altered to allow the development of deep operational experience through consecutive operational tours and the ability to remain in the cyberspace warfare mission area for most of an officer's career. Transitioning to a 17S and 17D structure would enable this recommendation, as cross utilization between two Air Force specialties would require deliberate action and a higher approval authority than in the current paradigm of a single Air Force specialty with a differentiating suffix ("shred"). Allowing an officer to spend much of their career in one of these operational areas will cultivate the deep operational expertise that is needed to be successful in an operational domain that grows more contested each year, while operations in all other domains continue to become more reliant on it. Further study is recommended to determine the specific accession and sustainment requirements and anticipated retention models that may drive cross flow or cross utilization between 17D and 17S, or even necessary cross flow in to or out from the 17XX functional area.

## COUNTERARGUMENT

Concerns have been expressed that a Cyberspace Warfare Operations (17S) career field will be too small to be viable. While there may only be about 250 "A-shred" requirements on the books today,[18] that number is expected to grow with the stand up of the U.S. Cyber Command Cyber Mission Force, and as Combatant Commands transform some their headquarters staffs from a communications focus to a cyber warfare focus with the stand up of Joint Cyber Centers. These changes will certainly put the proposed 17S career field in the same ballpark as rescue pilots (555) and experimental test pilots (141).[19]

Others have cautioned that retaining officers in such a niche mission area for most of a career will "stove pipe" their experience and limit promotion opportunity. To mitigate this outcome, viable career paths should be mapped out to provide commanders and assignment officers guidance and direction on how to balance depth and breadth of experience, while ensuring the necessary operational expertise (depth) is not sacrificed for the sake of breadth. Limited but deliberate cross flow between 17S and 17D should be explored as a potential solution.

## CONCLUSION

Despite concerns that a cyberspace warfare operations career field will be too small and limit promotion opportunities, the current strategy of cyberspace officers with an incredibly wide breadth of experience is limiting the AF's ability to develop true cyberspace operations leaders. Over the next decade, mid-level cyberspace operations leaders need to focus on developing a cadre of officers with deep operational expertise who are competitive for joint cyberspace operations leadership roles.

## Appendix

| |
|---|
| FY99 |
| FY00 |
| FY01 |
| FY02 |
| FY03 |
| FY04 |
| FY05 |
| FY06 |
| FY07 |
| FY08 |
| FY09 |
| FY10 |
| FY11 |
| FY12 |
| FY13 |

**Table 1**: 33S/17D End Strength by year[20,21,22]

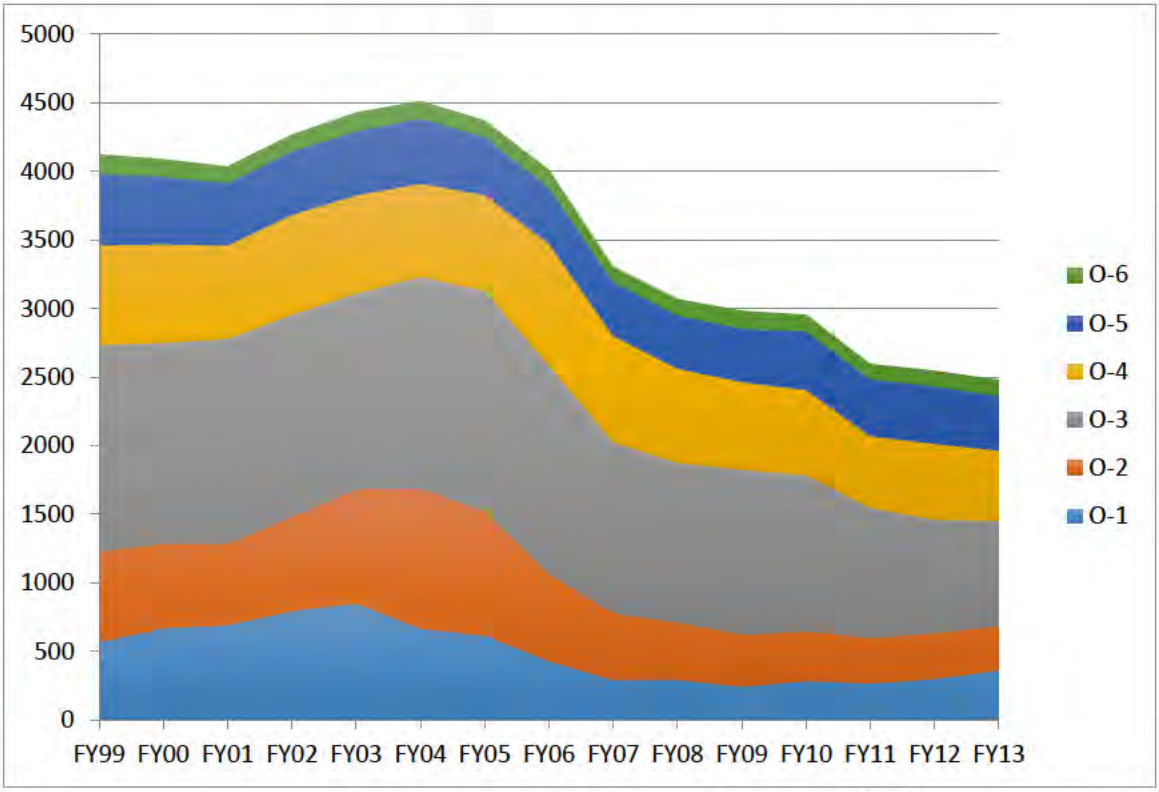



**Figure 1**: 33S/17D End Strength by year[23,24,25]

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] Terry, Katrina A. "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field", p17.
[2] Ibid, 32-33.
[3] Rolfsen, Bruce. "3,000 Officers Switch to Cyberspace Specialty".
[4] Terry, Katrina A. "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field", p37, 50.
[5] Lee, Robert M. "The Failing of Air Force Cyber".
[6] Air Force Personnel Center. Air Force Officer Classification Directory.
[7] U.S. Air Force. Interactive Demographic Analysis System (IDEAS).
[8] Harris, Shane. "The Complex".
[9] Air Force Personnel Center. "Cyberspace Operations - Spread the Word".
[10] Air Force Personnel Center. Air Force Officer Classification Directory.
[11] Hoffman, Mike. "Cyber Security, an Air Force punchline?"
[12] Air Staff, AF/A3O-COF. The Air Force Roadmap for the Development of Cyberspace Professionals (Change 1), p14-15.
[13] Air Force Personnel Center. "Cyberspace Operations - Spread the Word".
[14] Franz, Timothy. "The Cyber Warfare Professional", p93.
[15] Hammond, Mike. Initial Flight Screening Operations begin today.
[16] Air Force Personnel Center. Air Force Officer Classification Directory.
[17] Terry, Katrina A. "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field", p52.
[18] Air Force Personnel Center. "Cyberspace Operations - Spread the Word".
[19] U.S. Air Force. Interactive Demographic Analysis System (IDEAS).
[20] Air Force Association. "The Air Force in Facts and Figures". May 2005.
[21] Air Force Association. "The Air Force in Facts and Figures". May 2013.
[22] U.S. Air Force. Interactive Demographic Analysis System (IDEAS).
[23] Air Force Association. "The Air Force in Facts and Figures". May 2005.
[24] Air Force Association. "The Air Force in Facts and Figures". May 2013.
[25] U.S. Air Force. Interactive Demographic Analysis System (IDEAS).

## BIBLIOGRAPHY

Air Force Association. "The Air Force in Facts and Figures". Air Force Magazine, May 2013: 36-53.

Air Force Association. "The Air Force in Facts and Figures". Air Force Magazine, May 2005: 44-82.

Air Force Personnel Center. Air Force Officer Classification Directory. AFOCD, HQ AFPC/DPSIC, U.S. Air Force, Randolph AFB, TX: HQ AFPC/DPS, 2013.

Air Force Personnel Center. "Cyberspace Operations - Spread the Word". Briefing, Colorado Springs, CO, 2014.

Air Staff, AF/A3O-COF. The Air Force Roadmap for the Development of Cyberspace Professionals (Change 1). Washington, DC: U.S. Air Force, 2010.

Franz, Timothy. "The Cyber Warfare Professional". Air & Space Power Journal (Air University), Summer 2011: 87-99.

Hammond, Mike. Initial Flight Screening Operations begin today. October 13, 2006. http://www.aetc.af.mil/news/story.asp?storyID=123028911 (accessed March 8, 2014).

Harris, Shane. "The Complex". Foreign Policy. July 01, 2013. http://complex.foreignpolicy.com/posts/2013/07/01/air_forces_cyber_chief_for_frank_discussion_about_rules_of_network_war (accessed February 21, 2014).

Hoffman, Mike. "Cyber Security, an Air Force punchline?" Defense Tech. Sep 26, 2012. http://defensetech.org/2012/09/26/cyber-security-an-air-force-punchline/ (accessed Mar 5, 2014).

Lee, Robert M. "The Failing of Air Force Cyber". SIGNAL Magazine, Nov 1, 2013.

Rolfsen, Bruce. "3,000 Officers Switch to Cyberspace Specialty". Air Force Times. May 17, 2010. http://www.airforcetimes.com/article/20100517/NEWS/5170308/3-000-officers-switch-cyberspace-specialty (accessed March 8, 2014).

Terry, Katrina A. "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field". Graduate Research Project, Department of Electrical & Computer Engineering, Air Force Institute of Technology, Dayton, OH, 2011.

U.S. Air Force. Interactive Demographic Analysis System (IDEAS). January 31, 2014. http://access.afpc.af.mil (accessed March 8, 2014).

Cyberspace Leader Perspective on Mid-Level Cyber Leadership
Maj Reid Novotny, US Air Force, 35th Communications Squadron

**ABSTRACT**
There are three ideals that Cyber officers have chased throughout our history; consolidation, technology, and requirements. The evolution of the Air Force network from single computers connected on a base, to one base one network, followed by the Air Force Network (AFNET), and now moving toward the Joint Information Environment (JIE) is a prime example of chasing consolidation.[1] Within this philosophy and those of the past, Cyber officers have chased technology which is evident in the iPads and iPhones tethered off of our Microsoft based network.[2] Finally, mid-level Cyber officers are really good at chasing 100% requirements and that is exactly why, for example, we still do not have a cradle to grave system to process personnel data through within Military Personnel Data System (MilPDS).[3] This paper will cover the strengths and weaknesses of the current Cyber officer and propose an end state of what the specific job should be for a mid-level Cyber officer in the future by continuing or stopping to chase these ideals. The one thing that has not changed and will never change is the ability for mid-level Communication and Information now Cyberspace officers is the ability to master the art and science of the current technology and best apply it to accomplish the mission. With this in mind, there are a vast array of positions that a Cyberspace officer may hold within the DoD and in order to cover this topic as thoroughly as possible, this paper is written from the perspective of what a typical base Communications Squadron Cyber officer can bring to the mission of any Squadron, Group, Wing, and the Air Force at large.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
The AF vision entitled, "The World's Greatest Air Force; Powered by Airmen, fueled by Innovation"[4] is very applicable to what Cyber officers should focus on but often times miss the mark. Chasing technology and requirements are the two aspects of Cyber officers that must change and that do not directly map to our AF vision. Chasing consolidation is coping mechanism which is not totally aligned by our vision can will enable Cyber officers of the future to concentrate on innovation. This section describes examples of the result of these types of behaviors.

1. Cyber officers have always chased consolidation because we are stuck at the impossible apex of two opposing forces of Moore's Law and resource reduction through force management, force shaping, sequestration, and the like.[5] Sharing of information and more importantly creating a command and control structure for this information started from a memo written by Joseph Licklider in 1963 working for the Advanced Research Projects Agency (precursor to Defense Advanced Research Projects Agency or DARPA).[6] The Air Force was an early adopter of computing technology and networking technology.[7] Once it was established that technology was available to connect computers the amount of people needed to maintain connections has decreased based on better networking technology and the amount of information available has increased at that same rate. As discussed in Cyber 300's presentation of Situational Awareness, we have moved from needing 3 words per minute to execute command and control in the Civil War to possibly needing 1.5 trillion in future wars.[8] In order for the Cyber officer to maintain the balance between the signal demand of information and reduction they must champion consolidation at many levels. The latest iteration of chasing consolidation to save money and manpower is the push for JIE.

According to DISA, the JIE Target State, "optimizes the use of the DoD's IT assets by converging communications, computing, and enterprise services into a single joint platform…"[9]

2. Chasing technology for the sake of technology is one of the largest problems that Cyber officers have. At the base level, Cyber officers concentrate on the core services that are provided by the AFNetOps organization from their local Network Control Center to the consolidated Enterprise Service Unit (ESU). These core services that are delivered to their base users include standard desktop, email, unified capabilities, collaboration, and mobility solutions to name a few. Currently the Air Force runs Microsoft Windows 7 and soon to be Microsoft Windows 8 for the standard desktop, Microsoft Outlook and Microsoft Exchange for email, Microsoft Office Communications Server soon to by Microsoft Lync for unified capabilities, Microsoft SharePoint for collaboration, and BlackBerry Limited BlackBerry with BlackBerry Enterprise Servers for mobility.[10] As BlackBerry products lag behind perceptually the only logical option for the Air Force is to replace BlackBerry into this current Microsoft architecture with Apple iPhones with a Good Mobile server instead of Microsoft Windows Mobile phones tied directly to Microsoft Exchange. The only conclusion that can be drawn is that Cyber officers are chasing technology, most likely driven by senior leadership, versus making the logical decision to reduction the complexity of the network and increase the capability to the user by allowing them to access unified capabilities, collaboration, and email on their mobile device.[11]

3. Chasing requirements is not a unique problem to Cyber officers and there is a reason in which the Department of Defense (DoD) must carefully adhere to requirements development. This prevailing thought process stems from a few cultural items within the information technology community but a large driver of developing 100% requirements comes from the DoD Acquisition policy. Split into two overarching directives; DoD Directive 5000.01 for management principles and DoD Directive 5000.02 which explains in great detail the Defense Acquisition System, these two documents drive system acquisition within the DoD that is reportable to Congress, in general a program of $250,000 or more. Within the 232 page DoD Directive 5000.02 it says the word requirement 657 times. Although there is distinction made between a Major Defense Acquisition Program (buying a plane for example) and Major Automated Information System (buying a new Air Force Portal) there is still much to be desired on the speed of execution. This rigor in the acquisition process is value added to prevent waste of government funds and also to ensure that software written for military pay works as advertised. The problem with this mindset is that at the base level it is often times difficult to get a clear requirement from a customer and then the 100% solution is often too expensive or too time consuming to create.[12] [13]

**RECOMMENDATIONS**

Cyber officers in the future will have to change their purpose within the Air Force equated to not fighting a losing defensive war. From Sun Tzu himself, "…should he strengthen his left, he will weaken his right; should he strengthen his right, he will weaken his left. If he sends reinforcements everywhere, he will everywhere be weak."[14] In Cyber officer terms we must move away from focusing on net-centricity/technology and pivot toward exploitation of our inherent strength of mastering the cyber domain to increase warfighter effectiveness. This section covers the answer to the supporting questions to the topic which include enduring current strengths, current strengths that might change, and current weaknesses and if they can be overcome.

1. What are the current strengths and can/will they endure? Chasing consolidation is a means of survival for Cyber officers and it is imperative that it survives into the future. At the base level, there are two flights, Operations and Plans/Resources, which are both affected by consolidation. Resources will now be allocated at the Air Force level through the new establishment of the Installation and Mission Support Command (AFIMSC). This new command will take over base civil engineering and cyber requirements as their main tenants. "Although driven by budget constraints, this new organization provides the AF a once in a lifetime opportunity to more effectively and efficiently manage installation resources and ease the burden on mission commanders so they can focus on their core missions."[15] Within Operations, the Air Force currently has their portion of the DoD NetOps concept realized within the AFNETOPS organizational structure. A Cyber leader within a base is charged with supporting the touch maintenance of their network but the administration is executed at levels above the base. These efforts and similar concepts should continue to be strengths of Cyber officers in the future to save money, save manpower, and concentrate on ability to deliver the information required for Airmen at all levels of the Air Force.

2. What current strengths will wither by neglect or be overcome by change? Chasing technology is a losing battle for mid-tier Cyber officers and should wither and be overcome by change. Program Objective Memorandum and acquisition cycles will never keep pace with current technology improvements because they are based on acquiring tanks and planes[16] but that is not where we can have value added to the Air Force. A current strength of this group of officers is the ability to apply technology to problem sets. A decade old study from the Air Force Scientific Advisory Board about Human-Systems Integration in Air Force Weapon Systems Development and Acquisition states that, "…the ever-increasing demand for accurate rapid response to dynamic mission environments, the human capability to cope with information processing demands has become a limiting factor on system performance."[17] The Air Force has plenty of data we just need Cyber officers to lead the way in making this information relevant to Airmen.

Cyber officers at the Squadron level are uniquely positioned to reinvent their purpose in the Air Force as one of mastering the knowledge that we have, making it understandable and actionable to a commander, and improving processes along the way. Nowhere in the Air Force mission statement is there any evidence that having knowledge of how to route an enlisted performance report (EPR) will help us Fly, Fight, and Win. Creation of common operating pictures to exploit the digital landfills within the Air Force to create actionable knowledge for a commander is another role for Cyber officers. An EPR by itself gives little insight into the health of a Squadron or Wing but if you add all of the EPRs in the Wing, Fitness Scores, and training status for all Airmen for example; that creates a picture of readiness that is impossible to generate through reading spreadsheets. We need Cyber officers to advocate for changing Figure 1. Fitness Data to Figure 2. Fitness Picture. A good Cyber officer can and will break down the political barriers between the fitness scores, training statistics, and more data owners to create better situational awareness for the local commanders as in Figure 3. Readiness Status.

Fitness Data

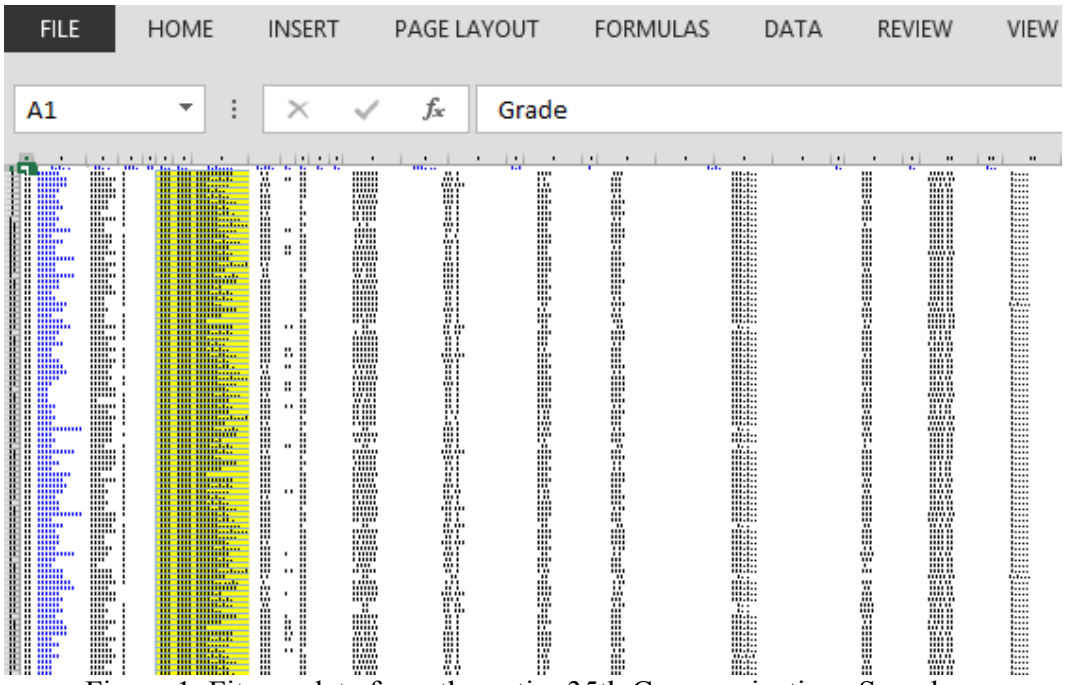



Figure 1. Fitness data from the entire 35th Communications Squadron

Fitness Picture

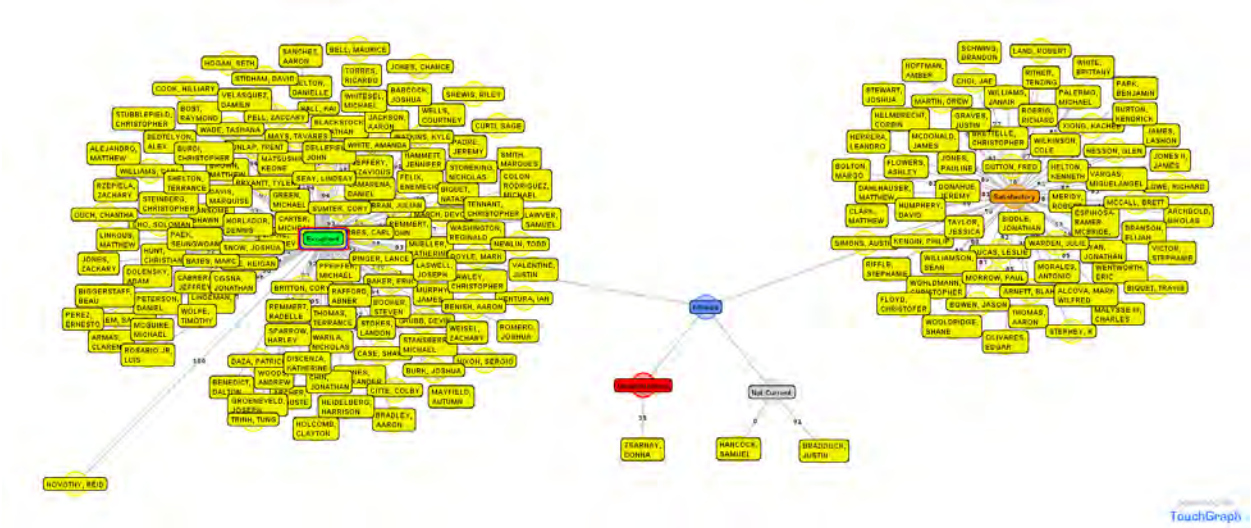


Figure 2. Fitness picture from the data below showing scores and categories

Readiness Status

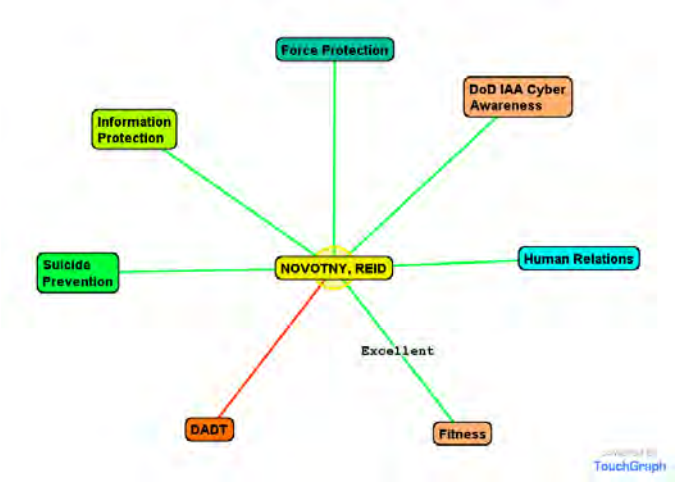



Figure 3. Readiness status for Maj Novotny

3. What are current weaknesses and will they persist? Can the weaknesses be rectified? Chasing requirements or what can be referred to as 100% requirement is a major weakness of Cyber officers and it needs to be rectified in the future. Air Staff should concentrate on using the DoD Acquisition guidance to obtain flexible platforms for Cyber officers to create solutions at the lowest level. An example would be the acquisition of an Air Force wide collaborative platform like SharePoint. Using the fact that EPR routing does not make a pilot more effective a Cyber officer created the Evaluation Management System (EMS) using SharePoint as a platform which does not come close to meeting the Air Force Personnel 100% requirement but is 100% better than nothing. During the initial development and rollout of EMS in 2007 and 2008, most personnel officers at all levels to include the Air Force Personnel Center and Air Staff pointed toward their own 100% solution that would once and for all create an automated lifecycle for all evaluations. According to the Personnel Services Delivery Transformation information on the Air Force Portal, "…this system will deliver a very robust capability to electronically create, process, store and access records necessary for completion of personnel transactions."[18] This program would have connections to the Automated Records Management System (ARMS) and MilPDS making a complete cradle to grave system for this vital aspect of all Airmen's careers. Furthermore as this system comes online in 2011, "estimated savings are huge: $1.5 million in the first year and $2 million per each subsequent year for a five-year total savings of $9.5 million"[19]. As you can imagine this capability is still not available and SES Robert Shofner from the Air Force Life Cycle Management Center said, "I have determined that it is in the best interest of the Air Force to stop further work on the eForms contract…since the program is not on path to deliver a sustainable solution."[20] EMS does not integrate with the personnel system to generate a RIP nor does it deliver the final product to ARMS and MilPDS. EMS does eliminate the need to have blue folders with floppy disks in them and automates the coordination process of performance reports throughout the majority of the Air Force. Cyber officers need to back away from chasing the 100% solution when they can and deliver solutions that Airmen need in order to execute their mission more effectively.

**COUNTERARGUMENT**

There are many counterarguments to why Cyber officers should or should not chase consolidation, chase requirements, and chase technology. With each consolidation the lowest level cyber leader loses more and more ability to have an immediate impact on delivering capability to their

customers. Within the AFNetOps structure there are a little over 100 services provided on the network from email and network authentication to firewalls and network traffic routing. Of those, the base communications squadron has administrative control over 19%. Saying that another way, not more than 10 years ago, a base would have had 100% control and now an Airmen must put in a ticket and wait in a queue if any of the 81% of the network services need support.[21] To reverse this trend, money and manpower must be returned to the base level.

Chasing requirements or a 100% solution is also not always a bad quality to have in a Cyber officer. Lyytinen and Robey wrote about why large information technology systems develops fail back in 1999 and the reasons are still true today. They wrote about how changing and unclear requirements often would push programs past schedule and over budget. For example, "Taurus was a very complex project, involving novel technologies and massive scale, ineffective project controls allowed requirements to change continuously throughout the project"[22] which eventually led to the complete failure of the development project. Establishing, maintaining, and reaching the requirements for programs should in theory deliver information systems that meet the needs of the users who developed the original requirements.

Chasing technology might always have a role within the Cyber officer toolkit for many reasons to include that many officers enjoy being technologists (aka tech-geeks). The argument can be made that without the first Airmen to purchase a hub to network two computers all the way to the Airmen who bought and iPad and made it work on our network we might not be at the current state of technology within the Air Force. The Air Force has a very large budget and expends a great deal of it on advances in technology to include cyber initiatives which end up supporting our mission. A comparison to our allies is that the Japanese Self Defense Forces Communications Squadron on Misawa Air Base has one computer connected to the Internet and it runs Microsoft Windows XP. Keeping up with the change in technology has merit especially because of the pace in which change happens within cyber. Without a cadre of Cyber minded officers to lean forward and try new technologies we might all be running XP and passing Morse code.

## CONCLUSION

The summation of the arguments presented in this paper point toward the specific question of. "What do mid-level cyberspace operations leaders see as their specific "job" for the next decade?" Continued chasing of centralization will enable Cyber officers to shift focus to see a need in their Squadron, Group, or Wing and apply the correct technology to fix to that problem. We need to stop chasing the 100% requirement and pursue quick kills that move the ball forward. No different than the call to action in 2006 by then Secretary of the Air Force the Honorable Michael Wynne when he challenged all Airmen to, "…ask yourself, 'What have I improved today?'"[23] which established the Air Force Smart Operations for the 21st Century. Finally we need to stop chasing technology because the majority of our fixes to problems are adding more technology. "Indeed, the entire IS (information system) profession perpetuates the myth that better technology, and more of it, are the remedies for practical problems"[24]. A mid-level cyberspace operations leader should master the information and capabilities that are already present in this domain and ensure that all Airmen can increase their mission effectiveness through increased situational awareness and better workflows.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

1. DISA, 2014.
2. Air Force Office of Cyberspace Operations, 4.
3. Gildea, 2013.
4. A Vision for the United States Air Force, 1.
5. Moore, 1965.
6. Waldrop, 79.
7. Rogers, 1962.
8. Naylor, 2014.
9. DISA, 5.
10. Novotny, 2013.
11. Air Force Office of Cyberspace Operations, 2013.
12. DoDI 5000.01, 2007.
13. DoDI 5000.02, 2013.
14. Tzu, Sun, Chapter VI.
15. AFIMSC, 2.
16. DoDI 5000.02, 2013.
17. Erickson and Zacharias, V.
18. PSDT, 2008.
19. Ibid.
20. Shofner, 2013.
21. Novotny, 2013.
22. Lyytinen & Robey, 85.
23. Wynn, 2006.
24. Lyytinen & Robey, 95

## BIBLIOGRAPHY

Air Force A7 (2014). *Air Force Installation and Mission Support Center* (*AFIMSC) Draft Strategic Intent.* Received from Air Staff A7, dated 29 April 2014.

Air Force Office of Cyberspace Operations (2013). *Air Force Mobile Device Strategy.* Retrieved from https://www.my.af.mil/USAF/AFP40/d/s2D8EB9D63C2AF7D8013C3AA2C25C00D9/Files/Cyber_Spt_Strategys/DRAFT%20AF%20Mobile%20Device%20Strategy.pdf (accessed 16 June 2014).

The World's Greatest Air Force Powered by Airmen, Fueled by Innovation: A Vision for the United States Air Force (2012). Retrieved from https://www.my.af.mil/gcss-afbvpcp/USAF/AFP40/d/s6925EC1356510FB5E044080020E329A9/Files/editorial/A_Vision_For_The_USAF.pdf?channelPageId=s6925EC1356510FB5E044080020E329A9&programId=t2D8EB9D62D713923012DA5B988A30B7F (accessed 13 June 2014).

Defense Information Systems Agency (2014). *Enabling the Joint Information Environment (JIE).* Retrieved from http://www.disa.mil/About/Our-Work/~/media/Files/DISA/About/JIE101_000.pdf (accessed 14 June 2014).

Department of Defense Instruction 5000.01 (2007). *The Defense Acquisition System.*

Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf (accessed 15 June 2014).

Department of Defense Instruction 5000.02 (2013). *Operation of the Defense Acquisition System.* Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/500002_interim.pdf (accessed 15 June 2014).

Erickson, Jeffery & Zacharias, Greg (2004). *Human-System Integration in Air Force Weapon Systems Development and Acquisition.* Retrieved from http://www.sab.af.mil/library/index.asp (accessed 14 June 2014).

Gildea, Debbie (2013). "MilPDS upgrade begins." *Air Force Personnel Center Public Affairs.* Retrieved from http://www.afpc.af.mil/news/story.asp?id=123338605 (accessed 15 June 2014).

Lyytinen, K. & Robey, D. (1999). *Learning Failure in Information Systems Development*. Information Systems Journal, 9: (pp. 85-101).

Moore, Gordon E. (1965). "Cramming more components onto integrated circuits." Electronics Magazine (p. 4).

Naylor, Jeffery (10 June 2014). Situational Awareness: 3103. *Cyber 300*. Lecture conducted from Wright Patterson Air Force Base, Oh.

Novotny, Reid J. (2013). Analysis of NetOps Services Delivered to Misawa Air Base.

Personnel Services Delivery Transformation (2008). *PSDT eForm Initiative*. Retrieved from https://www.my.af.mil/gcss-af/USAF/ep/contentView.do?contentType=EDITORIAL&contentId=c0ECF2BB843F9745201440284657A0063&programId=tA4057E1F2F0EE517012F21C6703E02E9&channelPageId=s6925EC1333480FB5E044080020E329A9 (accessed on 12 June 2014).

Rogers, E. M. (1962). Diffusion of innovations. New York: Free Press.

Shofner, Robert (2013). *Acquisition Decision Memorandum on eForms Application.* Signed 24 April 2013.

Tzu, Sun (1910). *The Art of War.* Translated by Lionel Giles. Retrieved from http://classics.mit.edu/Tzu/artwar.html (accessed 13 June 2014).

Waldrop, Mitch (2009). "DARPA and the Internet Revolution." DARPA Magazine (pp. 78-85).

Wynn, Michael, W. (2006). *Air Force Smart Operations 21.* Retrieved from https://www.my.af.mil/ gcss-af/USAF/AFP40/Attachment/20070705/Letter%20to%20Airmen_030806.pdf?programId=t5FDEA9F021DBFDC80121E3CF9AE9001F&channelPageId=s6925EC13515C0FB5E044080020E329A9 (accessed 15 June 2014).

The Us Air Force's Critical Offensive Cyberspace Capabilities: People & Partnerships

Maj Eric Stride, US Air Force, 315 Network Warfare Squadron

**ABSTRACT**

In the eight years since the United States Air Force has added cyberspace as a part of its mission statement, two capabilities have stood out as necessary for the success of offensive cyberspace operations, those are the people and the partnerships. Airmen that execute offensive cyberspace operations receive some of the most highly technical and challenging training of any career field in the United States Air Force. This training makes them extremely valuable to the military and to outside industry. The United States Air Force is not currently developing enough, nor retaining enough of these Airmen to meet the needs of the Joint Force and the Combatant Commanders. In order to do so, the United States Air Force needs to modify its training and retention strategies for this extremely talented cyber corps. The partnerships the United States Air Force has with other Department of Defense organizations, namely the National Security Agency (NSA), is a required force multiplier that enables successful, nation-state level, cutting edge cyberspace operations. Some military leaders erroneously believe that the service cyber efforts should be "divorced" from the NSA as soon as possible. The NSA has been engaged in the cyber domain longer than any of the services. The lessons learned over the years, the support infrastructure, technical development and fielding processes, tactics, techniques, and procedures (TTP), and domain insight will be difficult to replicate, and even if they could replicate it, doing so would be fiscally irresponsible. The services lack the depth of knowledge at this time to execute offensive cyber operations without the NSA partnership. A rushed "divorce" from the NSA and failure to maintain that partnership will result in failure for the services in offensive cyber.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

The demand for cyber personnel has finally been defined. The Cyber Mission Force is comprised of 6,244 operational billets from across all the services. The United States Air Force (USAF) is responsible for 1,715 of those billets.[1] Of the offensive cyber teams in this force, namely the National Mission Teams (NMTs) and the Combat Mission Teams (CMTs)[2], the USAF will field four of US Cyber Command's 13 NMTs and field eight of US Cyber Command's 27 CMTs[3]. Additionally, the USAF will field seven of the 25 associated direct support teams[4]. The remaining 20 of the Air Force's 39 teams will be Cyber Protection Teams.[5] The Cyber Mission Force build-out identifies for the first time for the USAF "hard requirements" for the numbers and mission break-out of cyber personnel, especially for the offensive cyber forces. Prior to this, it was difficult for the USAF to accurately quantify its personnel commitment to cyber. Even congress is concerned with how the USAF has been organizing and fielding cyber forces: "the [Subcommittee on Intelligence, Emerging Threats and Capabilities] believes that for the Air Force, it is particularly difficult to understand the breadth and depth of investment and focus in cyber given the dispersion of cyber manpower across multiple program areas and operating environments."[6] For both the offensive and defensive needs of the new cyber force, the USAF had only 451 existing billets available, leaving a remaining 1,264 to be sourced, assigned, filled, and trained between fiscal years 2014 through 2016 to meet the USAF's requirements of the Cyber Mission Force.[7]

This newly defined demand for cyber forces creates a problem for the USAF for two main reasons, the time required to train the members into one of the 42 cyber work roles[8] is significant, and that

the schoolhouse's throughput does not meet the demand. For the USAF Cyber Mission Teams, approximately 80% of the team will be military members, and of those military members, approximately 90% will be enlisted, so we'll focus on the enlisted aspect of the cyber force in this analysis.[9] Specifically, we will look at the cyber operator or cyber analyst work roles on the offensive teams.

The cyber operator career field, 1B4X1, and the cyber analyst career field, 1N4X1A, have different training tracks to lead an Airmen to qualified status, but both are lengthy. For the cyber operators, they begin their technical training at a 17-week Cyber Defense Operations (CDO) course, much of which mirrors the 24-week 17D-series officer Undergraduate Cyber Training (UCT) at Keesler AFB, Mississippi.[10] The goal of CDO/UCT is to serve as pipeline training, providing the fundamentals to "establish, secure, operate, assess and actively defend seven types of networks, including command and control systems, IP, telephony, satellite and mobile telecommunications."[11] When this course was created in 2011, the USAF's requirement for cyberspace operators was not fully realized, as a result, this course was designed with a throughput of only about 70 personnel per year, 50 active duty cross-trainees and 20 Air National Guard members.[12] Once complete with CDO, the 1B4 enlisted cyber operators and the 17DXA officers proceed to Intermediate Network Warfare Training (INWT) at Hurlburt Field, Florida. INWT teaches "advanced Cyber Operations fundamentals including policy, doctrine, employment, executing organizations and missions, operational functions, and law and ethics",[13] it is designed to be Initial Qualification Training (IQT) for the cyber space operators. INWT was designed with an annual throughput of approximately 192 students, both officer and enlisted, per year.[14] Following INWT, students would then report to an operational unit to begin their Mission Qualification Training. The Air Force sends all of its offensive cyber operators through a 5-week preparatory course, before sending them on to a 6-month joint service cyber operations course, which is currently only offered in Maryland. Finally before they become qualified, they must complete Job Qualification Standards (JQS) and evaluations. 18 months, two PCSs, multiple extended TDYs, and nearly $200,000 later, we have one qualified cyberspace operator – at the "basic level". It will take approximately five to six more months, and another training course, before they move up to the "apprentice" level where these cyberspace operators will be of the most utility to their assigned teams.

The cyberspace analysts have a similar lengthy training pipeline, to include a 22-week technical training course at Goodfellow AFB, Texas,[15] and a six-month PCS to Pensacola, Florida for the Joint Cyber Analysis Course. Once at their unit of assignment, they have at least another three months of USCYBERCOM-prescribed joint training courses coupled with on-the-job training (OJT) in order to become qualified in their cyber analyst work role.

The next issue facing the USAF when it comes to manning the Cyber Mission Force is retaining personnel. To the credit of the USAF, at least both of these enlisted Air Force Specialty Codes (AFSCs) were kept on the selective reenlistment bonus (SRB) list when they cut approximately 45 AFSCs from the list in late 2013.[16] The challenge that they face is two-fold, the service invests a significant amount of training, both in time and value into each of these Airmen making them extremely marketable on the outside, and currently the USAF does not ensure that it receives adequate return on investment.

"To continue recruiting and retaining talent ... we must build rewarding, long-term cyber career paths" Secretary of Defense Chuck Hagel stated at General Alexander's retirement.[17] This means that we need to ensure that the members are satisfied with their jobs, members have a defined path for progression, and we should be compensating members close to what their counter-parts in the civilian sector make. An E-5 with 10 years of service will make $52,000 - $62,000 annually, including allowances, depending on where they are living. Fortunately, when you include the SRB,[18] this brings the annual compensation to approximately $62,000 - $75,000. However, when you research the salary of a "Systems/Application Security Analyst", a comparable non-military job, we discover that the United States national average median salary plus bonuses is nearly $85,000.[19] Frequently, offensive cyberspace operators that have achieved the "apprentice" level certification can obtain 6-figure salaries outside of the military. The bottom-line is that we are under-paying these highly technical members of our force.

The next challenge for the USAF is ensuring proper return-on-investment for the expensive and time-consuming training we provide to these offensive cyberspace operators and analysts. Unlike pilots and navigators who incur a 10-year or six-year active duty service commitment (ADSC), respectively, upon completion of their lengthy and expensive training, the current provisions of Air Force Instruction (AFI) 36-2107 only allows for a three-year ADSC for completion of "technical training" – this is what applies to the cyber operators and analysts. The 2014 Quadrennial Defense Review (QDR) states "The Department of Defense will continue to invest in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel."[20] A proper strategy for retaining personnel includes a component for ensuring the proper return-on-investment policies are in place prior to a member entering the training pipeline. The USAF will have to make appropriate changes to both compensation and ADSC policies to ensure that it is meeting the DoD objectives with cyber personnel sustainment.

The next key capability for the USAF in offensive cyberspace operations is partnerships. Specifically, the partnership with the National Security Agency (NSA). This partnership is an extremely valuable force-multiplier for all of the services. However, there are leaders within the services that do not seem to fully grasp the value of this partnership, and believe that "divorce" from the NSA should be sought out quickly. Ellen Nakashima from the Washington Post summarizes many of the concerns in her January 27, 2013 article:

> Some military and defense officials question whether the Cyber Command can reach its full potential as a military command as long as it is so dependent on the NSA and is led by the NSA's director. The close relationship between the two has had its advantages, officials say: The agency can peer into foreign networks and provide the command with intelligence, including in cases in which an adversary is suspected of planning a computer attack or developing a potent virus.
>
> There's a "cogent argument" to be made that for the Cyber Command to become a true military command, "you sever that" relationship, one military official said.
>
> But, in fact, said one former intelligence official, the NSA uses military personnel to do much of its work and pays for a good portion of the services' cyber operators. "That's been

> the plan all along," the former official said. "Take the talent resident in NSA, turn it into [cyber] attack talent."[21]

The argument to "divorce" or "sever" the relationship between US Cyber Command and the NSA is frequently made by personnel that do not fully understand the cryptologic platform[22] and the significant advantages gained by the services by using it. The NSA has been engaged in the cyber domain longer than any of the services. The NSA has invested extensive resources into operations in this domain. The lessons learned over the years by the NSA feed into the current TTPs – which are always evolving. The former Commander of US Cyber Command and Director of the NSA, General Alexander, said it well during his testimony before congress on February 27th, 2014:

> At USCYBERCOM, we understand that re-creating a mirror capability for the military would not make operational or fiscal sense. The best, and only, way to meet our nation's needs today, to bring the military cyber force to life, and to exercise good stewardship of our nation's resources is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the resources nor the time to redevelop from scratch the capability that we gain now by working with our co-located NSA partners.[23]

The former Commander and Director is stating that the military services don't have the expertise to replicate the large and complex analytical infrastructure provided by NSA, and even if they did, it doesn't make fiscal sense. Moreover, if you try to rush a "divorce" from the NSA, the result will be the failure of the Cyber Mission Force, as the military services do not have the requisite experience in the domain to ensure safe, efficient, and effective operations. That is not to say that they could not get there eventually, but all of the services are a long way from realizing the capabilities to successfully execute offensive cyberspace operations at a nation-state-level without the assistance of the NSA.

**RECOMMENDATION**

Increasing the capacity of the schoolhouse training for the offensive cyber professionals is required if the USAF is going to meet the manning levels required to field and sustain the NMTs, CMTs, and their associated direct support teams. Fortunately, the USAF has already placed some resources towards this effort, as the service committed $8.3 million more in fiscal year 2015 than allocated in fiscal year 2014 specifically to the increase the throughput of the CDO course at Keesler AFB and INWT at Hurlburt Field.[24] The USAF will need to continue analysis of the throughput to ensure that the ongoing needs of the Cyber Mission Force is met and compensates for attrition.

The USAF needs to look at ways to make the training pipeline more efficient. It doesn't make fiscal sense to send personnel TDY to Keesler AFB, Mississippi for a 17-week course, and then TDY Hurlburt Field, Florida for a seven-week course. The Air Force should investigate co-locating these courses at the same base, and make the training a PCS. Moreover, for anyone going into an offensive cyberspace operator role, they should then keep them at that same training location, and bring the preparatory 5-week "Cyber Operator Training Course" to them. This would save on TDY expenses, but would also help minimize the tour time lost to the operational unit spent on training these operators. Additionally, the member's participation in the nearly 6-month

US Cyber Command prescribed joint operator training course should be a TDY from the training base, and not from the operational unit. Additionally, since this course is a contractor course, the service should work with US Cyber Command and the NSA to bring it on-site to the training base, as that will save a tremendous amount in TDY expenses (approximately $25,000 to $35,000 per student). This would allow offensive cyberspace operators to arrive at the operational unit at the "basic" level, which would save nearly a year off of their operational tour currently "tied up" in training.

The USAF needs to ensure it receives proper return-on-investment for the highly technical and expensive training given to these cyberspace operators and analysts. The ADSC for the cyberspace operators and analysts should be a minimum of six-years after completing their training. This would bring the ADSC in line with career fields like remotely piloted aircraft (RPA) pilots and navigators.

The USAF needs to bridge the compensation gap between these professionals and their civilian equivalents. Measures such as increasing the SRB or including bonus pay for achieving and maintain certain certification levels ("apprentice", "journeyman", etc.) should be explored.

The partnership between NSA and US Cyber Command, to include the service cyber components is critical to mission success in the cyberspace domain, especially for offensive cyber operations. The NSA and US Cyber Command have different missions that intersect and complement each other in the cyberspace domain. General Alexander stated the need for the relationship accurately in his testimony before congress in June 2013:

> Cyberspace is characterized by high levels of convergence of separate and different networks and technology that have come together to form something greater than the sum of the parts. In this regard, USCYBERCOM's co-location with NSA/CSS mirrors the convergence in cyberspace and is a direct result of that technological shift. What we have learned is that if convergence is the reality of the cyber environment, then integration must be the reality of our response. Co-location promotes intense and mutually beneficial collaboration in an operational environment in which USCYBERCOM's success relies on net-speed intelligence. Although they are separate and distinct organizations with their own missions and authorities, NSA/CSS is a major force multiplier for USCYBERCOM, pairing the Command's operators, planners, and analysts with the expertise and assistance of NSA/CSS' cryptographers, analysts, access developers, on-net operators, language analysts, and support personnel. These are close working relationships that enable seamless, deconflicted operations that are vital to the success of the cyber mission.[25]

While I believe that the services should seek out research, development, and acquisition efforts that provide additional capabilities beyond what the cryptologic platform provides, especially those that augment and enhance military response options in the cyberspace domain, it would be detrimental to "sever" our technical ties with the NSA and not use their resources to further our objectives.

**COUNTERARGUMENT**

*A lengthy ADSC will limit the personnel that want to go into the career field.* I disagree with this argument for multiple reasons, the first being that the desire to do this mission will drive the Airmen into the career field despite the ADSC, just as a love of or a strong desire to fly brings in pilots and navigators despite a lengthy ADSC. Additionally, the skills, training, and experience gained in this career field will enable the member to be extremely successful when they do leave military service, and they will see the ADSC as their way of "paying back" the service for the skills they have acquired.

Continuing to partner with NSA will result in military personnel being "absorbed", and then the USAF will just become a force provider to NSA. Additionally, the services need entirely different infrastructure and capabilities than the NSA, otherwise, the NSA will retain control. These arguments are ill-informed and usually are the result of FUD – fear, uncertainty, and doubt – from leaders that have no previous experience with the NSA or the cryptologic platform. The personnel assigned to NSA and to US Cyber Command have entirely distinct chains-of-command, and while cyber personnel will work in the same domain alongside NSA personnel interested in the same target space, they do so with different intent. This difference in intent will keep a natural line between those forces allocated for the different missions, but allow for synergy in operations. Moreover, the resolution to the NSA infrastructure argument is not to "go build your own", but instead provide monetary resources to the NSA to expand their infrastructure to provide dedicated resources to the Cyber Mission Force. This allows US Cyber Command to leverage all of the years of experience of the agency, but have "their own" resources dedicated to their operations.

**CONCLUSION**

The current USAF processes for training offensive cyberspace operators is inefficient and doesn't meet the need – an overhaul is needed to make the force "healthy". The USAF has not secured a good return-on-investment for training these individuals – given the cost, in both time and money, to train these individuals, an appropriate ADSC will ensure the USAF realizes appropriate return. There will be a point where love-of-mission simply will not be enough to keep the talented Airmen in the service. Without bonuses/special pay, the offensive cyber operator/analyst would be making approximately 50%-75% of what they could out of the service; we need to continue to close this gap, otherwise we have a mismatch that amplifies a retention problem.

While I understand the service's desire to "own" the platform and processes, trying to conduct offensive operations in this domain without the force multiplier of the NSA would be a foolish endeavor, at least today. If this end-state is desired, then the service must invest more personnel, more time, and more money into creating the experience and expertise, in addition to back-office support structure to facilitate success, should they desire to operate without the partnership of the NSA – today, this is not possible; especially if you want to operate as a cutting-edge nation-state-level cyber force.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

[1] (US Air Force SAF/CIO A6 2014, 4)
[2] (Sternstein 2013)
[3] (Ibid.)
[4] (Verton 2014)
[5] (US Air Force SAF/CIO A6 2014, 5)
[6] (House Subcommittee on Intelligence, Emerging Threats, and Capabilities 2014, 68)
[7] (US Air Force SAF/CIO A6 2014, 4)
[8] (House Subcommittee on Intelligence, Emerging Threats, and Capabilities 2013, 85)
[9] (Pawlyk 2014)
[10] (Ibid.)
[11] (Griggs 2010)
[12] (Griggs, 'Sheriffs of cyberspace': Enlisted course next step in cyber transformation 2011)
[13] (Blacke 2011)
[14] (Ibid.)
[15] (US Air Force n.d.)
[16] (Gildea 2013)
[17] (Harper 2014)
[18] (Pawlyk 2014)
[19] (Salary.com n.d.)
[20] (United States Department of Defense 2014, 32)
[21] (Nakashima 2013)
[22] (Alexander, Statement before the Senate Committee on Appropriations - "Cybersecurity: Preparing for and Responding to the Enduring Threat" 2013, 2)
[23] (Alexander 2014)
[24] (Greenyer 2014)
[25] (Alexander, Statement before the Senate Committee on Appropriations - "Cybersecurity: Preparing for and Responding to the Enduring Threat" 2013, 3)

## BIBLIOGRAPHY

Alexander, General Keith B. "Statement before the Senate Committee on Appropriations - "Cybersecurity: Preparing for and Responding to the Enduring Threat"." June 12, 2013. http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander,_General_Keith_Testimony_6.12.13_Cybersecurity_Hearing.pdf (accessed June 15, 2014).

—. "Statement before the Senate Committee on Armed Services." *United States Senate Committee on Armed Services.* February 27, 2014. http://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf (accessed June 15, 2014).

Blacke, Capt. Kinder. *Intermediate Network Warfare Training up and running.* March 03, 2011. http://www.afspc.af.mil/news/story.asp?id=123245023 (accessed June 15, 2014).

Gildea, Debbie. *45 AFSCs removed from SRB list as AF gets leaner, smaller.* November 26, 2013. http://www.af.mil/News/ArticleDisplay/tabid/223/Article/467611/45-afscs-removed-from-srb-list-as-af-gets-leaner-smaller.aspx (accessed June 15, 2014).

Greenyer, Fiona. *S&T Beyond the Budget Topline.* May 28, 2014. http://halldale.com/insidesnt/defence/st-beyond-budget-topline (accessed June 15, 2014).

Griggs, Susan. "New Officer Course Boosts Cyberspace Transformation ." *Weapons Systems Technology Analysis Center.* June 22, 2010. http://wstiac.alionscience.com/pdf/eNews_CC_062210.pdf (accessed June 15, 2014).

—. *'Sheriffs of cyberspace': Enlisted course next step in cyber transformation.* January 19, 2011. http://www.aetc.af.mil/news/story.asp?id=123238836 (accessed June 15, 2015).

Harper, Jon. *Wanted: Cyberwarriors, no experience or knowledge necessary (Stripes.com).* March 29, 2014. http://www.stripes.com/news/wanted-cyberwarriors-no-experience-or-knowledge-necessary-1.275172 (accessed June 15, 2014).

House Subcommittee on Intelligence, Emerging Threats, and Capabilities. *H.R. 4435—FY15 National Defense Authorization Bill.* Subcommittee Markup, Washington, DC: US Congress, 2014.

—. "Information Technology And Cyber Operations: Modernization and Policy Issues to Support the Future Force." *Subcommittee Hearing (March 13, 2013).* Washington, DC: U.S. Government Printing Office, 2013. 85.

Nakashima, Ellen. *Pentagon to boost cybersecurity force (The Washington Post).* January 27, 2013. http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_print.html (accessed June 15, 2014).

Pawlyk, Oriana. *MilitaryTimes: Cyber: The safest job in the Air Force?* February 20, 2014. http://www.militarytimes.com/article/20140220/CAREERS/302200015/Cyber-safest-job-Air-Force- (accessed June 15, 2014).

Salary.com. *Salary.com: Systems/Application Security Analyst (US National Averages).* n.d. http://swz.salary.com/salarywizard/Systems-Application-Security-Analyst-Salary-Details.aspx?&hdcbxbonuse=on (accessed June 15, 2014).

Sternstein, Aliya. *NextGov: PENTAGON PLANS TO DEPLOY MORE THAN 100 CYBER TEAMS BY LATE 2015.* March 19, 2013. http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948/ (accessed June 15, 2014).

United States Department of Defense. "Quadrennial Defense Review." Washington, DC, 2014.

US Air Force. *Careers: Network Intelligence Analyst Specialist.* n.d. http://www.airforce.com/careers/detail/network-intelligence-analyst-specialist/ (accessed June 15, 2014).

US Air Force SAF/CIO A6. "USCYBERCOMMAND Cyber Mission Force." May 12, 2014. http://www.safcioa6.af.mil/shared/media/document/AFD-140512-039.pdf (accessed June 15, 2014).

Verton, Dan. *fedscoop: Pentagon confirms cyber-workforce plan heading to Hill.* April 30, 2014. http://fedscoop.com/pentagon-confirms-cyber-workforce-plan-heading-hill/ (accessed June 15, 2014).

Revamping the Cyberspace Professional Training Model – The Weapon System Construct
Lt Col Joseph Wingo, Maj Stacie Rembold, Maj Cully Patch, Capt Scott Anderson, Capt Preston Iverson, Capt Jeremy Solmonson, CW4 Elbert Peak, Mr. Thomas Asojo

**ABSTRACT**
In order to maintain relevant cyberspace workforce development, the DoD must expand on the cyberspace weapon system model. This will provide the DoD Cyberspace workforce with the right training at the right time to ensure we are able to meet the demands of this ever growing and highly contested domain. The current training frameworks are unable to update curriculum fast enough to keep pace with the dynamic nature of the cyberspace domain. Changes to enlisted training that are not formally delivered are left to haphazard training and subject to fall out funds or open source research which can water down much needed training. Officers in cyberspace career fields generally receive technical school training early in their career with very little follow-on training that is specific to the systems they will be managing. Civilian training in the USAF lacks standardization because training requirements are not clearly documented and often don't exist possibly due to poorly written civilian Position Descriptions (PDs) and outdated career fields developed over fifty years ago. Although DoD 8570 professional certification policy is an attempt to address these training needs it does not address specific technologies and systems used by the DoD and doesn't address the "train the way you fight" mantra. Another critical failing of our cyberspace professional workforce training is the chasm between our cyberspace technology acquisitions processes and our cyberspace training processes. In order to meet the training needs of the DoD cyberspace professional workforce, we recommend the DoD expand on the "weapon system" concept in the cyberspace domain. The six Cyber Weapon Systems recently established by the Chief of Staff of the Air Force were developed in an attempt to posture cyber capabilities to better compete for funding and manpower. A fully developed cyberspace weapons system construct can provide the foundation for a holistic training approach by using a central managing office to focus the resources necessary for self-sufficiency, providing guidance from technical orders to training plans and operating instructions. These programs ensure that training and certification on new or upgraded systems are accomplished by all applicable technicians regardless of whether or not they are an "Apprentice", "Journeyman", "Master", Officer, or Civilian. Clearly defining the weapons system and associated training will allow for a constant feedback loop between technology, training, and mission effectiveness.

**PROBLEM/ISSUE**

> *People are the Air Force's most critical asset. Airmen turn competencies into required capabilities. For this reason, the art of employing Airmen with the requisite education, training, and experience is fundamental to the effectiveness of the Service, affecting current operations and future capabilities*[1].

We must provide the DoD Cyberspace workforce with the right training at the right time to ensure we are able to meet the demands of this ever growing and highly contested domain. The current training frameworks utilized across the DoD today simply are not working. This is due to two main reasons. First, the existing training frameworks are not capable of responding to the dynamic training requirements demanded by rapidly evolving technologies. Second, the training requirements are not directly linked to DoD acquisitions processes in a way that ensures newly

acquired technologies are received by a cyberspace workforce qualified to operate them. In order to maintain relevant cyberspace workforce development, the DoD must expand on the cyberspace weapon system model.

*Current Training Frameworks*

Our current enlisted training framework is based around an "Apprentice-Journeyman-Craftsman" model[2]. This is an age-old model applied to most trades throughout the years; however, it assumes a rather stable set of technologies and skills one must develop in order to achieve "Craftsman" status. The skills required to move from "Apprentice" to "Craftsman" are typically outlined in a Career Field Education and Training Plan (CFETP) authored by the Functional Manager for each career field. The initial set of skills generally required to be considered an "Apprentice" are learned in the career field specific technical schools. Unfortunately, existing curriculum development processes utilized in these schoolhouses often require years to implement robust training adaptable to constantly changing technologies. Furthermore, updating schoolhouse curriculum does not respond to the training needs of the vast majority of the workforce who are already in the field. These "Journeymen" and "Craftsman" technicians are responsible to manage train and mentor their new "Apprentice" technicians; however, they receive little, if any, programmatically delivered training on how to maintain and operate new technologies being fielded on the network. When these in-the-field training requirements are met, it is done haphazardly through the use of limited squadron training funds (often the first funds to get cut) and home-grown, open-source research. Furthermore, the commonly overused train-the-trainer approach, although fiscally prudent, generally results in watered down, non-standardized training for the masses. To combat this, training must be holistically planned in a manner that provides the right skills to the right people before they are required to operate those technologies in a mission environment.

The officer training framework is even less effective. Officers in cyberspace career fields generally receive technical school training early in their career with very little follow-on training that is specific to the systems they will be managing. The old axiom of "find a sharp NCO and follow them around" was good for self-motivated learners, but it provided commanders with no assurances that their officers were skilled in the specialty they were managing. As an officer moves from unit to unit, the training needed to be successful in the new job is a haphazard pick-up game in a sink-or-swim environment.

> *The effectiveness of the CMF [Cyber Mission Forces] depends on the right people (military and civilian personnel) being recruited, trained, and then appropriately equipped to accomplish assigned missions*[3].

Our civilian training framework is in even worse shape. It is imperative that civilians working alongside their military counterparts should be expected to receive the same type of training and education as their military counterparts. However, at this time civilian training in the USAF lacks standardization because training requirements are not clearly documented or communicated and often don't exist. A significant number of career civilians start off as interns or direct hires who are expected to complete an on the job training (OJT) program as part of their career growth. However, their training is often not mentioned and therefore glossed over. Unlike the military, civilian training is not mandated as part of a career advancement track. Additionally, poorly written

civilian Position Descriptions (PD) further complicates a commander's ability to mandate emerging training requirements for their civilian employees.

To further complicate civilian training, the civilian Communication and Information (C&I) career field is made up of 42 different occupational series based on the Office of Personnel Management (OPM) general schedule created about 50 years ago[4]. While most of these job series may have been relevant at that time, many of the sub categories such as typists, data entry clerks, and secretaries are now obsolete and irrelevant within the context of cyberspace operations. In 2009, OPM revised a document called "The Handbook" that discusses all the job series for federal employees[5]. Not a single series description identifies with cyberspace or the cyberspace workforce. The word "cyberspace" doesn't exist in this document at all. As a result, we have civilians working in the cyberspace workforce under nondescript job series such as 0300, 0800, and 2210. To properly determine who the civilian cyberspace workforce personnel are and to properly educate the civilian cyberspace workforce, "The Handbook" and the mindset for employing and equipping the cyberspace civilians definitely needs to change.

Another ineffective training framework is the DoD 8570 professional certification policy[6]. In an attempt to address the training needs of the cyberspace workforce, DoD 8570 requires all cyberspace professionals to acquire and maintain expensive, industry-based, certifications. These certifications can easily exceed $3,000 to $5,000 per person. Although these certifications provide good training base-lines, they rarely address specific technologies and systems used by the DoD. As a result of this mismatch, the military mantra, "Train the way you fight", is violated by 8570. The purpose behind this mantra is to expose service members to training that fully prepares them to manage the systems and situations seen in the operational environment. Relying on an 8570 certification as a baseline for cyber workforce development does not expose service members to how the military operates in an environment. Instead, the best that an 8570 certification can do is document that a certified member is able to demonstrate how to execute best practices within a specific, industry generic environment. This leaves a gaping hole between 8570 training tasks and true assurances that DoD cyberspace professionals can actually execute their missions.

*Acquisitions Shortfalls*

Another critical failing of our cyberspace professional workforce training is the chasm between our cyberspace technology acquisitions processes and our cyberspace training processes. Although many contracts require the vendor to provide training to a handful of DoD cyberspace professionals, this training rarely addresses the entire workforce who require the training, and this training is not programmatically implemented to ensure that it fully meets the needs of the workforce for the entire lifecycle of the system. Even if a cyberspace career field Functional Manager identifies the skills and writes them into an updated version of that Career Field Training Plan, there is no mechanism to deliver that training to people who have already received "Journeyman" or "Craftsman" status. Additionally, because of the required vetting and staffing processes, publishing a new Career Field Training Plans can take a year or more. We must establish a better process to ensure that the acquisition of new technologies automatically generates a holistic training plan which ensures authoritatively and confidently that the right skills are developed by all of the right people for the entire lifespan of the technology.

Additionally, cyberspace acquisitions processes generally do not develop the manpower assessments needed for the DoD to document and fund the billets required to maintain and operate the system. As a result, we not only shortfall training, but we field systems based off of manpower assumptions. These assumptions place the cyberspace workforce in a more vulnerable position for manpower cuts because they have no way to objectively describe the manning requirements for every system they operate and maintain.

**RECOMMENDATIONS**

In order to meet the training needs of the DoD cyberspace professional workforce, we recommend the DoD expand on the "weapon system" concept in the cyberspace domain. On 24 March 2013, the Chief of Staff of the Air Force (CSAF) signed a memo establishing six Air Force Cyberspace Weapons Systems. He established these weapons systems as "…a means to identify requirements and critical resources to ensure that they receive comprehensive and equitable consideration for program-associated funding"[7]. In short, sets of cyber capabilities were defined as "weapons systems" in order to better compete for funds. Our recommendation builds on this idea to fully exploit the potential benefits of the "weapons system" construct to not only ensure that cyberspace systems compete for funding, but also to establish rigor in the development, operations, and maintenance of these critical war fighting capabilities.

To understand the Air Force's paradigm shift in what constitutes a weapons system, we need to understand how the existing six are described. The Air Force Cyber Defense (ACD) weapon system describes the AF's capabilities to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks[8]. The Air Force Cyber Security and Control System (CSCS) weapon describes the organizational structure required to provide 24/7 network operations and management functions and enable key enterprise services within Air Force unclassified and classified networks[9]. The Air Force Intranet Control (AFINC) weapon describes how the AF provides a top level boundary and entry point into the Air Force Information Network (AFIN) and controls the flow of all external and inter-base traffic through standard, centrally managed gateways[10]. The Cyber Command and Control Mission System (C3MS) weapon system describes the 624th Operation Center's ability to synchronize other AF cyber weapon systems to produce operational level effects in support of Combatant Commanders worldwide[11]. The Air Force Cyberspace Defense Analysis (CDA) weapon system is described as the Air Force's capability to enhance Defensive Cyberspace Operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and USAF websites[12]. Finally, the Air Force Cyberspace Vulnerability Assessment/Hunter (CVA/Hunter) weapon system describes the capability to execute vulnerability, compliance, defense and non-technical assessments, best practice reviews, penetration testing and Hunter missions on AF and DoD networks & systems[13]. This "weapon system" paradigm shift is possible when weapons systems are thought of in terms of capabilities necessary for success in a war fighting domain. Instead of defining a weapons system as a specific piece of technology represented by a specific platform, weapons systems can be thought of as a conglomerate of technologies and process used to achieve a desired effect.

These currently defined cyberspace weapons systems are not granular enough to encompass all cyberspace missions the DoD owns and operates. They only encompass a portion of what Joint Publication 3-12 defines as "DODIN Operations"[14]. Additionally, these systems are Air Force

centric and would need to be refined to ensure they meet the needs of a joint operating environment.

A fully developed cyberspace weapons system construct can provide the foundation for a holistic training approach. Joint Publication 1-02, defines a "weapon system" as "a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency"[15]. It's important to note that personnel and training (as a means of delivery) are included in this definition. To realize a fully implemented cyberspace weapons systems, we must first designate additional cyberspace weapons systems based off of capabilities we desire to achieve (recommendations for additional weapons systems are addressed later in this paper). All cyberspace weapons systems must then be further defined by each technology being utilized to achieve the desired capability. When that is done, all of the skills and tasks required to operate and maintain that cyberspace weapons system can be documented in weapons system Technical Manuals (TM). These TMs become the basis of training plan (TP), operating manuals (OM), operating instructions (OI), and technical orders (TO). As such, they will not only drive our training systems, they will also be the foundation for Cyberspace Standardization & Evaluation (Stan/Eval) and Quality Assurance (QA) programs. When new hardware and software platforms are introduced as part of a planned weapons system upgrade, our existing methodologies dictate the update of existing OMs and TOs associated with those platforms. Existing Stan/Eval and QA programs are designed to ensure that operators and technicians receive all necessary training and certification on that weapon system platform before they touch it in a mission environment. These programs ensure that training and certification on new or upgraded systems is accomplished by all applicable technicians regardless of whether or not they are an "Apprentice", "Journeyman", "Craftsman", Officer, or Civilian.

Additionally, the weapon system construct directly links the acquisition and training processes together through the utilization of a management office. Currently, cyber platforms are contracted by whichever contracting organization or vehicle is available to the customer. As an example, the Air Force Combat Information Transport System (CITS) is a multi-billion dollar Air Force acquisition program designed to provide fixed-base information infrastructure and network management/network defense (NM/ND) capabilities to the Air Force[16]. However, as an acquisitions program, CITS has not historically been involved with training or TM development/distribution.

Like any other weapons system, these cyberspace weapons systems should be managed by a Program Office responsible for configuration control, upgrades, training materials development, and TM development. A fully realized cyberspace weapons system program office would fill the gap of not only managing acquisitions but also assume the role of TM integration into the existing training, Stan/Eval, and QA programs. Furthermore, they would determine all manpower requirements associated with each portion of the weapons system as part of the acquisition and fielding process. This ensures a fully documented manpower requirement tied directly to DoD mission capability.

## RECOMMENDED CYBERSPACE WEAPONS SYSTEMS

*Adaptive Vulnerability Management (AVM) Weapons System*

AVM can be described as the DoD's ability to defend the DODIN through constant vulnerability assessment and mitigation. As a manmade domain, cyberspace terrain can be maneuvered, molded, and redesigned at the speed of thought. New vulnerabilities are identified almost daily, and they must be mitigated with equal speed. This capability is critical to ensure a resilient defensive cyberspace posture.

AVM components could be defined as all of those systems internal to the DODIN which are used to identify potential points of adversary access and mitigate those vulnerabilities in a timely manner. These components would include network vulnerability scanners, system patching tools, anti-virus systems, firewalls, and proxies. In general, these components are operated and maintained by the same DoD career fields. This commonality would help to streamline AVM weapons system training implementation.

*Cyberspace Infrastructure Control (CIC) Weapons System*

The CIC weapons system can be described as the capability to define and re-define the DODIN network infrastructure in such a way as to enhance mission effectiveness and deter adversary access. IP space management can literally transport a potential target from one cyberspace location to another in a matter of seconds and control the means of access to that potential target. This ability to define and redefine the DODIN terrain is a critical piece of defensive maneuver that can be used to deter an adversary.

CIC components could be defined as all of those systems used to define the IP space. They would include IP address management systems, routers, switches, and access points. These components are also generally operated and maintained by the same career fields which would allow for ease of CIC weapons system training.

*Cryptographic Maintenance and Operations (CMO) Weapons System*

The CMO weapons system could be described as the capability to secure communications systems through the encryption of data moving through any medium and the encryption of data at rest. Inherent in CMO is the maintenance, tracking, configuration, and employment of COMSEC. Encrypting DoD data is critical to ensure the security and integrity of our information. Information reliability is crucial for any conflict.

CMO components could be defined as all of those systems used to encrypt data and any communications signal carried by any transport mechanism (RF, copper, fiber optic, etc..). These components would include encryption keys, key generation devices, and the encryption devices themselves. Although encryption specialists are generally in similar career fields, encryption device users span a wide variety of disciplines. Existing COMSEC training requirements and techniques could be modified as TMs for use by both encryption specialists and encryption device users.

*Potential OCO, OCEO, and DCO Weapons Systems*

Although this paper has largely dealt with cyberspace weapons systems in the context of DODIN Operations, the natural extension of the cyberspace weapons system is in the areas of offensive, defensive, OPE, and ISR cyberspace operations. Carefully crafting these capabilities as weapons systems will ensure appropriate funding, manning, and training.

Additionally, the systems used to gather intelligence and the systems used to achieve effects are often similar or the same. These systems are much like the popular Reaper RPA. They are not only an ISR platform, but an offensive weapon to rapidly act on the ISR gathered to achieve the desired mission effects. As a joint intelligence and operations weapons system, training can be focused on the Reaper's mission and more directly gauged to mission performance and effectiveness. In this way, training and mission effectiveness create a continual feedback loop to ensure the most effective training and education is provided to intelligence analysts and operators. Cyberspace weapons systems can follow this same model. Clearly defining the weapons system and associated training will allow for a constant feedback loop between the technology, the training, and mission effectiveness.

## CONCLUSION

We recommend that the DoD cyber professional training be based on the cyber weapon systems construct. This allows changes to the weapon systems to have corresponding changes to training which can be centrally managed. This addresses gaps that exist with the current training methods for enlisted, officer, and civilians in the DoD. Furthermore, aligning the training with the cyber weapon systems allows for better competition for funding. We recommend this because, as stated in Force Development doctrine, "the art of employing Airmen with the requisite education, training, and experience is fundamental to the effectiveness of the Service"[17]

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

[1] Air Force Doctrine, Section 5 Support, Force Development
[2] AFI 36-2201, Air Force Training Program
[3] Mission Analysis for Cyber Operations of Department of Defense
[4] From Serbu article, paraphrased from comments by Maj Gen Mathews to a luncheon of the AFCEA Northern Virginia chapter
[5] Handbook of Occupational Groups and Families from OPM
[6] DoD Directive 8570-01
[7] CSAF Memo
[8] Brig Gen Skinner Article
[9] Ibid
[10] Ibid
[11] Ibid
[12] Ibid
[13] Ibid
[14] Joint Publication 3-12, Cyberspace Operations
[15] Joint Pub 1-02
[16] Combat Information Transport System
[17] Air Force Doctrine, Section 5 Support, Force Development

## BIBLIOGRAPHY

"AFI 36-2201." *Air Force Training Program* (2013): 21-22. <http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2201/afi36-2201.pdf>.

Combat Information Transport System. "Information Transpoort System Architecture." 14 January 2010. <http://www.netcents.af.mil/shared/media/document/AFD-111122-065.doc>.

Department of Defense. "DoD Directive 8570-01." *Information Assurance Training, Certification, and Workforce Management*. 23 April 2007. <http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf>.

—. "Joint Pub 1-02." *Department of Defense Dictionary of Military and Associated Terms*. 15 January 2015. <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

—. "Joint Publication 3-12." *Cyberspace Operations*. 5 February 2013. <http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf>.

LeMay Center for Doctrine. *Force Development*. 18 November 2012. <https://www.doctrine.af.mil/download.jsp?filename=V5-D10-Force-Development.pdf>.

Office of Personnel Management. "Handbook of Occupational Groups and Families." May 2009. <http://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/occupationalhandbook.pdf>.

Office of the Secretary of Defense. "Mission Analysis for Cyber Operations of Department of Defense." 21 August 2014. <http://www.ngaus.org/sites/default/files/pdf/DODCYBER%20FY14%20NDAA%20Sec%20933%20REPORT%20FINAL.pdf>.

Serbu, Jared. "Air Force looks to reboot civilian cyber workforce." *Federal News Radio* 18 March 2013. <http://www.federalnewsradio.com/395/3254619/Air-Force-looks-to-reboot-civilian-cyber-workforce>.

Skinner, Robert J. "The Importance of Designating Cyberspace Weapon Systems." *Air & Space Power Journal*. September-October 2013. <http://www.airpower.maxwell.af.mil/digital/pdf/articles/2013-Sep-Oct/SLP-Skinner.pdf>.

# SECTION 2: JOINT INFORMATION ENVIRONMENT

# The Joint Information Environment: Recommendation for Air Force Network Operations

Mr. Hermon C. Armstrong, Jr., US Cyber Command

**ABSTRACT**

The intent of the Joint Information Environment (JIE) is to establish a common architecture and a command and control (C2) framework to operate and defend the DOD Information Network (DODIN). Within the JIE framework, a Global Enterprise Operations Center (GEOC) under U.S. Cyber Command (CYBERCOM) will execute C2 over Enterprise Operations Centers (EOC). The EOCs will provide enterprise DODIN capabilities as well as direct support to Combatant Commands (CCMD) within their area of responsibilities.[1] The Defense Information Systems Agency (DISA), as a DODIN enterprise service provider, has a significant role in JIE implementation.[2] In June 2013, the Joint Staff issued an Execution Order (EXORD) to U.S. Strategic Command (STRATCOM) with tasks directing development of a proposal to establish a formal operational C2 relationship between CYBERCOM and DISA. The EXORD also directed that the roles and responsibilities for DODIN Operations and Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) down to the base / post / camp / station (B/P/C/S) level of JIE be clearly illustrated. In turn, in July 2013 STRATCOM issued an EXORD to CYBERCOM to work with DISA to develop the recommendation. The establishment of this C2 relationship and the progress of the JIE framework will have a direct impact to the Air Force Network Operations (AFNETOPS) construct and cyberspace strategies. It will be imperative to integrate the AFNETOPS construct into the EOC framework to ensure Air Force equities on the DODIN are preserved.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

1. The JIE C2 relationships with respect to EOCs have to be further refined and inclusive of Air Force elements that have the capabilities to achieve the desired JIE end state. The current JIE CONOPS established a framework in which a several EOCs will be established that will have the responsibilities to provide support to one or more geographic CCMDs and providing applications, data, and core enterprise services. The GEOC will be responsible for global operations and the EOCs will be responsible for regional/functional operations within their geographic or logical area of support (AOS).[3] The CONOPS also specifies that DOD Agencies (CC/S/A) will manage their local infrastructure at the B/P/C/S level and any capabilities specific to each CC/S/A.[4] Within the Air Force a similar construct exists where the 624th Operations Center (624 OC) directs the operations of the Integrated Network Operations and Security Centers (I-NOSC). There is an overlap between roles and responsibilities at the base level and the delivery of enterprise capabilities with the JIE EOCs and the Air Force I-NOSCs that needs to be de-conflicted and integrated. This is necessary in order to achieve the goals and objectives of the DOD Chief Information Officer's NetOps Strategic Vision for shared Situational Awareness (SA), unified DODIN C2, and institutionalized NetOps,[5] as well as, the eleven objectives detailed in the U.S. Air Force Blueprint for Cyberspace.[6]

2. Designation of the type/role of each EOC and the DOD components that will staff them is still being determined. The first regional EOC has reached JIE Increment 1 initial operational capability (IOC) on 31 July 2013 in Stuttgart, Germany.[7] However, this EOC is staffed by the DISA Europe Field Command with the DISA NetOps Center (DNC) Europe executing EOC operations for U.S. European Command (EUCOM) and U.S. Africa Command (AFRICOM).

Although the JIE CONOPS specifies that the GEOC will have operational command (OPCON) over the EOC,[8] CYBERCOM at this time does not have a formal command and control relationship with DISA to exercise OPCON over its components. Additionally, there is no formally established GEOC. Currently the CYBERCOM Joint Operations Center (JOC) notionally takes on the role of the GEOC, but the long term intent is for the GEOC to be a CYBECOM component that reports to the JOC. To date the CYBERCOM JIE Operations Sponsor Group (JOSG) is still working to identify specific functions and roles of EOCs, as well as establishing the final criterion for their full operational capability. This includes determining which DOD components are best equipped to execute EOC roles/functions, how many EOCs will support a CCMD, how many EOCs will be Service-led or functional (provide DODIN wide enterprise services), and defining the areas of support for each EOC. These among other factors are at the core of the need for clarification of roles and responsibilities.

3. The effectiveness of the C2 construct for the EOCs is directly linked to the progress or delay of the implementation of the JIE common architecture. The progress of JIE towards a common infrastructure, single security architecture, and enterprise services will in turn determine who (EOC or I-NOSC) is responsible for what (i.e. DODIN security posture down to the base level). The efforts to accomplish the interim and desired end-state of JIE will have to be synchronized with the two phased approach described in the Air Force Blueprint for Cyberspace. There are two major groups that are coordinating JIE implementation, the JOSG, led by CYBERCOM, and the JIE Technical Synchronization Office (JTSO), led by DISA. Both report to the JIE Executive Committee for final decisions on JIE initiatives and implementation plans. The JIE Executive Committee is tri-chaired by CYBERCOM, the Joint Staff J6, and the DOD Chief Information Officer (CIO). The JOSG is focused on JIE C2 roles/responsibilities to include the C2 construct between the GEOC and EOCs. The JTSO is responsible for the development of JIE architecture and enterprise capabilities and coordinating their implementation.[9] The Air Force Network Integration Center (AFNIC) executes the same responsibilities for the Air Force Network (AFNET) architecture and enterprise capabilities.[10] As the JTSO and JOSG develop the implementation plans to achieve the JIE end states for C2, infrastructure and enterprise capabilities, the 24th Air Force/Air Force Cyber Command (AFCYBER) and the AFNIC will have to continue to assess AFNET to determine what specific portions of its infrastructure and capabilities will fall under JIE and be removed from AF ownership and responsibility.[11]

4. Future iterations of the Air Force's strategic cyberspace vision and technological initiatives will be influenced by JIE. Recently the Air Force Network Integration Center completed the migration of Air Force users to the Air Force Network (AFNET). This was considered a major milestone for aligning the Air Force's enclave on the DODIN with JIE. The next focus for the Air Force may need to shift to determining how, in the long term, AFNET will integrate with the JIE Core Data Centers (CDC), Installation Processing Nodes (IPN), Installation Services Node (ISN) and Installation Gateways (IG). CDCs, IPNs, ISNs, and IG will all play a role in the management of B/P/C/S infrastructure, CC/S/A-specific applications / enterprise capabilities, and end user devices as they will serve as the touch points between the core JIE architecture and the AFNET.[12]

**RECOMMENDATIONS**

1. Existing Air Force Network Operation Security Centers (NOSC) should transition into assuming roles and responsibilities of JIE Service-led EOCs with a focus on providing Air Force

unique / specific capabilities. There is a common thread in the responsibilities identified for an EOC and an I-NOSC as both provide regional and functional capabilities. Under the JIE construct each CC/S/A will be responsible for providing and managing their specific infrastructure and capabilities. Based on that construct an I-NOSC can transition to the role of a Service-led EOC and continue to manage the portion of the AFNET that will remain the responsibility of the Air Force once JIE reaches its end state. This should also ensure that the current Air Force C2 constructs for cyberspace operations as well as CYBERCOM authorities for DODIN Operations and DCO-IDM remain intact down to the B/P/C/S level. In this case the GEOC will direct the required actions on the DODIN (for DODIN Operations and DCO-IDM) and the Service-led EOC (I-NOSC) will ensure that those actions are properly executed on the AFNET and on any Air Force specific capabilities/applications across the DODIN.

2. As JIE consolidates DODIN core capabilities and the C2 relationship between UCSYBERCOM and DISA is established, then Air Force EOCs can remain focused on Air Force equities while the remaining DOD components adopt other EOC roles. In the response to the CJCS Cyberspace C2 EXORD, CYBERCOM is addressing this issue with a recommendation to establish a new CYBERCOM component, the Joint Force Headquarters (JFHQ) – DODIN (which will operate the GEOC) and subordinate DODIN Commands (which will operate the EOCs). Included in the response to further define the CYBERCOM and DISA C2 relationship is the recommendation to dual-hat the DISA Director, Lt Gen Ronnie Hawkins as the commander of the JFHQ-DODIN. The JFHQ-DODIN will be responsible for DODIN Operations and DCO-IDM and will have the necessary authorities delegated from the commander of CYBERCOM to accomplish this. This authority will be specified tactical command (TACON) of CYBERCOM components that are responsible for the execution of DODIN Ops and DCO-IDM. This TACON, however, does not include the subordinates of these components. This recommendation is currently going through Joint Staff Action Processing (JSAP) with the Joint Staff awaiting final adjudication and approval. Under this construct, the JFHQ-DODIN will issue the task to AFCYBER and in-turn AFCYBER will then determine the appropriate AFCYBER component to execute it (i.e. an Air Force Cyber Protection Team or an Air Force I-NOSC). The establishment of this C2 relationship is necessary in order to achieve true unity of command and avoid issues where one stakeholder responsible for JIE implementation (DISA) does not have an established command relationship with another stakeholder (AFCYBER). Under this construct all JIE components (GEOC and EOCs) are under the operational command (OPCON) of CYBERCOM. The I-NOSCs functioning as Air Force EOCs will be able to provide Air Force unique capabilities across the DODIN and coordinate Air Force and new requirements as they emerge. Additionally, the AFCYBER commander can coordinate with the JFHQ-DODIN commander as appropriate to represent Air Force cyberspace interests and support requests. This construct also allows CYBERCOM to delegate tactical DODIN Operations and DCO-IDM functions (such as global authorized service interruption adjudication) to a component and focus on the operational and strategic mission priorities, planning, and development of full spectrum cyberspace strategy for the DOD.

3. The Air Force will have to incorporate flexibility into the long term plans of the AFNETOPS construct to account for any changes in JIE timelines that may also shift C2 responsibilities. As the JOSG continues to define the next increments in JIE, planning by the AFNIC for AFNET and long term strategic plans being developed by the 24th Air Force will have to be synchronized. The current JOSG focus is at on the CCMD level with EUCOM, AFRICOM and PACOM for the next

series of EOC increments. As the JIE tactics, techniques, and procedures are refined and the lessons learned from Increment 1 are incorporated, close coordination between 24th Air Force, the JOSG, and JTSO to achieve this synchronization.

4. Future iterations of the Air Force's strategic cyberspace vision and technological initiatives will have to be integrated with JIE. Objective 1 in the Air Force Blueprint for Cyberspace identifies that it is necessary to position and differentiate unique Air Force cyberspace capabilities.[13] The Air Force will begin to develop the strategy to align with JIE and in turn, determine the best way to optimize its resources, update cyberspace professional development plans, and Air Force organizational roles / responsibilities to shift focus from those DODIN (operate and defend) functions / tasks for which the Air Force will no longer be directly responsible.[14] An example of this is the recent migration of Air Force Headquarters to the DOD Enterprise Email (DEE). According to Lt Gen Michael Basla, Air Force Chief of Information Dominance and Chief Information Officer, the continued progression of DEE across the Air Force, personnel that currently administer Air Force enterprise email services, will in the future likely transition to fulfill the Air Force's obligations to the Cyber Mission Force manning requirements and/or focus on the long term objectives identified in the Air Force Blue Print for Cyberspace.[15]

**COUNTERARGUMENT**

1. Challenges will arise with respect to how CYBERCOM global/strategic, CCMD, and Service (to include Air Force) priorities will be adjudicated for each EOC. Lt Gen Michael Basla, expressed these concerns in February 2014 indicating that one of the biggest challenges that the Air Force faces is being able to couple the ongoing processes that each of the services have been already implementing to modernize, consolidate, and gain information technology efficiencies with the capabilities that JIE will bring in the future.[16]

2. Ongoing force shaping efforts and the obligations the Air Force has to equip the cyber mission force will put a strain on Air Force cyberspace strategies. The Air Force has been obligated to provide personnel for the Cyber Combat Mission Force to support CCMDs, as well as, Cyber Protection Teams to defend the DODIN.[17] Additionally, as further re-alignments occur under the current Base Realignment and Closure, the Air Force may struggle to meet the demands of other Service's needs on Joint Bases in which the Air Force may be the lead JIE service provider or ensure all Air Force requirements are met on bases in which Air Force units are Joint-based under another service.[18]

3. Requirements for interoperability with JIE could potentially delay the ability to address rapidly evolving issues and emerging requirements on the Air Force's portion of the DODIN. It remains to be seen whether the next phase of JIE initiatives and the future establishment of EOCs will hinder the progress of objectives 7 and 8 in the Air Force Blueprint for Cyberspace which calls for strategies to improve and integrate network as well as mission architectures, standardize and baseline infrastructure, and develop future architectures.[19] The timelines for reaching JIE end states are still being established and in-turn will directly impact timelines that the Air Force is working to establish for the future of AFNET. This includes which portions of AFNET will align under JIE and become the responsibility of the GEOC/EOC and which portions of AFNET will remain with the Air Force. The Air Force will have to identify what are the dependencies between JIE and AFNET future implementation timelines and seek to overcome any disparities between

the two. This will continue to be a challenge while certain aspects of how JIE will be implemented are still yet to be determined.

## CONCLUSION

JIE has the goal of gaining significant information technology efficiencies over time. Additionally, the C2 framework is intended to ensure synchronized execution of DODIN operations (DO) and Defensive Cyberspace Operations (DCO) Internal Defensive Measures (DCO-IDM). The equities of each of the individual services will have to be preserved as this transition occurs. In turn, AFNETOPS strategies will have to integrate with the current and future JIE. As the goal of a defensible architecture is achieved, and the formal C2 relationship is established, C2 of DODIN Operations and DCO-IDM will be a singular unified effort likely executed mainly by UCYBERCOM and elements of DISA. This should allow the Air Force to focus and re-purpose resources to develop and implement the AFNETOPS cyberspace strategy of the future. The success and progress of JIE will also be dependent on strategic leaders in the DOD working to overcome inter-service rivalries and a narrowed view of their equities on the DODIN.[20] In-turn, the JIE Executive committee, JOSG, and JTSO must seek to leverage and integrate the progress that each service has made towards accomplishing the DOD NetOps Strategic Vision.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate bibliography entry.)

1 CJCS, "JIE White Paper," p. 6.
2 Gen Alexander, "Statement Before The Senate Committee On Armed Services," p. 1.
3 JOSG, "JIE CONOPS," p. 7.
4 Ibid., p. 8.
5 DOD CIO, "DOD NetOps Strategic Vision," p.7.
6 Gen Kehler, "The United States Air Force Blueprint for Cyberspace," p. 9-12.
7 DISA, News and Events, "JIE Reaches Milestone with First Regional EOC."
8 JOSG, "JIE CONOPS," p. 21.
9 Ibid., p. 17.
10 AFNIC, "Air Force Network (AFNet) Standards, Architecture & Engineering," p. 2.
11 SAF/CIO A6, "Cyberspace Operations and Support Community Transformation Plan," p.19.
12 JOSG, "JIE CONOPS," p. 30-34.
13 Gen Kehler, "The United States Air Force Blueprint for Cyberspace," p. 9.
14 SAF/CIO A6, "Cyberspace Operations and Support Community Transformation Plan," p. 17.
15 DISA, News and Events, "Air Force Headquarters Adopts DEE Service."
16 Pawlyk, "AF Panel: Industry, DISA Partnerships Essential to Deflect Cyber Threats."
17 Gen Alexander, "Statement Before The Senate Committee On Armed Services," p. 6.
18 DOD CIO, "DOD NetOps Strategic Vision," p.5.
19 Gen Kehler, "The United States Air Force Blueprint for Cyberspace," p. 11.
20 LTC Dawson, "Strategic Leadership Challenges with the JIE," p. 24-25.

## BIBLIOGRAPHY

Alexander, Keith, GEN, Commander, CYBERCOM (2013). *Statement of General Keith B. Alexander Commander United States Cyber Command Before The Senate Committee On*

*Armed Services, 12 March 2013.* Retrieved from http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf (accessed 27 March 2013).

Air Force Network Integration Center (AFNIC). *Air Force Network (AFNet) Standards, Architecture & Engineering*. Retrieved from http://www.afnic.af.mil/shared/media/document/AFD-121126-053.pdf (accessed 11 April 2014).

Air Staff, AF/A3O (2010). *The Air Force Roadmap for the Development of Cyberspace Professionals.*

Chairman of the Joint Chiefs of Staff (CJCS) (2013). *Joint Information Environment (JIE) White Paper 2013*. Retrieved from http://www.jcs.mil/Media/Publications.aspx (accessed 18 March 2014).

Cornn, Gary L., Lt Col, AFSPC (2013). *Operating Concept for Cyberspace Security and Control System (CSCS), 23 September 2013.* Retrieved from https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1344B60FB5E044080020E329A9/Files/editorial/Cyberspace_Security_Control_System_Final.pdf (accessed 3 April 2014). Document is UNCLASSIFIED//FOUO.

Dawson, Stephen Edward, LTC, USA. "*Strategic Leadership Challenges with the Joint Information Environment.*" Army War College Carlisle Barracks PA, 2013. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a589309.pdf (accessed 9 April 2014).

Defense Information Systems Agency, News and Events, 6 February 2014. *Air Force Headquarters Adopts DoD Enterprise Email Service.* Retrieved from http://www.disa.mil/News/Stories/2014/Air-Force-DEE (accessed 10 April 2014).

Defense Information Systems Agency, News and Events, 5 August 2013. *JIE Reaches Milestone with First Regional Enterprise Operations Center.* Retrieved from http://www.disa.mil/News/Stories/2013/jie_milestone (accessed 10 April 2014).

Grimes, John G., Department of Defense Chief Information Officer (2008). *Department of Defense NetOps Strategic Vision, December 2008*. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD_NetOps_Strategic_Vision.pdf (accessed 10 March 2014).

Joint Information Environment (JIE) Operations Sponsor Group (JOSG). *JIE Operations Concept of Operations (JIE Operations CONOPS),* 25 January 2013. Document is UNCLASSIFIED//FOUO.

Kehler, Robert Gen, Commander, AFSPC (2009). *The United States Air Force Blueprint for Cyberspace*.

Montanez, Ivan, COL, USA. *"Department of Defense Synchronization and Coordination via Joint Information Environment."* Army War College Carlisle Barracks PA, 2013. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA589506 (accessed 9 April 2014).

Pawlyk, Oriana (11 February 2014). "*AF Panel: Industry, DISA Partnerships Essential to Deflect Cyber Threats.*" Military Times. Retrieved from http://blogs.militarytimes.com/flightlines/2014/02/11/af-panel-industry-disa-partnerships-essential-to-deflect-cyber-threats/ (accessed 27 March 2014).

SAF/CIO A6, *Cyberspace Operations and Support Community Transformation Plan*. Retrieved from http://www.safcioa6.af.mil/shared/media/document/AFD-120312-011.pdf (accessed 10 April 2014).

Smith, Scott A, COL, USA. *Future of Department of Defense Cloud Computing Amid Cultural Confusion*. Army War College Carlisle Barracks PA, 2013. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA589506 (accessed 9 April 2014).

Assessing the DoD Strategy for Implementing the Joint Information Environment Using the Institutional Component of Risk to Force

Mr. Rudolph E. Butler III, Air Force Space Command Headquarters

**ABSTRACT**

In September 2013, the Department of Defense (DoD) Strategy for Implementing the Joint Information Environment (JIE) was published. Inside this strategy, the word, "risk," is used only eight times. In the same timeframe, the Chairman of the Joint Chiefs of Staff revamped the way he describes and assesses military risk based on the four types of risk identified in the 2010 Quadrennial Defense Review (QDR). Within military risk, there are two major categories: Risk to Mission and Risk to Force. Risk to Force is a combination of the old Force Management Risk and Institutional Risk from the 2010 QDR. This paper uses the institutional component of Risk to Force to assess the DoD Strategy for Implementing the JIE. By using the institutional component, there are several key insights gained including the identification of potential critical flaws, if not addressed. Two examples, involving resources and personnel, will be presented. Finally, the author recommends key DoD and AF decision-making organizations that should incorporate the CJCS Risk Assessment framework into their efforts to allow senior DoD and AF leaders to manage risk and work to mitigate any potential critical flaws.

**DESCRIPTION OF ISSUE**

1. On 18 September 2013, the Department of Defense (DoD) strategy for implementing the Joint Information Environment (JIE) (referenced as Strategy throughout the remainder of the document) was published. This document contained the vision; key milestones, metrics and resources; acquisition strategy and management plan; key technical and policy challenges; capability gaps and dependencies; and personnel challenges. "The vision of JIE is to ensure that DoD military commanders, civilian leadership, warfighters, coalition partners and other non-DoD mission partners have access to information and data provided in a secure, reliable and agile DoD-wide information environment."[1] The Strategy states it is an ambitious, multi-year IT modernization effort that will realign, restructure and modernize how the department's IT networks and systems are constructed, operated and defended.[2]

2. In the same timeframe, the Chairman of the Joint Chiefs of Staff (CJCS) streamlined his risk assessment framework while incorporating the Defense Risk Management Framework defined in the 2010 Quadrennial Defense Review (QDR).[3] Inside the new CJCS framework, the Chairman defined military risk by two categories, Risk to Mission and Risk to Force. Risk to Mission is defined as "the ability of the current force to execute strategy successfully within acceptable human, materiel, financial and strategic costs."[4] Risk to Force is defined as "the ability to recruit, train, educate, equip and retain the All-Volunteer Force and to sustain its readiness and morale. This includes Institutional challenges of addressing management and business practices to plan for, enable, and support the execution of DoD Mission in the near, mid and far terms."[5] Risk to Force is a combination of the old Force Management Risk and Institutional Risk from 2010 QDR. Figure 1 shows how Risk to Mission and Risk to Force comprise military risk.

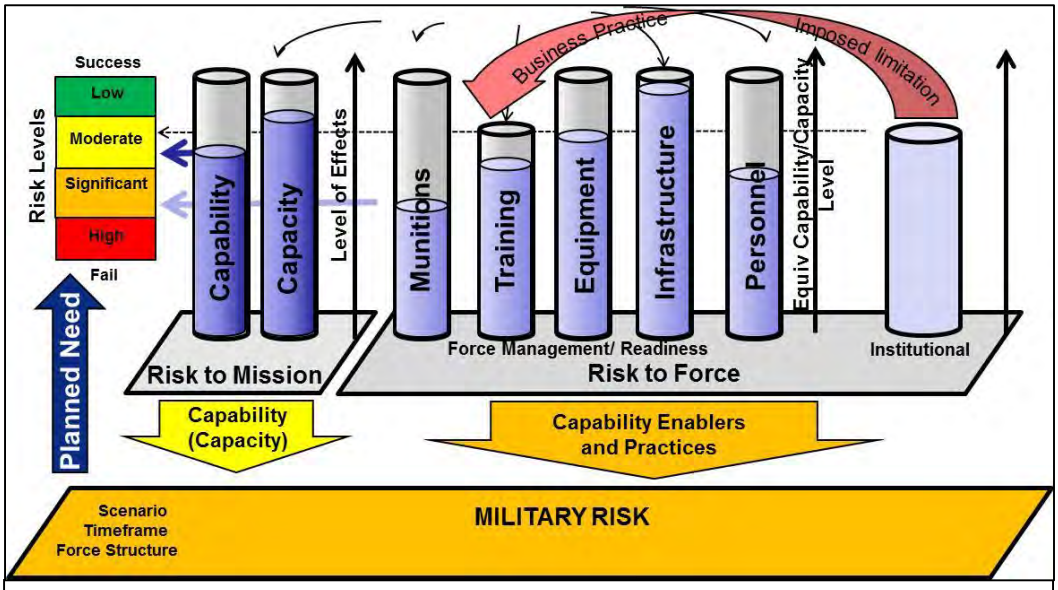



Figure 1: CJCS Military Risk Framework[6]

3. Inside the Strategy, risk is mentioned a total of 8 times. In most cases, the type of risk is not defined. This paper uses the institutional component of Risk to Force as a filter to assess the strategy and provides two examples of potential critical issues that could be mitigated during implementation, if recognized. Based on research, this paper recommends the CJCS Risk Assessment Framework using Risk to Mission and Risk to Force be adopted by the JIE Executive Committee, DoD's Cyber Investment Management Board and by Air Force Space Command inside the Cyberspace Superiority Core Function Support Plan to evaluate JIE efforts in terms used by other domains and organizations.

4. The Institutional component of Risk to Force addresses the management and business practices to plan for, enable and support the execution of DoD missions in the near, mid and far terms.[7] It was derived from the 2010 QDR. Inside 2010 QDR report, it provided insight that the Institutional component is concerned with resources, processes and organizations.[8] Examining the strategy using the institutional component as a lens, it is possible to recognize several potential critical flaws. This paper will highlight two potential critical flaws: 1) a resource flaw based on whether the strategy is executable given the current fiscal environment and 2) a process flaw based on not addressing the entire architecture in the strategy because the JIE "users" were not included.

5. Within the strategy, resources are addressed in one paragraph out of 48 pages. In that paragraph, it states, "Given the size and complexity of the DoD infrastructure as well as phased implementation, assessing the lifecycle costs and savings related to JIE is a highly complex exercise."[9] Further, it states, "As with most transformational efforts, initial activities may require some investment."[10] The strategy does not define an expected cost, but does define the need for initial investment upfront. In 2014, the DoD is subjected to an austere fiscal environment due to congressional guidance called sequestration. "In 2011, Congress passed a law saying that if they couldn't agree on a plan to reduce our deficit by $4 trillion, then about $1 trillion in automatic, arbitrary and across the board budget cuts would start to take effect in 2013."[11] "In response to sequestration, the SECDEF ordered a Strategic Choices and Management Review which proposed

options for implementing defense cuts required by the Budget Control Act of 2011."[12] The results of SECDEF's review were "Cuts, no matter how they are implemented, will dramatically reduce readiness and capabilities of the armed forces to the point U.S. national security will be in jeopardy."[13] Basically, when the DoD has to reduce readiness and capabilities to meet congressional direction, is it smart to modernize or recapitalize the DoD network infrastructure? Can the DoD or the nation afford to make strategic trades without having a price target to figure out whether it can afford this strategy? In a similar example, is it smart to build a new house without setting a price target or price cap if you know your income is going down over the next several years? In the Interim, DoD Directive 5000.02 states the need to define the total cost estimate, how it will be funded and the availability of funding.[14] Today, major programs are required to do an affordability assessment to determine if funding is available during its development, fielding and disposal. Since JIE is not a program, the strategy states 'implementing JIE depends on the success of existing DoD Component initiatives.'[15] These initiatives should be required to conduct affordability assessments. In an era where service budgets are decreasing, JIE's success depends upon recapitalization efforts that are "adequately resourced and executed on schedule."[16] Without overall guidance on resource target or cap, it appears DoD will need to sacrifice capability and/or capacity of critical weapon systems in order to fund DoD activities to 'realign, restructure, consolidate and standardize infrastructure' without a price target.[17] Based on this situation, the Institutional component would have driven the Risk to Force to a HIGH rating (i.e., worst rating available) which would have required senior leaders to reexamine whether they wanted to accept this risk or find ways to mitigate it. In a speech at the 29th National Space Symposium in 2013, Lt Gen Hyten, then Vice Commander of Air Force Space Command, appeared to agree with the Risk to Force rating when he stated the three major concerns with JIE. He pointed out that we need to answer the fundamental questions on 'what the security architecture is, define the environment and figure out how to pay for it.'[18] Furthermore, he stated, "If we can't do those three fundamental things, we're fooling ourselves."[19]

6. The second potential critical flaw is due to process challenges based on not looking at the entire architecture and addressing the most critical vulnerability to the network: people. The strategy has a dedicated, two-page section on personnel challenges associated with JIE that focuses on the cyberspace workforce and its development, but fails to address the user segment which could result in critical failures. According to Jeff Schmidt, author of the article, *How To Manage the Weak Link in Cybersecurity: Humans*, "the most significant security hurdle is users themselves-organizational stakeholders who have access to sensitive data and information. Even when they possess an awareness of the types of security threats directed at their organization, users (at all levels) often do not see themselves as responsible participants in the security process, but as beneficiaries of the organization's vast security infrastructure."[20] This important concern appears to be deemphasized in the strategy. The strategy states that JIE "will be akin to a utility—always available when and where it is needed."[21] Mr. Schmidt points out another critical concern, executive attitude, when he wrote, "Equipped with the latest authentication, encryption and threat monitoring technologies, executives have a misguided sense of invincibility, especially when the potential for human error, trickery and malicious intent are factored into the equation."[22] "No level of technological security can ever provide 100% security and even with the most robust systems, if the user does not understand and appreciate the nature of the threat, it will still remain the single-most important vulnerability in the cybersecurity discussion."[23] Finally, George Platsis, Program Director of the Centre of Excellence in Security, Resilience and Intelligence, sums it up best, "No

level of technology will be able to stop an attack if the user is uneducated and constantly circumvents (unknowingly) the security protocols in place designed to protect the network."[24] Using the Institutional component, the Risk to Force should be rated as HIGH because the process did not account for the entire JIE architecture which includes the users. If assessed properly, DoD senior leaders would have an opportunity to accept the risk or mitigate concerns.

**RECOMMENDATION**

1. To better evaluate JIE and improve its implementation, the CJCS Risk Assessment framework should be adopted by at least three key organizations. First, the JIE Executive Committee should adopt the framework as their risk methodology. As the Chairman's representative and one of the tri-chairs of the Executive Committee, the JCS/J6 could recommend adoption of the CJCS Risk Assessment framework within this forum. This result is important because the JIE Executive Committee "sets the JIE direction, establishes goals and objectives, provides oversight, and maintains accountability."[25] The JIE Executive Committee also provides strategic leadership and direction to the subordinate JIE working groups.[26] If adopted by the Committee, the CJCS Risk Assessment framework would become the standard for all subordinate working groups.

2. The second organization is the DoD Cyber Investment Management Board (CIMB). The Honorable Katrina McFarland, Assistant Secretary of Defense (Acquisition), testified to Congress that "The goal of the CIMB is to unite IT policy and operational requirements and identify gaps and resources to enable rapid acquisition and development of cyberspace capabilities."[27] As the Air Force representative, the Under Secretary of the Air Force, could recommend adoption of the CJCS Risk Assessment framework. This end state is important because through the CIMB the DoD "has achieved an understanding of cyber investment and mission alignment enabling future effective strategic management of the total cost of ownership and return on investment."[28]

3. The third organization is Air Force Space Command (AFSPC). AFSPC is the AF's lead Major Command to organize, train and equip AF cyberspace forces. Also, as the Air Force's Core Function Lead for Cyberspace Superiority, AFSPC develops the 20-year strategic plan (called the Core Function Support Plan) that lays out resourcing for developing, fielding and disposing of current and future AF cyberspace force structures within expected budget environments. Starting with the FY17 strategic plan (which is in development as of Aug 2014), AFSPC will incorporate the CJCS Risk Assessment framework to assess Risk to Mission and Risk to Force for Cyberspace Superiority overall force structures including down to core capability level of Defensive Cyberspace Operations, Offensive Cyberspace Operations, and DoD Information Network (DoDIN) Operations. This framework should enable better discussions among senior leaders about strategic trades and resource allocation.

**COUNTERARGUMENT**

The most likely counterargument to the recommendations is the CJCS Risk Assessment framework does not match Information Technology (IT) industry standards. Industry standards on risk assessment tend to focus on the equivalent of Risk to Mission where the main concerns are capability, capacity and future challenges (e.g., threats, dynamic environment, etc). The main benefit of using industry standards is it may enhance interagency cooperation across the U.S. Government to reach common standards and common solutions to risks. In the end, the recommendations in this paper remain valid because the DoD is not a business and its ability to

meet national objectives may require the DoD to be less efficient than industry in order to be effective. Also, the CJCS Risk Assessment framework is designed to describe military risk across all domains and among Services, Combatant Commands and Agencies to enhance integration of efforts and enable strategic trades at the DoD-level.

## CONCLUSION

By adopting the CJCS Risk Assessment Framework, DoD and Air Force senior leaders will have a better assessment of implementing JIE and will be using a framework that is common among domains and organizations. Assessing the DoD Strategy for Implementing the JIE using just the Institutional component of Risk to Force highlighted some potential critical flaws that could be mitigated during fielding. The recommendations target key decision-making organizations that provide guidance, resources and implement JIE efforts to achieve the desired end state.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

1. DoD CIO, 1.
2. Ibid.
3. QDR Report, 89-95.
4. CJCS, Figure 6, Page 7.
5. Henson and Herbranson, Slide 15.
6. Henson and Herbranson, Slide 17.
7. Henson and Herbranson, Slide 15.
8. QDR Report, 90.
9. DoD CIO, 17.
10. Ibid.
11. White House, 4 Aug 2014.
12. Bucci, Spring, Dodge and Carafano, 2 Aug 2013.
13. Bucci, Spring, Dodge and Carafano, 2 Aug 2013.
14. DoDD 5000.02, 17.
15. DoD CIO, 25.
16. DoD CIO, 25.
17. DoD CIO, 1.
18. Hyten, 2.
19. Hyten, 2-3.
20. Schmidt, 20 Dec 2011
21. DoD CIO, 6.
22. Schmidt, 20 Dec 2011.
23. Quoted in Platsis, 4 Aug 2014.
24. Platsis, 4 Aug 2014.
25. DoD CIO, 19.
26. Ibid.
27. McFarland, 5.
28. McFarland, 6.

## BIBLIOGRAPHY

Bucci, Steven P., Baker Spring, Michaela Dodge and James J. Carafano. "Pentagon Strategic Choices and Management Review: Early Warning Two Years Too Late." *The Heritage Foundation*, 2 Aug 2013. Web. 4 Aug 2014. <http://www.heritage.org/research/reports/2013/08/pentagon-strategic-choices-and-management-review-early-warning-two-years-too-late>

Henson, Robert and Travis Herbranson. "Risk Assessment Framework Instructional Brief." 27 Mar 2014. Print.

Hyten, Lt General John E., Vice Commander, Air Force Space Command. "Cyber 1.3 Luncheon." *29th National Space Symposium*. Colorado Springs, CO, 2013. Print.

McFarland, Honorable Katrina, Assistant Secretary of Defense (Acquisition). "Testimony before the Senate Armed Services Committee Subcommittee on Readiness and Management Support." *U.S. Senate*, 26 Feb 2014. Print.

Platsis, George. "The Real Vulnerability of the Cyberworld: You and I." *Schulich School of Business*. York University, Toronto, Canada, n.d. Web. 4 Aug 2014. <http://seec.schulich.yorku.ca/the_real_vulnerability_of_the_cyberworld_you_and_i.aspx>

Schmidt, Jeff. "How to Manage the Weak Link in Cybersecurity: Humans." C*RN*, 20 Dec 2011. Web. 4 Aug 2014. <http://www.crn.com/blogs-op-ed/channel-voices/232200743/how-to-manage-the-weak-link-in-cybersecurity-humans.htm>

United States. Chairman, Joint Chiefs of Staff. *Risk Assessment Process and Methodology for the 2014 Chairman's Risk Assessment (CRA) Information Paper.* Washington DC, 4 Jun 2013. Print.

United States. Department of Defense. Interim DoD Directive 5000.02, *Operation of the Defense Acquisition System*. 25 Nov 2013. Print.

United States. Department of Defense. *Quadrennial Defense Review 2014*. Washington DC, Feb 2014. Web.

United States. Department of Defense. *Quadrennial Defense Review Report*. Washington DC, 2010. Print.

United States. Department of Defense Chief Information Officer. *The Department of Defense Strategy for Implementing the Joint Information Environment*. Washington DC, 18 Sep 2013. Print.

"What You Need to Know About the Sequester." *White House*. White House. n.d. Web. 4 Aug 2014. http://www.whitehouse.gov/issues/sequester

# Joint Information Environment: Recommendations to Maximize Mission Effectiveness, Efficiency, and Security

Joseph S. DiGiovanni, US Transportation Command

**ABSTRACT**

The massive Joint Information Environment (JIE) effort was born out of operational, security, and economic concerns within the Department of Defense (DoD). According to Kirkpatrick (2012), the JIE is intended to maximize operational flexibility, increase cyber security, and improve efficiency via shared enterprise IT services. The question this paper will address is how to best organize and manage the JIE to achieve these objectives. Considering the desired effects of JIE, this problem spans the entire spectrum of Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P). Thus far, too much emphasis has been placed on the materiel aspects of JIE, to the detriment of non-materiel factors. Compounding this problem is the fact that within the materiel portion of JIE, there hasn't been enough focus upon the information considerations. The Chairman of the Joint Chiefs of Staff (2013) has stated one of the desired characteristics of the JIE was a shift from "network-centric to data-centric solutions" (p. 3). Yet when the JIE management structure was established, there were several operational and systems/services-oriented technical working groups chartered, but no data focused working group. Such a group is critical to ensure a data-centric architecture is developed, which in turn increases the chances of successfully meeting all JIE objectives.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

1. As Kirkpatrick presented to the Global Information Grid Information Assurance Portfolio and Defense Information Assurance Program (2012), the JIE was first conceived because the DoD's information environment, when evaluated enterprise wide, provided limited operational flexibility, was mostly undefendable, and delivered little IT efficiencies due to disjointed plans of Combatant Command, Services, and Agencies. So far, however, the management and initial execution of the JIE lacks sufficient emphasis on DOT_LPF-P and data architecture to achieve the stated objectives of resolving the three major shortfalls of the current environment.

2. The disproportionate attention afforded to materiel aspects of the JIE can be traced back to the DoD's IT Efficiencies initiatives. These initiatives are mainly about consolidation of various segments of the DoD IT enterprise, for example, data centers, enterprise services, and software license agreements. It isn't too surprising that the focus was on such elements of IT, given that historically it has been much easier to measure cost savings of materiel items versus non-materiel. The Executive branch led government agencies down the materiel path with directives such as President Obama's Executive Order 13589 – Promoting Efficient Spending (2011), which, from an IT perspective, mandated at least a 20% reduction from FY2010 levels by FY2013 for spending on employee IT devices. The DoD was already honed in on primarily materiel IT efficiencies when it established the high-level milestones for JIE in 2010. In fact, Kirkpatrick's (2012) JIE briefing reveals that only 22% of the high-level milestones over the JIE life cycle are DOT_LPF-P oriented. As the details of the JIE effort started to take shape in terms of the management construct, schedule, various working groups, and major deliverables, further evidence of the favor given to materiel components to the detriment of non-materiel concerns became apparent.

3. No IT program, project, or initiative in the DoD is complete without defined requirements and a concept of operations. These are especially critical to the success of such a huge initiative as JIE. Curiously, though, the capstone operational requirements document, the JIE Initial Capabilities Document, wasn't officially staffed until about three years into the effort. Related to this problem is the fact that the Combatant Commands, Services, & Agencies (CC/S/A) weren't formally tasked for requirements up front. Rather, such requirements were developed "bottom up" as part of the various technical design teams comprised of DISA, NSA, DoD CIO, and CC/S/A representatives. As for the JIE Operations CONOPS, the first version wasn't signed out by leadership until January 2013. Non-materiel aspects of JIE aren't the only thing lacking prioritization.

4. In a somewhat ironic twist, the Joint Information Environment so far doesn't appear to be much about information at all. Among fifteen JIE management, operations, and technical groups, no data working group exists! Rather, only a subset of data concerns are embedded in the Single Security Architecture and Identity and Access Management integrated design teams, and to some degree the Mission Partner Environment integrated working group. As a result, current JIE architectures are systems/services-focused, not data-focused. Why is this a problem? The Joint/NSA book *Information Operations* (2004) provides a strong clue, stating "Our belief is that information is now the most important element of power because it is the most transferable. The ability to transfer the power of information is what makes it so useful in the current political situation. Groups, organizations, nation-states and even individuals can now influence policy at the systemic level by using information" (p. 13). Clarke (2010) underscores the importance of information in *Cyber War* as follows, "As Admiral Mike McConnell has noted, 'information managed by computer networks—which run our utilities, our transportation, our banking and communications—can be exploited or attacked in seconds from a remote location overseas'" (p. 70-71). So what can be done to resolve the JIE shortfalls addressed in this section? We'll explore that next.

**RECOMMENDATIONS**

1. The JIE leadership and management team is in the midst of planning for the next major increment of the initiative, which, while focused in the Pacific region, will address numerous global capabilities. This is a golden opportunity to eliminate, or at least significantly reduce, the risks associated with the problems raised in the previous section of this paper. The rally point for the planners' focus is the JIE Integrated Master Schedule (IMS). Following the well-established capabilities-based analysis process, JIE planners should evaluate the current JIE baseline across all elements of the DOTMLPF-P spectrum. As evidenced by the content of the JIE Initial Capabilities Document recently staffed across the JIE stakeholders, much of this analysis has been done already, though much of it is dated (at least five years old) so would warrant a fresh evaluation. As the health of each area of DOTMLPF-P is assessed, then an integrated analysis should be done to identify the dependencies among all known gaps, shortfalls, and redundancies. The outcome of the analysis should then be used to update the JIE IMS to include all dependencies. This will allow planners to then determine critical path tasks, and thus optimize the effort across all capability lines to get to a more effective and sustainable Joint Information Environment. Albeit on a much smaller scale, USTRANSCOM has recently followed this approach to address shortfalls identified by the functional community in its information management environment. When the problem analysis was conducted, out of seven causes identified, all except one were non-materiel

issues. Thus priority was given in the schedule to resolving these problems, which centered largely around standardizing tactics, techniques, and procedures (TTPs), and associated training. The next recommendation is related, but focuses on a different aspect of the problem.

2. For a few decades now, executives and managers have studied and identified the key reasons that IT projects fail. On the short list of such reasons is poorly defined and managed requirements. As Hopkins and Jenkins (2008) put it,

> IT projects requirements are often divided into two categories: functional and nonfunctional…Unfortunately, nonfunctional requirements are often overlooked…The IT industry generally assumes that these two types of requirements encompass all requirements…However, we have observed a third kind of requirement: constraints. Despite being more numerous than the other requirements, constraints are often ignored—until it is too late.

As mentioned in the problem statement section, JIE was initiated without a formal requirements gathering effort. Now that the various working groups and integrated design teams are capturing at least some degree of all three types of requirements cited above, it is essential that the JIE community establish a master requirements management system to consolidate all requirements. Such a repository could then be linked to the governing strategy documents, and the JIE architecture repository. This linkage, even if only partially automated, would provide an essential element of success for JIE—requirements traceability. Without the ability to clearly trace requirements – functional, non-functional, and constraints – from governing strategy to architecture to system and service design, it will be difficult, if not impossible, to measure whether a given JIE capability is implemented in a way that meets the intended objectives and desired effects. In addition to these DOT_LPF-P recommendations, there is another key to the success of JIE that includes both materiel and non-materiel characteristics.

3. According to Libicki (2009), "The most common aim of hacking is to steal data" (p. 14). Given that our enemies have demonstrated the ability to penetrate network defenses of both military and contractor facilities and exfiltrate data, then it stands to reason that the last line of information protection lies with the data itself. While the architectures developed so far for JIE include numerous protection mechanisms for data and the systems involved in processing, transporting, and storing data, they apply a one size fits all approach due to the lack of consideration of the attributes of the data being protected.

> As stated in DoD Instruction 8320.02 (2013), Data, information, and IT services will be considered trusted when they have provided sufficient pedigree and descriptive metadata for consumers to rely on them as an authoritative data source (ADS), and comply with applicable information assurance and cyber security policies…DoD Components must ensure all DoD information programs, applications, and computer networks will protect data in transit and data at rest according to their confidentiality level, mission assurance category, and level of exposure. (p. 10)

While certain communities of interest (COI) across the DoD, such as the Intelligence COI (IC), have a very mature data management capability that can meet or exceed the objectives of DoDI

8320.02, most other functional areas aren't nearly as mature. This leads to the final recommendation, to establish a Data Management working group under the emerging Enterprise Data & Services Panel, as defined by the DoD CIO (2014) within its new IT governance structure (p. 2). Such a group should focus on creating an information architecture for JIE that addresses the requirements outlined in DoDI 8320.02, leveraging the successes of the IC. Considering the likelihood that the resulting protection policies and mechanisms still won't prevent data exfiltration, the Data Management working group and associated technical design teams should investigate critical information protection schemes that support remote or self-destruct capabilities for compromised data. Now that we've addressed ways to resolve the lack of non-materiel and data management in JIE, we'll explore the opposing viewpoints for these recommendations.

**COUNTERARGUMENT**

1. As previously noted, the imperative for the IT efficiency objective of JIE is tied to budgetary pressures from the President and Congress. The DoD must demonstrate significant savings in IT expenditures over the next several years. So while non-materiel considerations could indeed help the Department achieve JIE objectives, the time required to complete the needed full spectrum capability analysis would delay implementation of JIE capabilities that are expected to achieve the efficiency objectives demanded by the Executive and Legislative branches. Such a delay would likely be unacceptable to senior leadership within DoD and the Executive and Legislative branches.

2. When it comes to requirements gathering for JIE, traditional program-oriented methods don't necessarily apply. JIE leadership believes that sufficient requirements already existed in numerous Global Information Grid capabilities documents and architectures, and that the CC/S/As subject matter experts were expected to incorporate any new or modified requirements as part of JIE architecture development. The architectures alone should be sufficient to both capture requirements and demonstrate traceability between strategy and design.

3. As far as data management goes, efforts have been ongoing for decades with little enterprise-level progress. The JIE only needs to be concerned with providing the environment and associated capabilities for sharing and protecting data. The CC/S/As can manage their own COI vocabularies and data standards. Besides, formalizing a data management working group would have extended the overall JIE schedule beyond leadership's expected implementation targets.

**CONCLUSION**

Despite the lament of program managers that delivering systems fast, cheap, and good is nearly as impossible as proving that Bigfoot exists, the DoD has set quite high expectations for JIE. The objectives of maximizing operational flexibility, increasing cyber security, and improving IT efficiency are usually at odds with each other. So for a project as large and critical to the Department as JIE, even though not a formal program of record, it must follow sound enterprise systems and services engineering practices to maximize the chances of success. This means giving equal consideration for all elements of the DOTMLPF-P spectrum instead of the less difficult route of pursuing mostly materiel solutions. Also, the JIE schedule must contain enough detail and defined dependencies to minimize cost, schedule, and performance risks. Requirements need to be sufficiently defined and formally vetted with JIE governance to drive future JIE architecture development and associated capability gap/shortfall/redundancy analysis. The Department must

capitalize on this focused Joint initiative to finally get data sharing and protection policies architected and implemented as envisioned decades ago. Through all these actions, the Department will have a fighting chance at aligning the stars of Cyber effectiveness, efficiency, and security.

## BIBLIOGRAPHY

Clarke, R. A. (2010). *Cyber War, The Next Threat to National Security and What to Do About It,* 70-71. New York: HarperCollins.

Dempsey, M. E. (2013). *Joint Information Environment White Paper,* 3. Washington DC: Joint Chiefs of Staff.

Department of Defense Chief Information Officer. (2013, August 5). Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 10. Washington, DC, USA.

Department of Defense Chief Information Officer. (2014). Terms of Reference, Department of Defense (DoD) Chief Information Officer (CIO) Enterprise Architecture and Services Board (EASB), 2. Washington, DC, USA.

Hopkins, R., & Jenkins, K. (2008). *Eating the IT Elephant: Moving From Greenfield Development To Brownfield.* [Books24x7 version] Available from http://common.books24x7.com/toc.aspx?bookid=27519.

Joint Forces Staff College and National Security Agency. (2004). *Information Operations, Warfare and the Hard Reality of Soft Power,* 13. (L. Armistead, Ed.) Dulles: Potomac Books, Inc.

Kirkpatrick, D. (2012). *Joint Information Environment, GIAP/DIAP Forum,* 3. Retrieved from DoD JIE Collaboration Site: https://intelshare.intelink.gov/sites/dodjie/Shared%20Documents/Final%20Presentations/Others/JIE_to_GIAP.ppt

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar,* 14. Santa Monica: RAND Corporation.

Obama, B. (2011, November 9). *Executive Orders.* Retrieved from The White House: http://www.whitehouse.gov/the-press-office/2011/11/09/executive-order-13589-promoting-efficient-spending

# Joint Information Environment Operational Command and Control

Lt Col Samuel J. McGlynn, US Air Force, 854 Combat Operations Squadrojn

**ABSTRACT**

On 22 January 2013, General Martin Dempsey, Chairman of the Joint Chiefs of Staff released a white paper describing his vision for the Joint Information Environment (JIE) and how it would support operations in the years to come.1 This mandated transition is driving a reassessment of the most appropriate command and control (C2) structure to conduct operations within the domain. Attempts to achieve a standardized fully interoperable environment will only achieve limited success due to the innate variability and changing nature of technology, exacerbated by service unique capabilities and requirements as well as inconsistent funding. Existing C2 models either fail to address the uniqueness of operations in the cyber domain or otherwise fail to maximize cyber capabilities to their fullest extent. The Department of Defense (DoD) should transition to an operational C2 structure with shared responsibility between Joint Force Headquarters – DoD Information Network (JFHQ-DODIN) in direct support to the combatant commands (CCMDs) via regional operations centers, and service cyber components providing effects-based operations at the base level. To realize the goals of a more interoperable environment, the Air Force should continue consolidation of enterprise network operations security centers (NOSC) functions and build-in interoperability for Air Force cyber weapon systems.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

C2 of DODIN Operations (DODIN Ops) and Defensive Cyberspace Operations – Internal Defense Measures (DCO-IDM) within the DODIN requires a C2 structure simultaneously responsive to warfighter and service requirements but also flexible enough to maintain control of an evolving heterogeneous network. Developing the most effective C2 concept is challenging for the following reasons.

1. The characteristics of the Cyberspace domain are unique among warfighting domains in that is manmade, constantly changing and crossing geographic boundaries. The constantly changing nature of this manmade domain challenges the operator's ability to maintain situational awareness. Service and joint command networks are in a constant state of change with longer-term architectural changes, periodic tech refreshes, and near-constant addition and removal of devices from the network. In addition, this challenge is compounded, as there are myriad classified and unclassified networks beyond NIPRNet and SIPRNet, supporting service and joint command missions which are, in turn, evolving in their own unique manner. Furthermore, most all of these networks support non-standard program management office (PMO) controlled systems, which are not under the configuration control of either United States Cyber Command (USCYBERCOM), or the service cyber components. Finally, geographic boundaries delimiting the areas of responsibility (AORs) of the combatant commanders have limited significance in cyberspace. Friendly cyberspace forces can create near-instantaneous battlespace effects worldwide from their in-garrison locations, maximizing the flexibility of forces to support the combatant commander and service mission needs. The JIE's consolidation of core data centers (CDCs)2 will provide

supported commanders with access to applications and data that may or may not reside in their AOR.

2. Funding for the JIE will be inconsistent, which will frustrate efforts to fully standardize the JIE. According to the DoD Chief Information Officer, Teresa Takai, the JIE isn't a DoD system of record instead relying on annual DoD Operations and Maintenance funding.2 Without a consistent and reliable source of funding, individual segments of the network will progress at varying rates depending on the funds available and individual service and command priorities. As a result, the JIE will evolve in a heterogeneous manner, as has been the reality for the DODIN through the present day.

3. Existing joint C2 models are not suitable to the operational requirements. A number of existing joint C2 structures have been proposed as models for conduct of cyberspace operations within the DoDIN, however each of them have deficiencies with respect to the domain. In addition, the JIE global enterprise operations center and regional enterprise operations centers, currently being deployed as part of the current C2 concept, have spans of control beyond the capacity of these entities to manage. Current CCMD operational control (OPCON) of DODIN Ops and DCO-IDM capabilities will have limited effect if not synchronized with service enterprise capabilities, which are global in nature. Even with the consolidation of many core services under JIE, the most current concept3 has service cyber components maintaining responsibility for management of base-level network operations, which are supported by service component DODIN Ops and DCO-IDM capabilities. If we're to realize the force multiplying effects of combined cyber capabilities, we'll require a C2 structure that integrates all available forces to achieve the desired effect. Similarly, the role of the regional EOCs to maintain situational awareness and act as the CCMD contact for leveraging JIE capabilities also falls short of the robust C2 structure needed to leverage all available forces to support the combatant commands. Indeed, the worldwide scope, variability and rapid evolution of the DODIN would quickly exceed the capacity of a single operational-level C2 echelon to plan and direct operations in the face of escalating threats as we progress up the spectrum of conflict.

4. In March of 2013, the Chief of Staff of the Air Force designated 6 Air Force cyber weapon systems.4 This action was required as a first step to baseline current capabilities from which to develop future capabilities.5 As each current weapon system was developed outside of established weapon system acquisition processes, the standard requirements for weapon system interoperability were not met. As a result, most all of the communications between these weapon systems are manual in nature, significantly impacting the effectiveness of assigned cyber operators. Notably, significant effort is required to communicate situational awareness updates, mission status, and weapon system availability at the expense of the capacity to focus on ongoing missions and ability to respond to unforeseen events.

**RECOMMENDATIONS**

1. Transition towards a shared operational-level C2 structure between JFHQ-DODIN and service cyber components headquarters. JFHQ-DODIN would have overall operational-level

responsibility and direct responsibility for JIE components above the base level. Service cyber components would retain operational level command and control for operations at the base level in support of the JFHQ-DODIN and supported combatant commands. In addition, service cyber components would assume operational control of service-funded networks for DCO-IDM and DODIN Ops. Day-today DODIN Ops tasking of service-unique networks may be further delegated to aligned mission assurance centers (MACs) under C2 of the service cyber component in support of the service mission lead. Service cyber components would provide their common operational pictures to JFHQ-DODIN. C2 within CCMD-unique networks would be at the discretion of the CCMD with the option to request a service cyber component assume OPCON for DCO-IDM at the direction of USCYBERCOM. This C2 structure provides effective C2 oversight of the myriad networks and reflects the realities of operating largely service-funded networks that are funded and mission-prioritized by the services. Furthermore, by extending service cyber component C2 over service-funded mission networks, shared battlespace awareness will be further extended.

2. The operation-level tasking cycle should adopt a modified version of air tasking cycle as described in Joint Publication 3-30, Command and Control of Joint Air Operations.6 JFHQ-DODIN should provide apportionment allocation through a monthly cyberspace operation directive (CyOD) to the service cyber components or as needed if events require it. Based on the apportionment decision, service cyber components will provide an allocation request (ALLOREQ), identifying assets available for tasking under a current JFHQ-DODIN OPORD or FRAGO and requests for JFHQ-DODIN capabilities for supporting effects under their direct responsibility. All contingency/deliberate and most crisis action planning involving the capabilities and/or responsibilities of the service cyber components would begin with a PLANORD issued to the affected service cyber component headquarters, which would respond with a component commander approved estimate briefing. After reviewing, deconflicting and approving the service component estimates, the JFHQ-DODIN commander will approve an OPORD or FRAGO, directing follow-on operations. JFHQ-DODIN will issue a weekly CTO, directing current operations in support of JFHQ-DODIN OPORDs, or otherwise for operations where they have direct control of the AOR or where coordination for ongoing operations is required between the JFHQ-DODIN and one or more service cyber components. They may also issue a cyberspace control order (CCO) for periods of non-disruption (PONDs) or otherwise as required in support of CCMD requests. The JFHQ-DODIN would also issue appropriate orders for information assurance vulnerability alerts/bulletins or circuit disconnection orders. The service cyber components will receive the JFHQ-DODIN CyOD, and orders and release their own CyOD, CTOs and CCOs, which support the apportionment priorities and tasks as stated in the JFHQ-DODIN CyOD and orders.

3. Projects requiring significant commitment of resources and time should no longer be tasked to the services as operational orders as has occurred in the past (e.g.
USCYBERCOM orders directing implementation of DoD Visitor and Host Based

Security System). Future projects should be directed to the services via the Joint Chiefs of Staff process for inclusion in the POM and assignment of appropriate project management office for acquisition and deployment.

4. The Air Force Information Network should continue its evolution towards a more standardized architecture, which includes consolidation of existing NOSCs once the transition away from the MAJCOM-centric network architecture is completed. The current 3-NOSC structure struggles to provide the required network operations management needed in the face of insufficient resources and highly diverse architectures and inconsistent lines of responsibility between base and NOSC. Over time, these issues should be overcome and the organizational efficiencies can be realized. However, opportunities to extend the mission's strategic depth may also be possible using existing resources.

5. Future Air Force cyber weapon systems should be developed with interoperability as a core requirement. A key benefit will be the automated sharing of real-time situational awareness information, which will significantly reduce the friendly force commander observe, orient, decide, act (OODA) loop, which is critical to defeating future adversary operations against our networks and ensuring their availability for supported missions.

**COUNTERARGUMENT**

1. One proposal is that USCYBERCOM adopt the Special Operations C2 model. Under this model, COCOM of forces is maintained by the Commander, United States Special Operations Command (CDRUSSOCOM) however the geographic combatant commander (GCC) maintain OPCON for conduct of operations in theater via the theater special operations command (TSOC)7. This model supports the key command and control tenet of 'unity of command' by empowering the GCC with the single operational authority over all forces conducting operations in their AOR. An additional benefit of this model is that because CDRUSSOCOM has responsibility for organizing, training and equipping his forces, he's able to ensure that resources are fully aligned with his or her strategic priorities. Were this applied to the JIE, assuming CDRUSCYBERCOM will eventually be raised to a full unified command, they would be able to maximize the available resources to support USCYBERCOM priorities.

2. The Space Operations model has a single operational-level C2 organization for all operations with established relationships with CCMDs to provide warfighter support when required8. This model provides an effective C2 organization for capabilities that are inherently global in nature, which is also a key attribute of cyberspace capabilities. While assigned or attached forces are normally maintained under the unified command, it also provides the flexibility to transfer forces to the GCC if needed.

3. Another approach to consider is the joint spectrum management control model, which enables the joint force commander to manage the domain as a resource to allocate as required within their area of responsibility9. While not suitable for DCO-IDM, its model integrating operational requirements for spectrum management supporting theater DODIN Ops objectives, provides a

proven model that may suit the management of organic DODIN, coalition C4 and leased telecom resources.

## CONCLUSION

Transitioning from a legacy communications and information assurance management structure to an operational C2 structure with responsibility for operations within a common JIE must leverage the unique global capabilities of cyber while maintaining sufficient span of control over a dynamic and heterogeneous environment under constant threat. While existing joint C2 models aren't entirely suitable to the operational requirement, by implementing a shared operational C2 structure between JFHQ-DODIN and service cyber components, utilizing a synchronized tasking process based on the C2 of joint air operations model, we will provide the most effective C2 structure for DODIN Ops and DCO-IDM within the JIE. We must also remove massive projects from the operational tasking process to free the operators to focus on operations. The AFNETOPS construct must continue to standardize to gain efficiencies and maximize the effectiveness of our cyber operators. Finally, our cyber weapon systems must be developed with interoperability as core requirement, which will tighten our own OODA loop. By implementing an adapted C2 structure suitable to the operational environment and employing weapon systems communicating in real time we'll be best postured to denying future adversaries freedom of maneuver within the DODIN and ensuring freedom of maneuver of our own forces, leveraging our cyber capabilities.

## BIBLIOGRAPHY

1. Dempsey, Martin. "Joint Information Environment." Official Website of the Joint Chiefs of Staff. 22 January 2013. U.S. Department of Defense – Joint Chiefs of Staff. http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf (accessed 24 August 2014)

2. Takai, Teresa. "Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment." Hearing, Statement before the House Armed Services Committee, Subcommittee on Intelligence, Emerging Threats & Capabilities from United States House of Representatives, Washington D.C., 12 March 2014.

3. Defense Information Systems Agency. "Enabling the Joint Information Environment - Shaping the Enterprise for the Conflicts of Tomorrow." DISA | Joint Information Environment. http://www.disa.mil/About/Our-Work/~/media/Files/DISA/About/ JIE101_000.pdf (accessed 24 August 2014).

4. Host, Pat. "Air Force Details Six Cyber Capabilities That Are Now Weapon Systems - Defense Daily Network." Defense Daily. http://www.defensedaily.com/air-force-detailssix-cyber-capabilities-that-arenow-weaponsystems/ (accessed August 24, 2014).

5. Naylor, Jeffery. "History of Warfare and Cyber." Lecture, Cyber 300 Class-14I from Center for Cyberspace Research, Air Force Institute of Technology, Dayton, August 22, 2014.

6. U.S. Joint Chiefs of Staff. Command and Control of Joint Air Operations. Joint Publication 3-30. Washington, DC: U.S. Joint Chiefs of Staff, 10 Feb 2014.

7. U.S. Joint Chiefs of Staff. Special Operations. Joint Publication 3-05. Washington, DC: U.S. Joint Chiefs of Staff, 16 Jul 2014.

8. U.S. Joint Chiefs of Staff. Space Operations. Joint Publication 3-14. Washington, DC: U.S. Joint Chiefs of Staff, 29 May 2013.

9. U.S. Joint Chiefs of Staff. Joint Electromagnetic Spectrum Management Operations. Joint Publication 6-01. Washington, DC: U.S. Joint Chiefs of Staff, 20 Mar 2012.

The Joint Information Environment: Recommendations to Change Mindsets and Defense Department Culture

Maj Lee H. Miller, US Air Force, US Forces Korea

**ABSTRACT**

In today's cost-conscious fiscal environment, perhaps no program across the Department of Defense (DoD) offers more opportunities for cost savings and enhanced user capabilities than the Joint Information Environment (JIE) initiative. The JIE seeks military services to collapse existing networks into a consistent, shared information technology (IT) infrastructure that is easier to defend and provides more enhanced services and capabilities to the user.[1] JIE implementation will fix several problems found in the current DoD Information Networks (DODIN) architecture, ranging from differing architecture standards to security vulnerabilities. This framework presents a unique set of challenges and opportunities for cost savings if implemented correctly. Challenges come from overcoming a culture of service-centric parochialism in IT to changing the minds of military users who have grown comfortable with current service-centric, non-interoperable IT capabilities.[2] Opportunities range from cost savings from lower overhead costs per user and administration fees, fewer IT staff, data centers, desktop devices, and network operations centers. Security benefits, like fewer cyber security vulnerabilities from a single-security architecture proliferated with the mass distribution of thin-client systems, and mission benefits like portable virtual desktops utilizing single-sign-on authentication, will lead to better interoperability among America's mission partners.[3]

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

1. The current DODIN is ineffective and riddled with problems stemming from differing architecture standards and security vulnerabilities, and is too costly to maintain in today's fiscally constrained environment. The DODIN was built over previous decades by a variety of different services and government agencies, using a variety of different vendors, network architectures, and security postures, has become an enormous patchwork quilt that is nearly impossible to defend. Built primarily by services and government agencies to support their department-specific systems and IT resources, using different architecture standards, the present-day DODIN has grown into a heterogeneous mix of networks and domains that inhibits information sharing among different services and government agencies and lacks interoperability between different sets of users, according to Mr. Robert J. Carey, DoD principal deputy CIO.[4] The current security posture is acknowledged to be a "critical security vulnerability" by multiple strategic defense leaders including the last two Secretaries of Defense, Chairman of the Joint Chiefs of Staff, and Commander of United States Cyber Command.[5]

Multiple security vulnerabilities in the current DODIN leave it open to attack. The DODIN consists of "numerous disparate and uncoordinated security architectures that have rendered it virtually indefensible from a comprehensive, DoD level cyber defense perspective." [6] This architecture hinders our capabilities of protecting the DODIN, but enables our adversaries the ability to degrade, disrupt, or interdict our data.[7] Another security vulnerability stems from the realization that USCYBERCOM, the organization charged with securing the DODIN, "can only see about 10 percent of the network that we are charged with defending," according to US Army Brigadier General George Franz, USCYBERCOM Chief of Operations.[8] This is because of the disjointed nature of current network operations centers having visibility into small, service-centric

footprints of the DODIN, and only 10 percent of that network monitoring visibility currently passed up the chain to USCYBERCOM. These limitations, and lack of a consolidated network centric view of the DODIN will impact America's ability to rapidly project joint and coalition forces when the situation arises.[9]

2. The current service-centric funding process for IT procurement in the DoD are costly and unsustainable in the long run. Military services worry about losing funding from conceding control of networks to JIE. Title 10 of U.S. Code currently provides the authority for individual armed services to "train, organize and equip" themselves, which in the realm of IT has meant that they fund and build their own separate IT infrastructures, giving them no incentive to adhere to common standards that are interoperable with other services' networks.[10] This has led to a culture of services' fighting over IT dollars, effectively leading services to wrap their arms around their own piece of the DODIN. Consequently, services' have developed stove-piped applications and redundant infrastructures, including duplicative data centers and network operations centers. By centralizing the network architecture, one would completely eliminate the need for redundant personnel staffs and duplicative infrastructure. Redundant services do not make the best use of funding in today's cost-conscious fiscally constrained environment.

3. JIE implementation poses a unique set of implementation challenges. A culture of military services playing a zero sum game with regard to obtaining funding against other services, deeply seeded in parochialism and the need to control resources, will be the primary hindrance to JIE implementation. The patchwork DODIN problem exists today because control over a service's area of responsibility of the DODIN leads to additional service funding, resources, and personnel, equating to services' building and maintaining their own service-centric networks.[11] As long as services get their own IT funding, there will be no incentive to implement JIE. Furthermore, many military customers have grown comfortable with service-specific current IT capabilities and have become resistant to change. Many of these customers have weathered the storm of recent service-centered migration efforts, such as AFNET migration across the Air Force, each that came with its own challenges, and are weary of future efforts to migrate. Users need to be educated in both the fiscal and security benefits of JIE in order to support its implementation.

## RECOMMENDATIONS

1. Ultimately, the JIE is being constructed to design a secure, single-security environment, across the entire DODIN, to enhance mission effectiveness. In August, 2012, the Chairman of the Joint Chiefs of Staff formally approved the definition of JIE as "a secure joint information environment comprised of shared information technology infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies."[12] The JIE is operated and managed by the Defense Information Systems Agency (DISA) per the Joint Technical Synchronization Office (JTSO) using enforceable standards, specifications, and common tactics, techniques, and procedures.[13] Once implemented, the JIE will enable future users of the DODIN to utilize Unified Capabilities, including accessing a standard suite of enterprise services from any DoD location in the world. Coast Guard users, for example will utilize world-wide virtual desktop, Voice-over Internet Protocol (VoIP), mobile e-mail, and mobile Microsoft Lync (formerly Microsoft Office Communication Server) collaboration that will allow them to access their IT resources anywhere in the world through cloud computing technology.[14] Similarly, JIE will also be the linchpin for

the future DoD classified cloud, providing classified services, including Voice over Secure Internet Protocol and secure Enterprise E-mail, to a world-wide user base accessing the classified domain.[15] The JIE cloud-based capabilities will leverage commercial approaches and provide seamless, secure mobile communications to tomorrow's warfighter.[16] JIE Increment One was completed in July 2013 in Europe, and focused on enhancing and consolidating capabilities in EUCOM and AFRICOM's Area of Responsibility (AOR). Increment Two will focus on the PACOM AOR.[17] JIE will enable American warfighters more seamless access to Combined and Coalition Mission Partner Environment (MPE) architectures, like the Battlefield Information, Collection, and Exploitation System (BICES) and Combined ENTerprise Regional eXchange System-Korea (CENTRIXS-K), that will enable America and partner nations to more securely and effectively communicate during contingencies.[18] Future Increments of JIE will allow a fully-integrated MPE, allowing our coalition partners to connect different flavors of BICES, CENTRIXS-K, or any other future partner networks to each other that would be needed.

The end result of JIE will be a completely interoperable, defendable, maintainable DoD-wide network utilizing a single security architecture standard. JIE is being developed to help overcome architecture problems associated with the current DODIN. By standardizing architectures across the services, and gaining visibility into larger sections of the DODIN across service domains, the number of network operations centers across the DODIN will be reduced from 65 in FY12 to 25 by FY17, providing more effective visibility into the network and significant cost savings.[19] JIE's secure single-security environment, providing increased token-based access to systems and IT resources in both classified and unclassified domains, will make it much more difficult for intruders to gain access.

JIE must securely support cyberspace operations across all warfighting echelons. JIE's single security architecture, using the same standards of technical protocols with increased token access, will make the entire DODIN less susceptible to outsider attack. Another goal of JIE's design is establishing regional jointly managed Enterprise Operations Centers (EOCs), that will help eliminate the need for the current 65 service-centric network operations centers, for the consolidated defense of the entire DODIN.[20] These regional EOCs will disseminate their Common Operating Picture (COP) to the Global EOC at USCYBERCOM. By achieving this end state, these EOCs would give CYBERCOM the 100% visibility into the DODIN that it requires, in real time.

2. JIE implementation will provide cost savings to the DoD in many areas. Rather than multiple disparate and loosely connected networks, JIE will allow for one fully-integrated and centrally controlled network, eliminating costly capability duplication and redundancy. Consolidation of the current 800 data centers, to around 400 as LTC Dawson proposes, would lead to both up-front cost savings and reduced long-term investments in operations and maintenance costs associated with expensive facilities and support systems (heating, cooling, uninterruptible power supplies, fire suppression systems, etc).[21] In FY13, the DoD IT budget stood at $37 Billion which was 7% of the overall operating budget.[22] The DoD currently operates over 800 data centers, generally to meet service-specific requirements, 65,000 servers, 7 million computers and 250,000 mobile devices.[23] Cutting just 20% of this infrastructure would translate to a potential savings of over $7 Billion per year.

3. JIE will impose true Joint standards on the collective DoD signal corps and communications mindset and culture once fully implemented. Through establishing jointly-managed EOC's, the cyber community from all services will be working with each other, like never before, to defend the entire DODIN, rather than separately defending their service-specific footprint inside it. By migrating stove-piped service-provided applications to jointly managed enterprise solutions, personnel from the different services will also find efficiencies of utilizing economies of scale, leading to fewer redundancies from applications that serve the same purpose. Although not mentioned specifically in the JIE construct, additional cost savings could be gained by restructuring communications and signal corps cyber training schools for officers and enlisted personnel. These students would only attend service-specific schools after the majority of their time has been spent in a joint environment learning the basics of all communications training in a joint environment.

Lastly, for JIE to be effective, Congress must change Title 10 to allow DoD CIO to control and distribute services' IT budgets. By transferring this control and distribution of funding from the individual services to the office of the DoD CIO, all services will be forced to adhere to joint JIE standards for all future IT infrastructure projects. Without this, services will have no financial incentive to change, and can only give "lip service" to JIE, while maintaing the status quo. The Air Force, for example, directs Air Force Space command to support "organize, train, and equip cyberspace operations forces" on behalf of the Air Force.[24] Air Force Policy Directive 10-17 does not mention, however, integrating these forces with other services in support of JIE.[25] According to Air Force Lieutenant General Ronnie Hawkins, DISA Director, "The J word is very important. Especially as we go through the ties to the lack of resources, from a funding perspective down."[26] DoD Chief Information Officer, Ms. Teri Takai, however, claims that her office is not seeking to divert funding from the services for JIE as it is not a program of record. In speaking to the House Armed Services Committee in March, she stated her office "is not seeking to look at funding for the program, per se."[27] The issue of centralized funding from the Joint level will be at the heart of future JIE debates and whether the program can accomplish its objectives.

**COUNTERARGUMENT**

1. The first counterargument to implementing JIE is that the program is not necessary, and that service and functional architecture models are better suited to support warfighters' needs. There is no cookie-cutter approach to providing IT services. The current model meets the needs of the services, and JIE will not be robust enough to cater to the IT requirements for all users in all environments. Although services today are fighting more of a joint fight than ever before, the individual military services are still structured today to support, train and equip their particular forces with IT resources, and changing to a JIE model would require a serious culture change.

2. Another argument posed is that interoperable systems introduce security vulnerabilities onto other systems. These people would argue that a risk accepted by one is shared by all. By making networks more interoperable, any vulnerability from one application or service, when introduced to a larger cloud environment, becomes a risk to all systems that it is interoperable with. JIE implementation, in these people's minds, makes networks more vulnerable to network attack.

3. Others argue that JIE is a big idea but hasn't yet produced any tangible results. Brig. Gen. Kevin J. Nally, USMC, the Marine Corps director for command, control, communications and

computers (C4) and chief information officer, bluntly stated to an AFCEA conference in 2013 that after two years of work, "we're still at PowerPoint."[28] To some people, JIE's implementation timelines seem ambiguous and the description of JIE itself is not as tactical and straightforward as they want. There are not well-defined goals or pathways for obtaining JIE's objectives.[29]

4. Another failure, to date, of JIE implementation, is that JIE Enterprise Services has not effectively addressed Disconnected, Intermittent, or Low-bandwidth (DIL) users. These DIL users, usually located at the tip of the spear in tactical environments or aboard ships, simply don't have the available bandwidth to receive services from the enterprise cloud that now require even more satellite communications (SATCOM) resources. One way forward to help solve this includes analyzing available IP Space compression modeling techniques in order to get the most throughput for available SATCOM bandwidth. Another possible solution is to distribute the ability to host enterprises services for tactical users (e.g. giving Corps-level and below field units their own tactical mini-pod) so they have access to Enterprise Email in the field, without having to increase transport pipes to pull them from the DISA enterprise. Much more effort will need to be performed in the areas of maximizing available SATCOM resources to get these customers to change their mindsets regarding JIE implementation.

## CONCLUSION

Despite valid concerns that implementing JIE will not cater to the demands of all users, the benefits of JIE far outweigh the challenges. Today's current costs for maintaining and sustaining DoD IT infrastructure are not sustainable. The fastest way to achieve major cost savings is to change Title 10; thereby allowing the DoD CIO control over individual military services' IT budgets. Further cost savings would be obtained through JIE by lowering overhead costs per user and administration fees, fewer IT staff, reducing the inventory of over 800 data centers, and migrating the 65 existing network operations centers to 25 in support of the EOC construct. Security benefits, like fewer cyber security vulnerabilities from a single-security architecture, proliferated mass distribution of thin-client systems, and mission benefits like portable virtual desktops utilizing single-sign-on authentication, will be achieved and lead to better interoperability among America's mission partners. Additionally, the single security JIE architecture will be easier to defend with less resources and help to provide better overall mission effectiveness. Outside of the JIE construct, streamlining initial Comm/Cyber/Signal Corps training to a streamlined Joint 'basic' cyber training school set will see additional efficiencies and cost benefits from utilizing economies of scale and help effect cultural change on this community. These recommendations will help shape a future DoD warfighting network that is more defendable, portable, sustainable, and better suited to meet the needs of all users.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

1 Kelly, "Joint Information Environment" 2013

2 Deltek Report, "Defense IT Strategies Converge Around Interoperability, Security and Cost Reduction", 2014

3 Kelly, "Joint Information Environment" 2013

4 Kenyon, "Joint Information Environment is Under Way" 2013

[5] Dawson, "Strategic Leadership Challenges with the Joint Information Environment" 2013. p.1
[6] DISA Strategic Plan 2013-2018. 2013. pp. 9-10
[7] Joint Chiefs of Staff White Paper, "Joint Information Environment White Paper". 2013. p. 1
[8] DISA Strategic Plan 2013-2018. 2013. pp. 9-10
[8] Dawson, "Strategic Leadership Challenges with the Joint Information Environment" 2013. p.8
[9] Joint Chiefs of Staff White Paper, "Joint Information Environment White Paper". 2013. p. 4
[10] Dawson, "Strategic Leadership Challenges with the Joint Information Environment" 2013. p.8
[11] Ibid
[12] Kelly, "Joint Information Environment" 2013 p. 5
[13] DISA Strategic Plan 2013-2018. 2013 p. 5
[14] Day, "Joint Information Environment and Coast Guard" p. 25
[15] Leopold, "JIE is Linchpin of Next-Generation Classified Cloud" 2013
[16] Joint Chiefs of Staff White Paper, "Joint Information Environment White Paper". 2013. p. 6
[17] Kenyon, "Joint Information Environment is Under Way" 2013
[18] Kelly, "Joint Information Environment" 2013 p. ???
[19] Dawson, "Strategic Leadership Challenges with the Joint Information Environment" 2013 p.9
[20] Ibid, p. 16
[21] Ibid, p. 16-17
[22] Ibid, p. 9
[23] Ibid, p. 9
[24] Air Force Policy Directive 10-17, "Cyberspace Operations" 2012, p. 5
[25] Ibid
[26] Bernhart-Walker, "JIE Funding Must Also be 'Joint,' Says DISA Official" 2012
[27] Perera, "JIE Not a Program of Record" 2014
[28] Kenyon, "Marine Corps Enterprise Network Plan Gives JIE a Boost" 2013
[29] Corrin, "JIE's Murky Progress Raising Questions" 2013

## BIBLIOGRAPHY

Air Force Policy Directive (AFPD) 10-17 (2012). *Cyberspace Operations*. Retrieved from: https://cyber.iovermont.org/pluginfile.php/4274/mod_resource/content/1/afpd10-17.pdf (accessed 7 May 2014).

Bernhart-Walker, Molly (2012). "JIE Funding Must Also Be 'Joint,' Says DISA Official." *FierceGovernmentIT Newsletter*. Retrieved from: http://www.fiercegovernmentit.com/story/jie-funding-must-also-be-joint-says-disa-official/2012-10-01 (accessed 7 May 2014).

Corrin, Amber (2013). "JIE's Murky Progress Raising Questions." *Federal Computer Week Magazine*. Retrieved from: http://fcw.com/articles/2013/08/27/jie-goals-and-timelines-unclear.aspx (accessed 7 May 2014).

Dawson, Stephen E. LTC, US Army (2013) "Strategic Leadership Challenges with the Joint Information Environment." Mr. Brian A Gouker (Ed.). US Army War College Strategy Research Project, US Army War College, Carlisle Barracks, PA. Retrieved from: http://handle.dtic.mil/100.2/ADA589309 (accessed 7 May 2014).

Day, Bob. RADM, US Coast Guard (USCG). (2013). "Joint Information Environment and Coast Guard." USCG CG CIO & Director CG Cyber Command. Retrieved from: http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-Day.pdf (accessed 7 May 2014).

Defense Information Systems Agency (DISA). (2013). *DISA Strategic Plan 2013-2018*. Retrieved from: http://www.disa.mil/~/media/Files/DISA/About/Strategic-Plan.pdf (accessed 7 May 2014).

Deltek Report. (2014). *Defense IT Strategies Converge Around Interoperability, Security and Cost Reduction*. Retrieved from: http://www.deltek.com/company/mediacenter/pressreleases/2014/defense_it_strategies_converge_around_interoperability,_security_and_cost_reduction_according_to_new_deltek_repo (accessed 7 May 2014).

Joint Chiefs of Staff White Paper . Dempsey, Martin. GEN, US Army, (2013). "Joint Information Environment White Paper." . Retrieved from: http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf (accessed 7 May 2014).

Kelley, Olen L. LTC, US Army, (2013). "Joint Information Environment." Defense Information Systems Agency (DISA) JIE Technical Synchronization Office (JTSO) Cyberspace Operations. Retrieved from: http://www.itea.org/~iteaorg/images/pdf/conferences/2013_Annual/Panel_3_Kelley.pdf (accessed 7 May 2014).

Kenyon, Henry S. (2013). "Joint Information Environment is Under Way." Signal Magazine. Retrieved from: http://www.afcea.org/content/?q=node/11696 (accessed 7 May 2014).

Kenyon, Henry S. (2013). "Marine Corps Enterprise Network Plan Gives JIE a Boost." Signal Magazine. Retrieved from: http://www.afcea.org/content/?q=node/11111 (accessed 7 May 2014).

Leopold, George. (2013). "JIE is Linchpin of Next-Generation Classified Cloud." Defense Systems Magazine. Retrieved from: http://defensesystems.com/articles/2013/10/08/classified-cloud.aspx (accessed 7 May 2014).

Perera, David. (2014). "JIE Not a Program of Record." FierceGovernmentIT Newsletter. Retrieved from: http://www.fiercegovernmentit.com/story/jie-not-program-record-says-takai/2014-03-13 (accessed 7 May 2014).

Improving Cyber Command and Control Using the Joint Information Environment
Maj Kelly A. West (DISA)

**ABSTRACT**
The JIE stems from the Secretary of Defense's guidance to expedite IT efficiencies.[1] Our Joint Staff J3 published in December 2012 the JIE execution order disseminating the Secretary of Defense's guidance directing "…Department of Defense (DoD) Chief Information Officer (CIO), Director of the Joint Chiefs of Staff, and the Commander, United States Cyber Command, to provide JIE transformation planning, coordination and execution, in conjunction with Combatant Command, services and agencies, throughout the DoD".[2] Also, driven from the Capstone Concept for Joint Operations: Joint Forces 2020[3] and the DoD CIO Implementation Guidance letter dated 26 September 2013, the vision for JIE is to provide a single joint enterprise platform that can be leveraged for all DoD missions.[4] The Air Force can capitalize on the advantages a joint environment offers, particularly in the cyber command and control function. Embracing JIE's initial core data services element, defense enterprise email, single security architecture and identity access and management components as a starting point, cyber command and control can more quickly evolve from its current construct into an improved and more integrated joint cyber command and control system.[5] Culture, fiscal challenges, and command and control implementation guidelines are enormous hurdles to overcome during the transformation. The challenges are compounded when considering these elements between the cyberspace, space and ISR communities, three key components for a future generation cyber operations construct. If planned using the opportunities the JIE has to offer, the AF is capable of restructuring a flatter cyber command and control system and contribute leading capabilities into joint cyber command and control.

**DESCRIPTION OF ISSUE/ PROBLEM STATEMENT**
1. The JIE socialization phase is ongoing and many organizations have neither bought in nor tangibly seen the value it can bring to the holistic environment. This skepticism has the potential to delay and continually fragment JIE's end state of secure joint interoperability and information sharing. The JIE can be best visualized as an environment with similar characteristics to a service utility – available and accessible whenever and wherever DoD and coalition partners need.[6] Further, "The environment will include…a dynamic combination of technologies, people, and services for DoD… and summarily outlined below and in no particular order:

- A shared, standardized, secure, and resilient architecture;
- A trusted and highly accessible infrastructure governed by technical and operational standards;
- An optimized set of applications across DoD for similar functions;
- Highly trained workforce;
- set of commonly understood and infused operational tactics, techniques, procedures, roles, and responsibilities at various operational levels;
- Agile help desk user support."[7]

2. Current Air Force cyber command and control functions find it difficult to provide a total real-time mission network health picture to United States Cyber Command. Numerous Air Force sub-organizations and their associated information access controls present extraordinary challenges with interagency operations, from the most intricate programs to basic daily interoperability needs.

Many separate mission network environments, as they exist today, have their own management and security levels with separate credential-based access processes. This is a known and daily documented monitoring need for any organization, and while there's an outlined Air Force operational and reporting structure[8] there are still many mission systems not yet visible within current Air Force cyber command and control channels.

3. The Air Force cyber operations center must posture itself for integration into joint operations centers. Not all service components view cyber operations the same, nor do they weigh cyber operations on a playing field similar to land, air, sea, or space domains. For example, a Joint Forces Cyber Component Commander is not listed in documentation nor is any level of cyber operations within a joint operations center.[9] There are, though, inferences within the ISR division of a cyber "support" presence. This makes progress within a cyberspace domain difficult for any service's cyber operations teams to find their contribution avenues within a joint operations center.

**RECOMMENDATIONS**

1. On 22 January 2013, the Joint Chiefs of Staff committed to the JIE way ahead through the Joint Information Environment White Paper.[10] As a result, each service now needed to figure out how it would implement the transformation. Core data services such as defense enterprise email and cloud movements with single security architecture and identity access and management steps are beginning the transformation. The Air Force began its defense enterprise email journey in November 2013 and as more and more services are migrated, the higher the chances are of evolving a more efficient command and control system.

The defense enterprise email environment has the capacity to accommodate over 4.5 million users. The environment is ready, and although there's varied debate in few communities and challenges to overcome, budget cuts are quickly becoming the forcing functions to propel movement into the JIE.[11] Current enterprise email users at all levels have experienced enormous benefits, including collapsing long standing hurdles to communicate between other organizations via email into a single structure, reducing a single organization's cost of ownership and placing fiscal responsibility on DoD-level organizations, solving myriad similar dilemmas with one DoD solution will prevent sub-organizations from repetitively spending different monies on the same problem, and serving as a springboard to then pursue deeper information sharing capabilities, for example SharePoint services.

2. The Air Force's cyber command and control function needs complete visibility across the Air Force's cyberspace to truly accomplish operations and defense. Integrating into the JIE will exponentially increase the ability for the Air Force's cyber command and control system to "see" into and through cyberspace. One example is a consolidated insight into mission network health and recovery. A second example is that a DoD cloud and single security architecture solution will offer a common security layer among all communities built from technical and operational standards, a task the Air Force does not need to accomplish on its own, rather, integrate into a larger team with the same standards.[12] A third consideration is by implementing the DoD-directed identity access and identification management system. This joint solution will offer the Air Force an additional "flatter" and faster identification (find, track), analysis (track, assess) and remediation (engage, fix) cycle, potentially faster than it could accomplish on its own given DoD-wide budget and personnel reductions.

Joint Publication 3-60, Targeting, phase 5 of the joint targeting cycle identifies this "kill chain" and is further defined within each service component's targeting manuals.[13] The Air Force, through its AFDD 3-60 uses this fundamental execution cycle in air, space and cyberspace operations through its operations centers.[14] Current cyber command and control uses the air operations center construct with its combat ops, combat plans, ISR, and strategy divisions. The Air Force's single cyber operations center, similar to air and space operations centers must have a full operational picture of its own domain to better conduct operations. Also, each of these centers must have strong interconnectivity between one another, at all division levels to consider implementation strategies from each weapons system.[15]

3. The Air Force must consider cyberspace future in two major areas: cyberspace operations functions that overlap with ISR/space functions and future integration into joint doctrine. Cyber roles should be clearly and distinctly defined between the career fields to prevent redundant operations, possibly leading to evolving career fields or elimination of some. The Air Force must also lead the influence for joint doctrine to better incorporate cyber into the kill chain cycle for consideration. Cyber must also be a method of operation to consider when first strategically discussing targets, means and methods. The Air Force can help infuse cyber systems in joint doctrine through US Cyber Command with possibly forming a position similar to a Joint Force Cyber Component Commander who that can inject cyber capabilities into the operational planning cycle such that not all activities are war/conflict-related.[16]

**COUNTERARGUMENT**

1. The JIE, particularly enterprise email, is too expensive for the Air Force to migrate and they can perform a single network function cheaper. In light of the planning, budgeting, and ongoing implementation to a single Air Force email, it will be more effective for the Air Force to perform this function, and tie into JIE after their consolidation is complete. This will allow the Air Force to continue to control and operate all facets of its own network, yet still contribute to JIE on its own terms. Although the Air Force has begun its defense enterprise email migration there will be challenges to work through, such as temporary frustrations with the conversion from organization-centric to enterprise email, perceived slower recovery time with those personnel experiencing problems resulting in "not being able to effectively perform their jobs", and technical hurdles resulting in years of little-enforced standardized architecture or infrastructure enforcement.

2. There's not enough money in the Air Force budget for the cyber mission to make necessary changes to make the centers interoperable. The Air Force will need to find interoperability experts to assess the best approaches to connect them and that will take time in addition to money to achieve. If achieved, the Air Force will have to train an already small cadre of personnel in yet another set of tasks. There is already an overwhelming imbalance between too many missions versus not enough skilled personnel. To that end, the cyber operations center must prioritize which missions it needs visibility into and those areas deemed valuable to mission success will gain focus. Not all systems on the network are deemed mission critical. Therefore, in lieu of making the centers transparently interoperable, liaisons can perform those functions and keep the centers linked.

3. The joint community does not view cyber as the domain that air, land, sea, space are for the full spectrum of operations. The cyber domain does not require its own joint forces cyber component commander, for it is merely a support function alongside ISR within an operations center. Unlike the air, land and sea domains capable of experiencing and inflicting physical destruction to achieve objectives, cyber currently doesn't contribute that level of effect. Also, the cyber domain is not as developed to be considered a part of full spectrum operations commensurate with air land, sea and space.

**CONCLUSION**

The Department of Defense has an enormous challenge ahead of it to continue streamlining itself and draw down its budget and personnel. Simultaneously, the President, SECDEF, Chairman and Joint Chiefs, Combatant Commanders have all publicized the need for total interoperability among our personnel, coalition partners, fellow services, and other organizations throughout the entire spectrum of operations. In order to build for the next generation of capabilities, our communities must be integrated into a single standardized environment capable of seamlessly sharing information amongst one another.

Core enterprise service initiatives such as defense enterprise email, cloud services and identity access and management will help the Air Force achieve network consolidation while reducing the Air Force's total cost of ownership. It will also help provide a more secure, collaborative environment based on a common set of standards and security controls. This will immensely benefit the Air Force by offering an enhanced ability to more efficiently conduct cyber operations and defense through the entire service's cyberspace. Hence, the Air Force can increase its cyber command and control capability.

The Air Force's cyber operations center is constructed similar to air and space operations centers; however, when considering cyber as a domain, there's no establishment of a similar position to a Joint Force Cyber Component Commander as there are with air, land, sea, space. This will present a problem when considering strategic, operational and tactical targets and the ability for a coalition or the United States to decide conflict responses. The cyber operations presence is predominantly located in the ISR division but must be strongly represented in every division. The Air Force has the ability to help influence joint cyber operations during the full spectrum of conflict by helping to establish clearer and more precise cyber command and control channels. Currently joint operations doesn't prevalently discuss cyber operations in a domain context, rather it discusses cyber as an element of other disciplines.

The JIE has the potential to eliminate consolidation hurdles for the DoD in a way they, including the Air Force, may not have been able to overcome on their own given personnel and budget reductions. It is this time that the Air Force can capitalize on consolidated communication collaboration such as enterprise email, unified communications, and defense connect online. It can also provide a standardized secure infrastructure through its cloud environment and secure enterprise directory services such as identity access and management. Portability and mobility through the JIE will enhance the users' ability to retrieve, use, share, send information anywhere, anytime, he or she needs. It will be the environment for years to come and cyber command and control can significantly evolve as a result.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] OSD. "Track Four Efficiencies Initiatives Decisions", 2.
[2] "Guidance for Implementing the Joint Information Environment", 1-2
[3] Gen Dempsey, Martin. "Joint Force 2020", 4.
[4] Takai, Teri. "Joint Information Environment Implementation Guidance", 1.
[5] AF/A3O-AC. "Operational Procedures-Air Operations Center", 12-13.
[6] "Guidance for Implementing the Joint Information Environment", 1.
[7] Ibid, 1-2.
[8] Pawlyk, Oriana. "Air Force Boosts Cyber Mission Capabilities", 1.
[9] Joint Staff. "Command and Control for Joint Air Operations", II-1-2.
[10] Gen Dempsey, Martin. "Joint Information Environment", 5.
[11] Defense Information Systems Agency. "DISA Core Enterprise Data Services", 12.
[12] Ibid, 5.
[13] Joint Staff. "Joint Targeting.", II-1-6.
[14] Ibid.
[15] Pawlyk, Oriana. "Air Force Boosts Cyber Mission Capabilities", 1.
[16] Joint Staff. "Joint Targeting", II-1-6.

## BIBLIOGRAPHY

AF/A3O-AC. "Operational Procedures-Air Operations Center." *Air Force Instruction 13-1AOC*v3, no. 18 May 2012 (2011): 12-13, 23-24, 107. http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi13_1aocv3/afi13-1aocv3.pdf (accessed December 6, 2013).

CSAF. "Targeting." *Air Force Doctrine Document* N/A, no. N/A (2011): 29-30, 48-53. www.fas.org/irp/doddir/usaf/afdd3-60.pdf (accessed December 6, 2013).

CSAF. "Cyberspace Operations." *Air Force Doctrine Document 3-12* N/A, no. N/A (2011): 14, 20-28. www.fas.org/irp/doddir/usaf/afdd3-12.pdf (accessed November 29, 2013).

JCS, Staff. "Cyberspace Operations C2." Address, JCS OPSDEP TANK from Joint Chiefs of Staff, Washington D.C., October 26, 2013.

Defense Information Systems Agency. "DISA Core Enterprise Data Services." *The Joint Information Environment (JIE)* 1, no. 1 (3012): 12.

Gen Dempsey, Martin. "Joint Force 2020." *Capstone Concept for Joint Operations* N/A, no. N/A (2012): 4. https://acc.dua.mil/adl/en-US/347752/file/48933/CCJO%20Joint%20Force%202020%2010%20Sept%2012.pdf (accessed December 9, 2013).

Gen Dempsey, Martin. "Joint Information Environment." *White Paper* N/A. N/A (2013): 5.

"Guidance for Implementing the Joint Information Environment." *Department of Defense Guidance* 1, no. 1 (2013): 1-6.

Joint Staff J3. "DOD Joint Information Environment (JIE) EXORD." *DOD Joint Environment (JIE) EXORD* N/A, no. 1 (2012): 3-4.

Joint Staff. "Joint Targeting." *Joint Publication 3-60* N/A, no. N/A (2007): II-1-6. www.aclu.org/files/dronefoia/dod/drone_dod_jp3_60.pdf (accessed December 9, 2013).

Joint Staff. "Command and Control for Joint Air Operations." *Joint Publication 3-30* N/A, no. N/A (2010): II1-2, III1-3. www.dtic.mil/doctrine/new_pubs/jp3_30.pdf (accessed December 9, 2013).

OSD. "Track Four Efficiencies Initiatives Decisions." *Memorandum for Track Four Efficiency Initiatives Decision* N/A, no. N/A (2011): 1-48. www.defensetravel.dod.mil/Docs/OSD_02974-11.pdf (accessed December 9, 2013).

Pawlyk, Oriana. "Air Force Boosts Cyber Mission Capabilities." *Air Force Times* N/A, no. 29 May 13 (2013): N/A. www.airforcetimes.com/article/20130529/NEWS/305290027 (accessed December 12, 2013).

*Presidential Strategic Guidance*. Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense. January 3, 2012, 4-6.

Takai, Teri. "Joint Information Environment Implementation Guidance." *Joint Information Environment Implementation Guidance Memorandum* N/A. N/A (2013): 1.

# SECTION 3: NEW PARADIGMS

What are the USAF Leadership Cyberspace Challenges?
Wing Commander S. D. Keen, Royal Air Force, SAF CIO A3CS/A6CS

**ABSTRACT**
The significance of USAF operations in cyberspace is readily apparent. Not only is cyberspace vital to today's fight, but also it is key to the continued US military advantage over its enemies. In the Diplomatic, Information, Military, and Economic (DIME) model of national power, the ability to carry out the information portion is dependent on our networks. In cyberspace, our networks are the platform, information is the payload.[1] Consequently, the Air Force is steadfastly intent on providing a full range of cyberspace capabilities to the Joint Force Commanders, whenever and wherever needed.[2] Cyberspace is an increasingly contested man-made domain. However, the Air Force currently finds itself struggling to develop a clear and common vision for cyberspace across the service, which is compounded with the lack of an authorized and accountable single owner. The cyberspace challenges within the Air Force are wide-ranging, from: responsibility conflicts, varying definition interpretations, cultural and an unclear strategy. These challenges impact the Air Force's ability to progress in cyberspace, ultimately affecting its competitive edge and risk its operational mission. This is all taking place within a backdrop of some significant Department of Defense (DoD) challenges: resource constraints, force structure, readiness, modernization and sequestration. The main challenge is unity of effort and to rightly develop the knowledge and skills as a cyberspace workforce with the ability to operate effectively in this environment; this is how our adversaries operate. The Air Force's ultimate success will be measured by its ability to achieve and maintain the "information advantage."[3]

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
There is currently no Air Force unified approach and designated single lead for cyberspace and Information Technology (IT). This is as a result of conflict in specific roles and responsibilities as defined in United States Code (U.S.C.), DoD Instructions (DoDIs), Air Force Instructions (AFI) and decision briefs. The Chief Information Officer (CIO) is responsible for and accountable to deliver integrated IT capabilities through such laws as Title, 10, 40, 44 U.S.C. that requires a single agency CIO. The Core Function Lead Integrators (CFLIs) are responsible for Core Function Master Plans (CFMPs) and Program Objective Memorandums (POMs); introducing multiple IT/cyberspace stovepipes. There is no formal documentation defining the CFLI roles and responsibilities as Air Force Policy Directive (AFPD) 90-11 has yet to be published. This is further complicated at the DoD level where the Unified Command Plan states that STRATCOM (CYBERCOM is not specified) is responsible for directing information network operations and defense, whilst DoDI 5144.02 states that the DoD CIO is responsible for all matters relating to network operations. From an IT perspective, this conflict continues to be the case even after being a topic item during Spring CORONA Top 2013. Unfortunately, this was a missed opportunity to resolve the cyberspace and IT conflicts. The decision was made that the Air Force required a CIO and the primary agent for IT was SAF/CIO A6. However, in reality the conflict has not been addressed and continues to this day. So, who is the IT and cyberspace primary agent and what is the Air Force Cyberspace and IT Strategy for the future? This is so important as it is very much in the realm of the possible that the next battle fought will not be on land, sea, air, or space – but within the cyberspace domain itself. Therefore it is essential for the Air Force to be effectively postured to learn to fight and defend as one entity in this man-made domain because that is how

adversaries have approached it. Otherwise, the Air Force runs the risk of losing a conflict without a shot being fired.[4]

The Secretary of the Air Force (SecAF) and Chief of Staff Air Force (CSAF) CFLI Roles and Responsibilities decision brief on 25 Jun 12 charged the CFLIs with integrating Service Core Function (SCF) capabilities across the Air Force enterprise and advocate within the Air Force Corporate Process. This involves guiding all SCF related operate, maintain and investment priorities in collaboration with key stakeholders, prioritize these investments, and operate and maintain inputs for AF/A8 centralized POM development and authoring the CFMP. During the 2013 AFCEA Cyberspace Symposium, Gen Shelton stated: "the Secretary and the Chief have charged me with being the single commander responsible not only for operation, maintenance, sustainment and defense of the Air Force Networks, but also developing, fielding, and employing operationally relevant cyber capabilities and effects. Bottom line: the buck stops with me."[5] This statement conflicts with the CIO in that the law states the CIO is ultimately responsible for Air Force Networks and causes confusion both internally and externally to the Air Force. Gen Shelton further stated: "until very recently some of our 24th Air Force Airmen were a little bit confused about what was expected of them because we had not provided them with the operational guidance needed to accomplish their mission."[6]

The Air Force continuously struggles to achieve consensus regarding what cyberspace is and definitions therein. An Air University student, Lt Col Farenkrug states: "there is a wide range of thoughts about the extent of cyberspace or what should be included in cyber warfare."[7] This confusion was further reinforced by Gen Shelton's recent AFCEA Cyberspace Symposium remark: "since the Air Force and the DoD started down the path of establishing cyberspace, we've been challenged to clearly articulate what's cyber, what's IT, and what's communication and information. Definitions in DoD, Joint and even Air Force policy can be interpreted in multiple ways leading to confusion, duplication and unnecessary work."[8]

The relationship between cyberspace domain and IT is not codified in law. The SAF/CIO A6 and Cyberspace CFLI interpret the IT and cyberspace relationship differently, experiencing continual debate on whether the cyberspace domain is a subcomponent of IT or separate and distinct. Joint Publication 1-02 defines cyberspace as being a: "global domain within the information environment consisting of the interdependent network of information technology...." This definition provides guidance to this relationship and is further supported by Title 40 U.S.C Subtitle III, Ch 111: "IT includes computers, ancillary equipment… peripheral equipment…, and related resources." However, debate continues due to interpretation differences of these definitions and understanding of what constitutes IT and cyberspace. This confusion results in Airmen being inefficiently utilized due in part to an Air Force internal definition debate as opposed to advancing the Air Force cyberspace mission.

There are significant cultural and mindset challenges of cyber employment and ubiquity. Historically, any new weapon has been seen as an enabler before it became a true weapon. One of the most classic examples is the longbow in England which was often seen as a "peasant's weapon" until the Battle of Agincourt where it proved effective against the French.[9] A more recent example is the airplane which was originally used solely for reconnaissance and is now a powerful weapon of power projection. So too, the cyber battlefield.[10] This relates to the cyberspace environment and

as VADM Brown, USN stated: "to fully integrate and implement the transition to cyberspace superiority, the Air Force needs to transcend paradigms entrenched in the purely kinetic traditions of warfare, and transform the force to achieve cross-domain dominance of air, space and cyberspace."[11] There are wide ranging views and understanding of cyberspace and what it means to the Air Force, from those that believe it is just Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) to those that believe it is OCO, DCO, Department of Defense Information Network Operations (DINO) and the maintenance and sustainment of the network. So when policy is looking to get coordinated and released, consensus is difficult to achieve and the language becomes less effective to appease all relevant stakeholders. The fundamental imperative for maturing understanding is to treat cyberspace as a place, not a mission. Gen L Welsh describes cyberspace as a domain in, from, and through which military operations create intended effects and has a significant difference in that it is constructed by man and constantly evolving. "The fundamental military objectives relative to this domain are essentially the same as in the other domains, again – land, sea, air and space. The primary objective is freedom of action in, through, and from cyberspace as needed to support mission objectives."[12]

These roles and responsibility conflicts, coupled with chain of command disagreements, present significant issues for the Air Force. As per MD 1-26, the SAF/CIO A6 serves as an agent of the SecAF providing guidance, direction, and oversight for all matters pertaining to the formulation, review and execution of Air Force IT and National Security Systems (NSS) plans, policies, programs and budgets. In addition, SAF/CIO A6 provides policy and guidance to develop the total force in coordination with AF/A2 and AF3/5. SAF/CIO A6 also develops, analyzes and advocates career field structure capabilities packaging and force organization. These authorities are reinforced by the Office of Management and Budget (OMB) M-11-29 CIO Authorities stating the CIO has responsibility over the entire IT portfolio for an agency, accountable for the performance of IT program managers. Therefore, a 3-star is responsible for the strategic direction and guidance for Air Force IT and a 4-star is then meant to take that strategy guidance and deliver the operate, train and equip aspects. In reality, this does not work, due to the chain of command and the inability to enforce strategic direction because resources are managed at the delivery end.

It has been evident from the 3-star Integrated Project Team, which is tasked with looking out to 2023 and defining the Air Force priorities, core competencies, structure and shape, who analyzed the future as being more joint across the full range of military operations. This increased joint approach will provide more efficiency and improved interoperability in all areas. However there are a number of Air Force organizations that are resisting this, which again is causing confusion. An example of this has to do with Defense Enterprise Email, a DoD-led initiative that AFSPC is reluctant to support mainly due to financial constraints and would rather continue with Air Force Network (AFNET) migration, in spite of a number of other areas of Defense being widely supportive of this initiative.

The cyberspace and IT conflicts in the Air Force are occurring amidst a very dynamic and challenging strategic landscape. As acting Secretary Fanning stated in his 'State of the Air Force' at the Air Force's Association (AFA) Conference 2013 when he quoted Winston Churchill: "gentlemen, we have run out of money. Now we have to think."[13] The Air Force is currently focused on three main areas; readiness, force structure, modernization/recapitalization in response to the current financial situation of Sequestration and the Continuing Resolution. Gen Shelton

stated at the AFA Conference 2013 that: "sequestration is the biggest threat to the nation's space and cyberspace capabilities."[14] The Air Force needs to significantly change its approach in order to ensure effective advancement in cyberspace to deliver the Air Force's ability to fly, fight, and win in air, space, and cyberspace.

Ultimately, the current situation of not having an Air Force designated single approach for IT and cyberspace is significantly affecting its internal and external credibility and reputation. The strategic messaging is confused at best. Airmen are unsure of the direction of where the Air Force is heading in both these disciplines. Additionally the other Services, other government departments and industry are not clear either. Historically, the Air Force has a reputation of innovators and a service that generally is in the lead. This was reaffirmed by Gen Welsh in his 2013 'Vision for the United States Air Force' where he stated: "the story of the Air Force is a story of innovation. Airmen using their unique perspective have long stood for and pioneered innovative ways to win and fight while shaping the future."[15] Due to this conflict the Air Force no longer leads in IT and cyberspace and is currently on a reactive footing.

**RECOMMENDATIONS**

It must be a priority to resolve this current situation. A primary agent for Air Force IT and cyberspace needs to be designated in order to declare a united Air Force corporate perspective, and eliminate ambiguous and contradictory guidance. This fosters Air Force unity and synergy and ensures integration, interoperability, cohesion and resource efficiency. It also creates the situation of a single entity accountable for making all corporate IT and cyberspace decisions to best enable the Air Force's 3 priorities and 5 enduring contributions. Therefore, the recommendation is the SAF/CIO A6 be the primary 'integrator' for IT and cyberspace, providing the environment for which cyberspace operations are conducted. AFSPC will execute direction provided by the SAF/CIO A6, continuing to operate, train and equip and by extension be the operational cyberspace arm to the joint community with operational guidance from HAF A3/5.

The Air Forces strategic direction needs to be centralized to the primary agent. This agent needs to be in an impartial position, as the honest broker that can provide the best Air Force view to the SecAF and CSAF to ensure the most informed decision can be determined. One way of ensuring unity of effort and proactive advancement in the cyberspace area is through an Air Force Strategy. This strategy needs to articulate from the 'as is' through the 'to be', encapsulating the 'ends, ways, means' and coherent with the wider Air Force and DoD. The strategy should be tiered in nature to ensure it starts at a high level describing its overall contribution and value to the Air Force moving to more detailed aspects relevant to the specialized communities.

To be successful, it is important the chain of command structure follows a traditional top down approach. The strategic direction and guidance is a responsibility of the HAF/SAF and should be acted on by the delivery elements, as opposed to the current situation of direction being issued by the HAF/SAF and the Lead Command/CFLI choosing whether or not they follow it. By structuring in the traditional manner and centralizing the single agent and strategic direction, will help negate the current Lead Command and CFLI tendency to deliver MAJCOM-specific solutions that may not take account Air Force-wide mission integration with both IT and cyberspace operational mindsets. Even with the responsibilities de-conflicted, until this change in command and control takes place no improvement will be realized.

Ultimately, the Air Force needs to protect cyberspace capabilities and integrate them with other domains to enable joint warfighting effects greater than the sum of their parts.[16] This can only be effectively achieved if the Air Force works as a unified team toward a common end-state, following the proven centralized control and decentralized execution concept.

**COUNTERARGUMENT**

The HAF/SAF location for making mission decisions is too removed from the mission delivery end. Lt Gen C Miller (Deputy Chief of Staff for Strategic Plans and Programming) explained this problem and developed a solution explaining CFLI Roles and Responsibilities via a SecAF and CSAF Decision Brief for CORONA 2012. The CFLI definition was broken into a number of areas. Firstly, the SecAF/CSAF designated leaders who serve as the principle integrators for their assigned SCFs and the corresponding Air Force CFMPs. The CFLIs guide the SCFs and all SCF-related operate and maintain investment priorities by orchestrating the strategic development of the SCF in collaboration with key stakeholders across the Air Force, including MAJCOMs, the Air Reserve Components, and functional authorities. Secondly, CFLIs have tasking authority with regard to SCF planning and programming issues, to identify enabling capabilities in, and integration requirements/opportunities with, other SCFs, joint forces, civilian government and non-government organizations, and allied/partner nations. Thirdly, CFLIs participate at all appropriate levels of the Air Force Corporate Structure. CFLIs will chair or co-chair all SCF related governance structures.[17] One of the major benefits with the authority remaining at the Lead Command/CFLI is it strengthens the 4-star role in planning and programming systems.

Lead Commands and CFLIs are essentially the ten MAJCOMs designated responsibility for particular missions. In case of cyberspace operations, AFSPC has responsibility to operate, train and equip Air Force forces and deliver those detailed defense planning assumption tasks. The commander of this mission is in the best place to determine the requirements, capability and investment program for the Air Force. He is closest to the fight and understands the operational requirement thus ensuring effective delivered solutions. The Lead Command and CFLI are also able to flexibly respond to any changes required. Unlike the HAF/SAF who is generally slower to implement effective change in what is a fast moving environment. In addition AFSPC also serves as the Air Force component to the U.S. Cyber Command as AFCYBER.

The decentralization of responsibility provides the overwhelming majority of subject matter experts located in a single location ensuring the best possible posturing of forces to complete the required Air Force mission.

**CONCLUSION**

Gen. Larry D. Welsh USAF (Ret.) stated: “the most fundamental objectives in cyberspace are similar to the objectives in the other domains – land, sea, air, and space. The objectives are freedom of action to create desired military effects and ability to deny such freedom of action to adversaries at times and places of our choosing.”[18] Operations in cyberspace can magnify military effects by increasing the efficiency and effectiveness of air and space operations and by helping to integrate capabilities across all domains.[19]

However, the Air Force finds itself in a position of not having a unified approach or single authoritative lead for cyberspace and IT. There are role and responsibility conflicts, which are significantly hampering the Air Force cyberspace advancement and ultimately damaging its mission effectiveness and credibility. Historically, the Air Force has been known for its innovation and taking the initiative in areas it has been involved with, unfortunately in this case it has fallen behind. It has no clear cyberspace vision or strategy detailing what the Air Force should be doing and how it needs to be postured for the future. In an environment that has increasing strategic challenges, the Air Force should focus its effort to forging ahead as opposed to spending its resource time and effort inwardly debating. The way to achieve this is through unity of effort supported by retired MGen Vautrinot's view: "we are in a decade of decisive action for cyber, which means the military must have the patience for and a vision of future cyber capabilities. This can only be realized though a single vision that is completed and supported across the whole Air Force with a single, authoritative lead."[20] It is recommended the SAF/CIO A6 be the primary 'integrator' for IT and cyberspace, and AFSPC will execute the HAF strategic direction. This will only work if the chain of command follows a traditional hierarchy.

"As we consider the future, it's daunting to imagine the changes that may by in store for our nation,"[21] said Secretary Donley. "But if the transformative air and space technologies of the 20th Century are any guide to where we may be headed with cyberspace in the 21st Century, we are in for an exciting time."[22] The current CSAF, Gen Welsh III at the AFA 2013 Air & Space Conference and Technology Exposition stated his focus areas being – win the fight, always first; strengthen the team; shape the future. The cyberspace force needs to embrace this mantra,[23] ultimately leading to improved force cohesion and the Air Force's ability to effectively fly, fight, and win in air, space, and cyberspace. The Air Force has an opportunity – will it waste it?

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

1 Air Force Space Command. The United States Air Force Blueprint for Cyberspace, p.3.
2 High Frontier. Cyberspace - The Journal for Space & Missile Professionals, p.7.
3 Ibid., p.7.
4 Ibid., p.6.
5 Gen Shelton. "2013 AFCEA Cyberspace Symposium Remarks."
6 Ibid.
7 Fahrenkrug. "Cyberspace Defined." The Wright Stuff.
8 Gen Shelton. "2013 AFCEA Cyberspace Symposium Remarks."
9 High Frontier. Cyberspace – "The Journal for Space & Missile Professionals", p.6.
10 Ibid., p.6.
11 Hare and Zimmerman G. "The Air Force in Cyberspace: Five Myths of Cyberspace Superiority."
12 Gen Welsh. "Cyberspace – The Fifth Operational Domain", p.2-7.
13 Mr Fanning. "State of the Air Force". Air Force Association – Air and Space Technology Exposition.

[14] Gen Shelton. "Cyberspace," Air Force Association 2013 Air and Space Conference & Technology Exposition.
[15] Gen Welsh, CSAF. "A Vision for the United States Air Force."
[16] Air Force Space Command. "The United States Air Force Blueprint for Cyberspace," p4.
[17] Lt Gen Miller. "Core Function Lead Integrator Roles and Responsibilities, SECAF and CSAF Decision Brief."
[18] Gen Welsh. "Cyberspace – The Fifth Operational Domain", p.2-7.
[19] Fiscal Year 2014 Air Force Posture Statement, p. 16.
[20] McCullough. "At a Cyber Crossroads." Air Force Magazine: The Online Journal of the Air Force Association.
[21] Ibid.
[22] Ibid.
[23] Gen Welsh. "Air Force Update". Air Force Association 2013 Air and Space Conference & Technology Exposition.

## BIBLIOGRAPHY

Air Force (2013). *USAF Posture Statement 2013.* Retrieved from http://www.af.mil/Portals/1/documents/budget/2014-budget-posture-statement.pdf (accessed 19 November 2013).

Air Force, CSAF (2013). *Air Force Vision Statement.* Retrieved from https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC13560F0FB5E044080020E329A9/Files/editorial/AFD-130110-114.pdf (accessed 19 November 2013).

Air Force Doctrine Document 3-12 (2010). *Cyberspace Operations*. Retrieved from https://cyber.iovermont.org/pluginfile.php/3548/mod_resource/content/2/afdd3-12.pdf (accessed 19 November 2013).

Air Force Policy Directive 10-17 (2012). *Cyberspace Operations.* Retrieved from https://cyber.iovermont.org/mod/resource/view.php?id=1973 (accessed 19 November 2013).

Air Force Space Command (2009). *The United States Air Force Blueprint for Cyberspace.* Retrieved from https://cyber.iovermont.org/pluginfile.php/3527/mod_resource/content/2/USAF_Blueprint_for_Cyberspace_AFSPC_-_Nov_2009_.pdf (accessed 19 November 2013).

Air Staff, AF/ST (2012). *Cyber Vision 2025.* Retrieved from https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC1355090FB5E044080020E329A9/Files/editorial/00Cyber%20Vision%202025%20FINAL%203-21-13.pdf (accessed 19 November 2013).

Army (2010). *Cyberspace Operations Concept Capability Plan 2016-2028.* TRADOC Pamphlet 525-7-8.

Basla M. Lt Gen (2013). *Air Force Association 2013 Air and Space Conference &Technology Exposition – Cyber*. Retrieved from http://www.af.mil/Portals/1/documents/af%20events/af-130917-AFA-Cyber%20Panel.pdf (accessed 19 November 2013).

Chairman of the Joint Chiefs of Staff Instruction (2013). *Joint Community Warfighter Chief Information Officer.*

Department of Defence (2011). *Department of Defense Strategy for Operating in Cyberspace.* Retrieved from http://www.defense.gov/news/d20110714cyber.pdf (accessed 19 November 2013).

Department of Defense (2013). Memorandum of the Military Departments – *Defending Department of Defense Networks, Systems, and Data: Strategic Choices for 2020.* Document is CLASSIFIED SECRET.

Department of Defense (2012). *Sustaining U.S. Global Leadership: Priorities For 21St Century Defense.* Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed 19 November 2013).

DoD Directive 5144.1 (2005). *Assistance Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer.* Retrieved from http://dodcio.defense.gov/Portals/0/Documents/DoD%20Directives/514401p[1].pdf (accessed 19 November 2013).

Fanning E. (2013). State of the Air Force. *Air Force Association 2013 Air and Space Conference & Technology Exposition.* Retrieved from http://www.af.mil/Portals/1/documents/af%20events/af-130916-AFA-Fanning.pdf (accessed 19 November 2013).

Fahrenkrug, David, T. (2007). "Cyberspace Defined." *The Wright Stuff.* Retrieved from http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (accessed 19 November 2013).

Hare F. B. and Zimmerman G. (2009). *The Air Force in Cyberspace: Five Myths of Cyberspace Superiortiy.* Retrieved from https://cyber.iovermont.org/pluginfile.php/3529/mod_resource/content/2/Military_Perspectives_Cyberpower_2009.pdf (accessed 19 November 2013).

Headquarters Air Force (2012). MD 1-26. *Chief of Information Dominance and Chief Information Officer.* Retrieved from http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/hafmd1-26/hafmd1-26.pdf (accessed 19 November 2013).

High Frontier (Vol 5, Number 3). Cyberspace - *The Journal for Space & Missile Professionals.* Retrieved from http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf (accessed 19 November 2013).

Joint Publication (JP) 1-02 (2010). *Department of Defense Dictionary of Military and Associated Terms*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed 19 November 2013).

Joint Publication 3-12 (2013). *Cyberspace Operations.* Document is CLASSIFIED SECRET.

McCullough Amy (2012). At a Cyber Crossroads. *Air Force Magazine: The Online Journal of the Air Force Association.* Retrieved from http://www.airforcemag.com/MagazineArchive/Pages/2012/June%202012/0612crossroads.aspx (accessed 20 November 2013).

Miller G. Lt Gen (2012). Core Function Lead Integrator Roles and Responsibilities*, SECAF and CSAF Decision Brief.*

Navy (2011). DON Memorandum - *Information Management/Information Technology/Cyberspace Campaign Plan for Fiscal Years 2011-2013.*

Sheldon, John (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly* (pp. 95-112).

Shelton W. Gen (2013). Cyberspace. *Air Force Association 2013 Air and Space Conference & Technology Exposition.* Retrieved from http://www.af.mil/News/ArticleDisplay/tabid/223/Article/467153/shelton-talks-space-cyberspace-at-afa-air-and-space-conference.aspx (accessed 19 November 2013).

Shelton, W, Gen (2013). *2013 AFCEA Cyberspace Symposium Remarks*. Retrieved from http://www.afspc.af.mil/library/speeches/speech.asp?id=728 (accessed 19 November 2013).

Siegl, Michael (2008). Military Culture and Transformation. *Joint Forces Quarterly, 49* (pp. 103-106).

Welsh M, A. Gen (2013). Air Force Update. *Air Force Association 2013 Air and Space Conference & Technology Exposition.* Retrieved from http://www.af.mil/Portals/1/documents/af%20events/af130917AFAWelshfinal.pdf (accessed 19 November 2013).

Welsh Larry, D. Gen (Ret.) (2011). Cyberspace – The Fifth Operational Domain. *IDA Research Notes (p. 2-7)*. Retrieved from http://cryptome.org/2013/09/ida-cyberspace.pdf (accessed 26 November 2013).

White House (2009). Information Technology Strategic Plan. Document is UNCLASSIFIED//FOUO.

Risk Management Framework for Cyberspace Operations
Maj Michael L. Ortego

**ABSTRACT**
Air Force Cyber Operations currently lacks a standard framework to measure and control risk to enable leadership to make calculated risk decisions. This paper takes a look at the Air Force's Risk Management Process and how this well documented process can be integrated into Air Force cyber operations with specific focus on the application of force. The five step process of identify the hazards, assess the hazards, develop controls and make decisions, implement controls, and supervise and evaluate will serve as a good start at defining a standardized process that can be applied to cyber operations. The cyber community often takes the position that cyber operations are different. There are many aspects to the man-made cyber domain that may be different to the physical domains of air, land, and space especially when it comes to cyber acquisition. However, the cyber community should work to integrate cyber operations into already established processes so senior leaders at the combatant command (COCOM) and component levels understand how to integrate cyber capabilities into future operations.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
1. As early as 2005, the United States Air Force began messaging that Cyberspace was a warfighting domain when the SECAF and CSAF added Cyberspace to the Air Force's mission statement (Wynne and Moseley 2005). The Air Force has been working to operationalize cyberspace for several years, but in 2009, the Commander, Air Force Space Command, as the lead MAJCOM for cyberspace, published the United States Blueprint for Cyberspace, which provided guidance and intent to shape Air Force actions to organize, train and equip cyber operations to build cyber capacity (AFSPC 2009). Although cyber has been referenced in several top level national strategy documents before, the 2010 Quadrennial Defense Review described cyberspace as just as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space (DoD, 2010). Within the 2011 DoD Cyber Strategy, Strategic Objective 1 was to treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential (DoD, 2011).

2. In order for supported commanders to embrace the use of cyber operation, the Air Force cyber community must understand how to articulate the associated risk to the supported commander. Unfortunately, Air Force cyber operations lack a standard process to manage risk from the tactical level through the strategic level of warfare. Senior leaders tend to be risk adverse when it comes to cyber so establishing a well codified risk process can provide levels of confidence to the decision maker that can accept the risk.

3. Risk is inherent in all military operations. Time can be a key factor of whether or not risk can be mitigated during deliberate planning or mission execution. During the planning process, significant time should be spent identifying risks associated with conducting the operation. This is the best time to mitigate risk. During the tactical execution of cyber operations, there may be little to no time to consider risk mitigation strategies. Operators will often rely on controls already identified during deliberate planning. If no process exists, the risk adverse culture will continue.
4. There are many hazards that must be considered when conducting cyber operations. Risks associated with friendly forces may include lack of clearly defined mission, lack of intelligence,

inadequate training, low state of readiness, etc (USAF 2013). Understanding your adversary is also very important with respect to determining risk. Does your adversary have sophisticated technical means to detect your cyber operation? Are there obstacles within the cyber terrain that may affect mission accomplishment such as access to target, link latency, etc.

5. The lack of a common understanding of the risks associated with conducting cyber operations may cause decision makers to not rely on cyber operations to meet operational objectives. If the cyber community cannot clearly articulate risk to the decision makers, why would a commander risk mission failure or maybe even escalation of hostilities? It is our responsibility to identify risks, predict the probability of occurrence, severity of the risk, and exposure of the hazard in order to clearly articulate to the decision maker what risk he is accepting.

**RECOMMENDATION**

1. The Air Force cyber community has made progress at operationalizing cyber operations within the past couple of years, but still has lots of work to do. Establishing a codified risk management framework will serve in a positive step in the right direction. The Air Force already has published guidance on managing risk (USAF 2013). The cyber community does not need to invent something new. In fact, cyber operations should adapt the Air Force's risk management process to work within cyber operations so the risk decisions are presented in a way that senior leaders and decision makers already understand. There are many ways that the man-made cyber domain is different than other warfighting domains, but I do not think risk is one of those ways.

2. The Air Force Risk Management process identifies two levels of risk, which are deliberate and real-time (USAF 2013). These risk levels are primarily differentiated by the amount of time available to manage risk. Deliberate risk happens during the planning process where there is time to go through the entire 5-step risk management process to identify and mitigate risk prior to execution of cyber operations. Real-time risk happens during execution of cyber operations. During mission execution, there may be insufficient time to identify risk and receive a decision from the person assuming the risk within an acceptable timeline. This why it is crucial to make deliberate decisions or pre-approved actions during the planning phase to enable cyber operators to respond rapidly. Figure 1 shows the relationship between deliberate and real-time risk.


Figure 2 (USAF 2013)

3. Step 1 within the AF Risk Management process is Identify the Hazards (USAF 2013). AFPAM90-803 defines a hazard to be any real or potential condition that can cause mission degradation, injury, illness, death to personnel or damage to or loss of equipment or property. AFPAM90-803 highlights two different models that can be used to identify hazards, which are METT-TC Model and the 5-M Model.

a. The METT-TC Model is a United States Army risk model described in Army Doctrine Reference Publication (ADRP) 3-0 (USA 2012). The METT-TC Model has six categories for

identify risk associated with operational variables which include: mission, enemy, terrain and weather, troops and support available, time available and civil considerations (USA 2012). Understanding the mission is the first step in identifying hazards with the specific mission. Does the mission present significant risk? Do I have the intelligence that I need to plan the mission? Are there any priority intelligence requirements that need to be fulfilled to be successful? Do I need to conduct Cyber ISR or Cyber Operational Preparation of the Environment to gain more intelligence? Within the category of terrain and whether, some variables to consider are fields of fire (visibility of the adversary terrain), cover and concealment, obstacles, key terrain, avenues of approach, and weather (USA 2012). The Troops and Support category covers the support needed by friendly forces. This can be in terms of training, equipment condition and availability, health of personnel, etc. Many of these items are included within readiness reporting such as the Status of Resources and Training System or SORTS, and Defense Readiness Reporting System or DRRS.

b. Air Force Pamphlet 90-803 also covers an additional risk management model called the 5M Model, which focuses on the areas of man, media, machine, management, and mission (USAF 2013). The METT-TC and 5-M models share many similarities such as Mission, and Media/Environment, but the 5-M Model places more emphasis on friendly force considerations whereas the METT-TC places more emphasis on the mission and enemy/environment. As depicted in Figure 2, the mission is the central element of this risk model. Within the "Man" risk area, some potential hazards to consider are training (currency and proficiency), stress, inadequate rest, task saturation, poor morale or environmental conditions. This risk area could also be used to analyze the enemy forces, but is primarily focused on friendly forces within the pamphlet. The risk area "Media" shares many of the same considerations as Terrain and Weather within the METT-TC Model explained above. Within the Machine risk area, potential hazards or risk considerations are weapon system limitations, maintenance and logistics. Lastly, the Management risk area covers many forms of operational guidance such as regulations, instructions, rules of engagement, checklists, technical orders, etc.

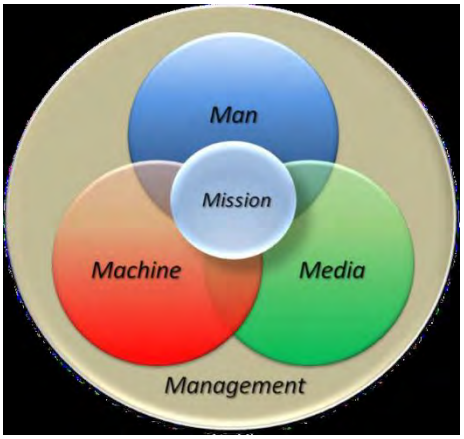


**Figure 3 (USAF 2013)**

c. Additional concepts to consider that are not covered in the Air Force's Risk Management Process are Intelligence Gain/Loss, Operations Gain/Loss, Technical Gain/Loss, and OPSEC. The intelligence, operations, and technical gain/loss concepts are balances between risk and reward within each respective area. Figure 3 depicts the overlapping relationship between these risk considerations. Leveraging cyberspace operations to accomplish a military objective may mean the potential loss of future intelligence so this requires coordination across the combatant commands and the intelligence community so the decision maker fully understands the risk versus reward. Technical gain/loss is a new term, used in place of "Network Gain/Loss" depicted in Figure 3, that has been used within cyber operations for the last couple of years, which compares and contrasts the potential technical gain of conducting an operation in terms of capability and access to a target as opposed to the potential exposure of capability or tools and loss of access. According to Gen Larry Welch, USAF Retired, operational commanders must fully understand

the full set of gain/loss risks and be the primary influence on gain/loss decisions (Welch 2011). OPSEC is another important factor in identifying risk. According to Joint Publication 3-13, OPSEC is a standardized process designed to meet operational needs by mitigating risks associated with specific vulnerabilities in order to deny adversaries critical information and observable indicators (CJCS 2012).

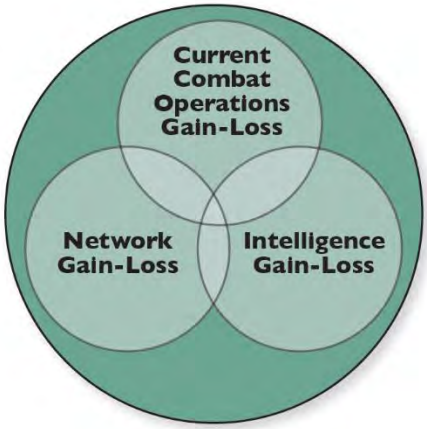



**Figure 4 (Welch 2011)**

d. The output of the hazard identification step should be a list of potential hazards along with the cause of each of these hazards.

4. The second step in the Air Force Risk Management process is Assess Hazards (USAF 2013). The Air Force defines hazard assessment as the process which associates hazards with risks (USAF 2013). The hazard assessment should identify the probability of occurrence, severity of risk, and exposure to the hazard (USAF 2013). Figure 4 provides a tool for assessing risk in terms of probability and severity to define the overall risk assessment. Risk assessment can be very subjective so guidance may be needed for consistent application of the risk assessment process. At the conclusion of step 2, the output should be a prioritized list of assessed hazards based on the most severe risk.

**Figure 5 (USAF 2013)**

5. Step 3 of the Air Force Risk Management Process is Develop Risk Control and Make Decisions (USAF 2013). Within this step, there are several sub-steps identified which are: identifying control measures available, determining the effects of each control, prioritizing the best controls and strategies, select the risk control measures, and deciding whether or not to accept risk (USAF 2013). The AF's process also identifies five types of controls (engineering, physical, administrative, educational, and operational (USAF 2013). In the subsequent paragraphs, I will discuss specific examples of risk controls associated these five categories.

a. Engineering controls use engineering controls to reduce risk by design, or material solutions. This type of control may relate to the mission or enemy within the METT-TC risk identification model as the mission may require the development of a new capability or modification to an existing capability. Engineering controls also relates directly to the machine risk identification category within the 5-M model.

b. Physical controls may come in the form of barriers or guards preventing access to a hazard (USAF 2013). Physical controls are less relevant within cyberspace operations because most cyberspace operations primarily exist within a virtual environment. Some physical controls that

can be considered are access to weapons or cyber tools until authorization has been given for their employment. Other physical controls maybe access controls that only allow access to the specific target environment or cyber terrain. This would prevent or mitigate creating unintended effects.

c. Administrative controls reduce risk through specific administrative actions (USAF 2013). Administrative controls may come in the form of guidance such as policies, operating instructions, standard operating procedures, rules of engagement, checklists, tactics, techniques and procedures. Administrative controls may be the easiest to implement, but they need to be integrated into the other types of controls to ensure success such as educational controls.

d. Educational controls are knowledge, skills, and abilities of the cyber personnel. Educational controls can be integrated into initial skills training, formal training units, initial qualification training, mission qualification training, continuation training, certification and evaluations, and joint and service exercises to continue to improve personnel readiness to conduct cyberspace operations.

e. Operational controls are defined as operational actions such as pace of operations, battlefield controls, rules of engagement, airspace control measures, map exercises, and rehearsals (USAF 2013). Establishing the operational procedures and rigor are critical to mitigating risks associated with cyberspace operations. Establish formal processes for command and control between higher headquarters and all subordinate units. These processes and procedures are critical to conducting successful operations such as tasking orders, special instructions (SPINS), rules of engagement, common terminology, communication systems, and brevity codes to ensure consistent and repeatable operations. Conducting exercises, mission rehearsals, and operational tests can help to increase readiness of personnel, identify risks, and identify if implemented controls are effective. Establishing tactics, techniques and procedures for cyberspace operations gives operators authoritative guidance while allowing them to deviate if necessary to ensure mission success. If deviations are required to meet mission objectives, conducting a debrief is helpful to discuss and document the reason for deviation. These debriefs can drive lessons learned and changes to TTP. The cyber weapons officer community is still in its infancy, but is actively working to normalize tactics development across the operational cyber community.

f. Each of the identified controls must be analyzed to determine whether the control method has mitigated the risk to an acceptable level. The decision authority must then choose whether or not to accept the risk and move forward to implementation of the approved control method. The decision authority may be several echelons above so it is important to involve your leadership and/or command and control elements in the risk management process to determine who is the approval authority for the various degrees and categories of risk. As stated earlier, the cyber operations community is still in its infancy and many leaders are risk adverse due to the lack of a well understood process.

6. Step 4 of the Air Force Risk Management process is Implement Controls (USAF 2013). Once risk control decisions have been made, an implementation plans must be developed. The Air Force's process highlights three actions that are required, which are "*Make Implementation Clear, Establish Accountability, and Provide Support."* This may be the most straight foward step, but the most important. If the risk control is not implemented the risk will not be mitigated. Here are

some common issues that cause risk controls to fail: control is inappropriate; operators dislike it; leaders dislike it; too costly; conflicting priorities; control is misunderstood (USAF 2013). The risk controls should complement the culture of the organization; otherwise it will likely not be embraced by those affected.

7. The final step in the Air Force Risk Management process is Supervise and Evaluate, which involves determining the effectiveness of risk controls throughout the operation (USAF 2013). This step should be a continual effort. We operate in a dynamic environment and must continue to evaluate our processes and procedures. Consider establishing a process such as an Operations Review Panel, which is an review and approval process to review all changes to operational procedures such as checklists, tactics, operating instructions, etc. This process serves to ensure that all stakeholders review procedural changes to ensure gaps and seams are not introduced.

**COUNTERARGUMENT**

Maybe the Air Force cyber community should not establish a risk management framework for cyber operations. USCYBERCOM has been driving the organize, train, and equip standards at the joint level through their Cyber Mission Force construct (Alexander 2014). The Air Force does not need to establish their own cyber operations risk management framework since USCYBERCOM will likely establish their own process to manage risk. The former Commander of USCYBERCOM, Gen Keith Alexander, requested that the Department of Defense promote USCYBERCOM to a Unified Command with acquisition authorities similar to United States Special Operations Command. One of my primary concerns with this construct is that USCYBERCOM will not take advantage of the unique capabilities that each of the serves can offer cyber operations especially concerning access such as air enabled access, sea enabled access, etc. If USCYBERCOM is the primary organization focused on cyber acquisition, the military services will likely prioritize funding for other areas.

**CONCLUSION**

Air Force Cyber Operations is still a very immature operational domain as compared to air operations. The cyber community tends to be very risk adverse likely because there are so many variables and unknowns when it comes to defining risk. Establishing an Air Force risk management approach for cyberspace operations that adapts the Air Force standard will serve as a step in the right direction. Enabling senior leaders to understand risks associated with cyber operations will give them better situational awareness of knowing whether or not a cyber capability will generate the desired effect instead of solely relying on a kinetic effect.

**BIBLIOGRAPHY**

AFSPC, Air Force Space Command. *The United States Air Force Blueprint for Cyberspace.* November 2, 2009.

Alexander, Keith B. (Former DIRNSA and CDR USCYBERCOM). "Statement of General Keith B. Alexander, Commander USCYBERCOM Before the Senate Committee on Armed Services." *United States Senate Committee on Armed Services.* February 27, 2014.

http://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf (accessed June 14, 2014).

CJCS, Chairman of the Joint Chiefs of Staff. *Joint Publication JP3-13, Information Operations.* November 27, 2012.

DoD, Department of Defense. *Quadrennial Defense Review Report.* February 2010.

DoD, Department of Defense. *Strategy for Operating in Cyberspace.* July 2011.

Pellerin, Cheryl, American Forces Press Service. "CYBERCOM Activates National Mission Force Headquarters." *United States Department of Defense.* September 25, 2013. http://www.defense.gov/news/newsarticle.aspx?id=120854 (accessed June 14, 2014).

USA, Department of the Army. *Army Doctrine Reference Publication (ADRP) 3-0, Unified Land Operations.* May 16, 2012.

USAF, Secretary of the Air Force. *Air Force Pamphlet (AFPAM) 90-803, Risk Management Guidelines and Tools.* www.e-publishing.af.mil, February 11, 2013.

Welch, Larry D., Gen USAF (Ret.). "Cyberspace-The Fifth Operational Domain." *IDA Research Notes* (IDA Research Notes), 2011: 6.

Wynne, Michael W (Former Secretary of the Air Force, and T. Michael (Former CSAF) Moseley. *Letter to Airmen, Air Force Releases New Mission Statement.* December 7, 2005.

# SECTION 4: POLICY AND DOCTRINE

Protecting the Nation in the Cyber Domain
COL Jonalan Brickey, US Army, Army Cyber Command

**ABSTRACT**
Cyberspace is a complex, fragile, and ever-changing ecosystem. America is growing more dependent on it with each passing day, connecting more than two billion people around the globe to conduct business, share information and ideas, and socialize. At the same time, cyber threats continue to increase in sophistication and volume, putting the nation at risk. Increased cyber security is vital to protecting America's national security interests, critical infrastructure, and intellectual property. Adversaries ranging from foreign state actors to corporate spies continue to exploit vulnerabilities in U.S. networks, systems, and practices. The risk of cyber insecurity is most troubling in the case of companies that operate critical infrastructure such as the electric grid, dams, and the servers that process financial transactions. These companies are clear targets since their operations affect public safety. While most companies accept at least a degree of responsibility for the protection of their own networks, it not clear that they are capable of providing themselves with robust security.[1] Currently, there is no Federal agency charged with protecting America's interests in cyberspace; nevertheless, the nation will likely turn to its military in times of crisis. Though the Department of Defense (DoD) has considerable capabilities for cyberspace operations (across DOTmLPF-P), including securing and defending the DOD information networks, defending the nation in cyberspace is a Herculean task. Considering current cyberspace capabilities, the DoD is not postured to (adequately) protect the nation up to and just before conflict due to shortfalls in policy (P), organization (O), and personnel (P). The purpose of this paper is to propose recommendations that address these shortfalls and, ultimately, reduce the risk to national security.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
1. The United States lacks appropriate policy for the Department of Defense (DoD) to protect the nation from cyber threats prior to conflict. In fact, no single agency is vested with comprehensive cyber security authorities and responsibilities in the United States. Instead, there is a division of labor based on the motive and presumed identity of the actor: cyber crimes (including terrorism) fall under the jurisdiction of the Department of Justice (DOJ) in Title 18 of the U.S. Code; cyber intelligence activities fall under several agencies within the intelligence community under Title 50; and acts of cyber war fall under the DoD in Title 10. Additionally, Presidential Policy Directive 21 (PPD-21) assigns responsibilities to no less than 10 agencies to achieve national unity of effort to" strengthen and maintain secure, functioning, and resilient critical infrastructure."[2] Due to the attribution challenge in cyber attacks, "it may be difficult or impossible to discern the actual source of a threat" until well after 'the boom,' making it tricky to determine jurisdiction *a priori* and "in time to affect operations."[3] While the Department of Homeland Security is responsible for securing unclassified federal civilian government networks, existing laws only give DHS the authority to "work with critical infrastructure owners and operators, combat cyber crime, build a national capacity to promote responsible cyber behavior," and cultivate future cyber professionals.[4] DHS has neither the authorities nor the capabilities to protect the nation's critical infrastructure (CI), especially the vast majority that is owned and operated by the private sector. Meanwhile, DoD has the tools—in terms of laws and authorities—it needs to defend its *own* networks; however, it has no standing authorities for operating outside its networks, beyond a fairly restrictive standing rules of engagement. Conventional wisdom and Murphy's Law dictate

that a cyber attack against CI will most likely strike between the seams of authorities and capabilities, where protection measures and other capabilities are the weakest.

2. Another cyber policy shortfall is DoD's lack of situation awareness (SA) of non-DoD CI and restrictions on information sharing. If the nation turns to the DoD for protection in cyberspace up to and just before conflict, the DoD must be able to 'see' cyber threats across the nation and share information with CI owners and operators to gain situation awareness. In recent Congressional testimony, General Alexander, Commander of U.S. Cyber Command and NSA Director, said it would be difficult to defend the financial sector because his organizations "cannot see attacks going against Wall Street today."[5] Even if US policy provided authorities for the DoD to operate in the nation's (non-DoD) networks, the DoD would need a priori access, knowledge, and monitoring capabilities to properly identify threats and conduct cyberspace operations to defeat them. The DoD has struggled for years to achieve situation awareness of its own networks, something department leadership hopes to achieve as it adopts the Joint Information Environment (JIE) in the near future.[6] The terrain of cyberspace is vast and nebulous; there are few—if any—experts who may have the expertise to navigate, troubleshoot, and defend the plethora of networks across the nation's CI landscape. Even the most skilled DoD cyber warriors would need extensive training on the networks, devices, and processes comprising the nation's CI.

3. The third DOTmLPF-P shortfall in cyberspace capabilities is a lack of skilled personnel—cyber warriors—and a career management field to manage this unique band of warriors. Protecting the nation as a whole in the cyber domain may take considerably more forces, possibly more than DoD can recruit and retain in the current market. Federal agencies are already witnessing attribution in the cyber workforce due to competition for skilled workers in the private sector.[7] The DoD has neither the quantity nor quality in the cyber workforce to scale beyond current mission requirements and, according to an Army conceptual paper, the demand for cyber warriors is likely to increase: U.S. Cyber Command will task Army Cyber Command "to provide an increasing number of offensive and defensive cyberspace forces and capabilities" as part of a joint operational construct.[8] As far back as 2008, the U.S. Comprehensive National Cybersecurity Initiative (CNCI) recognized that "there are not enough cybersecurity experts within the Federal Government."[9] Additionally, the military services do not have a good track record of managing cyber and related technical workforces, which may contribute to a more general trend in the military of losing top officer talent due to frustration with the promotion system.[10] The services tend to value and promote operational specialists— infantrymen, pilots, and surface warfare officers—while those in the more technical support career fields rarely achieve executive-level status.[11] If DoD cannot manage the cyber workforce effectively, it will lose current and future potential talent to the civilian sector and the resulting DoD force will consist of second-rate cyber security personnel at best.

**RECOMMENDATIONS**

1. (Policy: P and Organization: O) If an adversary strikes American CI, the nation cannot wait for authorities while its CI falls to cyber attacks— the United States simply cannot expect the private sector to protect and defend itself, especially against sophisticated and resourced nation states.[12] The current approach to protecting CI from cyber attacks consists of workarounds and coordination upon coordination, which is like putting Band-Aids® on top of Band-Aids®. Congress should pass legislation authorizing a hybrid cyber protection organization within the

DoD that has the full range of authorities—eg., Titles 10, 18, 50, and others as necessary—to conduct cyberspace operations in defense of the nation. Instead of forcing these authorities upon existing branches of the military, Congress should establish a separate military service to "provide [the] nation with the capability to defend our technological infrastructure" and to "serve as a strong deterrent for our Nation's enemies."[13] Retired Admiral James Stavridis advocates a new cyber service in DoD as a "drastic but timely innovation for America's military," though the forces he proposes would have limited authorities in domestic scenarios.[14]

2. (Policy: P) Addressing the policy issues related to situation awareness and information sharing does not require a new engineered materiel solution—technology exists today to do both. Instead, government and the CI owners and operators need policies and processes that provide relevant information, at the appropriate time, to the entities capable of action in cyberspace. All of this needs to be done without overwhelming users with irrelevant data. DoD and DHS already implement robust SA tools on government networks; EINSTEIN is an intrusion prevention and detection system deployed across the federal government and monitored by DHS.[15] The nation's CI owners and operators should implement an existing EINSTEIN-like capability as an industry standard and formulate policies and procedures to share threat information with DoD. New policies and procedures will require, at a minimum, a whole of government solution, but perhaps even a public debate on how much DoD presence is acceptable to the public in order to maintain the desired level of security. The private sector and the American public must have a voice in this matter. In the post-Snowden era, there must be transparency and open debate on risk management—nothing can be accomplished in this area without trust. NSA reports that it touches just 1.6% of the Internet; plans—initially announced pre-Snowden and scrapped since his revelations—to protect the nation against cyber attacks on CI would have required more invasive data collection, even if it only called for more 'metadata' instead of actual content.[16]

3. (Personnel: P) The third and final issue in this paper calls for aggressive personnel programs to improve the supply of cyber warriors in DoD and to effectively manage the cyber career workforce. The first step has to begin with increased emphasis on cyber education in grades K-12 and more robust programs at the university level. As noted in the Comprehensive National Cybersecurity Initiative (CNCI), this requires a "national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge."[17] Another strategy to attack the supply side of the problem is to apply a total force concept that relies on Reserve and National Guard cyber forces already working in the cyber domain in civilian jobs, oftentimes in the CI sector. Also, the DoD must structure employment incentives to compete with industry. One incentive the DoD should offer is an enlistment and retention pay bonus for cyber warriors, just as it does for pilots, doctors, and other high-demand specialties. Finally, the DoD should carefully manage the cyber workforce by developing a separate cyber service in the DoD. Several experts in the military offer compelling arguments for developing a new cyber service,[18] which should have specialized career managers for each of the seven categories of cyber specialty areas identified by the National Initiative for Cybersecurity Education.[19]

**COUNTERARGUMENT**

1. In order to properly posture itself prior to conflict, the Federal Government (including the DoD) will require access to the nation's critical infrastructure, including privately owned cyberspace capabilities. Without sophisticated, transparent security mechanisms in place, this will likely

encroach upon civil liberties or at least give the appearance of doing so. For good reasons, Americans oftentimes have a weak stomach for even apparently minimally invasive government—this is especially true in a post-Snowden era, which makes standing up a separate cyber service in the military a steep uphill battle.

2. The chilling climate presents a situation where defense leaders "will be constantly challenged with navigating this legal and policy morass and petitioning policy makers for updated laws."[20] The DoD has been working with Congress for years trying to influence the passage of cyber security legislation encouraging or mandating information-sharing with the private sector; however, the fundamental concepts are controversial. Thus, the only notable action at the Federal level has been Executive Order 13636—the President's attempt to might a solution through voluntary measures. The Federal Government has a poor track record of regulating industry in general and even itself. There is a strong case to be made that federal regulations of industry are not going to help. It is more likely that industry will step up their game when cyber security affects the bottom line.

3. Major organizational changes in the Federal Government only take place every so often as a reaction to significant, catastrophic events. For example, the Goldwater-Nichols Act of 1986 established joint military commands in DoD as a reaction to the disastrous Iranian hostage rescue attempt.[21] The attacks of September 11, 2001 were the impetus for DHS and U.S. Northern Command. Unfortunately, it may take a cyber attack with effects on par with those from the attacks on 9-11 or a natural disaster like Hurricane Katrina to force major organizational change. Absent such an event, it is unlikely that existing military services will support any move to establish a separate cyber service.

## CONCLUSION

The risk of cyber insecurity is especially high and alarming in the case of companies that operate critical infrastructure such as the electric grid, dams, and the servers that process financial transactions. Though the U.S. DoD has considerable security and defensive cyberspace capabilities across DOTmLPF-P to protect its own networks, it is not properly postured to protect the rest of the nation up to and just before conflict. Therefore, the Federal Government must take decisive action to provide capabilities to the DoD to develop better cyber defenses and responses in coordination with the private sector and key elements of American society. The capability gap that currently exists is not due to technological shortfalls; rather, it results from limitations in current policies concerning authorizations, organizations, and personnel. Establishing a separate military service for cyber seems like a prudent course of action aimed at defending the nation's critical infrastructure. Of course, merely creating a new DoD organization for cyber means little without also granting new hybrid authorities to address the full spectrum of cyber threats. The recommendations provided in this paper offer realistic, objective steps toward devising a strategy to protect the nation in the cyber domain, without forfeiting civil liberties in the process.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] O'Gorman and McDonald, "The Elderwood Project."
[2] Presidential Policy Directive 21.
[3] O'Neil, "Cyberspace and Infrastructure," p. 133.
[4] DHS Congressional Testimony, "Threats to the Homeland," p. 2.
[5] General Alexander, Armed Services Committee Statement.
[6] Institute of Land Warfare, "Modernizing LandWarNet," p. 7.
[7] Ballenstedt, "Federal Agencies Start to Lose Competitive Edge."
[8] Army Cyber Command, "The U.S. Army LandCyber White Paper," p. 33.
[9] President Obama, CNCI.
[10] Kane, "Why Our Best Officers Are Leaving."
[11] Conti and Surdu, "Is it Time for a Cyberware Branch of Military?"
[12] Cilluffo, "The U.S. Response to Cybersecurity Threats."
[13] Conti and Surdu, p. 16.
[14] Stavridis and Weinstein, "Time for a U.S. Cyber Force," p. 3.
[15] DHS Congressional Testimony.
[16] Sanger, "NSA Leaks."
[17] President Bush, CNCI.
[18] Conti and Surdu
[19] NIST, "Cybersecurity Framework."
[20] Miller, et al., "Why Your Intuition About Cyber May Be Wrong," p. 3.
[21] Goldwater-Nichols Act of 1986.

## BIBLIOGRAPHY

Alexander, Keith (2013). Senate Committee on Armed Services Statement. Retrieved from http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf (accessed 7 February 2014).

Ballenstedt, Brittany (2013). "Federal Agencies Start to Lose Competitive Edge for Cyber Workers." NextGov.com. Retrieved from http://www.nextgov.com/cio-briefing/wired-workplace/2013/05/federal-agencies-losing-competitive-edge-cyber-workers/63004/ (accessed January 23, 2014).

Beers, Rand (2013). Senate Testimony of DHS Acting Secretary, "Threats to the Homeland." Retrieved from http://www.hsgac.senate.gov/hearings/threats-to-the-homeland (accessed 6 February 2014).

Conti, Greg and Surdu, John (2009). "Army, Navy, Air Force and Cyber—Is it Time for a Cyberware Branch of Military," IA Newsletter, 12:1. Retrieved from http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf (accessed 22 January 2014).

Cilluffo, Frank (2012). "The U.S. Response to Cybersecurity Threats," Defense Dossier, Issue 4. Washington, D.C.: American Foreign Policy Council. Retrieved from www.afpc.org/files/august2012.pdf (accessed 21 January 2014).

Institute of Land Warfare (2012). "Modernizing LandWarNet: Empowering America's Army," *Torchbearer National Security Report*. Arlington, VA: Institute of Land Warfare, AUSA.

Kane, Tim (2011). "Why Our Best Officers Are Leaving." The Atlantic. Retrieved from http://www.theatlantic.com/magazine/print/2011/01/why-our-best-officer (accessed 9 February 2014).

Miller, Matthew, Brickey, Jon and Conti,Gregory (2012). "Why Your Intuition About Cyber Warfare is Probably Wrong," *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong (accessed January 20, 2014).

O'Gorman, Gavin and McDonald, Geoff (2012). "The Elderwood Project." Mountain View, CA: Symantec. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf. (accessed 11 September 2012).

O'Neil, William D. (2009). "Cyberspace and Infrastructure." Kramer, Franklin, Starr, Stuart, & Wentz, Larry (Eds.), *Cyberpower and National Security*. Washington, D.C.: National Defense University.

Sanger, David (2013). "NSA Leaks Make Plan for Cyberdefense Unlikely," New York Times. Retrieved from http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyber (accessed 5 February 2014).

Stavridis, James and Weinstein, David (2014). "Time for a U.S. Cyber Force." Proceedings Magazine, U.S. Naval Institute: http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force (accessed 23 January 2014).

United States Army Cyber Command (2013). "The U.S. Army LandCyber White Paper 2018-2030." Fort George G. Meade, MD: U.S. Army.

United States Congress (1986). Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433. Retrieved from https://www.govtrack.us/congress/bills/99/hr3622 (accessed 9 February 2014).

White House (2012). Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience." Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed 7 February 2014).

White House (2009). "Comprehensive National Cybersecurity Initiative (CNCI)." Retrieved from http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (accessed 7 February 2014).

Making the Cyber Environment Defensible and Resilient: the Big Three: Sequestration, Strong CIO, Executive Order 13636

Major Kevin Childs, US Air Force

**ABSTRACT**

Today, Americans know cyber capabilities have transformed daily life unlike anything the Nation has seen since Thomas Edison invented the incandescent light bulb. President Obama realized the importance of this new domain and declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."[1] On 12 Feb 2013, the President issued Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity". Part of that EO was for the National Institute of Standards and Technology (NIST) to create a cybersecurity Framework to assist organizations in addressing a variety of cybersecurity challenges. In FY13, the federal government's Budget Control Act of 2011 (i.e., Sequestration) kicked in with an overall mandate to eliminate $1.1 Trillion in defense and non-defense spending cuts through 2021. During a 2013 CORONA, USAF leadership aligned the AF Chief Information Officer (CIO) position with DoD CIO mandates and created a stronger position to "provide strategic vision for Information Technology investments, including funding, acquisition & requirements, as well as strategic direction for the cyber domain"[2]. The reality is the USAF has two tools to navigate through a constrained fiscal environment to improve cybersecurity: NIST framework and a strong CIO.

**PROBLEM STATEMENT**

1. The Air Force does not have a consistent and repeatable framework to identify, assess, and manage cyber security risks. In today's fast paced environment, there are too many security flaws, too many nefarious actors, too many things that compete for time, not enough cyber operators, and a $500 Billion reduction in the DoD's budget over the next 8 years due to Sequestration. Adding those challenges into consideration, Air Force leaders must have a strong, centralized process in place to ensure material and non-material resources are committed at a specific place and the right time to ensure the AF Information Network (AFIN) is properly defended and resilient.

2. The current cybersecurity risk model is not ideal. When new Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or orders from USCYBERCOM are released, each Service produces additional orders to instruct network operators to patch software flaws, add new capabilities, reshape the cyber domain, etc. These orders are called Time Compliance Network Orders, Time Compliance Technical Orders, Maintenance Task Orders, or Cyber Control Orders. The system that pulls all the orders together for 24 AF oversight is called AFNetOps Compliance Tracker, or ACT. Unfortunately, organizations across the spectrum – tactical, operational, and strategic, utilize ACT to provide a snapshot of the security posture of the AFIN. Some Communication Squadron Commanders don't utilize ACT and this is a problem. They don't have regularly scheduled meeting to review the orders and inquire where they stand on compliance. Instead, they rely on the 83/561 Network Operations Squadrons (NOS) and the 299th Network Operations Support Squadron (Guard NOS) to complete all actions when many orders require their participation. If this overreliance on the NOS takes place, ACT does NOT get updated properly and the 624 Operations Center does not

have an accurate security risk assessment. Instead of utilizing a tool, we must use a process to assess cybersecurity risk.

3. True risk management will drive cyber security expenditures. Currently, the Air Force does not have a consistent, repeatable model to *tactically* assess weapon system material gaps for the Air Force Corporate Structure (AFCS) Program Objective Memorandum (POM) inputs to the Future Years Defense Programs (FYDP). Lt Gen Basla, AF CIO, said at an Armed Forces Communications Electronics Association Air Force Information Technology (IT) Day, "As I look at how we provision IT capabilities in the past, it became obvious to me that only about half of our IT investments were done under the purview of the CIO. That status quo is not an option anymore." At the tactical level, it's very obvious that programs of record are not synched with mission priorities and operational constraints. Even in a normal budget/continuing resolution year, non-synchronization was a huge negative factor in program planning. Sequestration will dramatically reshape how capabilities and modernization is delivered to the USAF and make the acquisition calculus much more difficult. With limited funds available, Cyber will rigorously compete with Air and Space programs. Cyber operators, planners, and staff officers must be able to articulate the need for new programs and cybersecurity/modernization capability gaps in current programs. Sequestration will force more synchronization down to the tactical edge like never before. Risk must be articulated clearly, prioritized, and aligned to DoD IT modernization priorities and Combatant Commanders Operational Plans.
4. As the great Chinese military leader Sun Tzu stated in *The Art of War*, know yourself and you will win all battles. As the AF NIPRNet and SIPRNet Computer Defense Service Provider, AFCYBER has not incorporated a total *holistic* approach to grade itself in order to continuously increase cybersecurity and assess risk accurately. For example, as the AF migrated from a NCC/MAJCOM to a NOS/NAF centric structure, the security model naturally focused its weight and effort on units within the 67 and 688 Cyber Wings. Planners routinely identified gaps in the AFSPC six approved cyber weapon systems[3] but not down to the base level below the Internal Router.

Due to confusion in the NOS/NAF security model, some local communications squadron commanders totally defer to the 83/299/561 to operate, maintain, and defend their networks through the Cyber Security & Control System (CSCS) weapon system. However, commanders must reverse this misnomer and consistently evaluate their own security posture. The NOSs do not manage local base infrastructure or Program Management Office (PMO) networks. Therefore, a blind spot does exist in the current model. Are local communication squadrons grading their own cybersecurity below the NOS demarcation point? Some are and some are not. NOSs are organizing Scan, Patch, Host Base Security System results so commanders can know themselves better and identify plans and requirements to increase cybersecurity and drive down risk. DISA/USCYBERCOM realize the internal base networks, DMZ networks, and PMO systems are the soft under belly of Service networks and implemented a new Command Cyber Readiness Inspection (CCRI) to evaluate those networks and hold the local communications squadron commander accountable for those vulnerabilities and the cybersecurity of their base[4]. A consistent framework that is common across all MAJCOMs is needed to evaluate cybersecurity risk.

During previous POM submissions, the commander that articulated the best justification was successful; however, the organization that needed the most help and wasn't clear in their

submission continued to struggle. In cyber, the weakest link will impact the entire network. The AF needs to identify the entire cyber community security needs (local squadrons, weapon systems, PMOs, Active, Guard, Reserve, etc.) and ensure risk management is properly applied across the entire force. It's vital to bring the PMOs into a holistic cybersecurity risk model.

**RECOMMENDATIONS**

1. As the AF Strong CIO mandate moves forward and an implementation plan is approved, Lt Gen Basla should immediately implement a team to oversee a capabilities/budget review using framework created by President Obama's Executive Order 13636 "Improving Critical Infrastructure Cybersecurity". The NIST preliminary cybersecurity framework created three tools that can help identify, assess, and manage cyber security risks in a repeatable and consistent manner. Led by the AF CIO office, this team can utilize the framework tools to influence prioritization efforts across all cyber portfolios leading up to the POM submissions.

> "With an understanding of risk tolerance, organizations can prioritize systems that require attention. This will enable organizations to optimize cybersecurity expenditures. Furthermore, the implementation of risk management programs offers organizations the ability to quantify and communicate changes to organizational cybersecurity. Risk is also a common language that can be communicated to internal and external stakeholders."[5]

2. The first recommended tool is called the *NIST Framework Core*. As mentioned in a former problem statement, a quasi-risk management tool called ACT is only a compliance tracker and does not provide overview for Senior Leadership to manage risk. Fortunately, the Framework Core does just that. It creates a GO/SES high-level, strategic view across five functions that are common throughout industry. These functions are the basic cybersecurity activities organized at the highest levels. They are (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. To illustrate the NIST Framework Core, this paper will focus on the Detect function.
Detect is broken down into 3 categories: (1) Anomalies and Events, (2) Security Continuous Monitoring, and (3) Detection Processes. Detection Processes is divided into 5 subcategories. Each subcategory links to industry standards for more details. The five subcategories are as follows:

a. Roles and responsibilities for detection are well defined to ensure accountability
b. Detection activities comply with all applicable requirements, including those related to privacy and civil liberties
c. Detection processes are exercised to ensure readiness
d. Event detection information is communicated to appropriate parties
e. Detection processes are continuously improved

With the implementation of the NIST Framework Core, 24 AF can baseline the AFIN holistically and identify areas of risk for Senior Leader discussion, a task that has not yet occurred. Synchronization efforts with other Services using this framework could lead to a better cybersecurity posture and increased resilient networks.

3. The second tool is called the *NIST Framework Profile*. As mentioned previously, the AF does not have a consistent, repeatable model to *tactically* identify material gaps for the FYDP. This

tool enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organization goals and reflects risk management priorities. "Front-line" organizations can identify DOTMLPF model capability gaps by comparing "Current" profile with "Target" profile (i.e., industry standards). Gaps with material solutions can become prioritized requirements for POM inputs to the FYDP, but gaps with non-material solutions can be prioritized, managed, and implemented by 24 AF.

Again, for illustration purposes, the Detect function will be dissected using the DOTMLPF[6] model to see if the subcategory "Detection Processes" has any gaps. The NIST Detection Processes definition is "Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events."
Detect -> Detection Processes -> Question: Are there any capability gaps associated with the USAF's ability to detect anomalous events through processes and procedures?

Doctrine: Do I have TTPs, local job guides, AFIs, etc. that provides for timely/adequate awareness?
Organization: Do I have enough units and tools placed in the right location that allows for the correct detection of anomalous events? Is the DOC statement accurate?
Training: Are cyber operators trained before arriving to organizations? Are they receiving world class training? Is the training adequate? How do we compare to other units during exercises, site visits, etc?
Material: Are the tools easy to learn, operate, and maintain? What's the mean-time between failures? Can I virtualize the tools? What data center will house the tools? Can I remotely manage them? Are there procedures in place to troubleshoot tools?
Leadership & Education: Does Senior leadership understand the process and procedures we use to detect anomalous events? If not, what's the plan to teach them?
Personnel: Do we have enough people to maintain awareness? Can we do it with less?
Facilities: Is the data center prepared to accept new servers with future upgrades? Does it have redundant power, UPS, generators, proper HVAC? Is it is an area prone to natural disasters?

If there is a gap in the DOTMLPF model than that information is added to a Target profile. As mentioned earlier, if the gap requires a material solution, then it may become a capabilities requirement. If it requires a non-material solution, it should be passed to 24 AF and, based on risk management, prioritized and tracked.

4. The third tool that can make the cyber environment more defensible and resilient is called *NIST Framework Implementation*. This tool describes how cybersecurity risk is managed by labeling an organization to a specific Tier; from the least mature to the most mature. Tier 1, or Partial, means an organization's risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner, does not have processes in place to coordinate internally or with other organizations. Tier 2, or Risk-Informed, means the organization has an internal risk management process but does not adapt to changing threats, it understands its role in the larger cyber ecosystem but is unable to share information with external agencies. Tier 3, or Risk-Informed and Repeatable, means an organization's risk management processes are formally approved and expressed as policy, there is a large awareness of risk management practices in place

and can respond to change in risk, and changes internal risk management based on external collaborations. Tier 4, or Adaptive, means an organization adapts to cybersecurity based on lessons learned and predictive behaviors, continuously improves by observing a changing cyber landscape, risk management is part of the culture and continues to evolve, and actively shares info with partners to improve cybersecurity before an event occurs.
In an effort to quickly label all cyber organizations in the AF, 24 AF/A3O could immediately build an equivalency model to synchronize the most recent CCRI results with the *Framework Implementation Tiers*. Those organizations that scored double EXCELLENT or OUTSTANDING or a combined EXCELLENT / OUTSTANDING would be Tier 3, or Risk-Informed and Repeatable. Those organizations that fell outside the EXCELLENT range on either NIPR or SIPR would be a Tier 2 or Risk-Informed. Additionally, each organization within 24 AF could conduct complete NIST framework reviews to identify where they fall in the Implementation Tiers model.

All three tools, the NIST Framework Core, Framework Profile, and Framework Implementation Tier provide a repeatable process to identify a prioritized, fiscal path that can create a more defensible and resilient AFIN. This path includes collaborating with operational and financial/programmatic organizations. Currently, the AF does not have a holistic approach that ties tactical organizations directly into the FYDP but the NIST model encourages that interaction. The adjacent illustration provides a NIST cycle that links the Senior Executive Level (Joint IT Governance Board that can include the DoD CIO, USCYBERCOM, Air Staff and AFSPC) with the Business Process Level (24 AF) and the Operation Level (Cyber Wings.)


**COUNTERARGUMENTS**

1. The NIST Preliminary Framework is just that – preliminary. It could change. HHQ (USCYBERCOM, DISA, and AF CIO) may decide to implement another solution to id, assess, and manage cybersecurity risks. A process itself does NOT make the cyber environment defensible and resilient and this framework could fail if there is no collaboration at the tactical, operational, and strategic levels. Even though the DOTMLPF is a DoD requirement policy, the AF does NOT routinely use this process.

2. Additionally, if the AF CIO does not appoint an Air Staff Division to champion this process, it can easily fissile out after a short time. Many Action Officers reinvent the wheel because they are uninformed. Over time, this process could become another plan that collects dust on a shelf somewhere. However, assigning an Air Staff Action Officer and tasking AFSPC to conduct NIST framework reviews will mitigate this counterargument.

3. Finally, the NIST Framework Implementation Tiers could be viewed as a negative annotation and not a way to prioritize risks. Local Communications Squadron Commanders may argue their way to a Tier 3 ranking and thereby miss an opportunity to achieve more cybersecurity capabilities through the POM process.

## CONCLUSIONS

By adopting the common NIST preliminary framework, all organizations (Air Staff, AFSPC, AFLCMC, AFNIC, 24 AF, 624 OC, 67 CW, etc.) could operate from the same risk management view and the Air Force Corporate Structure (AFCS) would have a prioritized, tactically coordinated, and integrated budget proposal designed to make the cyber environment defensible and resilient. Today's AFCS Panel Chairs do NOT get a holistic view from the war fighter, but a myopic, segmented view from MAJCOM Action Officers, Program Mgmt Offices, etc. and this leads to security gaps and increased cybersecurity risks. With Sequestration the law of the land, the AF CIO must do better to synch all organizations to create more capabilities with less money. If these recommendations are put in place and working well, then tactical organizations should see prioritized cyber security capability gaps filled or at least have a plan to increase security and resiliency.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.)

[1] Executive Order 13636
[2] Lt Gen Basla speech to AFCEA. Nicole Black Johnson article.
[3] USAF Designates 6 Cyber Weapon Systems. Skinner article.
[4] Email discussion with 24 AF/A3O
[5] NIST framework
[6] DOTMLPF framework. DAU Manual for the Operation of JCIDS.

## BIBLIOGRAPHY

Budget Control Act of 2011. Pub. L. 112-25. 125 Stat. 240-267. 2 Aug. 2011.

Congressional Budget Office. Long-Term Implications of the 2013 Future Years Defense Program. 11 July 2012. https://www.cbo.gov/publication/43428

Defense Acquisition University. *Manual for the Operation of the Joint Capabilities Integration and Development System*. 19 Jan 2012.

Defense Information System Agency. *Compliance Inspections*. N.p., n.d. Web. 15 Dec. 2013.
Exec. Order No. 13636, 3 C.F.R. 217 (2014).

Johnson, Nicole Blake. "Air Force giving CIO more oversight over IT Spending." 13 Dec. 2013. http://c4isrnet.com/article/M5/20131211/C4ISRNET14/312110029/

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0. 12 Feb 2014.

Skinner, Robert J. "The Importance of Designating Cyberspace Weapon Systems". Air and Space Power Journal. Sep-Oct 2013.

Tao, Hanzhang. *Sun Tzu, The Art of War*. Ware: Wordsworth Reference, 1993.

Prioritizing Cyber Capabilities: to Protect U.S. Critical Infrastructure
Mr. Zachary Nunn

**ABSTRACT**
The safety of the United States depends upon a reliable and functioning network of national, international and local critical infrastructures and key resources (CI/KR). America, more than any other nation, runs on a host of private and public networks that ensure 84% of our clean water, maintain energy from 6,413 power plants, operate air travel for 19,450 airfields, secure trillions of dollars in daily banking and financing, as well as sustain a dozen other core sectors as identified by the US Government in Presidential Policy Directive-21 (Department of Homeland Security, Feb 2013). The greatest threat to America's critical infrastructure is the inherent vulnerability of these sectors to network exploitation through cyberspace.

Cyber-borne threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy, communications, public safety, and health at risk. To best prioritize America's resources to address these risks, we must implement a national strategy to action the President's directives in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (White House, 12 Feb 2013). In the E.O., the White House established "…the Policy of the United States to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (Executive Office of the President, 12 Feb 2013).

Successful realization of this policy requires a tailored strategy to prioritize and protecting the most important components of the country's CI/KR. It must capitalize on the symbiotic strength and investment in both the public and private sectors. It must be maintained as a shared responsibility between government and industry. And it must assure standards to quickly identify, tier, and manage solutions for cybersecurity risks.

Foundational to this strategy is implementation of a cyber risk management program to:
1. Identify the nation's critical assets.
2. Identify their vulnerabilities.
3. Prioritize them based on risk.

**THE NEED**
In the on-going Crimea conflict, Russian and Ukrainian ground forces are keeping their conventional weapons holstered for now, but it is an escalating shooting war in cyberspace. Ukrainian government communications infrastructure was a primary target of 42 separate cyber effects during the Crimea referendum on 16 March. The powerful cyber distributed denial-of service (DDoS) attacks were launched against Ukraine from Russian-based control nodes (Arbor Networks Inc., 14 Mar 2014). These DDoS strikes are notable for being thirty-two times more intense than the largest known denial-of-service attack during Russia's invasion of Georgia in 2008. The following day Russian websites were targeted by an even more muscular counterstrike (Clayon, 18 Mar 2014).

This latest conflict showcases a world entering a dangerously unstable and suspicious era, all the more troubling because cyber conflicts can rage with no physical-world aspect apparent – until a power grid blacks out a populace or cell phone towers go off-line. Yet only the United States has – accurately – ranked cyber incidents as its top national security issue for 2014, ahead of terrorism and weapons of mass destruction. (Clapper, 7 Mar 2013, p. 2)

As alarms go off in Ukraine and all over the world, the cybersecurity situation demands leadership that can only come from the US. Both Presidents Bush and Obama identified policy mandates for securing America's cyberspace – particularly in the arena of safeguarding the nation's critical infrastructure.

Now the next step must be taken of implementing a public-private cybersecurity strategy at the national-level to prioritize the integrity and security of the vast networks, systems, and information enabled enterprises, that keep the United States operating.

**THE CHALLENGE**

The cost of ubiquitous cyber attacks and cyber probes in the United States and the rest of the world is a staggering and ever-growing challenge. Antivirus firm Symantec estimated the 2012 global price tag of direct financial loss and the cost of remediating attacks at "$338 billion, excluding the theft of intellectual property and damage from data breaches" (Symantec Corporation, Sep 2013). When theft of intellectual property is factored in, "the figure soars past $1 trillion," according to MacAfee's annual report, a concern echoed by the former head of the NSA, General Keith Alexander, as "the greatest transfer of wealth in history" (Rajagopalan, 1 Aug 2012).

Cyber threats to Critical Infrastructure and Key Resources then are a major national security challenge for both the public and private sectors of the United States. In an assessment by the Office of the Director of National Intelligence's counterintelligence team, it is estimated there are 250,000 probes and intrusions into US government networks an hour – the equivalent of 6 million a day. In this onslaught of cyber-enabled incursions into government agencies are sophisticated foreign adversaries, including an estimated 140 foreign spy organizations. The presence of foreign intelligence services in US networks, coupled with a soaring increase in the number of data breaches – 41,776 in 2010, a 650% increase since 2006 – indicates adversaries are not only committed to exploiting our public and private networks, but finding it a high yield target for their own national interests. In response, the US has offered little resistance from either the government, or private companies (National Counterintelligence Executive, 2012).

With clear evidence from both corporate shareholders as well as Executive branch agencies, the lack of a comprehensive strategy to defend the nation's critical infrastructure is of immediate concern. Three major challenges impede the implementation of the President's policy guidance in E.O. 13636, and PPD-21 as it applies to CI/KR:

1. a lack of awareness as to where physically and virtually America's infrastructure resides;
2. as a result an inability to proactively identify vulnerabilities in network architecture;
3. and ultimately a failure to correctly prioritize resources to secure CI/KR where it is most vulnerable.

Distinctly, CI/KR cannot be a government-only mandate, nor is the government solely positioned to safeguard the enterprise. Over 80% of America's critical infrastructure is owned and operated by the private sector (Lewis, Dec 2008). Add to this private sector majority, thousands of independent entities that own limited or even sub-enclave specialties that individually have a limited role in the operation of a major infrastructure system – but holistically are a core component in its security.

There are notable economic inhibitors for small and mid-sized companies to maintain the rigorous and constantly evolving security requirements to best secure the nation's patch work infrastructure. Take for example a local plumbing company's prohibitive operating costs to update expensive system patches in the control system of a municipal water plant. These exposures are known, and it was exactly this type of vulnerability exploited by China's electronic warfare Unit 61398, in an attempt to target the industrial control system for a US water plant (U.S.-China Economic and Security Review Commission, Nov 2013, p. 242).

This exploit is not singular. Cyber-enabled target acquisition by the Peoples‟ Liberation Army actively seeks to identify "critical U.S. infrastructure for potential disruption during a future conflict," reports the congressional U.S.-China Economic and Security Review Commission. A function of China's wartime computer network operations is to "disrupt and damage the networks of [an adversary's] infrastructure facilities, such as power systems, telecommunications systems, and…to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure" (U.S.-China Economic and Security Review Commission, Nov 2013, p. 243)

Despite known threats, there are strong disincentives for companies to fully report a cyber intrusion. Several US banking institutions simply accepted the financial costs of weeks of targeted DDoS attacks by Iranian actors versus reporting major on-line banking outages and risk consumer flight from tens of thousands of clients (Perlroth, 8 Jan 2013, p. B1). Those companies that are forced to public report, as witnessed by Target Corporation's security breach that hemorrhaged up to 40 million customers‟ credit card details, find themselves exposed to industry fines topping $1 billion (Webb, 30 Jan 2014, p. 1B).

Ultimately, this model of individual liability and lack of industry standards creates shared public-private vulnerability for the entire critical infrastructure network. A solution requires partnership across government and industry's cyber „areas of responsibility‟ to execute effective, coordinated, and prioritized security solutions

**THE RECOMMENDATION**

To best address the opportunities and challenges cyber presents to the operational resilience of the nation's critical infrastructure, the White House must lead a risk-based strategy for the public and private cybersecurity of the CI/KR. Policy guidance outlined in Homeland Security Presidential Directive-7, and reinforced by Presidential Policy Directive-21, gives clear mandate for a national strategy to execute objectives essential for our national security.

This recommendation operationalizes voluntary concepts developed by the National Institute of Standards and Technology's (NIST) "Cybersecurity Framework" as a process to identify the

nation's core critical assets. Beyond NIST‟s user-level identification and self-assessment, the US must effectively assess and quantify the vulnerabilities of America's CI/KR, and prioritize their diverse security needs based on overall risk to the nation.

First, an effective National Strategy for the Cybersecurity of Critical Infrastructure must recognize the constituencies collectively responsible for ensuring its safety:

- Suppliers: the broad set of partners that enable the means for cyber connectivity, including the Internet Service Providers (ISPs), software and hardware producers, telecommunications operators, etc.
- Users: ultimately the individual, but inclusive of small/large business and industry sectors, institutions, associations, as well as government entities from the federal to the local level and foreign partners.
- Government: first, in its role a regulator of the market and protector of the public interest, and second, as a massive consumer, heavily dependent on CI/KR to provide for the citizenry.

No single constituency can operate effectively without the voluntary cooperation and coordination of the suppliers, users, and government.

## I. IDENTIFY

To accurately identify the nation's critical infrastructure, constituencies must work to define common cybersecurity actions, outcomes, and references across CI/KR sectors. These actions enhance CI/KR cybersecurity by assembling standards, guidelines, practices and appropriate oversight to the most relevant constituencies in the supplier, user, or government area of responsibility.

Much good work has voluntarily been accomplished in this arena by NIST (National Institute of Standards & Technology, 12 Feb 2014). The next step is a carrying the framework to all constituencies with the prerequisite of identifying their role in the CI/KR enterprise.

## II. VULNERABILITY

As with all risk management, the best defense of CI/KR cannot be 100% security, 100% of the time, but effective assessment of where vulnerabilities most imperil the ability of the larger enterprise to function. Appropriately, the Defense Acquisitions University, models risk as:

$$\text{Composite Risk Index} = \text{Impact of Risk event} \times \text{Probability of Occurrence}$$

This requires stakeholders in each constituency to undertake fulsome self-evaluation. In order to achieve sector specific standards, users must be able to manage risk in a cost-effective way based on business needs without unnecessary regulation. Equally, government must ensure the operability of its core mission to serve the populace and execute those actions necessary to protect the nation's security and economic well-being. Through collaborative assessment (i.e. the likelihood of a cyber incident against critical infrastructure × the impact of vulnerabilities exploited) suppliers, users, and the government can better determine the risk tolerance for each sector's role in critical infrastructure. Now operational risk decisions can be made in a clearly expressed and legally compelled structure.

In a shared CI/KR risk management model, cyber exploitable vulnerabilities can be identified by multiple defenders and quickly reviewed by relevant sector constituencies to pool funding, resources, and capabilities, while ensuring „fair-play" and transparency in investment across CI/KR enterprise. Moreover, this will help to define requirements through sector profiles, risk tolerances, and alternative operability options.

III. PRIORITY

With a national cybersecurity strategy for critical infrastructure, constituencies will gain long-range planning to enable shared sector expertise, joint vulnerability assessments across constituencies, and a means to evaluate enterprise risk (symbiotic threat/impact to all) and critical risk (catastrophic threat/impact to a single sector). These foundational elements enable measureable validation for cyber risk management. Importantly, they prioritize overarching constituency resources and vulnerabilities to inform and align public-private partnership needs based on evolving cybersecurity operations, defenses, and threats.

This assessment of cyber risks tiers CI/KR defense on multiple levels, incentives stakeholders to pivot in support of unknown/emerging vulnerabilities of higher priority, and allocates assets to gravest dangers in a timely fashion. Early users and suppliers then, emerge as stakeholders in driving sector standards, applying „best practices" of risk management, and improve the security and resilience of networks throughout across CI/KR. Equally, the government enters into a relationship with all constituencies to help safeguard shared infrastructure, particularly where key resources overlap or require interoperability.

Thus, a risk-based strategy for cyber protection of critical infrastructure enables multiple constituencies across a diverse array of sectors to nominate assets, assess vulnerability, and establish clear prioritization to identify, defend, respond, and recovery from a cyber incident.

**THE COUNTERPOINTS**

The solution to critical infrastructure protection in cyberspace requires more than a strategy. Institutional challenges as witnessed in the failure of the 2012 Cybersecurity Act and pledge by the President to veto Congress" Cyber Intelligence Sharing and Protection Act, are leading causes for hesitation among public and private sector entities (Couts, 2 Aug 2012), (Smith, 25 April 2013). For industry users, the competitive market place presents clear challenges with the price of cybersecurity requirements cited as cost prohibitive to the CI/KR business models if not uniformly deployed across the sector. Industry users and network supplier at times argue cybersecurity is a law enforcement or national defense responsibility and should be protected by the Federal Government, or conversely demand operability free from regulation to best manage their network defense (Beauchesne, 12 Feb 2014).

Ultimately, however, the cyber domain overwhelming favors the attacker. To ensure cybersecurity for the nation's CI/KR, network defense is a joint responsibility. While financial challenges in the short-term favor those users who „opt out" of joint defense, long-term users, suppliers, and government entities will benefit from shaping an enterprise beneficial to their daily dependency on CI/KR. Institutional challenges in both government and certain sectors may prove systemic, but eventually a forcing mechanism, like a true cyber attack on a key resource, or a network failure

of a critical infrastructure will demand change. The only question is what price will Americans incur before elected leaders define a plan to safeguard them?

## CONCLUSION

Cybersecurity for America's Critical Infrastructure/Key Resources is in an embryonic stage; strategic questions are manifold, but the US and its private and public sectors partners are best equipped to answer them. America must lead in establishing a strategy – failure to do so invites a vacuum in the world's cyber standards, and gives rise to self-serving cyber-enabled tactics as seen in Russia, China and elsewhere. The course America chooses in defining cyber strategy will have far-reaching implications for our national security, economic integrity, and humankind.
Thus, as the world adopts digital technologies faster than it can mitigate potential risks, there is opportunity to lead in securing our CI/KR. These safeguards can be successful only through the partnerships of users, suppliers, and the government to employ a risk management to ensure our infrastructure is resilient, interoperable, transparent, and worthy of trust.

To achieve the strategy to defend the country, there must be clear leadership at the national level, a defined plan for translating policy into action. Direction must come from the White House; it must cultivate coalitions with CI/KR constituencies; and it must define priorities in order for all entities to have a reasonable expectation of security in cyber.

In aligning shared priorities, all constituencies are invested in a solution; mitigations can be implemented across networks and sectors; and a threat present to one entity can rely on the defensive power and full resources of the entire nation. The American people will not tolerate a failure of leadership from either the public or private sector when solutions are available and leaders choose not to act.

## BIBLIOGRAPHY

Arbor Networks Inc. (14 Mar 2014). Dell Security Works. Burlington, MA: Arbor Networks Inc.

Beauchesne, A. M. (12 Feb 2014). *U.S. Chamber Statement on Cybersecurity Framework.* Washington, DC: U.S. Chamber of Commerce.

Clapper, J. (7 Mar 2013). Clapper, James. (ODNI Director's Statement to the Senate Select Committee on Intelligence) Worldwide Threat Assessment of the US Intelligence Community. *Statement for the record: Senate Select Committee on Intelligence* (p. 2). Washington, DC: United States of America.

Clayon, M. (18 Mar 2014). Massive cyberattacks slam official sites in Russia, Ukraine. *Christian Science Monitor*, http://www.csmonitor.com/tags/topic/SecureWorks+Inc.

Couts, A. (2 Aug 2012). Senate Kills Cybersecurity Act 2012. *Digital Trends*, http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/#!DOlcz.

Department of Homeland Security. (Feb 2013). *Critical Infrastructure Sectors.* Washington, DC: Office of Infrastructure Protection National Protection and Programs Directorate.

Executive Office of the President. (12 Feb 2013). *Presidential Policy Directive 21 (PPD-21): "Critical Infrastructure Security and Resilience".* Washington, DC: White House.

Lewis, J. A. (Dec 2008). *"Securing Cyberspace for the 44th Presidency," CSIS Commission on Cybersecurity.* Washington, DC: Center for Strategic and International Studies.

National Counterintelligence Executive, N. (2012). *Report to Congress: "Foreign Spies Stealing US Economic Secrets in Cyberspace".* Washington, DC: Office of the Director of National Intelligence.

National Institute of Standards & Technology. (12 Feb 2014). *"Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.* Washington, DC: NIST.

Perlroth, N. (8 Jan 2013). Bank Hacking Was the Work of Iranians, Officials Say. *New York Times*, B1.

Rajagopalan, P. M. (1 Aug 2012). Does Cybercrime Really Cost $1 Trillion? *ProPublica*.

Smith, G. (25 April 2013). "Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill". *Huffington Post*.

Symantec Corporation. (Sep 2013). *Symantec Corporation, 2012 Norton Cybercrime Report.* http://www.norton.com/2012cybercrimereport.

U.S.-China Economic and Security Review Commission. (Nov 2013). *2013 Annual Report to Congress, Section 2: China's Cyber Activities.* Washington, DC: USCC.

Webb, T. (30 Jan 2014). "Analyst sees Target data breach costs topping $1 billion". *Twin Cities' Pioneer Press*, 1B.

White House. (12 Feb 2013). *Presidential Executive Order 13636: "Improving Critical Infrastructure Cybersecurity".* Washington, DC: Executive Office of the President.

# SECTION 5: TACTICS

Enabling Army Commanders to More Effectively Integrate Cyberspace Operations
Mr. Victor Delacruz

**ABSTRACT**
Cyberspace Operations was officially introduced into Army doctrine in 2012.[1] Although the doctrine is relatively new, the Army's emphasis on cyberspace and cyberspace operations has been a constant theme in senior leader dialogs since 2010 following the publishing of the U.S. Army's Cyberspace Operations Concept Capability Plan.[2] Army commanders have been slow to integrate cyberspace operations specifically into their training plans and related events for various reasons. Among those reasons is a lack of knowledge/understanding of cyberspace operations, a lack of resources to conduct cyberspace operations, and increased responsibility for leading related changes. Commanders can take actions to address these challenges by instituting certain programs, leveraging existing resources, and modifying training priorities. However, their approach should be comprehensive and their leadership of this change characterized by flexibility and determination.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
1. In May 2012, Army commanders were introduced to Cyberspace Operations (CO) in Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations*.[3] A year later, Army commanders were directed to develop and implement training plans for Cyber Electromagnetic Activities (CEMA) inclusive of CO.[4] Army doctrine describing the fundamental tactics and language of CO was published in February, 2014.[5] Although commanders had access to these doctrinal publications and were aware of the emphasis on the new cyberspace domain, they were slow to integrate CO into their training plans largely due to a lack of knowledge/understanding of what CO was and how they could integrate it into their training and operations.[6]

Army commanders and their staffs attempting to understand and integrate CO first rely on doctrine, training materials, and commander's guidance from higher headquarters that currently lack sufficient detail to enable effective implementation.[7] JP 3-12, "Cyberspace Operations" (2013) and Field Manual (FM) 3-38, "Army Cyberspace Operations" (2013) define and describe the missions and functions of CO but these descriptions are fundamental and limited in their linkage to operational principles and supporting tactics. Specific to Army doctrine, these key terms and concepts lack a clear linkage to the Army operations process and supporting warfighting functions. For instance, in JP 3-12, the emphasis on *intent* and the specification of *actions* conflicts with the Army's use of *intent* and *activities*, respectively. These differences between joint and Army doctrine are common; however, in the case of new content as with CO, the negative impacts of these differences are exacerbated.[8] As a result of what appears to be disconnects on taxonomy and overall lexicon, the manner in which CO could be integrated throughout the operations process remains ambiguous to commanders and their staffs.[9]

The lack of sufficient detail to enable effective implementation of CO operations applies mostly to offensive cyberspace operations (OCO) and defensive cyberspace operations-response actions (DCO-RA) which occur primarily outside of the DOD information network (DODIN).[10] The remaining CO functions are codified and disseminated across the Army Signal community and the challenges with implementation inside of the DODIN are not as pronounced.[11] Nonetheless, doctrine such as the FM 7-15, "Army Universal Task List" (2012) only previews overarching tasks

with minimal details on measures and supporting actions. Similarly, training materials, if accessible, are not adequately codified, narrow in context, and in early stages of development falling short of qualifying as best practices.[12] Thus, the published doctrine on CO lacks depth and utility for commanders especially at the corps, division, and brigade levels.[13]

2. The Army Cyber/Electromagnetic Contest Capabilities Based Assessment (C/EM CBA) published in 2011 identified 27 capability gaps preventing Army forces from integrating CEMA to include CO.[14] More recently, the Army Cyberspace Operations CBA published in June 2014 identified 33 capability gaps specific to the conduct of CO.[15] These studies represent large research efforts that analyzed the Army's ability to conduct CO and concluded that numerous material and nonmaterial solutions were needed. While Army commanders are being instructed to integrate CO into their training plans, there is clear acknowledgement that they lack the resources to accomplish the related CO tasks.[16] For instance, units at corps and division exercises currently struggle to train on CO because it is difficult to develop a common operational picture of cyberspace to enable commanders to understand, visualize, describe, and direct courses of action leveraging cyberspace capabilities.[17] These conditions are applicable to CO focused primarily on OCO and DCO-RA. Both material and nonmaterial solutions are being developed to address the lack of resources, but they are not currently available and this is preventing Army commanders from effectively integrating CO into training. Similarly, simulation systems cannot fully replicate cyberspace or the effects that can be produced in cyberspace. Workarounds are common during training but they can be overly complicated, time-consuming, and still fall short of achieving a realistic training effect.[18] Thus, material resources are not currently available to support major training exercises conducted at corps, division, and brigade levels.

3. The military's emphasis on cyberspace as an operational domain and the need for Army forces to conduct CO in support of unified land operations will continue to increase in importance.[19] Army commanders will be required to lead and train their staffs to plan, coordinate, and conduct (as required) CO despite resource shortfalls to include doctrinal deficiencies. For instance, General Allyn, Commander of the U.S. Army Forces Command (FORSCOM) provided formal guidance to Army commanders to incorporate CO training and to provide feedback on a monthly basis.[20] See Figure 1-1 for an extract from the FORSCOM Memorandum for Commanders.

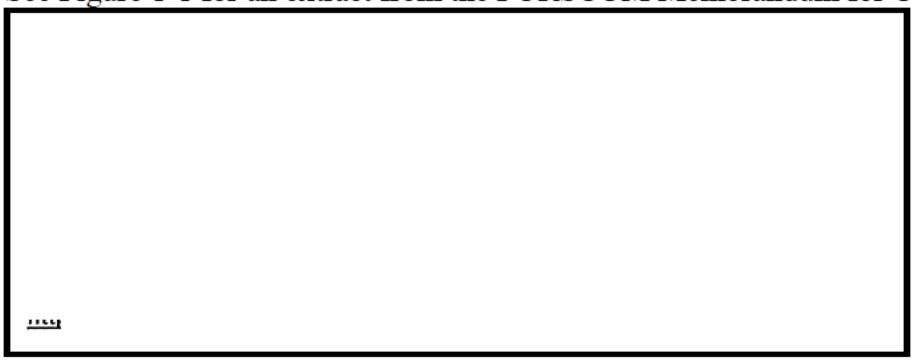


**Figure 1. Extract from FORSCOM Memorandum for Commanders**[21]

Leading CO requires commanders to provide a continuous flow of guidance to their staffs for both planning and operations. Due to the new nature of CO to Army, staffs are not adequately trained and skilled resulting in deficiencies specifically across the mission command, intelligence, and movement and maneuver warfighting functions.[22] While Army commanders have considerable expertise in leading the operations process, they are challenged to lead their staffs because they

themselves lack requisite training and expertise on cyberspace operations.[23] Commanders already maintain considerable responsibility for training their units and the addition of CO coupled with limited resources and staff training are proving problematic. For instance, unite training priorities and related plans reflect a minimal focus on CEMA which includes CO.[24] The expansion of duties and related skills are expected to characterize the integration of CO in the years to come.[25]

## RECOMMENDATIONS

1. Understanding cyberspace as a new operational domain and integrating cyberspace operations (CO) as a military function to enable freedom of action in cyberspace are two daunting and enduring challenges for the Army. Army commanders should institute programs to embrace current and emerging doctrine with a focus on joint doctrine and lower tier Army techniques publications. See Figure 2 for a status on current and emerging doctrine for CO.

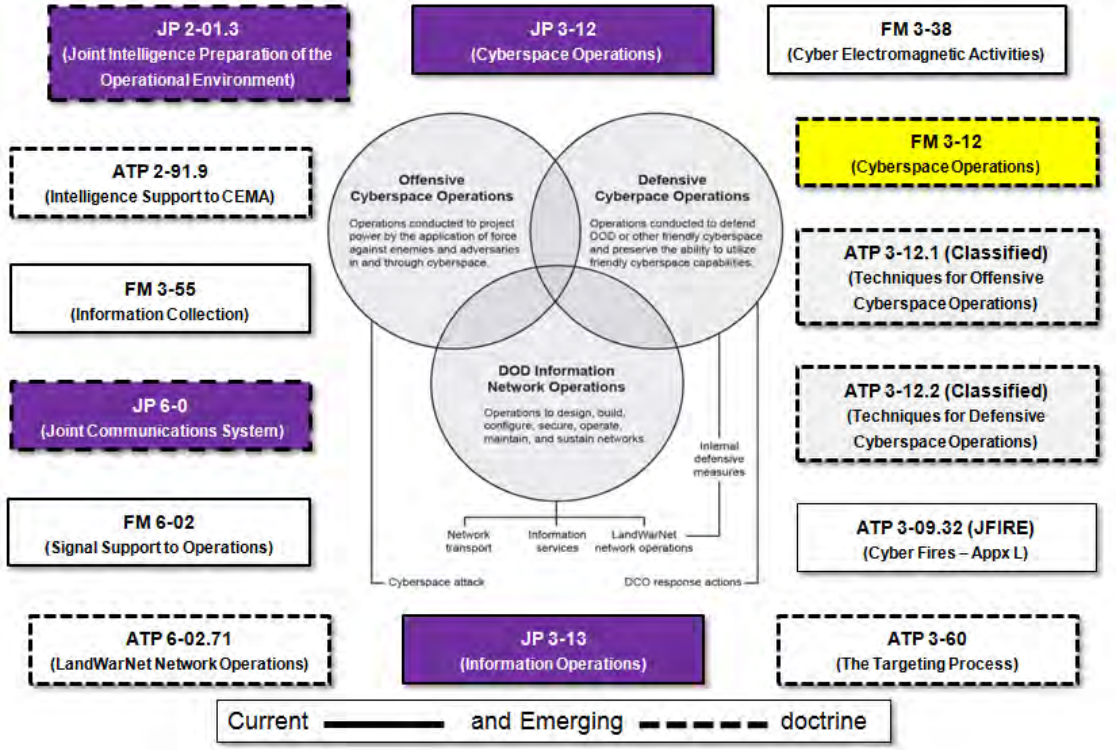



**Figure 2. Status of doctrine for cyberspace operations**

The JP 3-13, "Information Operations" series and the current JP 2-01.3, "Joint Intelligence Preparation of the Operational Environment" provide foundational knowledge upon which JP 3-12, "Cyberspace Operations" builds and expands. FM 3-38, "Cyber Electromagnetic Activities", FM 6-02, "Signal Support to Operations", and the draft FM 3-12, "Army Cyberspace Operations" provide the Army's translation of and nesting to overarching joint doctrine. The principles and tactics in these publications should be applied during unit training events across all warfighting functions and at all echelons.

Army commanders should coordinate with the Army's Combined Arms Doctrine Directorate at Fort Leavenworth, Kansas to be added to the distribution list for doctrine staffing. This will allow units to receive and review emerging doctrine at various stages of development and to reach out to doctrine authors and other subject matter experts to enhance their knowledge and understanding.

Once linked into the doctrine review process, units can submit comment resolution matrices and engage in collaborative forums to further enhance their understanding of cyberspace operations. Similarly, commanders should take actions to link to the combat training centers to obtain CO products.

2. Material solutions to enable the development of network topologies and related OPORD products will not be available in the immediate future. Commanders should instruct their staffs to create these products in accordance with published and emerging doctrine to facilitate training. Given the circumstances aforementioned, commanders should allow for the usage of emerging doctrine for home station training even though these documents have not been approved for implementation. It is common practice for draft products to be used in some manner by Army forces.[26] Similarly, outputs from exercises and experiments where CEMA and CO have been trained should also be incorporated into unit practices. Training packages should be developed to include division OPORDs and brigade OPORD products complete with the CEMA appendix and supporting tabs as listed in Figure 3.

| **Cyberspace Operations –** Final OPORD products | **CEMA –** Final OPORD products |
|---|---|
| • Final Tab A (Offensive Cyberspace Operations) to Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations)<br><br>• Final Tab B (Defensive Cyberspace Operations – Response Actions) to Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations)<br><br>• Final CO input to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal)<br><br>• Final CO input to Appendix 2 (Network Operations) to Annex H (Signal)<br><br>• Final CO input to Annex L (Information Collection). | • Final Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations).<br><br>• Final CEMA input to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal).<br><br>• Final CEMA input to Appendix 2 (Information Network Operations) to Annex H (Signal).<br><br>• Final Appendix 6 (Spectrum Management Operations) to Annex H (Signal).<br><br>• Final CEMA input to Appendix 14 (Military Deception) to Annex C (Operations). |

**Figure 3. Final OPORD products to support cyberspace operations[27]**

Commanders can request for external support. The World Class Cyber OPFOR and other CO training teams can be coordinated through the U.S. Army Cyber Command and/or U.S Army Cyber Center of Excellence. Additionally, commanders can coordinate with the Forces Command (FORSCOM) staff for CEMA training options for home station training.[28] Given the general lack of resources for the conduct of CO, commanders will need to look to others to obtain assistance.

3. Army commanders are responsible for leading and training their units to ensure mission accomplishment. Although the integration of CO imposes additional demands upon the commander resulting in increased responsibility with no additional resources, commanders must be flexible, determined, and innovative in their approaches to CO training.[29] Commanders should initially focus their training plans on cybersecurity training which will account for DCO and DOD information network operations functions. Commanders should select Soldiers for attendance at

the Army's Cyberspace Operations Planners Course (ACOPC), the Air Force Institute of Technology (AFIT) Cyber 200 and Cyber 300 courses, and other courses as appropriate. A command emphasis on education to support CO-related training will provide a long-term solution for the implementation of CO into training. To address staff deficiencies, commanders should schedule frequent command post exercises or similar training events to allow the staff to apply the Military Decisionmaking Process (MDMP) and targeting process (i.e., D3A) specifically to CO. This focus on education and training will allow the staff to improve their knowledge and skills and this will enable more effective integration of cyberspace operations into training.[30]

**COUNTERARGUMENT**

1. The current doctrine on CO is sufficient to enable basic understanding and implementation. Initial dissemination of doctrine to meet training demands coupled with subsequent inculcation particularly in a community that is resistant is expected to be problematic, and it is therefore incumbent upon commanders to anticipate and mitigate negative outcomes.[31]

2. Given the absence of material solutions to enable full implementation of CO training, the commander's expectation of the staff to produce OPORD products or to coordinate externally to obtain support to training is not uncommon. However, direct coordination from all echelons within FORSCOM to other organizations as discussed could prove problematic. Distribution systems are already established which leverage the chain of command and efficient organizational function. Commanders need to understand that required capabilities for CO at all echelons have already been determined and processes are ongoing and expected to lead to eventual fielding of material and nonmaterial solutions.[32]

3. Focusing on CO training tasks inside the DODIN is only half of the solution. While DCO and DOD information network operations are critical to CO, the other tasks within OCO and DCO-RA are just as important because they enable the commander to create effects outside of the DODIN in support of the scheme of maneuver.[33] Moreover, from a doctrinal viewpoint which is informed by how units train in the field and contribute to the evolution of tactics, techniques, and procedures, the Army MDMP requires revisions to account for all CO functions and related tasks and this cannot be achieved if one approach is favored over another.[34]

**CONCLUSION**

The introduction of cyberspace as an operational domain coupled with the integration of CO as a set of functions to enable Army forces to achieve freedom of action in cyberspace in support of unified land operations is a historic event for Army. Army commanders have an opportunity to embrace this advent and they are challenged to demonstrate leadership characterized by flexibility, curiosity, and determination. The challenges discussed have accompanied any significant change within the Army. Doctrine development will lag behind practice, resources will not be immediately available, and the emphasis to embrace something new will conflict with current priorities. Indeed these challenges are daunting but commanders cannot afford to delay what appears to be the inevitable… a future operating environment where "Army cyber units will be nested within joint global, expeditionary cyber constructs at every echelon to synchronize and deliver commander's effects."[35] We can accept to a degree that this integration will take time but the "operationalization" of CO requires that the Army apply what is known about operating in the land domain to this new contested domain.[36]

**NOTES**

(All notes appear in shortened form.
For full details, see the appropriate entry in bibliography.

[1] ADRP 3-0, "Unified Land Operations," page 3-3, paragraph 3-14, "…Cyber electromagnetic activities consist of cyberspace operations, electronic warfare, and electromagnetic spectrum operations."
[2] TRADOC PAM 525-7-8, "The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028."
[3] ADRP 3-0, "Unified Land Operations,"page 3-3, paragraph 3-14, "…Cyber electromagnetic activities consist of cyberspace operations, electronic warfare, and electromagnetic spectrum operations."
[4] FORSCOM memorandum for commanders, Subject: FORSCOM Command Training Guidance, FY 2014, pp. 15-18.
[5] FM 3-38, "Cyber Electromagnetic Activities", Chapter 3 (Functions of Cyberspace Operations), pp. 3-1 to 3-12.
[6] Hernandez, "Preparing the Army to Prevent, Shape And Win in Cyberspace," p. 194; Williams, "Cyber ACTS/SAASS", Roeder, "Cybersecurity: It isn't just for Signal officers anymore,"; Adams, "Interview with Lt. Gen. Edward C. Cardon, Commander of the US Army Cyber Command (ARCYBER);" Boland & Lawlor, "The Cyber Army of the Future;" and Caudle, "Decision-making uncertainty and the use of force in cyberspace: A phenomenological study of military officers," and Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report"
[7] Martin, "Army Cyberspace Operations Capabilities Based Assessment," Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report," and Personal communication with COL Mark W. Russell, Commander, Operations Group S, Mission Command Training Program on July 17, 2014.
[8] Personal communication with Mr. Mike Scully, Combined Arms Doctrine Directorate, June 26, 2014.
[9] Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report," Personal communication with COL Mark W. Russell, Commander, Operations Group S, Mission Command Training Program on July 17, 2014.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Personal communication with Mr. Mike Scully, Combined Arms Doctrine Directorate, June 26, 2014. and Martin, "Army Cyberspace Operations Capabilities Based Assessment."
[14] Martin, "Army Cyber/Electromagnetic Capabilities Based Assessment."
[15] Martin, "Army Cyberspace Operations Capabilities Based Assessment."
[16] Hernandez, "U.S. Army Cyber Command: Cyberspace for America's Force of Decisive Action;"
[17] Personal communication with COL Mark Russell, Commander, Operations Group S, Mission Command Training Program, July 17, 2014.

[18] Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report," and Personal communication with Mr. Arlen Logan, Scenario Design, Mission Command Training Program, June 14, 2013.
[19] Hernandez, "U.S. Army Cyber Command: Cyberspace for America's Force of Decisive Action;" Cacas, "Cyber Train as you Fight;" Brown & Tullos, "On the Spectrum of Cyberspace Operations;" Parker, "The Utility of Cyberpower,", Steel, "Cyber Warriors Draw a Line in the Silicon," and Williams, "The Joint Force Commander's Guide to Cyberspace Operations."
[20] FORSCOM memorandum for commanders, Subject: FORSCOM Command Training Guidance, FY 2014, p. 5.
[21] Ibid.
[22] Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report"
[23] Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report" and Personal communication with COL Mark Russell, Commander, Operations Group S, Mission Command Training Program, July 17, 2014.
[24] Morrow and Melton, Network Integration Evaluation CEMA Demonstration Report"
[25] Roeder, "CyberSecurity: It Isn't Just for Signal Officers Anymore"
[26] Morrow and Melton, "Network Integration Evaluation CEMA Demonstration Report," and Personal communication with Mr. Mike Scully, Combined Arms Doctrine Directorate, June 26, 2014.
[27] FM 3-38 (CEMA) and FM 3-12 (Army Cyberspace Operations)
[28] Personal communication with MAJ Kevin James, FORSCOM G-39
[29] Druben, "Army Looks to Blend Cyber, EW Capabilities on the Battlefield"; Dutt and Gonzales, "Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory".
[30] Fink & Wells, "Considerations for Offensive Cyberspace Operations"; Gould, "Army needs better cyber management."
[31] Personal communication with Mr. Mike Scully, Combined Arms Doctrine Directorate, June 14, 2013.
[32] Martin, "Army Cyberspace Operations Capabilities Based Assessment."
[33] Fink & Wells, "Considerations for Offensive Cyberspace Operations"; Gould, "Army needs better cyber management, " and Brown & Tullos, "On the Spectrum of Cyberspace Operations;" and Parker, "The Utility of Cyberpower,"
[34] Personal communication with CW4 Paul Morrow, U.S. Army Cyber Command, May 12, 2014
[35] Hernandez, U.S. Army Cyber Command: Cyberspace for America's Force of Decisive Action.
[36] Cardon, "2014 AUSA Winter Symposium."

## BIBLIOGRAPHY

Adams, R. (2014). Interview with Lt. Gen. Edward C. Cardon, Commander of the US Army Cyber Command (ARCYBER). *Military Technology, 28*(5). 44-44. Retrieved from http://militarytechnology.com

Army Doctrine Reference Publication (ADRP) 3-0 (2012). *Unified land operations.* Retrieved from http://www.apd.army.mil

Birdwell, B. M., (2011) War Fighting in Cyberspace. *Air & Space Power Journal, 24*(1). 26-36. Retrieved http://www.airpower.maxwell.af.mil/

Boland, R., & Lawlor, M. (2011). The Cyber Army of the Future. *Signal, 66*(2). 69-72. Retrieved from http://www.afcea.org/

Brown, G. D, & Tullos, O W. (2012). On the Spectrum of Cyberspace Operations. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com

Cacas, M. (2013). Cyber Train as you Fight. Signal. 27-28. 2p. *Signal, 67*(10). 27-28. Retrieved from http://www.afcea.org/

Cardon, E. C. (2014). 2014 AUSA Winter Symposium. Speech on Cyberspace Operations. Retrieved from http://youtube.com

Caudle, D. L. (2010). Decision-making uncertainty and the use of force in cyberspace: A phenomenological study of military officers. Retrieved from ProQuest database.

Drubin, C. (2013). Army Looks to Blend Cyber, EW Capabilities on the Battlefield. *Microwave Journal, 56*(12). 39-40. Retrieved from http://www.microwavejournal.com

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(*6). 33.33. doi. DOI: 10.1177/0018720812464045

Field Manual 3-38 (2013). *Cyber Electromagnetic Activities*. Retrieved from http://info.publicintelligence.net

Fink, K. D., Jordan, J. D, Wells, J. E. (2014). Considerations for Offensive Cyberspace Operations. *Military Review, 92*(3). 26-11. Retrieved from http://usacac.army.mil

Forces Command (FORSCOM) Memorandum for commanders (2013). Subject: FORSCOM Command Training Guidance, FY 2014, June 12, 2013.

Gould, J. (2013). Army needs better cyber management, *Army Times, 26*. Retrieved from http://www.armytimes.com

Hernandez, R. A. (2012). U. S. Army Cyber Command: Cyberspace for America's force of decisive action. *Army Magazine, 53*(7). 205-208. Retrieved from http://www.ausa.org

Hernandez, R. A. (2013). Preparing the Army to prevent, shape and win in cyberspace. *Army Magazine, 63*(10). 191-194. Retrieved from http://www.ausa.org

Joint Publication 3-12 (2013). *Cyberspace Operations*. Retrieved from http://www.dtic.mil

Martin, M. (2011). US Army Cyber/Electromagnetic (C/EM) Contest Capabilities Based Assessment (CBA) Final Report. Retrieved from http://info.publicintelligence.net

Martin, M. (2014). US Army Cyberspace Operations Capabilities Based Assessment (CBA) Final Report. Retrieved from http://info.publicintelligence.net

Morrow, P. R. & Melton, W. M. (2012). *Network Integration Evaluation (NIE) CEMA Demonstration Report*. Retrieved from https://www.jllis.mil

Parker, K. L. (2014). The utility of cyberpower. *Military Review, 92*(3). 36-33. Retrieved from http://usacac.army.mil

Roeder, D. B. (2014). Cybersecurity: It isn't just for Signal officers anymore. *Military Review, 92*(3). 38-42. Retrieved from http://usacac.army.mil

Steele, D. (2014). Cyber warriors. *Army Magazine, 64*(3). 34-38. Retrieved from http://www.ausa.org

Training and Doctrine Command (TRADOC) Pamphlet (PAM) 525-7-8 (2011). The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028. Retrieved from http://www.apd.army.mil

Williams, B. T. (2014). The joint force commander's guide to cyberspace operations. *Joint Force Quarterly, 73*(2). 12-19. Retrieved from http://www.dtic.mil

Williams, P. D. (2009). Cyber ACTS/SAAS: A second year of command and staff college for the future leaders of our cyber forces. *Air & Space Power Journal, 21(*2). 21-28. Retrieved http://www.airpower.maxwell.af.mil/

# Commanders Risk and Social Media

LTC Eric A. Healey (USARCENT/G34)

**ABSTRACT**

Secretary of Defense Robert Gates published in the June 2008 National Defense Strategy under Future Challenges, "Although our advanced space and cyber-space assets give us unparalleled advantages on the traditional battlefield, they also entail vulnerabilities."[1] Secretary Gates also noted in his conclusion, "The United States, and particularly the Department of Defense, will not win the Long War or successfully address other security challenges alone. Forging a new consensus for a livable world requires constant effort and unity of purpose with our Allies and partners."[2] In order for the Department of Defense and its services to pave this way ahead, cultivate, and maintain relationships with allies and partners they must communicate. Social Media through the cyberspace domain provides the world with global platforms to communicate. The Department of Defense policy and guidance regarding internet based capabilities and social media is appropriate. The DoD acknowledges the enabling capability of cyberspace and social media to communicate to mass audiences. U.S. Department of Defense maintains an online policy library for Web and Internet-based Capabilities (IbC) at http://www.defense.gov/webmasters/. Fitting that at the bottom of the webpage there are links provided for Social Media sites. The focus of this paper is on the challenges faced by the responsible heads and commanders that must manage and mitigate risks associated with Social Media. Service members and leaders are key targets of social engineering techniques such as spear-phishing and whaling for the purpose of gaining access to the Department of Defense Information Network (DODIN). Social Media enables the social engineering aspects of an attack.

## DESCRIPTION OF ISSUE / PROBLEM STATEMENT

Commanders and department leadership need to communicate to internal and external audiences. Internal communications contains department or command specific information of an administrative or operational nature. Orders, training directives and inspections are a few examples. Internet based Social Media tools are not good instruments for internal communications. Accidental release of internal communications could pose a threat to Operations Security (OPSEC) of an organization's mission(s), plans or personnel. When commands utilize Social Media means to communicate to external audiences they are responsible for the content reliability and accuracy of the information. This is typically the responsibility of the units Public Affairs staff. Public Affairs ensure messages are in accordance with Public Affairs guidance and nested with higher headquarters' messages. Viewing from an OPSEC perspective and the Operational Context, "Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed to the field conducting actual operations."[3] Social Media provides an additional lens to observe. OPSEC planning and execution in Army units are the same for Joint forces. "OPSEC is an operations function, not a security function".[4] Army units have Functional Area Information Officers trained to perform OPSEC roles. OPSEC staff review messages to ensure essential elements of friendly information are not inadvertently released. The staff review process for external communications is an essential requirement to ensure accurate and secure information publication regardless of the media platform. Social Media introduces risk to the commanders' mission in the form of Official external communications, personal, service members, government employees, contractors and family members.

1. The first area to explore is Official external communications. More and more senior leaders are signing up for official Social Media sites. Official sites procedures are governed by enclosure 3 of DODI 8550.01 DoD Internet Services and Internet-Based Capabilities. The first two provisions under the Official Use section under Internet based capabilities are:

> *"(1) DoD and OSD Component Heads and official-use account users must be prepared to account fully for exercising sound judgment within the authority and scope of official activities.*
>
> *(2) Liaison shall be conducted with public affairs and OPSEC staff to ensure organizational awareness of their authorized, mission-related public communication."* [5]

These provisions help to protect the official use owner but gets increasingly complicated below O6 level commands where lack of Public Affairs and OPSEC staff are not authorized. Social Media is being leveraged by the DoD and its services to execute it mission. President Obama published in the 2010 National Security Strategy a definition for Strategic Communications in the Strengthen National Capacity section.

> *"Strategic Communications: Across all of our efforts, effective strategic communications are essential to sustaining global legitimacy and supporting our policy aims. Aligning our actions with our words is a shared responsibility that must be fostered by a culture of communication throughout government. We must also be more effective in our deliberate communication and engagement and do a better job understanding the attitudes, opinions, grievances, and concerns of peoples—not just elites—around the world. Doing so allows us to convey credible, consistent messages and to develop effective plans, while better understanding how our actions will be perceived. We must also use a broad range of methods for communicating with foreign publics, including new media."*[6]

Over the past two years in USARCENT, I have noticed an increased use of Social Media to maintain relationships between senior US officers and officers of partner countries. The exchange goes beyond business and training exercises. Common examples of exchanges are links to articles, socially polite comments to items posted, or invites to visit training exercise or Academy graduation events. The friendships are leading towards trust and confidence while building combined capacity. Installation commanders are using Social Media to engage the local population and civic leaders. The I Corps Commander at Joint Base Lewis-McChord uses Facebook and Twitter for the normal Public Affairs task of telling the I Corps Story. He also uses it as a bulletin board to announce to the community, commands, and partners relevant local issues. Recently the commander held a town hall meeting to discuss issues relating to Sequestration and potential impacts to the Greater Joint Base Lewis-McChord. Pictures and notes of the town hall meeting are posted on Social Media for further discussion or, if someone could not make the meeting, they can read the notes and post comments. Social Media is helping the I Corps Commander achieve command Community Connecter goals of "increase interaction between JBLM and local communities, enhance understanding of today's Army and JBLM, [and] develop and maintain strong and positive community partnerships".[7] Threat groups that target senior

leaders and executives develop social engineering techniques from information provided on Official sites. General Officers and senior executive names are readily attainable through open source due to their position and close contact to public and media community. "The practice of targeting CEOs and other high-ranking execs is being dubbed as whaling."[8] Senior Officers and Executives should be well-versed in identifying "whaling" techniques due to the high volume of emails they process daily. Should they use their staff to screen email traffic, the staff should also be well trained in social engineering techniques in order to protect their boss and the DODIN. "Cyber intelligence firm iSight Partners released a report 27 May 2014 that states a group of hackers, allegedly from Iran, have been participating in an elaborate three-year campaign dubbed Newscaster to spy on high-ranking defense officials".[9]

2. The second area that commanders need to evaluate risk relates to their service members, government employees, contractors, and family members personal use of Social Media. "The OPSEC process is a systematic method used to identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations and other activities".[10] Out of this process commanders identify critical friendly information that they need to protect from the enemy. This is also known as "essential elements of friendly information — Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness."[11] Are they discussing work-related unclassified information that may be For Official Use Only (FOUO) or releasable information that when aggregated could reveal essential elements of information (EEFI) the commanders want to protect? What security practices are they using with their Social Media exploits, security settings, or are they open to the world? Are Family Support volunteers circulating or posting Personal Identifying Information (PII) on Social Media? Each of these areas could cause vulnerabilities that could potential hurt organization members or their families and/or the unit mission. The more information personnel share on Social Media, the more susceptible they are for a socially engineered attack.

> *"The latest twist on phishing is spear phishing. No, it's not a sport, it's a scam and you're the target. Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC."*[12]

3. The third area commanders should concern themselves is the damage Social Media could pose on their personnel. "Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey worried aloud Wednesday that the next generation of possible military recruits is ignorant about the damage that can come from showing bad or illegal behavior online."[13] Social Media users can post photos, videos, and comments. Users interact with other users, friends, family, and possibly strangers. The disassociated nature of Social Media emboldens some to make comments that they would not necessarily make in person, post embarrassing photos, or videos. This behavior could lead to cyber bullying, threats, and harassment. Service members are accountable for their actions and the expectations of service members are that they live by their service values on and off duty. Association and participation with extremist and racist organizations through Social Media could negatively impact security clearance investigations and do not conform to good order and conduct. These organizations do utilize Social Media and conduct on line recruiting to target service members. "The Homeland Security assessment specifically says that right-wing extremists will

attempt to recruit and radicalize returning veterans in order to exploit their skills and knowledge derived from military training and combat."[14] All users that enable their GPS in their smart phones or use geo tagging functions linked to their Social Media accounts open themselves to being tracked or having patterns of life information gathered. Pictures posted on Social Media could have metadata embedded with specific time, date, and location the picture was taken.

> *"The hackers created over a dozen fake profiles across various social networking platforms and filled their profiles with fictitious content. They also posted links to non-malicious content, such as videos and news articles posted on NewsOnAir.org, a fake news website that published articles ripped off from CNN and BBC and created by the hackers to further bolster their bid for trust.*
>
> *The hackers would then reach out to the targets' family, friends or old classmates from high school before initiating contact with the targets themselves. Once trust is established, they would send malware-embedded links that led to false pages asking for the targets' credentials."*[15]

**RECOMMENDATIONS**

1. The DoD should continue to utilize Official Use Social Media as a tool to communicate to external audiences. It provides a cost effective means to communicate to mass audiences, responsive feedback capability and can be used to assess command messages. Units with Official Use sites ensure compliance with DODI 8550.01 DoD Internet Services and Internet-Based Capabilities. The DoD should also ensure site operators receive cyber awareness training to recognize social engineering threats, identify OPSEC violations, and quickly remove and report inappropriate activity. Well trained operators will assist in protecting the DODIN. Commanders should have staff processes and standards in place to develop and screen for accuracy and security prior to posting. Well trained staff and processes facilitate timely communications to accomplish the commanders Strategic Communication objectives.

2. Commands at the O5 level and below are challenged due to personnel limitations and do not have manning authorizations for Public Affairs and OPSEC subject matter experts. They will require assistance in meeting required criteria to establish an Official Use site. The command should leverage their next higher command and installation experts to establish their program. They should establish a team of site operators and message developers. Utilize the experts on the installation to train the media team. The media team should receive additional cyber awareness training and the commands' subject matter experts on Social Media. The media teams are the trainers of the organization to educate the command on responsible Social Media conduct. The media team coordinates with the operations section to schedule leader development training and reoccurring soldier training. They should also look for opportunities to train family members at family readiness meetings or conferences. Education of threats and best practices will assist the command in limiting the amount of risk associated with Social Media.

3. Protecting unit members and families at home falls into three areas: secure devices, secure practices, and secure behavior. The key to success in protecting unit members and families at home starts with their first line leaders. Squad and team leaders should include discussions with subordinates during monthly counseling on Social Networking. Topics to cover are antivirus for

their devices, as well as to provide assistance or direction to free software and how to set it up. Discussions should include the practice of backing up data and setting recovery points. Leaders should ensure subordinates understand Personal Identifying Information and risk associated with posting any work related information. Leaders should also discuss privacy setting and warn subordinates about the potential target they are just for being in the Military. Leaders should ensure subordinates understand the rules of engagement for behavior on Social Media and should ask to see their Social Media sites and provide feedback and guidance. Discussions should occur on the threats of criminals, hackers, terrorist and adversaries and how it relates to them, their family, and their use of Social Networking. Service members and their families are targets on Social Media they need to understand the threats. First Line Leaders compliment the commanders Cyber Awareness program.

**COUNTERARGUMENT**

1. "Wisconsin National Guard said it was suspending a member from honor guard duty after she posted a picture on Instagram of a group of soldiers striking comedic poses around an empty, flag-draped coffin."[16] Incidents involving indiscipline while in the service uniform continue to be posted on Social Media. The DoD should reanalyze it's policy relating to Social Media. Service members continue to publicly embarrass themselves and share with the world. We like to say every Service member in uniform is an ambassador. Every incident erodes at the positive perception the Department of Defense has worked so hard to attain. The following quote is in response to the four Marines urinating on dead Taliban fighters, "For the Pentagon, it is clear that these images cause more damage than all of the Taliban's attacks, and serve to delegitimize American military actions in Afghanistan and beyond."[17]

2. Extremists will continue to target our returning troops and veterans. Social Media sites are ideal hunting grounds for recruiters. "The Homeland Security assessment specifically says that right-wing extremists will attempt to recruit and radicalize returning veterans in order to exploit their skills and knowledge derived from military training and combat."[18] This is trouble looking for the Service member. Personnel could be lured into joining discussions, making comments that could cost a security clearance and possibly a career. Shortly after the young Soldier ducking out of Honors to the Flag incident went viral, "A Facebook page called "Military Social Media Idiots" was promptly set up to highlight service members who appear to be embarrassing the armed forces."[19] The site owner is under an alias and suggests that he does not live in the United States. Adversaries could use this tactic to attack national and international perceptions of US Service members thus preying on young impressionable Service members that have not fully been cultured into the profession.

**CONCLUSION**

The advantages of using social media to communicate the DoD organizations messages is in keeping with the evolving social change. Leaders and site managers that are trained and use procedures to screen content prior to posting can mitigate operational security concerns. Brigadier General Volesky, Army Chief of Public Affairs states, "in today's information environment, when news breaks, one of the first places people turn to is social media as army communicators, we must utilize social media platforms to report the most accurate and up-to-date information."[20] Social Media is an operations area in the information environment to execute Strategic Communications. Enemy threats of Spear Phishing and Whaling should not deter this enabling platform. Vigilance

and training the force, site operator's staff, and Media Teams with help mitigate risks. "We will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment".[21] We cannot stop all threats and must be prepared to fight through disruption and quickly recover from attacks. Our First Line Leaders are key to ensuring Service members and families are aware of threats and understand how to protect their devices, information, and selves. They also monitor behaviors and provide on the spot corrections and mentoring to teach their subordinates best practices.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] Gates, R. M. (2008). *National Defense Strategy.*
[2] Ibid.
[3] CJCS. (4 JAN 2012). *Joint Publication 3-13.3 Operations Security.*
[4] Ibid.
[5] Takai, T. M. (2012, September 11). *Defense.gov.*
[6] Obama, B. (2010). *National Security Strategy.*
[7] Lanza, L. S. (2014, June 14). *I Corps*.
[8] Goodin, D. (2008 , April 16). *Fake subpoenas harpoon 2,100 corporate fat cats.*
[9] Arce, N. (2014, May 29). *TechTimes.com*.
[10] CJCS. (4 JAN 2012). *Joint Publication 3-13.3 Operations Security.*
[11] CJCS. (2014). *JP 1-02.*
[12] *Norton*. (2014, June 14). Retrieved from Spear Phishing: What It Is and How to Avoid It.
[13] Jelinek, P. (2013, December 04). *Clevland.com*.
[14] Hudson, E. L. (2009, April 14). *WashingtonTimes.com*.
[15] Arce, N. (2014, May 29). *TechTimes.com*.
[16] Ortiz, E. (2014, February 27). *NBC.NEWS.com*.
[17] Warner, M. B. (2012, January 13). *Spiegel.de*.
[18] Hudson, E. L. (2009, April 14). *WashingtonTimes.com*.
[19] Ibid.
[20] Volesky, B. G. (2013, January). *jber.af.mil*.
[21] CJCS. (2011). *NMS.*

## BIBLOGRAPHY

Arce, N. (2014, May 29). *TechTimes.com*. Retrieved from Iranian hackers spy on U.S. officials, defense contractors using social networks: http://www.techtimes.com/articles/7720/20140529/iranian-hackers-use-social-networks-to-spy-on-u-s-officials-defense-contractors.htm

CJCS. (2011). *NMS*. Retrieved from The National Military Strategy of the United States of America: http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf

CJCS. (2014). *JP 1-02.* Washington D.C.: Joint Staff.

CJCS. (4 JAN 2012). *Joint Publication 3-13.3 Operations Security.* Washington D.C.: Joint Staff.

Gates, R. M. (2008). *National Defense Strategy.* Washington D.C.: Department of Defense.

Goodin, D. (2008 , April 16). *Fake subpoenas harpoon 2,100 corporate fat cats.* Retrieved from The Register : http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/

Hudson, E. L. (2009, April 14). *WashingtonTimes.com*. Retrieved from Federal agency warns of radicals on right: A Facebook page called "Military Social Media Idiots" was promptly set up to highlight service members who appear to be embarrassing the armed forces.

Jelinek, P. (2013, December 04). *Clevland.com*. Retrieved from Top U.S. general warns teens about ramifications of social media: http://www.cleveland.com/nation/index.ssf/2013/12/top_us_general_warns_teens_abo.html

Lanza, L. S. (2014, June 14). *I Corps*. Retrieved from Lewis-McChord Community Connections Map: http://www.lewis-mcchord.army.mil/ICorps/community-connector.html

*Norton*. (2014, June 14). Retrieved from Spear Phishing: What It Is and How to Avoid It | Norton: http://us.norton.com/spear-phishing-scam-not-sport/article

Obama, B. (2010). *National Security Strategy.* Washington D.C.: White House.

Ortiz, E. (2014, February 27). *NBC.NEWS.com*. Retrieved from String of Social Media Scandals Plagues Military: http://www.nbcnews.com/news/military/string-social-media-scandals-plagues-military-n40501

Takai, T. M. (2012, September 11). *Defense.gov.* Retrieved from Department of Defense Web and Internet-based Capabilities (IbC) Policies: http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf

Volesky, B. G. (2013, January). *jber.af.mil*. Retrieved from United States Army Social Media Handbook: http://www.jber.af.mil/shared/media/document/AFD-130211-058.pdf

Warner, M. B. (2012, January 13). *Spiegel.de*. Retrieved from The World from Berlin: Urination Video 'Causes More Damage than Taliban Attacks': http://www.spiegel.de/international/world/the-world-from-berlin-urination-video-causes-more-damage-than-taliban-attacks-a-808942.html

Cyber Hunt: Integration and Employment

Squadron Leader Paul Jennings, Royal Air Force, 24 AF/A3

**ABSTRACT**

Defensive cyber operations have evolved through the years from traditional network defense to the current status of synchronizing cyberspace operations with critical Air and Space operations through innovation and application of expertise and technology. This evolution has matured the United States Air Force cyber philosophy from attempting to protect entire Air Force networks to protecting critical Air Force missions. Operational necessity and its inherent reliance on cyber dependencies means that shutting down a network as a result of a known adversary cyber presence is counterproductive in terms of overall mission success. In modern warfare, the availability of mission systems and associated tools and applications is essential, and therefore there is an increasing requirement to fight through a cyber attack to provide mission assurance in order to prevent degradation to kinetic operations.

> "The military advantages that net-centricity provides the U.S. military concomitantly offer an adversary affordable attack vectors through cyberspace against critical missions and advanced weapon systems." [1]

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

1. An advance persistent threat is defined as:

> "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." [2]

Conventional cyber defense methods are becoming increasingly ineffective in both deterring adversaries who pose an advanced persistent threat (APT) and preventing cyber intrusions on U.S. Air Force networks.

2. Cyberspace is defined as:

> "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3]

A relatively new warfighting domain, cyberspace is an amalgamation of hundreds of thousands of man-made physical components providing the platform on which data and information traverses. Historically, the emphasis, from both a military and commercial perspective, has been on making these communications tools faster and more readily available for the user community. Back in 1996, Joint Vision 2010 was published by the Chairman of the Joint Chiefs of Staff and it stated:

> "The unqualified importance of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology."[4]

As such, the decision was made to migrate to a single, standardized and centrally managed network solution, known as the AFNet. The benefits to this enterprise approach are clear. Over the last two decades the Air Force has had to manage hundreds of legacy IT networks that grew up organically according to their own rules and local IT strategies; this was an expensive and inefficient approach to the provision of communications systems and the user experience varied from base to base. Consolidating this into a single enterprise is a huge improvement in terms of availability and standardization. The other side of the coin, however, is that the Air Force now has a single, wide and flat attack surface within which any of the aforementioned components could be used as a potential entry point to the network. With "approximately 850,000 users worldwide, at more than 100 locations"[5] the AFNet is too large for the Air Force to defend efficiently with its finite resources.

3. Military operations are becoming increasingly net centric. Be it Joint Tactical Information Distribution System (JTIDS) data, mission support systems for fifth generation fighter aircraft, mission planning systems or command and control systems within a Combined Air Operations Center (CAOC), the operational battlespace is now intrinsically reliant on cyber systems and their underlying infrastructure.

> "The continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission."[6]

This cyber dependency means that it is no longer an option to simply disconnect a network once an intrusion has been discovered and to do so would degrade or limit military operations. It could potentially result in loss of critical military communications, decreased situational awareness of the battlespace, an inability to command and control military assets and even render aircraft and ships dysfunctional. It would be, in effect, a self-inflicted denial of service attack with a potentially fatal consequence.

4. Traditional boundary defense approach fails to consistently prevent unauthorized access from a determined adversary using advanced multi-vector attack methods over a prolonged period of time. Current methods of enterprise protection rely on signatures from the commercial sector and a band-aid approach of patching software and blocking malicious IP traffic. The APT actor is too agile, flexible and adaptable for this methodology to prevent intrusions and such incidents have "cost US entities hundreds of millions of dollars over the past decade as a result of harvesting enormous amounts of critical information including proprietary data, source code, negotiation tactics, and strategic operational plans. These actors have also breached networks containing sensitive national security information."[7]. Additionally, Computer Network Defense Service Provider (CNDSP) activities provide no tangible intelligence on enemy tactics, techniques and procedures (TTPs) once they have penetrated the AFNet, resulting in little to no understanding of what it is the enemy is trying to achieve within friendly networks. Without knowing what the enemy is attempting it is extremely difficult to posture against it.

**RECOMMENDATION**

1. In an ideal world, any organization, both in the public or private sector, would have a 100% resilient network. However, given the increasingly agile and sophisticated APT actors targeting networks with which the Air Force has a finite resource allocated for defense, it is imperative that a decision is made as to which parts of the vast cyber infrastructure are critical to mission success. The focus needs to be on assuring the mission, not assuring the network. If an Air Operations Center (AOC) mission was to fail as a result of an adversary intrusion to its primary chat tool used for command and control, mIRC, it is of no comfort to the C/JFACC that the neighboring base library had 100% network availability.

What is mission assurance? *DoD Policy and Responsibilities for Critical Infrastructure, 2012, (p18)* defines mission assurance as "a process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition."[8]

Cyber systems and tools are critical to the execution of Air Force missions and therefore, we must learn to operate through the cyber attack as to not degrade our ability to project Air and Space power, while implementing an active defensive counter cyber solution, known as cyber hunt, to restrict the adversary's freedom of movement within our networks and limit any potential damage. This is a mindset change for personnel who have a background in pure communications, but it is an important one as we strive toward the operationalization of cyberspace as a warfighting domain.

2. In order to provide mission assurance in cyberspace, it is essential that there is an understanding of "mission essential functions (MEFs)" in addition to "mapping mission dependence on Cyberspace"[9] within a given AOR. Mission oriented mapping is a key enabler for successful hunt missions, however, the supported operational community will not be able to inform the cyber operator of all the cyber dependencies critical to the mission as they would normally be focused solely on the user end of any given mission support system. The requirement, therefore, is to engage with the all the mission shareholders within a given focus area to understand their missions and capture information regarding the cyber systems critical to enabling mission success. This work will enable the cyber operators to develop a Critical Asset List (CAL) for the cyber components, based off "criticality, vulnerability and threat."[10] By analyzing and prioritizing the CAL, based off dialogue with both local cyber defenders and the A3/J3 community, the cyber planner can develop the Defended Asset List (DAL) which is "the prioritized assets from the CAL to be actually defended with resources available."[11] Once the DAL has been ascertained, every underlining cyber process that supports assets listed within the DAL, as well as their internal and external connections, should be mapped out. True understanding of the key mission cyber terrain should include hardware, software, information flow and data. This requires an exchange of network information between the hunt team and the local system maintainers, for example, an Air and Space Communications Squadron (ACOMS) unit within an AOC. "Situational awareness of the friendly network is developed through a review of previous cyber evaluations, regular reporting and discussions with local cyber defense personnel."[12] This will, in turn, enable an assessment of the vulnerabilities and offer immediate remediation recommendations to the system owners/maintainers in order to reduce attack vectors.

3. A successful hunt mission begins with the approach of assuming that the enemy is already operating within the perimeter of the friendly network and then employing active defense methods to engage malicious activities to clear and sweep mission enclaves of network threats. The installation of sensors at key points across the key mission cyber terrain allows the hunt team to monitor traffic traveling between key nodes within the enclave/network. This is an enduring presence, actively searching for anomalies in both data flows and active processes within the network in order to identify and counter detrimental behavior to protect the United States Air Force's ability to project Air and Space power. This approach should not take place in isolation. Cyber defense in depth provided by coordinating defensive actions with both local defenders responsible to for the mission systems as well as 24 Air Force units operating under the jurisdiction of the Computer Network Defense Service Provider (CNDSP) authority for the AFNet. The hunt mission is a key piece in United States Cyber Command's Cyber Protection Team concept as part of the new Cyber Mission Force construct and the Concept of Employment document stresses the need for "synchronized capabilities in coordination with organic defenders to achieve maximum effect."[13] Many Air Force systems have touch points to the AFNet but have a local system owner who is designated as the CNDSP. In cases such as this, both the local system owner as well as 24th Air Force units acting as the Air Force Enterprise CNDSP, i.e. 33 NWS, 561 NOS, 83 NOS and 26 NOS, can all be considered "organic defenders" in terms of having a responsibility for defending that system and contributing to mission assurance.

The hunt concept, however, is an active, more mission focused approach to defense; CNDSP, conversely, is a broader network focused approach. As such, how can Air Force enterprise CNDSP forces be brought to bear against an adversary within the hunt concept? The answer is through the employment of a Defensive Cyber Operations Tactical Coordinator (DCO-TC). The DCO-TC works in support of an Air Force mission to fuse hunt team efforts with other available defensive capabilities. As part of the planning process to stand up the enduring hunt mission, an analysis of mission pertinent actions and effects available within both local and enterprise CNDSP forces must take place. These Pre Approved Actions (PAAs) can then be executed by the DCO-TC on delegated authority from the local Designated Approval Authority (DAA) and 624 OC respectively. The 33 NWS, 83 NOS, 561 NOS and 26 NOS are formally notified of the delegated authority via reference to a Mission Pack (MP) published with the 624 OC Special Instructions (SPINS). Figure 1 (below) shows a hierarchical structure of the employment of the DCO-TC. Note that the DCO-TC is NOT in command of the CNDSP units, but similar to a TAC-P calling for Close Air Support (CAS) from an F16 in close orbit, the DCO-TC only has the authority to call for specific actions within the boundaries detailed in the Mission Pack.

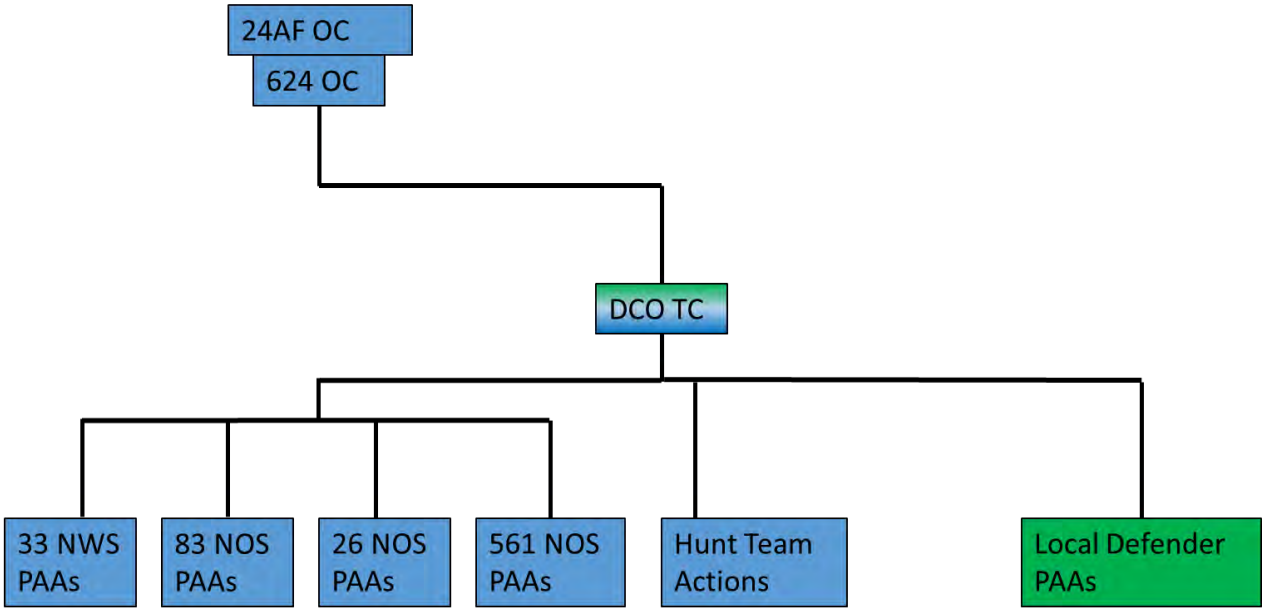



Figure 1.

The DCO-TC construct has been successfully employed at both Exercise TERMINAL FURY and RED FLAG and now has operational precedence in the form of an enduring mission in support of Air Mobility Operations. This had led to the validation the DCO-TC and subsequent publication of Flash Bulletin 12-12, *DCOTC Planning and Execution for AFTTP 3-1.CWO* by 561st Joint Tactics Squadron at Nellis Air Force Base.

4. As this approach is based off active engagement with adversaries inside the friendly network, there are many opportunities to characterize enemy activity by monitoring and observing the behavior of the APT to develop an understanding of their TTPs. Gathering this intelligence on the enemy will help in both the development of active hunt TTPs to counter a specific enemy as well as informing configuration changes at both the local and enterprise level in order to offer enhanced resiliency against a known enemy.

**COUNTERARGUMENT**

1. Hunt missions are extremely resource heavy and the lead time required to stand up a hunt mission in support of an Air Force mission can take in excess of six months. Additionally, this concept is not something that can be employed for a finite amount of time to fix a problem and then be extracted. Hunt missions are enduring in nature and need to remain in place to assure the mission by actively engaging adversary cyber activity in a specific AOR. The concern is that the success of previous hunt operations has led to an increase in opinion that this is the best approach to providing cyber defense. But with limited resources, in what areas does 24th Air Force stand up these missions? Critical AOCs? All AOCs? Air Defense Systems? ISR platforms? There is not enough resources to cover everything so it then becomes a priority issue.

2. The success of the hunt concept could start to shift focus from CNDSP efforts towards active defense, particularly as there is more convergence with air operations in terms of comparing Active Defensive Counter Cyber to Defensive Counter Air etc. It will resonate more with existing

operational doctrine and military leaders with little to no technical background can easily buy into its successes. The danger, however, is that there could be a detraction from efforts to aim towards a hardened and impregnable enterprise solution. Notwithstanding the fact that this is probably unachievable and realistic across the whole enterprise, striving towards the most resilient and robust network possible should remain an aim of 24th Air Force. We should not let the enemy into our networks simply because we have a world class technique of pushing them out again.

## CONCLUSION

Cyber hunt strategies are essential in providing mission assurance on specific key cyber terrain, hence why United States Cyber Command is making them a core part of the Cyber Protection Team. For maximum effect, however, they should not be employed in isolation. Active defensive counter cyber efforts should be layered with traditional CNDSP activities, at both the local and enterprise level, in order to achieve maximum cyber defense in depth in support of the projection of Air and Space power. Headquarters Air Force (HAF) needs to prioritize where the hunt mission is employed as this finite resource cannot be stretched to provide protection to every area of the AFNet and every enclave on a permanent basis. Finally, it is absolutely imperative that the success of cyber hunt missions does not detract from the requirement to keep the AFNet as robust and resilient as possible. Traditional CND activities are still as important, if not more important, than they have ever been in the past. These efforts should continue in parallel to refining hunt strategy and TTPs.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

1. Jabbour, Kamal , Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no.2 (2011), p61.
2. National Institute for Standards and Technology, “Managing Information Security Risk” (2011), appendix B-1.
3. Joint Publication 1-02, *DoD Dictionary of Military and Associated* Terms (2013), p64
4. Chairman of the Joint Chiefs of Staff , *Joint Vision 2010*, (1996).
5. 67 NWW, *PERFORMANCE WORK STATEMENT For INTEGRATED AFNET OPERATIONS AND SERVICES* (2012), p2.
6. Department of Defense, *Strategy for Operating in Cyberspace* (2011), p1
7. FBI Cyber Division, *APT Actors Increased Interest in the Aviation Industry,* (2013), p1
8. Department of Defense, *DoD Policy and Responsibilities for Critical Infrastructure*, DoD Directive 3020.40 (2012), p18
9. AFDD 3-12, (2010), p7
10. JP 3-10, *Countering Air and Missile Threats* (2012), chapter 3, p20
11. JP 3-10, *Countering Air and Missile Threats* (2012), chapter 3, p21
12. USCYBERCOM, *Cyber Protection Team Concept of Employment* (2013), p9
13. USCYBERCOM, *Cyber Protection Team Concept of Employment* (2013), p5

## BIBLIOGRAPHY

USCYBERCOM. *Cyber Protection Team Concept of Employment* Version 1.2 (2013)

Joint Publication 5.0. *Joint Operational Planning* (2011)

AFDD 3-12 *Cyberspace* Operations (2010)

Jabbour, Kamal , Ph.D. and Muccio, Sarah , Ph.D.. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no.2 (2011)

Maj David Neuman, *Flash Bulletin 12-12*, "DCOTC Planning and Execution" (2012)

National Institute for Standards and Technology, "Managing Information Security Risk" (2011)

Joint Publication 1-02, *DoD Dictionary of Military and Associated* Terms (2013)

Chairman of the Joint Chiefs of Staff, *Joint Vision 2010*, (1996)

Department of Defense, *Strategy for Operating in Cyberspace* (2011)

Joint Publication 3-10, *Countering Air and Missile Threats* (2012)

FBI Cyber Division, *APT Actors Increased Interest in the Aviation Industry,* (2013)

Department of Defense, *DoD Policy and Responsibilities for Critical Infrastructure*, DoD Directive 3020.40 (2012)

Cryderman, Jay. "CY-39 Interceptor Weapon System Cyber Vulnerability Assessment (CVA/HUNTER) Architecture, version 1.0". 92 IOS, (2013)

# Bring Your Own Device: Arguments For and Against DoD Use

Major Samuel N. Miller, US Air Force, AMC/A6E

**ABSTRACT**

The Department of Defense (DoD) is currently looking to cut costs where possible after drawing down from contingency operations in two separate theaters. The concept of Bring Your Own Device (BYOD), which allows users to "choose the devices, programs and services that best meet their personal and business needs, with access, support and security supplied by the (DoD), often with subsidies for device purchases",[1] is at first glance an appealing solution. However, the DoD information and fiscal environments present unique challenges that would require the implementation of an adequate, secure technical solution, and a change in policy to encourage user buy-in and imply willingness to accept a certain amount of risk.

**PROBLEM STATEMENT**

1. A 2013 study by the Pew Research Center found that, for the first time, over half of the American adult population owned a smartphone or tablet, and over 90% owned a cell phone of some sort, up from 65% in 2004. This percentage linearly increases for younger generations: approximately 97% of 18-24 year-olds own a cell phone.[2] According to additional studies, over 90% of smartphones and tablets being shipped today are running the Apple and Android operating systems.[3] The user experience for these operating systems significantly differs from what the DoD has largely maintained as the standard for its workforce since the mid-to-late 1990's: standardized desktops running Microsoft-based operating systems.

Many corporations, businesses, and even educational institutions have attempted to capitalize on employee and student satisfaction and productivity while saving on device and service costs by permitting BYOD in the workspace. It is estimated that over 62% of all U.S. employees use their own smartphone for work purposes every day, and over 90% at least weekly. Furthermore, over 90% didn't receive any compensation for these devices,[4] and this trend has not gone unnoticed. A recent Gartner study estimates that by 2017 half of all employers will require employees to supply their own device for work purposes in a model where BYOD is effectively written into the employer's contract.[5]

Adopting a similar model within the DoD certainly could, on the surface, realize significant cost and manpower savings. As an example of potential savings, the Air Force's Air Mobility Command (AMC), currently maintains an inventory of approximately 46,500 desktops and 16,500 laptops for its personnel. Its Directorate of Communications attempts to refresh approximately 25% of these devices at average cost of about $830 per device every 4 years, or about $208 per device per year on hardware alone.[6] From a software perspective, the DoD recently spent $617 million in 2012 on a 3-year Joint Enterprise License Agreement (JELA) with Microsoft, effectively ensuring the services will be using Microsoft's standard suite of products through 2015.[7]

2. The DoD IT processing environment presents challenges not seen in the commercial and education sectors. The DoD has policies and tools to implement and enforce user authentication, information assurance, configuration management, and device and transmission path security for all devices that connect to the DoD Information Network. Current DoD policy specifically states that "personally owned or contractor owned [Commercial Mobile Devices] must not be used to

transmit, receive, store, or process DoD information or connect to DoD networks", [8] which has effectively limited pursuit of any BYOD endeavor.

In addition to the moratorium on personally-owned and contractor-owned mobile devices, certain handling restrictions exist for the bulk of government-owned data. The processing of Confidential Unclassified Information (CUI) or higher on government-owned CMDs requires data-at-rest (DAR)[9] and data-in-transit (DIT) encryption.[10] CUI at a minimum requires Federal Information Processing Standard 140-2 encryption, and most commercially available mobile devices and supporting solutions are not generally equipped to meet this standard (DISA STIG WIR1445-01). Devices without proper encryption standards are subject to confiscation and/or wiping if data higher than the prescribed classification level finds its way onto the device.

Data is not the DoD cyber community's only concern. The DoD currently has tools in place to actively manage, monitor, and update computer networks and systems to ensure policy compliance. The ability to make significant administrative changes on any managed device is significantly limited to the user, and mitigations are in place to quarantine any compromised systems. Most commercial mobile devices currently popular on the market today were not envisioned as enterprise devices with central management and tight configuration control. The ability to download nearly any application and customize today's most popular commercial mobile devices in accordance with user desire runs counter to current DoD policy.

Additionally, most commercial mobile devices are configured out-of-the-box not for security, but for usability. Location-service based software that broadcasts location of the device is often activated by default on many mobile operating systems. Also, the open-source Android operating system, can and often is, customized in many different ways depending on vendor.
Furthermore, some DoD missions require data and network reliability fundamentally not conducive to a mobile environment, such as that in a Sensitive Compartmented Information Facility, or otherwise deemed location-sensitive by the information owner. Some data and information may require a degree of assurance and reliability that requires wholly government-controlled assets.

Additionally, the question of connectivity for BYOD devices within the workplace itself would need to be addressed. As mentioned, current DoD policy does not allow personally owned CMD's to connect to DoD networks. Also, commercial high-speed cellular and Wi-Fi coverage, typically required for BYOD, is often not prevalent on bases in more remote locations.

3. Personnel and processes are currently not aligned to support a BYOD environment in terms of device and application support. In the Air Force, the 3,000-person 3D1X1 career field (Client Systems), is dedicated to supporting these government-provided laptops and desktops, and two others (3D1X2, 3D1X7) devote at least some of their manpower and time towards the supporting infrastructure. Current Air Force schoolhouse curriculum for the 3D1X1 career field does not provide Apple or Android training for cyber maintainers, and any knowledge concerning non-Microsoft or Blackberry Commercial Mobile Devices is either locally- or self-taught. Freeing up personnel from the responsibility of supporting government-provided devices and supporting infrastructure could result in significant manpower savings.[11]

Additionally, the DoD's ability to produce and maintain applications for BYOD devices would need to be closely examined. Specialized user applications for all end-user government-owned devices are generally procured or developed through a DoD-vetted evaluation process that is generally not rapidly responsive. As of the time of this writing, the Air Force Designated Approval Authority has approved 350 mobile applications for Air Force-owned iOS devices, in a process that has taken anywhere from 15 to 180 days, and approved apps are currently hosted on its applications store. None have been approved for Android devices.[12] DISA's mobility program currently supports 16 mobile applications and is in the process of vetting more than 90 additional applications.[13]

In the Air Force, the 500-man 3D0X4 career field responsible for programming currently does not focus on application development for iOS and Android operating systems, although they maintain competencies in HTML, JAVA, and other usable programming languages. Additionally, this career field is currently largely organized to support specific missions, such as the 375 Communications Support Squadron's support to AMC, and not the community at large.[14] The ability to produce, approve, host, and distribute specialized applications to support a sea change towards a BYOD environment would require augmentation.

**RECOMMENDATION**

1. Allowing users to choose any mobile device with any operating system, and subsequently providing applications and secure, mobile access to relevant data in a manner supported by all operating systems, would likely be cost prohibitive. As long as the DoD continues to levy requirements for protecting government data from unwanted access, and as long as it requires specific non-commercially-available applications, it will be very difficult to allow for a pure BYOD environment, where users can bring in any device with any operating system. However, providing a list of devices and operating systems to choose from in a Pick-Your-Own-Device model (PYOD) that the DoD is willing to support may be more feasible. I recommend supporting the two most popular operating systems: Apple iOS, and Android.

The first step in moving towards a PYOD model would be to perform a business case analysis that factors in the user community that must remain in the current processing environment of government-owned end-user devices and infrastructure due to the sensitivity of their data and work. This cost of continuing to support this community, plus the cost of transition to and sustainment of a new PYOD model that potentially makes users more productive will be needed to determine cost effectiveness.

Gaining user buy-in may be the most difficult challenge. Many users may not already have devices and operating systems supported by a selected DoD-mandated management solution. Additionally, many users may not initially be willing to cede even partial control and monitoring of their devices to a government entity. A solution to this may be to give them monetary incentive to purchase and maintain devices, and I believe that this can be accomplished by providing these users access to the Blanket Purchase Agreement (BPA) the Army and Air Force has with major cell phone vendors to get devices and service for a significantly discounted rate.

As of January 2014, the minimum price for an individually obtained cell phone plan with 450 minutes per month and unlimited text and data is $70 per month.[15] The same level of service

through the BPA can be obtained for only $45 per month.[16] Initial purchase and refresh of devices through the BPA are also generally provided at a significantly reduced, and sometimes free, cost depending on the vendor and device. Expanding this agreement to cover individuals as they purchase their devices and plans of choice could be an incentive for many to accept a certain amount of government handling of their otherwise personal devices, including possible confiscation in the event of device or data compromise.

2. Before the devices begin processing government information, a mobile device management and mobile device content solutions must be established that enables secure transmission over commercial with and processing of government data on CMDs in compliance with DoD policy. A well known government-provided mobile device implementation that has successfully met the DoD's current encryption and management standards is the commercially-available Blackberry Enterprise Solution (BES), widely adopted by all DoD services and agencies since the beginning of the millennium. The BES, originally designed to provide users mobile access to corporate e-mail via commercial networks and later expanded to provide additional applications, provides DIT, DAR for up-to-CUI data, and access to government data via backbone infrastructure. Additionally, Blackberry has recently come out with the DISA-approved protected container application with DAR encryption which is advertised as ensuring "work information is kept separate and secure so that users' personal apps cannot access work information, and work information cannot be copied and pasted into personal apps or e-mail".[17] Unfortunately, Blackberry as a company has suffered a recent decline in the commercial mobile device market share, to less than approximately 1% in 2013, due largely to its significantly limited capacity to provide the application-centric environment popular with Android and Apple iOS users that control the market. Currently, potential PYOD users are largely not using Blackberry devices for their personal lives.

However, the recent DISA approval of Apple iOS 6 and Samsung Knox devices running Android on variations of Samsung Galaxies have opened the door for implementation of non-Blackberry solutions in a mobile device management framework, similar to what Blackberry has implemented.[18] DISA has recently contracted vendors to provide a mobile device management solution, MobileIron, and a protected container application, Fixmo, to support iOS and Samsung Knox devices.[19,20] Although the specific architecture has yet to be fully codified, presumably it will work much in the same way as Blackberry's solution in providing a logically protected container for government data processing and reachback to government data via commercial networks. The NSA's mandate for the implementation of Suite B encryption by 2015 could allow for Secret, and possibly higher, data and processing on these devices.[21] Also, a certain amount of configuration control could optionally be provided on the device to lock down undesirable default features, such as location services.

Additionally, the supporting infrastructure to provide connectivity on each base would need to be addressed. The DoD could revoke their current policy and enable a solution that would allow PYOD devices to connect directly to the current network infrastructure, but give up any potential savings that might be gained by abandoning said infrastructure. An alternate solution may be to competitively lease land where needed on DoD installations for cellular carriers to erect cell towers providing high-end service for the required population. This may be appealing to vendors, as improved coverage could make them more competitive for potential PYOD users. Certain

facilities may be impervious to cellular signals due to previous hardening efforts, and will require additional infrastructure support. Alternately, commercial carriers could provide commercial internet connectivity in locations where other options are not available. Installations in areas with no previous infrastructure can cost upwards to $15,000.[22]

3. Finally, realigning and augmenting the personnel and processes required to support a BYOD environment will be necessary. I would recommend modifying the BPA to include contract device hardware support, and restructure the services' career fields to find a correct balance between contract and government support.

The ability to produce DoD-specific applications for mission and other purposes may be one of the larger challenges. The 375th Communications Support Squadron at Scott AFB has established some organic capability to develop mobile applications, and has begun tracking development and production costs in an effort to assist any subsequent manpower studies aimed at supplementing the career field. As an example, in their efforts to develop, upgrade, and provide technical support for a single iOS application that collects and displays Morale, Welfare, and Recreation event data from participating Air Force bases, the My Military Communities app, available on the iTunes store, was developed by a unit that spent nearly 1000 man-hours at an estimated cost of $65,000.[23] A full assessment of the current and desired capacity to produce, approve, and field DoD-wide and mission-specific applications in a timely fashion must be assessed, and this assessment should not only include coding standards and a response process for rapid approving application development, but also should possibility of incorporating user-developed (i.e. non-programmer) applications.

**COUNTERARGUMENTS**

1. The argument that users will be willing to provide the DoD access, and possible control, to their personal and personally funded devices, especially in light of the recent disclosure of government surveillance methods, may be a show stopper for a PYOD model. If a significant portion of the potential population won't "buy in", or expects a more significant reimbursement, such as a device allowance similar to a clothing allowance, then the significant savings proposed may be lost. A potential mitigation strategy may be the concept of Corporately Owned, Personally Enabled (COPE). COPE implies DoD-owned devices in a framework that supports personal use. However, using the data plan described previously in the BPA construct, assuming suitable COPE devices could be procured or refreshed at $100 per year, and assuming the cost to provide supporting infrastructure for COPE device use in the workplace, e.g. Wi-Fi, cellular coverage, etc., is approximately the same as our current cost, then the cost per COPE device is approximately $400 per year *more* than our current device refresh strategy.

2. The argument that there even is a need to change is very difficult to quantify. At present, our current government-provided, largely-Microsoft model, although expensive, is sustainable for the foreseeable future. Government-provided devices are currently able to meet the mission, and processes and personnel to sustain these devices have been established. Fiscally, the future remains unclear, and the 3-year JELA with Microsoft is a sunk cost through 2015.[24] A similar enterprise licensing agreement would likely need to be established with the mobile device management and mobile content management solutions, as well as with any necessary enterprise-wide applications. Additionally, given the DoD's mission, turning over control of infrastructure

and devices to contract service providers, especially when and where a certain level of responsiveness may be required to mitigate mission downtime, might be a bridge too far.

3. Finally, the transition costs of standing up a BYOD/PYOD model may be a non-starter, particularly in this current fiscal environment. Even if all users were able to cut over from government-owned devices one day to personally owned devices the next, there would still be long lead-up time to prepare the environment for such a construct. Checklist items such as ensuring widespread connectivity, preparing the environment for application development, and training support personnel, generally two years in the Air Force process,[25] would take some time to implement. A transition period where resourcing both the legacy and new BYOD/PYOD models would need to occur.

## CONCLUSION

The concept of BYOD presents an interesting opportunity to get the DoD out of the business of supporting a large amount of IT equipment. The technology exists to implement it, and the recommendation provided could lead to an adequate, secure technical solution. However, it is the author's opinion that an adequate Business Case Analysis will be required before making the leap. The costs to transition to such a construct may be more than what the Air Force is willing to spend.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] Proffitt, Brad. "Forget Bring Your Own Device – Try Corporately Owned, Personally Enabled", 1.
[2] Smith, Aaron. "Smartphone Ownership 2013", 1.
[3] Netmarket Share. "Mobile/Tablet Operating System Market Share", 1.
[4] Cisco Systems. "BYOD Insights 2013: A Cisco Partner Network Study", 4.
[5] Gartner, Incorporated. "Gartner Predicts That by 2017, Half of Employers Will Require Employees to Supply Their Own Device for Work Purposes", 1.
[6] Howell, Robert. Chief, Programming & Budget Branch, Headquarters Air Mobility Command Directorate of Communications.
[7] Lyle, Amaani. "DoD Awards First Joint Licensing Agreement", 1.
[8] DISA Security Technical Implementation Guidance (STIG) WIR0010-01.
[9] Grimes, John G. DoD Chief Information Officer. To Secretaries of the Military Departments. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage, 2.
[10] DoD Instruction 8220.02, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, 12.
[11] Campbell, CMSgt Charles E. AMC Cyber Ops Functional Manager, Headquarters Air Mobility Command Directorate of Communications.
[12] Stady, Major Thomas. Chief, Technology Advancement Branch, Headquarters Air Mobility Command Directorate of Communications.
[13] Defense Information Systems Agency (DISA). "DISA Announces Initial Release V1.0 of DoD Unclassified Mobility Capability", 1.
[14] Peterson, Captain Joseph S. Chief, Software Engineering, 375th Communications Support Squadron.
[15] Wall Street Journal (WSJ). "WSJ's Wireless Savings Calculator".
[16] Air Force Portal, "Blanket Purchase Agreement (BPA) - Cellular Service and Devices".
[17] Thuermer, Karen E. "Clearing the way for Mobile Security", 25.
[18] Ibid, 24
[19] Ibid, 25.
[20] Walker, Ward A. Chief Technology Officer, Headquarters Air Mobility Command Directorate. of Communications.
[21] Willson, Donald. "Suite B Encryption Talking Paper".
[22] Walker, Ward A. Chief Technology Officer, Headquarters Air Mobility Command Directorate. of Communications.
[23] Peterson, Captain Joseph S. Chief, Software Engineering, 375th Communications Support Squadron.
[24] Lyle, Amaani. "DoD Awards First Joint Licensing Agreement", 1.
[25] Campbell, CMSgt Charles E. AMC Cyber Ops Functional Manager, Headquarters Air Mobility Command Directorate of Communications.

## BIBLIOGRAPHY

Air Force Portal, "Blanket Purchase Agreement (BPA) - Cellular Service and Devices". Accessed 9 February 2013. https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC1335690FB5E044080020E329A9.

Campbell, CMSgt Charles E. AMC Cyber Ops Functional Manager, Headquarters Air Mobility Command Directorate of Communications. Multiple Interviews between 6-27 January 2014.

Cisco Systems. "BYOD Insights 2013: A Cisco Partner Network Study". Cisco Concierge. March 2013.

Defense Information Systems Agency (DISA). "DISA Announces Initial Release V1.0 of DoD Unclassified Mobility Capability". Press Release, 16 January 2014. http://disa.mil/News/PressResources/2013/Mobility-Capability.

DISA Security Technical Implementation Guidance (STIG) WIR0010-01. General Mobile Device Overview. 26 July 2013.

DISA Security Technical Implementation Guidance (STIG) V-12164. Blackberry Secure Technical Implementation Guidance. 12 March 2013.

DoD Instruction 8220.02, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies. 3 November, 2009.

Gartner, Incorporated. "Gartner Predicts That by 2017, Half of Employers Will Require Employees to Supply Their Own Device for Work Purposes". http://www.gartner.com/newsroom/id/2466615.

Grimes, John G. DoD Chief Information Officer. To Secretaries of the Military Departments. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage. Memorandum, 3 July 2007.

Howell, Robert. Chief, Programming & Budget Branch, Headquarters Air Mobility Command Directorate of Communications. Multiple Interviews between 6-27 January 2014.

Lyle, Amaani. "DoD Awards First Joint Licensing Agreement". Armed Forces Press Services, U.S. Department of Defense. Press Release, 28 December 2012. http://www.defense.gov/news/newsarticle.aspx?id=118887.

Netmarket Share. "Mobile/Tablet Operating System Market Share" Accessed 9 February. http://netmarketshare.com/mobile-market-share?qprid=8&qpmr=100&qpdt=1&qpct=3&qpcustomd=1&qptimeframe=M.

Ordonoff, Mark S. Chief Information Assurance Executive, Defense Information Systems Agency. Memorandum for Distribution, SUBJECT: Department of Defense Mobile Governance. 3 May 2013.

Peterson, Captain Joseph S. Chief, Software Engineering, 375th Communications Support Squadron. Interview on 31 January 2014.

Proffitt, Brad. "Forget Bring Your Own Device – Try Corporately Owned, Personally Enabled". ReadWriteWeb. 19 October 2012. http://readwrite.com/2012/10/19/forget-bring-your-own-device-try-corporate-owned-personally-enabled#awesm=~ouLOgRTIHA3Xi2.

Smith, Aaron. "Smartphone Ownership 2013". Pew Internet and American Life Project, 5 June 2013. http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx

Stady, Major Thomas. Chief, Technology Advancement Branch, Headquarters Air Mobility Command Directorate of Communications. Multiple Interviews between 6-27 January 2014.

Thuermer, Karen E. "Clearing the way for Mobile Security". Military Information Technology 17, Issue 9 (December 2013) [23-25].

Wall Street Journal (WSJ). "WSJ's Wireless Savings Calculator". http://graphics.wsj.com/PhonePlan/?mg=inert-wsj. Accessed 3 February 2014.

Walker, Ward A. Chief Technology Officer, Headquarters Air Mobility Command Directorate of Communications. Multiple Interviews between 6-27 January 2014.

Willson, Donald. Architecture and Engineering Branch, Headquarters Air Mobility Command Directorate of Communications. "Suite B Encryption Talking Paper". 30 April 2012.

USCYBERCOM Best Cyber 300 Paper Recipient for FY 14
Monitoring: Protection vs Privacy in the Cyber Realm
Maj Jessica A. Rose

**ABSTRACT**
President Obama wrote: "Our national security depends on our ability to share the right information, with the right people, at the right time" [1]. Conversely, this information could fall into the proverbial wrong hands as the United States faces worldwide threats that are expanding globally in both complexity and opportunity. There is a clear and present need to leverage cyber capabilities that specifically include monitoring and tracking electronic communications in order to intercept critical information, identify enemy combatants and thwart attacks before they occur.

This necessity is in conflict with long-standing principles of a right to privacy and democratic freedoms of our nation's citizens. Individuals and corporations vary widely in their willingness to relinquish privacy, and this is highly dependent on the perceived benefits of monitoring. Monitoring should not happen without transparency, oversight, and accountability between private citizens, organizations and governments. This will ensure that there is a reasoned and mutually agreed upon balance between providing security while protecting civil liberties, diplomatic relations and economic interests.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**
Current monitoring practices are unsustainable due to the following two major factors:
1) Current US Constitutional and Legislative laws are not keeping up with technology
2) Citizens are concerned about their privacy being violated without just cause

The 'right to freedom' and to privacy enshrined in the Constitution are fundamental ideals that have helped define America since its birth. Specifically, the Fourth Amendment protects US Citizens from unreasonable searches and seizures by the government (note this does not cover searches from private entities). The Amendment reads:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

This raises two major questions : whether electronic communications are within the scope of the protection conferred by this Amendment on citizens' "*persons, houses, papers, and effects"*, and what constitutes a citizen's *"reasonable expectation of privacy"*.

To date, the US Supreme Courts' rulings on the first question have followed a very narrow interpretation of the text in which only physical material effects are protected by the Fourth Amendment—nothing within the virtual technological realm we now live in. Supreme Court Justice Louis Brandeis, writing the dissenting opinion for Olmstead vs. US minority in 1928, expressed the intuition that as private life was just starting to be conducted over telephone wires, it would become necessary, in order to protect citizens' privacy to the same extent envisioned by

the framers of the Fourth & Fifth Amendments, to translate those amendments to current times.[2] This has not happened. As a result, we are left with the US Supreme Court's strict adherence to the letter of the law, which arguably fails to uphold the spirit of the law.

The US Supreme Court's literal-mindedness regarding technological advances has additional ramifications. Further to the text of the Fourth Amendment cited above, a search is considered illegitimate when the government violates a person's "reasonable expectation of privacy", where "expectations of privacy are established by general social norms"[3]. Currently, the US Supreme Court's interpretation allows for nearly no legally legitimate expectation of privacy for any communication or activities that ordinary members of the public use on widely available technologies.[4] These ubiquitous technologies include phones, GPS, cameras, computers, and could be interpreted to include the internet and social media. The Court's justification is that these technologies traverse the open public space and are not confined to an individuals' private nor federal protected space, and that any means of intercepting information that is available to the public can be used by governmental intelligence and law enforcement agencies. Since extremely sophisticated monitoring equipment can be obtained on the consumer market and civilian hackers can be found anywhere in cyberspace, this permits the US Government to observe, collect and analyze everything conveyed by the above technologies--conversations, tracking/monitoring, identification, emails, surfing, metadata--all while staying within the bounds of the US Constitution without violating US Citizen's privacy rights. While material-related privacy in ones' own home still stands, US citizens are left with very little technology-related privacy, if any, according to current interpretation of the US Constitution.

Since Constitutional laws have not been meaningfully adapted for the advent of electronic communications technology, Congress has tried to fill these gaps with Legislative Laws such as the Privacy Act of 1974, the Electronic Communications Privacy Act in 1986 and the Freedom of Information Act in 1996. One of the major responses to September 11, 2011 was that Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, more commonly known as the USA Patriot Act. The act's overall intent was to strengthen national security by directly giving more authority to various federal agencies charged with carrying out operations that purport to protect the nation—including tools such as monitoring communications.

The USA Patriot Act takes advantage of the Fourth Amendment clause that covers the "emergency aid exception". A warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[5] This exception is made to override the lengthy judicial process of getting a warrant when there is a time-sensitive need to protect & preserve life and avoid serious injury.[6] Proponents of intensive monitoring practices believe that the stated goal of protecting and defending the United States against terrorist and foreign intelligence threats falls under this "protect & preserve life" exception, in particular because cyber actions that could cause grave harm to the United States happen so quickly. However, the burden is on the government to justify warrantless searches and seizures occurring under this exception, and many opponents of these practices consider that the government has not met this burden of proof.

A useful way to evaluate the legitimacy of the USA Patriot Act is to view it in light of the principle of proportionality, a key principle in the examination and application of US Law. This principle states that, in order to evaluate whether a law is just and can be applied to a situation, there are two factors that must be weighed against each other. In the context of what constitutes a reasonable search under the Fourth Amendment, the two factors are: 1) the scale of intrusion on an individual's privacy rights and 2) legitimate government interest such as public safety and national security.[7] In order for a search to be legitimate, the benefits to national security should be great enough to compensate for the intrusion on the individual's privacy. In this respect, one key problem with the USA Patriot Act is that the benefits cannot be clearly demonstrated because the scope is too vaguely defined.

Citizens vary widely in their willingness to relinquish privacy, and this is highly dependent on the perceived benefits of monitoring practices.[8] Most consumers are familiar with the practice of companies tracking online habits and purchases, which provides them with personalized content and enhanced online experience. Citizens are also generally receptive to the idea that certain levels of monitoring empower law enforcement and federal organizations to fight crime and improve public safety. However, many citizens are concerned that they are being asked to give up too much in exchange for too little. These concerns are two-fold. One, citizens have no way of knowing what is the level of monitoring placed upon them because of the "emergency aid expectation" clause. This clause is invoked by agencies performing monitoring operations on the reasoning that in the world of cyberspace, threats can emerge so quickly, there may not be time to obtain a warrant and inform US citizens of "*the place to be searched, and the persons or things to be seized*." While this can be a legitimate justification for certain operations, it is hardly reasonable for ongoing long-term operations. Second, citizens are not informed of what are the concrete benefits of these operations because results are systematically classified by the government. This makes it very difficult for them to evaluate whether the degree of intrusion on their privacy rights is ever really compensated by the outcomes of the legitimate government interests (national security and public safety).

In fact, there is evidence that the verdict is not positive. The Presidential Privacy and Civil Liberties Oversight Board report, along with the Senate Judiciary Committee chairmen's views, conclude that "the [USA Patriot Act] Section 215 bulk phone records program has not been critical to our national security, is not worth the intrusion on Americans' privacy, and should be shut down immediately".[9] There have also been some very public failures: "We have been repeatedly told that these surveillance programs would have been able to stop 9/11, yet the NSA didn't detect the Boston bombings—even though one of the two terrorists was on the watch list and the other had a sloppy social media trail. Bulk collection of data and metadata is an ineffective counterterrorism tool".[10] Based on this, current known monitoring operations do not seem to be benefiting the public.

Finally, there is great potential for abuse of power by individuals and misallocation of resources due to investigators' personal prejudices. The latest example of this issue is the case in which the DoD collected intelligence on members of harmless organizations such as Planned Parenthood, antiwar groups and nonviolent Muslim conferences.[11] At the very least, this represents a serious misallocation of resources, and at worst, ideological and prejudice-based targeting practices that are not acceptable in a pluralistic democratic society.

**RECOMMENDATIONS**

Moving forward, we can outline two key principles: that laws should reflect the current state of communication technologies and their use by citizens, and that monitoring should not happen without transparency, oversight, and accountability to the nation's citizens.

In practice, there are two concrete solutions that can be implemented:
1) Set up a legal review process to update US laws for life in the 21st Century;
2) Establish guidelines for oversight and accountability within and across organizations that are involved in monitoring operations, starting at the level under our control: the US Air Force.

As described above, the disconnect between technological developments and the US legal and regulatory systems have left members of the public at risk of privacy breaches. The ideal long-term solution would be to trigger a process of reviewing and revision of US laws in light of today's technological capabilities. This may seem overly ambitious and difficult to achieve, but there is precedent for such an undertaking. Our European allied neighbors have put a lot of effort into developing a Convention for the Protection of Human Rights and Fundamental Freedoms, which takes into account the people's extensive use of electronic communication channels. The European Union is preparing to sign the agreement, creating a common European legal space for over 820 million citizens in the 47 member states in the Council of Europe.[12] In particular, this Convention addresses privacy issues in:

> *Article 8 - Right to Respect for Private and Family Life -- 1. Everyone has the right to respect for his private and family life, his home and his* ***correspondence****. (emphasis added)*[13]

While not a catch-all, a key change relative to previous laws is the addition of "correspondence", which can be applied both in the physical and virtual world. This is at least a start in the right direction to grant protection to individuals in their private communications, while still allowing exceptions to accommodate the need for public safety and national security.

Revising the laws should go hand-in-hand with enhanced procedures to ensure transparency, oversight, and accountability, which will guarantee that the law is applied as intended. This involves three major components specifically: judicial transparency, Congressional oversight and some declassification of documents.

Judicial transparency is absolutely essential in order to preserve the democratic process. Currently, select US Courts such as the Foreign Intelligence Surveillance Court (FISA), act within a secret and closed system. This goes against the general judicial practice of holding courts responsible in case those courts (read: humans) make mistakes. "When that happens, the losing party has the right to appeal, and the erroneous decision is reversed. That process cannot happen when a secret court considers a case with only one party before it."[14]

Congressional oversight is also a basic requirement in order to ensure that citizens' interests (both in terms of their privacy rights and the use of their tax dollars) are protected. "America needs competent and effective intelligence-gathering agencies … and Congress must exercise prudent

and diligent oversight to assure the American taxpayer is getting what it's paying for."[15] Unfortunately, the tendency to over-classify documents is a major barrier to effective oversight. If too much of the documentation that describes monitoring methods and their results is classified and therefore inaccessible to the representatives of the public, it is difficult or even impossible to evaluate whether they are conducted with respect for the law and whether they are an effective use of public resources.[16] "Organizations such as the NSA need to change their culture of secrecy, and concentrate their security efforts on what truly needs to remain secret. Their default practice of classifying everything is not going to work anymore."[17]

Such a process, if it happens, will surely be lengthy and fraught with political difficulties, yet today's world, given the velocity of cyberspace, will not wait. We must therefore start implementing important changes at the level that we control: US military policies. The US military is constrained by US law as regards the outer bounds of what it is allowed to do, but this does not mean it cannot formulate its own inner bounds: there is no law precluding the military from exercising less power than it is legally allowed. There are historical instances where the military has taken the moral high road, and cyberspace needs not be any different. The US military needs to ensure it has clear and well understood cyber policies available for all personnel. These policies should cover what are the acceptable uses of monitoring practices, how to implement effective oversight methods, and how transgressions should be handled. For example, there should be internal procedures in place to enable personnel to report violations of the guidelines, so that the important civic function of whistleblowing can be performed without actually risking critical information leaks.

**COUNTERARGUEMENT**

Proponents of intensive monitoring practices are quick to point out that requiring transparency and increased oversight for what are quintessentially covert operations is counterproductive and can weaken or compromise the mission. Certainly, there is no telling the damage done to national security by leaks of classified information from spies like former FBI Intelligence Agent Robert Hanssen, informers from the US Military such as Army Private First Class Chelsea (born: Bradley) Manning and whistleblowers such as former CIA Agent & NSA Contractor Edward Snowden. Adding more people to the list of those who "need to know" can only increase the chance that some information will get out – the longer the pipe, the more chances it's going to spring a leak. Evidently, there needs to be a balance, and careful vetting of what information gets released to whom.

There is a similar concern that imposing legal limitations on what can and can't be monitored will cripple the intelligence gathering process and limit the effectiveness of these practices. This is true, but the same goes for conventional warfare practices. The US military chooses not to employ certain weapons capabilities (such as chemical or biological weapons) because, although they could effectively end conflicts more quickly, they are considered unacceptable among civilized nations. Just because something can technically be done does not mean it should be done – the ends do not justify all possible means. This line of argumentation actually underscores the need for a public conversation about what is acceptable in the cyber monitoring space. That decision cannot be left to the judgment of those who are responsible for carrying out the mission, because they are subject to a conflict of interest – by definition, any limitations will make their job harder.

Finally, there is the old adage: "If you aren't doing anything wrong, you shouldn't have anything to hide". Typical responses range from "If I'm not doing anything wrong, you have no reason to watch me", "The government keeps changing the definition of what's right or wrong" or "Someone might do something wrong with my information". Aside perhaps from the latter (which may be a legitimate concern), these rather glib responses miss the point, because they are based on the idea that the purpose of privacy is to hide wrongdoing. But as Bruce Schneier so eloquently puts it: "It's not. Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."[18] Indeed, as human beings, we crave privacy primarily because it makes us feel whole and empowered, while the lack of privacy makes us feel violated and out of control.

## CONCLUSION

Having acknowledged that some kinds of monitoring operations are essential for the security of our nation, we face a critical choice as to how they should be implemented; whether "surveillance is a secret, one-way panopticon or a mutual, transparent kind of coveillance that involves watching the watchers"[19] If our nation is to remain a free democratic society, the public must know what it is subjected to, how and what are the actual benefits received. Democracy does not work unless constituencies know what the government is doing on their behalf.[20] The German Justice Minister wrote "The more a society monitors, controls, and observes its citizens, the less free it is. In a democratic constitutional state, security is not an end in itself, but serves to secure freedom"[21]. Benjamin Franklin was deeply aware of this when he wrote in 1775: "They who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[22] While the government is acting within current Constitutional and Legislative laws, US citizens deserve to know what is going on to protect the fundamental democracy and freedoms we expect as Americans (otherwise the terrorists have already won).

## BIBLIOGRAPHY

Barrack Obama, *National Strategy for Information Sharing and Safeguarding*, December 2012, http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf

Jeffrey Rosen, "Technological Change and the Constitutional Future" in *Constitution 3.0 Freedom and Technological Change*, ed. (Washington, D.C: Bookings Institution Press, 2011), p 3.

Memorandum Opinion for the General Counsel - Department of Defense, *Fourth Amendment Implications of Military Use of Forward Looking Infrared Radars Technology for Civilian Law*, March 4, 1992, pp 43 - 45. http://www.justice.gov/olc/opiniondocs/op-olc-v016-p0041.pdf

Jeffrey Rosen, "The Deciders: Facebook, Google, and the Future of Privacy and Free Speech" in *Constitutions 3.0 Freedom and Technological Change*, ed. (Washington, D.C: Bookings Institution Press, 2011), p 71.

John Yoo, *Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose " Standard for Searches,* September 25, 2001. http://www.justice.gov/olc/docs/memoforeignsurveillanceact09252001.pdf

Michael Pettry, J.D., "The Emergency Aid Exception to the Fourth Amendment's Warrant Requirement", March 2011, assessed on May 10, 2014, http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/march_2011/copy_of_perspective

Administrative Office of the U.S. Courts on behalf of the Federal Judiciary, "What Does the Fourth Amendment Mean?" assessed on May 5, 2014, http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/fourth-amendment-mean.aspx

Sean Madden, "Tech that Tracks Your Every Move Can Be Convenient, not Creepy", *Wired,* March 10, 2014, http://www.wired.com/2014/03/designers-tracking-tradeoffs/

Even Perez, "Privacy Board: NSA telephone records program illegal", *CNN*, January 23, 2014, assessed April 21, 2014 from http://www.cnn.com/2014/01/23/politics/nsa-telephone-records-privacy

Bruce Schneier, "How the NSA Threatens National Security", *The Atlantic*, January 6, 2014, assessed April 21, 2014, https://www.schneier.com/essay-469.html

Christopher Slobogin, "Is the Fourth Amendment Relevant in a Technological Age?" in *Constitutions 3.0 Freedom and Technological Change*, ed. (Washington, D.C: Bookings Institution Press, 2011), pp 20-21.

Council of Europe, European Convention on Human Rights, assessed on May 10, 2014, http://human-rights-convention.org/

Convention for the Protection of Human Rights and Fundamental Freedoms, June 1, 2010, assessed on May 10, 2014, http://conventions.coe.int/treaty/en/treaties/html/005.htm

Elizabeth Goitein, "The Spying on Americans Never Ended," *Wall Street Journal*, June 6, 2013, assessed on April 22, 2014, http://online.wsj.com/news/articles/SB10001424127887324798904578529763558353462

Cynthia Lummis and Peter Welch, "Intelligence Budget Should Not Be Secret", *CNN*, April 21, 2014, http://www.cnn.com/2014/04/21/opinion/lummis-welch-intelligence-budget/

Cyrus Farivar, "If Bruce Schneier ran the NSA, he'd ask a basic question: "Does it do any good?" *ARS Technica*, August 7, 2013, assessed on April 26, 2014, http://arstechnica.com/tech-policy/2013/08/if-bruce-schneier-ran-the-nsa-hed-ask-a-basic-question-does-it-do-any-good/

Bruce Schneier, "The Spooks Need New Ways to Keep their Secrets Safe", *Financial Times,* September 5, 2013, assessed May 5, 2014, https://www.schneier.com/essay-449.html

Bruce Schneier, "The Eternal Value of Privacy", *Wired News,* May 18, 2006, assessed April 20, 2014, https://www.schneier.com/essay-114.html

Kevin Kelly, "Why You Should Embrace Surveillance, Not Fight It," *Wired*, March 10, 2014, assessed April 21, 2014, http://www.wired.com/2014/03/going-tracked-heres-way-embrace-surveillance/

Bruce Schneier, "NSA Secrets Kill Our Trust", *CNN*, July 31, 2013, assessed April 21, 2014, https://www.schneier.com/essay-435.html

Sabine Leutheusser-Schnarrenberger, "US Prism Scandal: 'Security is Not an End in Itself'", *Spiegel Online International*, June 11, 2013, assessed May 8, 2014, http://www.spiegel.de/international/world/minister-leutheusser-schnarrenberger-criticizes-us-over-prism-scandal-a-905001.html

Benjamin Franklin, "Pennsylvania Assembly: Reply to the Governor dated November 11, 1755" in *Votes and Proceedings of the House of Representatives, 1755-1756*, (Philadelphia, 1756), pp 19-21.

Bring Your Own Device (BYOD): Vulnerabilities vs. Effectiveness

Mr. Warren D. Stull (SAF/AAIE)

**ABSTRACT**

Today's Department of Defense (DOD) increasingly relies on collaborating and sharing information instantaneously. It saves lives, puts bombs on target, and ensures supplies deploy to the right place at the right time. In today's tight fiscal environment, the future of information sharing and collaboration relies upon new technologies replacing old technologies without compromising mission security and effectiveness. One new technology effort involves the DOD Commercial Mobile Device Implementation Plan, which is a cost effective approach to deploying mobile non-tactical applications within the DOD Enterprise, and depends on leveraging commercial off-the-shelf solutions. In 1997, the first successful mobility initiative involved BlackBerry devices supporting email. This initiative has since changed, and the Air Force is replacing BlackBerry devices with IOS and Android. DOD has pushed aggressively to deploy mobile devices to more than 600,000 users. However, DOD has not included a BYOD strategy[1]. BYOD offers the possibility of additional cost savings, enhanced productivity, and better information sharing and collaboration notwithstanding security liabilities and infrastructure costs required to implement such a strategy. Despite fiscal challenges, commercial best practices have successfully achieved 20-30% cost savings implementing BYOD. Due to shrinking budgets, DOD should consider mitigating vulnerabilities and deploying an effective BYOD solution.

**DESCRIPTION OF ISSUE/PROBLEM STATEMENT**

1. Analysts concluded that more than 75% of mobile applications fail even the most basic security tests[2]. With more than 1.2 million applications advertised on each of the IOS, Android and Microsoft stores it becomes impossible for any DOD entity to ensure that every application used on an approved device would not be the weak link in security. When consideration is given to incorporating a BYOD strategy, security concerns become even more complex as non-standardized device configurations get injected into the environment, and little is done to control the software installed on the mobile platform. In 2004, the FBI uncovered approximately 400 counterfeit Cisco routers shipped to the U.S. from China. Their sole purpose was to infiltrate U.S. Federal Government and private industry networks to disrupt service and deteriorate cryptographic infrastructure. These routers shipped to U.S. military installations and defense contractors such as Raytheon, who make key missile and weapons systems[3]. The counterfeit routers were an intricate, elaborate conspiracy with years of planning, and it took years for the FBI to prosecute the owners of the company, Syren Technology. Today, a hacker from China would not need to develop such a complicated plan. They could simply develop a mobile application that would appeal to the masses, inject a logic bomb into the application code with hopes that a Government Employee or Defense Contracting Employee using a Government sponsored BYOD device installed the software to deliver their payload. Software becomes the most critical vulnerability with mobile devices. An agency may consider thwarting the software vulnerability by developing all their applications in-house. Due to decreasing budgets and the sustainment and maintenance of these applications being cost prohibitive, more than 90% of industry takes advantage of third party Commercial Off the Shelf (COTS) software for their mobile BYOD strategies[4]. Mobile application security testing should include methods that determine the behavior of the software. This method of testing focuses on the analysis of what the code of the application is doing outside its normal functions and logic. It can also look for behaviors commonly utilized by hackers. Unfortunately,

this method of testing has not fully matured for mobile device applications and hackers constantly changed their strategies or delay their attacks by setting their activations periods out to a longer timeframe to bypass behavioral test emulators. Even if DOD were to perfect the art of application security testing, it would need to be an efficient, repeatable, expedient process as application vendors regularly release security patches and updates to their software.

A significant aspect of BYOD is securing data in transit and at rest. More than 4.5 million smartphones were lost or stolen in 2013[5]. Many of these devices did not have password protection and the data on these devices became vulnerable. Data resides in many locations from backend servers, in transit, and mobile device web browser cache. Many experts agree that data encryption of 128 bits or higher should enough to effectively deter potential hackers. However with no policies in place on where to store the private keys, if these keys remain on the device or in an application used on the device, the encryption becomes ineffective. Mobile applications that utilize HTML5 do not natively have the ability to encrypt code or data being sent to a mobile device, therefore, in transit data is at risk without other methods of security put in place[6]. It is important to understand that mobile web applications do not provide encryption for data at rest, encryption for application code, and do not encrypt data in transit end-to-end[7]. Mobile applications are also vulnerable to several attacks that personnel have become accustomed to not being a significant risk in typical desktop applications. Risks such as Cross-Site Scripting, which enables and attacker to inject scripting language into a web page. SQL Injections to attack databases through websites. Even XPath Injections to create malicious XML queries to steal data[8]. Data protection becomes even more critical when considering the possibility of classified information spillage. The NSA and DOD entities have released instructions on procedures to handle situations where classified data has leaked into an unclassified network, however these policies would need to be adjusted to apply to a BYOD strategy.

2. Securing a BYOD device extends beyond the device itself. There is the supporting infrastructure such as the Mobile Application Store (MAS), which provides access to a collection of approved applications and the Mobile Device Management (MDM), which provides the means to centralize the administrative management (e.g., auditing, alerting controls, remote wiping) of the devices. It is important to understand that the MAS and MDM are two separate entities; therefore, security requirement guides must be applied respectively[9]. As of today, risk mitigation of using MAS and MDM for BYOD within DOD has not been considered. Hosting these services on the DOD network to support BYOD raises concern for security. The owner of a privately owned device has the capability to connect to other application stores and perform security related configurations, such as authentication and connectivity that will most likely conflict with required settings pushed by MDM and risk data leaks. Not all configurations of mobile devices can be controlled by MDM, and the user can change the configuration of their personally owned device.

Commercial vendors release their latest and greatest gadget nearly every other month, and all of them have known security flaws. For example, the Apple iPhone does not afford the ability for organizations to reset Apple ID passcodes or to enforce a complex password strategy via MDM. The device also sends email notifications in clear text containing the iOS device name; the user of the device can set this name, and it may contain PII information or other sensitive data[10]. Native applications such as email and web browsers do not provide non-repudiation utilizing hard token (CAC) authentication.

3. When initiating a BYOD program within DOD, one must consider the concerns of software compliance. Users have the ability to install applications and accept the license agreements. If they utilize these personally downloaded apps for work, not only could it be a security risk, they may be violating the license agreement for the software. Most mobile applications have "Click-Wrap" license agreements, which allow companies to have contracts with a large group of customers, ensuring legal liability for how they use the provided software. What legal ramifications need consideration if end users are not allowed to accept license agreements for personally downloaded software?[11]

With users installing software willy-nilly and vendors continuously updating their software, tracking methodologies or any method of version control logic becomes an asset managers concern due to the impact a BYOD solution will have on the amount of manpower to conduct and review device inventories. Do they track all software on the device so that security analysis can be conducted from these inventories to assess vulnerabilities and trends? Alternatively, do they just track a vetted list of applications provided and purchased by the DOD entity and ensure licensing compliance for those specific apps? How do they even access the device to conduct an inventory? How is it determined what software is government provided and what the end user owns?

4. The significant shift in the usage of mobile devices, including BYOD, is a corporate decision to focus of multiplatform development. If DOD will allow users to bring their own device and there is a massive influx of mobile device usage, one could conclude that many mission applications would integrate into the mobile device platform or what's the point of providing this capability? Consider the tremendous undertaking that in the near term would be dictated by mission need and budgets. One could argue that the Project Management Office (PMO) would need to be stood up, and decisions made about costs and system consolidation to reduce the footprint of the software application portfolio. New development methodologies such as HTML 5, Xamarin (.NET C# codebase deployable to iOS/Android/Microsoft devices), and Kendo UI (JavaScript based utilizing HMTL5 features) allow for deploying a single codebase of an application to a variation of mobile devices that utilize different languages and code compilation techniques.

Procurement strategies for supporting infrastructure (e.g., MDM/MAS servers) should align with current processes, however there will be the realization of additional procurement needs. Does DOD enter into a "shared cost" agreement to provide partial reimbursement for the user's device? Will there be any reimbursement of software downloaded that is use for both personal and work? Will there be any impact on help desk support or will users be responsible for their own device? Stipends, reimbursements and allowances can quickly become a very complex situation; consider the enactment of teleworking where policy to reimburse teleworks for their home Internet provider service or home office expenses required to perform mission tasks is not clearly defined and left to the agency[12].

**RECOMMENDATION**

Applications provide the most risk to data leakage in a BYOD environment. DOD must define a strategy for mobile application risk management that utilizes static, dynamic and behavioral analysis to expose unwanted application behaviors. Define a risk policy that is enforced not on the

device itself, where the end user could manipulate the policy, but through the supporting infrastructure or a cloud-based hosted service. A proactive stance would need to be taken to utilize adaptive technologies that can automate the review of mobile device applications and not only apply a scoring system against the mobile application, but also against the companies that develop mobile devices. Providing a grade to the company who develops the application would allow DOD to conduct trend analysis over time and understand which companies are taking security seriously enough to become "application security partners" with the DOD. This adaptive system would need the ability to learn what is and is not an acceptable behavior for an application, becoming more accurate in its scoring system and security analysis over time.

The ambiguity of software license agreements requires a clear understanding of terms such as what defines a device and the user when applied to mobile applications. Approved software will need to be defined for BYOD to meet mission requirements. A clear line must be drawn to differentiate between personal use applications and mission applications. Educating users about established policies with the understanding the user is entering into an agreement to abide by the policy or lose their right to have their own personal device on the network. Ensure the user understands the importance of doing their part to assure data and network security. Agencies will need to determine if they have software inventory management capabilities in place or if they will need to purchase a server or cloud-based solutions sufficient to monitor devices and track software licensing. All software on the device needs inventorying so that potential security concerns between personal and corporate software can be cross-referenced and mitigated.

Mobile virtualized platforms need deployed on personally owned devices. These virtualized solutions loads an entire corporate infrastructure into a virtual machine on the supported device. The virtualized area is sandboxed, encrypted, and doesn't allow bleed over into the source operating system (iOS, Android, Microsoft), effectively separating the end users personal environment from their corporate environment. If the user loses their device, MDM solutions allow for wiping the corporate sandbox remotely ensuring no compromised data or corporate access. The virtualized sandbox must provide secure authentication via fingerprint verification or Common Access Card (CAC). DOD would need to provide approved STIG configurations for these sandbox environments to ensure standardization of deployment.

(Retired) Gen. Keith Alexander, former Commander of the Air Force Cyber Command CYBERCOMM) and former Director of the National Security Agency (NSA) was a guest speaker at the 2014 Citrix Government Mobility Event in Washington DC. He outlined five key components to implement a successful BYOD strategy. (1) Create a defensible architecture and ensure the integrity of the network, utilizing thin virtual clients and cloud solutions as part of the strategy. (2) The most important component is to provide high-quality training to support staff and end users. (3) Ensure a common operating picture, simplifying and streamlining solutions. (4) Establish cyber legislation and policy. Share with commercial industry counterparts. Establish partnerships that ensure security and integrity of solutions at all levels. (5) Establish command and control regimes and issue guidance and direction to ensure best practices get executed. Be ready to protect the environment and critical data[13].

Over the past few years, DOD has established policy for commercial cloud solutions. The Secretary of the Navy ordered the movement of all public facing applications to commercial cloud

solutions. Security has been at the forefront of this effort and new programs such as FedRAMP have been established to ensure vendors meet the requirements to provide high quality, secure services. Currently, movement to the cloud has been controlled, and only those systems that host publicly releasable data can be moved to commercial cloud. Over the next 1-2 years, systems that host Privacy Act Information (PII) and For Official Use Only (FOUO) will move to commercial cloud. The same steps need to be taken with a BYOD strategy, putting programs in place for vetting commercial vendors and placing restrictions on accessible data, eventually extending that to data layers three and above. Ensuring data protection is most critical.

**COUNTERARGUMENT**

Continuous lifecycle management of mobile applications is a challenging terrain, especially when there is no control over what gets installed on the mobile device. If focus is placed only on the approved mission applications the target base shrinks; however, software tracking and license management will double if not triple in size. There will need to be investment in tools and training of personnel to assess and identify the quality of the security for mobile device applications. The fact that this software may or may not be government owned software drastically complicates the matter and dives into legal implications. Providing global situational awareness of BYOD vulnerabilities, reporting them to the 624th Operations Center and network operations, and security centers will initially complicate things.

There are many vendors that provide mobile virtualized platforms and they are very new to the game. One example is Samsung's Knox BYOD software, which provides a secure, encrypted sandbox for BYOD. A security weakness was found, which allows a malicious application to "listen in" on the data transferred within the secured sandbox, also known as a "man in the middle attack[14]." This technology needs to be scrutinized until the product matures.

**CONCLUSION**

DOD is leaning forward to change the mission footprint with the implementation of commercial cloud solutions, bridging the gap of budget shortfalls and tackling critical security concerns. BYOD solutions within DOD have the capacity to provide a similar layer of cost savings. DOD should tread carefully, providing initial solutions that control the level of data exposed in a BYOD solution. Most BYOD users will want immediate access to prominent services such as email, file services, and Share Point. Moving forward slowly and ensuring that security is in place to protect resources and that legal considerations are mitigated needs to be part of our vision. Integration with other systems and services must be in the BYOD vision.

**NOTES**

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] GNC Media Group article, website, para1.
[2] Feiman, Joseph. Zumerle, Dionisio, Strategic Planning Assumption, pg2.
[3] Clarke, Richard A. Knake Robert K., Cyber War, pg. 55-56
[4] Feiman, Joseph. Zumerle, Dionisio, Strategic Planning Assumption, pg6.
[5] Los Angeles Times Newspaper Article online.

[6] Appcelerator Whitepaper, Layer 3, App Security Code, pg7.
[7] Appcelerator Whitepaper, Layer 6, App Distribution & Mgt., pg11.
[8] Appcelerator Whitepaper, Layer 6, App Distribution & Mgt., pg12.
[9] Apple Corporation and DISA, Section 3, pg. 8.
[10] DISA, IOS 7 Security Technical Implementation Guide, Section 3, pg.9
[11] O'Brien, Frances, Cut the Software Compliance Risk of BYOD, pg. 5 section 4.
[12] OPM, Telework Guide, pg12. Bullet 5.
[13] Gen Keith Alexander, Guest Speaker Citrix Mobility Event, Washington DC
[14] Hachman, Mark, Vulnerability in Samsung's Knox BYOD Software, PC World

## BIBLIOGRAPHY

Hickey, Kathleen, "DOD Plan for mobile not BYOD-ready", *GNC Media Group*, 01Mar13, accessed 23Jun14, http://gcn.com/Articles/2013/03/01/DOD-plan-for-mobile-not-BYOD-ready.aspx?Page=1

Feiman, Joseph. Zumerle, Dionisio, "Technology Overview: Mobile Application Security Testing for BYOD Strategies, *Gartner Group*, 30Aug13, accessed 23Jun14, https://www.gartner.com/doc/2583017?ref=SiteSearch&sthkw=mobile%20application%20security%20testing&fnl=search&srcId=1-3478922254

Clarke, Richard A. Knake Robert K., Cyber War, The Next Threat To National Security And What To Do About It (HarperCollins Publishers, 2010), pg. 55-56

Rodriguez, Salvador, "4.5 Million smartphones were lost or stolen in U.S. in 2013", *LA Times*, 17Apr2014, accessed 23Jun14, http://www.latimes.com/business/technology/la-fi-tn-45-million-smartphones-lost-stolen-2013-20140417-story.html

Appcelerator, Inc., "The 6 Layers of Mobile Security", *Appcelerator Inc.*, date unknown, accessed 23Jun14, http://www.appcelerator.com.s3.amazonaws.com/pdf/whitepaper-mobile-security.pdf

Apple Corporation and DISA. "Mobile Application Store (MAS) Security Requirements Guide (SRG) Technology Overview, *DISA*, 18Dec13, accessed 23Jun14, http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Apple Corporation and DISA, "IOS 7 Security Technical Implementation Guide (STIG), *DISA*, 13Jan13, accessed 23Jun14, http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

O'Brien, Frances, "Cut the Software Compliance Risk of BYOD", *Gartner Group*, 16Apr13, accessed 23Jun14, https://www.gartner.com/doc/2429816/cut-software-compliance-risks-byod

Willis, David, A., "BYOD: The Results and the Future", *Gartner Group*, 05May14, accessed 23Jun14, https://www.gartner.com/doc/2730217/bring-device-results-future

Office of Personnel Management, "Guide to Telework in the Federal Government", *OPM*, April 2011, accessed 22Jul14, http://www.telework.gov/guidance_and_legislation/telework_guide/telework_guide.pdf

Alexander, Keith, General (Retired), Guest Speaker, *Citrix Government Mobility Event*, Washington DC, 10Jun14.

Hachman, Mark, "Researchers discover vulnerability in Samsung's Knox BYOD software", PC World, 09Jan14, accessed 24Jul14, http://www.pcworld.com/article/2082311/researchers-discover-vulnerability-in-samsungs-knox-byod-software.html

Integrating Cyberspace into Anti-Access/Area Denial Strategy: Interconnecting in Blue and Purple

Mr. Theodore C. Trakas (346TS/TEA)

**ABSTRACT**

Cyberspace is an integral part of how the Air Force (AF) operates as an organization and fighting force. Further, the AF has recognized Cyberspace as a new domain for military operations. Therefore, to meet new challenges with the Anti-Access/Air Denial (A2/AD) mission sets of the future, the AF needs to effectively integrate Cyberspace, its newest domain for operations, into A2/AD strategy. In order to put cyber integration into context and identify issues and constraints, two general and two specific ways that Cyberspace integrates into A2/AD mission sets are identified: the Enterprise/Military Enablers and A2/AD Avoidance/and Counter-A2/AD Attack. The AF is assessed to be most capable in terms of the cyber integration of enterprise and military enablers. Integration of cyber actions for A2/AD avoidance is less mature, but appears to be evolving, particularly given creation and designation of new cyber mission teams. Cyber integration into the larger campaign for counter-A2/AD attack is assessed to be more problematic, in terms of developing warfighters, maintaining currency and priorities, overcoming conflicting equities, and establishing inter-functional communications. Arguably, developing and maintaining expertise and capabilities for effective integration of A2/AD missions in and through Cyberspace will require sustained, deliberate, and senior level attention.

**DESCRIPTION OF ISSUE / PROBLEM STATEMENT**

1. In 2005, the Air Force (AF) announced a new mission statement: "to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace" where "(t)he term cyberspace includes network security, data transmission and the sharing of information."[1] In current doctrine, the AF refined its definition for Cyberspace by adopting the joint definition "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2,3]

The fundamental roles of military components (Army, Navy and AF) are to organize, train and equip forces for employment by combatant commanders. The AF has been preeminent in the development and application of new, cutting edge technologies in order to accomplish missions and protect members, but will face new challenges in the future with Anti-Access/Air Denial (A2/AD) mission sets.[4] "Adversary anti-access capabilities will continue to improve, challenging US ability to project power and influence. Countering these capabilities is vital to assure freedom of action to, through, and from air, space, and cyberspace."[5] Acquisition of new cyber technologies and capabilities presents a generational opportunity to add to the tool kit for achieving A2/AD mission objectives. However, in order to maintain a reasonable scope for this paper, acquisition issues, e.g., the identification and definition of cyber requirements, research and development, acquisition and testing of capabilities, and so forth, will not be addressed to any significant depth.[6] In the paper, we will address policies and concepts to organize and train cyber forces. We shall argue that these forces can and should be integrated into the A2/AD mission in a number of general and specific ways.

In order to put cyber integration into context and identify issues and constraints, the analysis looks at four core ways that Cyberspace integrates into A2/AD mission sets: The Enterprise, Military Enablers, A2/AD Avoidance, and Counter-A2/AD Attack. Admittedly, the first two to three ways may not be explicitly included into an AF A2/AD strategy, but all have important ramifications and impose constraints on how the AF has, can or should incorporate Cyberspace into A2/AD mission conduct and strategy formulation. The goal for this integration is to achieve unique contributions in Cyberspace for the AF to succeed in countering the A2/AD capabilities of adversaries.

2. Cyberspace provides the means, methods and milieu (the new 'ether') for modern creation, transmission, storage, and presentation of information. This core, day-to-day sustainment of the AF in and via Cyberspace provides a huge contribution to the AF as a viable and effective organization (or 'enterprise') and fighting force. Cyber capabilities yield crucial, cost effective means for the 'must pay' obligations of the AF, e.g., personnel, logistics, accounting, morale, etc. Without belaboring the point, the importance for achieving enterprise efficiencies in and through Cyberspace, or any other means, cannot be overstated, given the probability and severity of budget constraints in the future.[7] To the extent that "An army marches on its stomach," it could now rightly be said that the AF "flies by its computers" in Cyberspace, whether from a cubicle, command console, or cockpit. This observation may seem obvious, but some non-intuitive implications of it for A2/AD will be shown.

Through its various "information technology infrastructures," the AF exposes national, international, and global attack surfaces to the world in general and adversaries of various types (nation-states, terrorists, and other cyber miscreants). The AF is always under cyber attack, even in periods of nominal peace.[8] By almost all objective measures, be it dollar investment, support manpower, bandwidth utilization, etc., sustainment and defense of these infrastructures consume the largest portion of financial and human resources and senior leadership attention. Consequently, the AF is best positioned in terms of policies and manpower for network defense, which is undisputedly the most mature and battle hardened sub-domain of Cyberspace. AF's commitments to these networks are understandable, but produce subtle biases in policies, priorities and decisions which may tend to be counter-productive to smaller, specialized, military-unique mission sets such as A2/AD. For example, the AF created the 17D Cyberspace Operations Officer career field in 2010 by essentially rebranding all 33S Communications and Information Officers.[9] The AF established unique, but rather minor, training requirements for the new field and made this training available. However, issues remain with the career field dominated by personnel with backgrounds and expertise in communications and information technology (IT).[10]

3. Cyberspace logically organizes and expands traditional military communication links, and in effect creates new, robust pathways, or 'pipes', and frameworks for collecting, communicating, organizing, and presenting information. Effective employment of cyber capabilities has already yielded a quantum leap in the amount, quality, resolution and timeliness of data collected and distributed for military applications: Intelligence, Surveillance and Reconnaissance (ISR), command and control (C2), situational awareness (SA), and so forth. This trend will continue in the future, as more dense hardware components are manufactured with tighter design tolerance and line spacing, and new software and network capabilities become more available or mature,

e.g., Voice over Internet Protocol (VOIP), Internet Protocol Version 6 (IPv6), Cloud Computing, etc.

A few publicly known examples have provided clarion calls for more assured integration of military functions in and through Cyberspace. In 2009, "U.S. forces had discovered that insurgents in Iraq, using inexpensive, off-the-shelf software, had been able to hack into video feeds from the drones."[11] In 2011, Creech Air Force Base, which is a control center for worldwide drone flights, was hit by a virus.[12] According to official sources, a "virus infected a ground system that runs backup power supplies, environmental controls and workstations," but the possibility that such an infection could jump to other official or mission systems is not without precedence, e.g., the compromise of Target Stores in 2013.[13] Hence requirements and standards for confidentiality, integrity, and availability, which are common for networks in the commercial world and AF enterprise, need to be applied more consistently and rigorously to specialized military systems and networks. Given the relative maturity and expertise of enterprise defenders, the AF is well staffed and organized to leverage and incorporate corrections, mitigations and enhancements to specialized military networks, once gaps are identified and priorities placed.[14]

4. Another important way to indirectly integrate Cyberspace into an A2/AD strategy is include planning decision points for use of direct, non-kinetic cyber attack actions against targets, in lieu of kinetic strike options. In effect, cyber action can attain military objectives, or "effects", by way of A2/AD area avoidance, and have other attractive characteristics. Historically, cyber attacks have been less provocative, and so presumably could be launched during various phases of conflict. If planned and executed with finesse, attribution for the attack may be difficult.[15] Kinetic weapons blow up things and can kill people, whereas Cyberspace Attack Capabilities (CAC) inherently need not and so have categorically lower margins for collateral damage and loss of human life.[16] CACs may also provide a range of selectable effects, e.g., the 'D5s' of Degrade, Deceive, Destroy, Deny, and Disrupt, and may be tailored to have transient, persistent or permanent duration. Thus Cyberspace in effect opens an additional dimension to avoid, or side step, and A2/AD physical space, if the required communication connections (accesses) in Cyberspace exist.

The AF is building "the cyber mission force" teams.[17] Concurrently, the AF is in the process of normalizing and modernizing "the 624th Operations Center, which is the cyber equivalent of an Air Operation Center, an AOC."[18] These actions are not occurring in a vacuum. The other services and Department of Defense (DoD) organizations are staffing similar teams, as put in motion by General Alexander, recently retired Commander of United States Cyber Command (USCC). By 2016, the total DoD force "should number over 6,000 professionals."[19] Staffing, training and qualifying these teams are important steps in developing and fielding forces to conduct defensive and offensive missions in Cyberspace. In times of conflict, forces are presented to the applicable combatant commander. In the not too distant future, USCC is expected to be elevated as the tenth combatant command (for Cyberspace), in order to focus expertise and coordination actions in Cyberspace. Thus the DoD is placing the right cyber chess pieces on the board, but will it know how to play them adroitly in a conflict, and especially for a specialized military mission set?

5. The most direct, and potentially effective, way to integrate Cyberspace to the A2/AD missions will be to define employment concepts, mature policies and groom warfighters to apply unique

cyber attack techniques and capabilities against adversarial air forces sensors, networks, and decision makers. The specific kinds of cyber attack that might be possible are beyond the classification of this paper, but in general, they are only constrained by budgets, connectivity, and the ingenuity of technologists, planners and warfighters.[20] As in any A2/AD campaign, careful timing and coordination of all elements would be crucial, in order to achieve combatant commander objectives. There are a number of current issues and constraints.

First, combatant commands, including USCC eventually, are dependent on the components to provide knowledgeable, effective warfighters to serve in their organizations. The current manning and expertise of these forces, as applicable to the A2/AD mission set, is uneven. For planning and targeting of cyber actions in support of an A2/AD strategy, the status is not robust, given the preponderance of the AF cyber force with strictly IT and communications support backgrounds. For execution of cyber actions, AF is on a firmer footing: groups are already established, to varying degrees of expertise and maturity, and are evolving, as more regular units under the moniker of cyber mission teams. Second, major peer or near-peer conflicts, which include significant A2/AD challenge, will (hopefully) tend to be infrequent to non-existent in the future. Consequently the number of actual cyber taskings in support of counter-A2/AD or similar missions may be infrequent. Under a strictly cyber viewpoint, the need to organize, train and equip forces for counter-A2/AD mission sets is not obvious. Third, as a collateral consequence, offensive cyber capabilities that might be current and available for use in a potential counter-A2/AD mission will tend to be have been developed by other partners and have applicability to multiple target and mission sets. Thus the equities for use of these capabilities may be contentious. Fourth, organizing AF cyber forces under the 24th Air Force and AF Space Command provides synergies from a strictly Cyberspace standpoint, but weakens its organizational and doctrinal relationships with other important AF groups and functions which are relevant to A2/AD, e.g., intelligence, electronic warfare and air component groups. Fifth, the rationalizing and synchronizing of cyber vs. physical actions will probably be more complicated in the future. USCC, the presumed Cyberspace command, will order cyber actions, whereas the applicable geographical combatant command, including its planning staffs and operations centers, will order the other physical actions. Hence identification and development appropriate cyber courses of action (COA) and subsequent execution of actions in Cyberspace will cross command boundaries.

**RECOMMENDATIONS**

1. Our analysis identifies enterprise operations and defense as the most mature part of Cyberspace, but this assessment is not intended to imply that successful network defense is to be taken for granted, particularly prior and during a conflict requiring an A2/AD strategy. Such a conflict would generally involve a peer or near-peer adversary, since it presumes an adversary possessing advanced anti-aircraft capabilities, Integrated Air Defense Systems, and so forth. Cyberspace attacks against friendly networks thus would conceivably become more frequent, effective and malicious prior to and during such a conflict.[21] Hence the ability to triage friendly networks by quarantine of non-essential or infected sub-networks, connections or services would be critical mission assurance measure to maintain an effective fighting force. Advanced planning to take these measures, proactively or retroactively, should be included in applicable Operations Plans (OPLAN). Practicing such measures should be considered for inclusion as disrupted and degraded network operation ("taking the gloves off") during discrete exercises, and perhaps even during

more general base INFOCOM exercises – the cyber equivalent of having to wear Nuclear, Biological and Chemical gear – within reason.[22]

2. Full employment of air ISR assets will of course be restricted in A2/AD airspaces in applicable OPLANs. Communications links relying on radio frequency (RF) signals may be restricted, disrupted or degraded in these airspaces. Hence, as with enterprise services, planning must include mitigation measures for these constraints, and training and exercises should include these factors. Access and coverage gaps for relevant intelligence should be identified and prioritized for possible military-unique material or non-material solutions. Effective situational awareness of network operations and application of mitigation measures to maintain the greatest mission assurance should be addressed by models and simulations, tests and exercises. Network outages and degrades due to geospatial and EM spectrum restrictions should be included.

3. To effectively contribute to A2/AD Avoidance and Counter-A2/AD mission planning, the AF must enhance opportunities to develop airmen with multi-domain knowledge, expertise and experience. The AF should continue to evolve courses and programs that blend the applicable concepts of Offensive Cyberspace Operations, Electronic Warfare, Integrated Air Defense Systems (IADS), air forces employment, etc. A reasonable goal for such training would be to develop a relatively small cadre of tech-savvy planners and warfighters, ideally from multiple Air Force Specialty Codes (AFSC) and other DoD groups, who are cognizant of many capabilities and methods in multiple domains that can be applied to A2/AD problem sets. The importance of personal relationships and mutual trust between this small AF group and other DoD groups, developed over many years, cannot be overstated.

4. The concepts of Information Operations stressed the need for combined actions in Computer Network Operations (CNO), EW and Influence Operations; these concepts remain valid for A2/AD operations; and awareness of them must be instilled in at least a small group of the cyber forces. Regular interactions between the different functional areas, in terms of requirements, technologies and tactics, planning, etc. should be encouraged, within the AF (Blue) and with other community partners (Purple). Leveraging adversarial systems knowledge from ISR, EW and aircrew personnel is particularly crucial. Awareness of unique A2/AD networking characteristics is key.[23] Development opportunities are well presented on joint planning staffs of geographical combatant commanders and in evolving course offerings.

**COUNTERARGUMENTS**

Frankly, current AF policy direction for cyber integration into A2/AD or other mission sets are stated in terms of rather vague or overly optimistic end-state goals. Air Force Directive Document 3-2, Cyberspace Operations, asserts that the "core of cross-domain integration is the ability to leverage capabilities from different domains to create unique — and often 'decisive' — effects."[24] USAF Space Command articulates an overarching goal to groom airmen possessing a wide range of technical and operational competencies. "Airmen will stop thinking of themselves as operators, communicators, intelligence experts, etc. but rather as an integrated team of multi-disciplined well-trained cyber professionals with the technical and tactical skills needed to execute any and all missions."[25] These expectations for our cyber airmen are attractive and understandable but probably not achievable.[26]

## CONCLUSION

Under current doctrine, Cyberspace is exclusively defined in terms of cyber entities, i.e., "a global domain within the information environment consisting of the interdependent network of information technology." This exclusivity in defining the domain is not so prominent for the other, more mature AF domains; for instance, space operations are not conceptualized in terms of exclusive interaction of assets within the vacuum of space. At this phase of its development, the emphasis to distinguish and establish Cyberspace as a domain of operation is understandable, but cyber forces of AF and other services will need to mature this conceptualization. What appears lacking in policy, especially given the relatively recent divorce of the Cyberspace from the rubric of Information Operations in the AF, is the need to develop cyber plans and actionable measures that link multiple domains, air, space and cyber.

## NOTES

(All notes appear in shortened form.
For full details, see the appropriate entry in the bibliography.)

[1] *AF Print News*, "Force releases new mission statement"
[2] JP 1.02, *Definitions*
[3] AFDD 3-12, *Cyberspace Operations*, pg 1
[4] These cutting-edge technologies have included over the years: high performance engines and airframes; radar and missile warning devices; self-protection jammers and expendables operating in multiple spectrums; standoff jammers against adversarial radars and communication links; low observable materials and shapes; remotely piloted vehicles for decoy and intelligence; and so forth. Obviously, the Air Force will monitor development and application of technological advances, and particularly disruptive ones, as they relate to friendly and adversarial air forces, in order to leverage friendly use and mitigate adversarial use of new technologies.
[5] Joint Forces FOE, pg 9
6 In terms of scope, this paper does not address cyber integrations with coalition personnel and networks
[7] General Schawrtz, "Sustaining Readiness with Constrained Budgets"
[8] Cyberspace is contested environment in a continual state of conflict or undeclared guerilla war. Ironically, US rules of engagement (ROE) in Cyberspace have unfavorabe parallels with those during the Vietnam War. In Vietnam, due to political concerns, the US placed personnel and assets in hardened locations within enclaves; in Cyberspace, DoD puts data and systems in restricted networks behind network defenses. In Vietnam, base defenders freely returned suppressing counter-fire against attackers; in Cyberspace, due to legal concerns, network defenders may return suppressing cyber counter-fire against attackers, assuming legal approval. In Vietnam, US forces performed armed patrols in civilian areas to seek out and destroy adversaries; in Cyberspace, DoD does not patrol US civilian networks to detect and remove malware or respond to hacker attacks on US persons (without escalation to war status). Arguably, in Vietnam, US ROEs did not support a winning strategy; in Cyberspace, restrictive cyber ROEs guarantee that DoD will have limited effectiveness in protecting US national interests. And these restrictions could draw into question the whole value-added of DoD. In other words, what value is a military that only defends itself? Arguably, the manifest destiny for DoD cyber forces may be as a multi-department, national organization.
[9] Terry, "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field"
[10] Lee, "The Failing of Air Force Cyber"
[11] Washington Post, "Encryption of drone feeds won't finish until 2014, Air Force says"
[12] Los Angeles Times, "Air Force denies that computer virus compromised drone aircraft"
[13] Tripwire, "How Target's Point-of-Sale System May Have Been Hacked"
[14] But employing ISR assets in a conflict against a peer or near-peer adversary introduces important issues for physical access of these assets, which have not been a serious issue in recent conflicts over many decades: "Because of the uncontested environment for the operation of an ISR family of systems over Iraq and Afghanistan, the platforms, supporting sensors, and C2 connections cannot simply be lifted and relocated to a new theater of operations." Hence access of air breathing ISR platforms will fold into the problem set for A2/AD. (See Air and Space Journal, "Joint Intelligence, Surveillance, and Reconnaissance in Contested Airspace.")
[15] A relatively recent, preeminent example of which is *Stuxnet*, which was a computer worm attacking Siemens programmable logic controllers of Iranian nuclear enrichment

centrifuges; external groups have speculated that this malware was created by certain nation-states, but no one has found clear, smoking contrails leading back to its point(s) of origin. (See Wikipedia, *Stuxnet*.)

[16] Cyberspace attack capabilities are not without their own unique disadvantages or limitations of course. True, they can be programmed to damage/degrade physical entities, networks and information, while sparing people (the opposite of the neutron bomb of Cold War days), but on the other hand, they do not necessarily destroy themselves upon use and therefore could be found, replicated cheaply, and fired against friendly military or even civilian targets.

[17] General Shelton, "Integrating Air, Space & Cyberspace Capabilities"

[18] Lt Gen Hyten, "Cyber 1.3 Luncheon at the 29th National Space Symposium"

[19] Chuck Hagel, "Retirement Ceremony for General Keith Alexander"

[20] For instance, one could imagine, as in a Tom Clancy novel: 'hacking into' an adversary's air defense system; 'looking over his shoulder'; reading his understanding of the air battle space; adjusting or reacting in a timely (or 'just in time') manner with other measures, such as standoff jamming, re-vectoring of attack packages, and so forth. Once into an enemy's system, presumably one could introduce false targets into the adversary's systems: a large number (or 'flood'), overwhelming human operators or exceeding system processing limits; a few menacing false strike packages, headed towards high-valued centers of gravity, such as palaces, command posts, air fields, defense centers; and so forth.

[21] The success, or even likelihood, of pre-emptive Cyberspace attacks (a modern day 'Pearl Harbor' by zero-day exploits) cannot be discounted.

[22] Within reason, such exercises should be wisely circumscribed in terms of affected areas and timing given the pervasive reach of networks and the potentially severe economic impact of these self-imposed denials or services.

[23] Unique A2/AD network characteristics include: dynamic Blue and Red spatial movements of network components (e.g., aircraft and mobile ground units) and reconfigurations of network topologies; possible war reserve modes; networked or autonomous operation of adversarial forces; fragility of (RF) communications links; unique protocols; military grade crypto; etc.

[24] AFDD 3-12, "Cyberspace Operations," pg 19

[25] AFSPC, *USAF Blueprint for Cyberspace, 2* November 2009

[26] AFDD 3-12, "Cyberspace Operations," pg 19, addresses "Integration of Cyberspace Operations Across Domains." This short (half page) section has only one reference, to 2007 Air War College Maxwell Paper No. 40 by Convertino et al. The Convertino paper surveys various broad aspects of cyber history, policy, and predictions, but is rather dated, as indicated by references to an old policy and research (e.g., crybercraft) topics, and does not specifically address the A2/AD issue.

## BIBLIOGRAPHY

Air and Space Journal, "Joint Intelligence, Surveillance, and Reconnaissance in Contested Airspace," May-June 2014, Dr. Robert P. Haffa Jr. and Anand Datla

Air Force Directive Document (AFDD) 3-12, *Cyberspace Operations,* 15 July 2010, Incorporating Change 1, 30 November 2011. Retrieved from http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf

Air Force Print News, "Force releases new mission statement," published 8 December 2005

Air Force Space Command, "The United States Air Force Blueprint for Cyberspace," 2 November 2009

Converntino, Sebastian, DeMattei, Lou Anne, and Knierim, Tammy. "Flying and Fighting in Cyberspace," Air War College Maxwell Paper No. 40. Maxwell AFB, AL: Air University Press. Retrieved from http://www.au.af.mil/au/awc/awcgate/maxwell/mp40.pdf

Hagel, Charles, "Retirement Ceremony for General Keith Alexander," Fort Meade, MD, 28 March 2014

Hyten, John E., "Cyber 1.3 Luncheon at the 29th National Space Symposium," 29th National Space Symposium, Colorado Springs, Colo., 8 April 2013

United States Joint Forces Command Publication, "Joint Operational Environment 2008 – Changes and Implications for the Future Joint Force," November 25, 2008, (JOE); and HQ USAF/A8X draft "Future Operating Environment" (FOE), 2008.

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Lee, Robert M., "The Failing of Air Force Cyber," Signal Magazine, 1 November 2013

Los Angeles Times, "Air Force denies that computer virus compromised drone aircraft," W.J. Hennigan, 14 October 201. Retrieved from http://articles.latimes.com/2011/oct/14/business/la-fi-drone-virus-20111014

Schwartz, Norman, "Sustaining Readiness with Constrained Budgets," Air Force Association Air Warfare Symposium, 23 February 2012

Shelton, William L., "Integrating Air, Space & Cyberspace Capabilities," Air Force Association, Air and Space Technology Exposition, National Harbor, Maryland, 17 September 2013

Terry, Katrina A., "Overcoming the Support Focus of the 17D Cyberspace Operations Career Field," Graduate Research Project, 2 June 2011

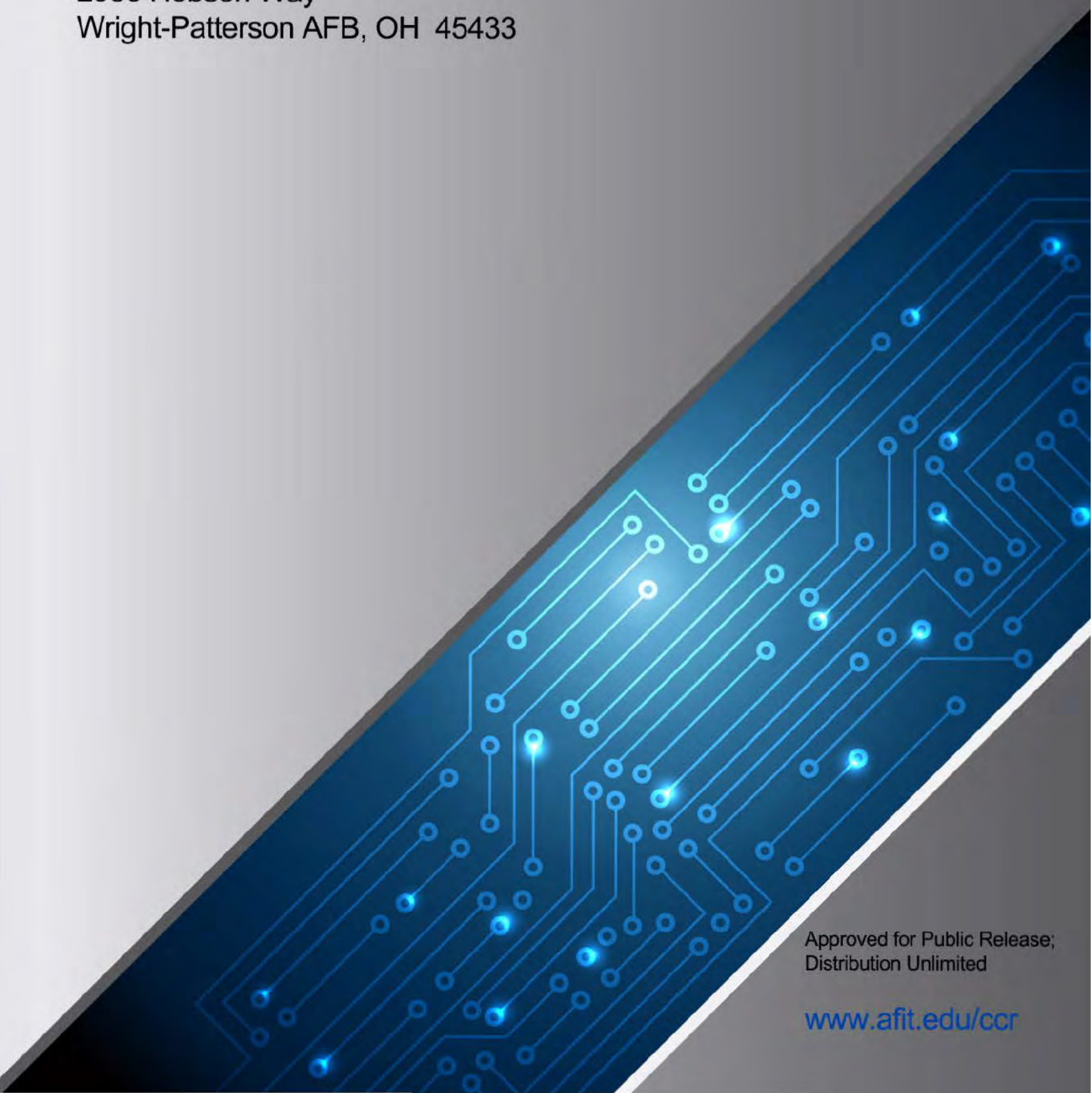
Tripwire, "How Target's Point-of-Sale System May Have Been Hacked," Ken Westin, 14 January 2014. Retrieved from http://www.tripwire.com/state-of-security/vulnerability-management/targets-point-sale-system-compromised/

Washington Post, “Encryption of drone feeds won't finish until 2014, Air Force says,” Ellen Nakashima, 19 December 2009 . Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/12/18/AR2009121804281.html

Wikipedia, *Stuxnet* (http://en.wikipedia.org/wiki/Stuxnet)

**Cyber Professional Continuing Education**

Air Force Institute of Technology
Air Force Cyberspace Technical Center of Excellence
Center for Cyberspace Research
2950 Hobson Way
Wright-Patterson AFB, OH 45433





www.afit.edu/ccr