SMALL WARS JOURNAL

Towards A Career Path in Cyberspace Operations for Army Officers

*By **Todd Arnold**, **Rob Harrison** and **Gregory Conti***
Journal Article | *Aug 18 2014 - 10:37am*

Towards A Career Path in Cyberspace Operations for Army Officers

Todd Arnold, Rob Harrison, and Gregory Conti

Introduction

In the past five years, the Department of Defense (DoD) recognized the emergence of cyberspace as an operational domain and created U.S. Cyber Command (USCYBERCOM). These events were the result of the realization that cyber operations are both a critical vulnerability and a massive opportunity. Within the Army, U.S. Army Cyber Command (ARCYBER) was created as the single command to conduct and oversee the Army's operations in cyberspace.

ARCYBER's personnel and unit structure to carry out its mission within the Cyber Mission Forces (CMF) are still evolving. Critical to the Army's success in cyberspace is the need for integrated career timelines for officers, warrants, and enlisted Soldiers. The need for a unified cyber career path is driven by operational necessity and a demand for efficiencies as our nation faces a critical national threat in cyberspace**[i]** coupled with a lack of sufficiently trained personnel.

To properly face the numerous threats in cyberspace, the Army needs to invest in the development of 'cyber leaders' who will possess the technical acumen and strategic vision to build and lead its forces in cyberspace.**[ii]** Initial planning for career paths in cyberspace operations is in progress. In order to help assist current and future analysis, we propose a model for what a mature Army cyber officer career path may look like. This is an updated and condensed version of our earlier work.**[iii]**

Current State

In combat arms branches, the Army accepts nothing less of its officers than total mastery of a particular warfighting function and a demonstrated potential for increased responsibility before an officer is considered for promotion. For the Army to be effective in cyberspace, it must produce leaders who understand the intricate aspects of operations in cyberspace with the same level of competence and confidence as combat arms officers do in their domain.

Within the current Army model, leaders capable of serving in the cyber domain are developed in an ad-hoc manner; in most cases this development occurs in spite of the current personnel management system, not because of it. A unified career path would allow personnel to gain expertise and experience by building on foundations learned prior to commissioning and expanded during assignments of increasing difficulty and responsibility, buttressed by tailored education, training, and assessment programs.

Challenges

While the Army is improving its efforts to grow a professional cyber force, it has, thus far, been unable to unify these efforts into a cohesive plan for conducting cyberspace operations due to several challenges. Some Army organizations have appended the term “cyber” to label job titles and training courses without substantive alteration commensurate with the title – such arbitrary misapplication of the term “cyber” only serves to further obfuscate the distinction between actual cyber operations and the periphery. There also exists a lack of unity between all of the communities who currently own a fraction of the overall cyber fight because qualified cyber leaders and true cyberspace operations jobs exist only at the fringes of longstanding branches and functional areas (in Figure 1, we depict branches and functional areas who doctrinally control a portion of what we define as cyber and comprise the preponderance of existing cyber leaders).

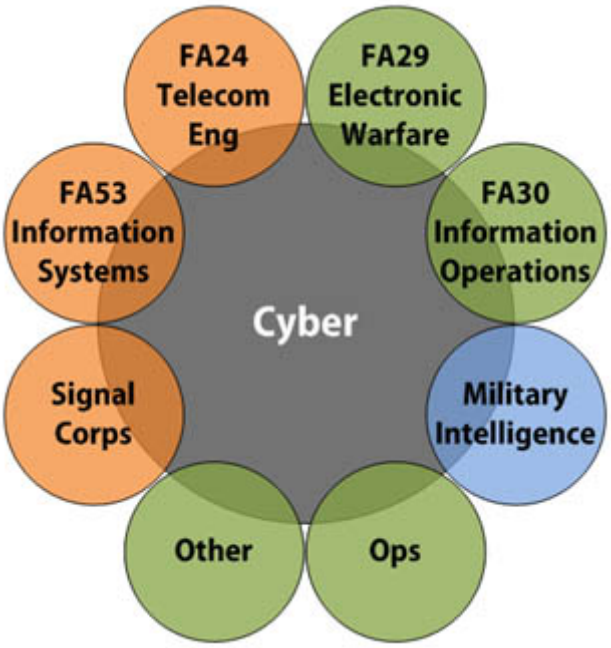

Figure 1: In this figure, we can see the different branches and functional areas which perform a portion of cyber operations as well as the existing gap covered by no existing career specialty.

A pervasive misconception is that a “good leader” can lead any type of unit. In reality, a maneuver officer is expected to follow a branch-specific, career-long development model in which they proceed through assignments of increasing responsibility, gaining experience and expertise with each successive assignment (as depicted in Figure 2) in order to command at the highest levels. This purposeful, developmental process creates a professional officer corps capable of leading our Army in difficult environments. Similarly, the Army should expect its cyber leaders to possess a level of expertise in their chosen field on par with that required from combat arms officers – leaders who are as respected in their trade-craft as combat arms officers are in theirs (see Figure 2 for a visual representation of today’s divergent career path development).

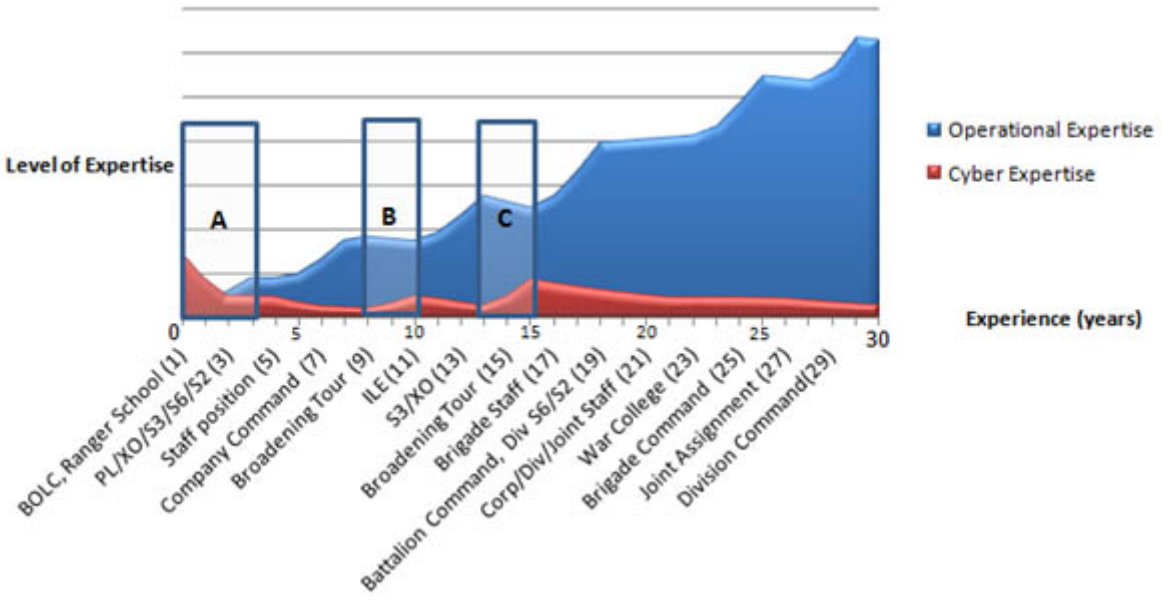

Figure 2: Based on typical officer positions held during a 30 year career, this is a visual representation of the expertise and experience gained by combat arms officers (represented in blue) who enjoy consecutive assignments in their domain reinforced by kinetic warfare-centric professional military education. Officers who focus in cyber (depicted in red) are typically forced out of a cyber position after a single tour (although this is currently being remedied). Note area A, which depicts the amount of expertise an officer enters the Army with if they studied a cyber related discipline. These skills diminish rapidly vice the operational officer, who rapidly gains experience after initial entry. Areas B and C depict what happens to a combat arms officer's operational expertise during their time away from troops, such as on a broadening tour; in contrast, these are one of the few times for an officer focused in cyber to develop professionally and gain further expertise in technical aspects of cyberspace operations.

Progress

We believe that the issues mentioned can be ameliorated or corrected through a unified cyber career path. Such a career path would help retain the talent we already have in uniform and reorganize it in a meaningful way. Retaining and expanding this talent pool is critical to the long-term success of the Army in cyberspace; as a result the Army is already in the process of addressing some of these challenges along several fronts:

> • **Cyber Skill Identifier:** The Army created the E4 Skill Identifier (SI), which can be awarded by ARCYBER to identify Soldiers, warrant officers, and officers who have served within operational cyber billets or who possess the required skills to conduct cyberspace operations.**[iv]**
>
> • **Creation of Human Resources Command Cyber Branch:** While not equivalent to a full Branch, such as Armor, Quartermaster, etc., Human Resources Command (HRC) created a provisional cyber branch to provide for the management of personnel being assigned to cyber units. When combined with the E4 SI, HRC will be better able to maintain visibility

of enlisted Soldiers, warrants, and officers with the requisite skills and talents for assignment decisions.[v]

• **Extended Tours for Cyber Personnel:** To allow Soldiers to develop the level of expertise required to be effective cyberspace operators, a normal length tour (two to three years) for Soldiers under ARCYBER is not effective. Rather, a tour length closer to five years is more appropriate and is under consideration.[vi]

• **Development of Cyber Military Occupational Specialists:** The Army has developed three primary cyber Military Occupational Specialties (MOS), one for the warrant officer corps and two for enlisted: 255S (Information Protection Technician Warrant), 25D (Cyber Network Defender), and 35Q (Cryptologic Network Warfare Specialist). These first two MOSs fall under the Signal Corps and the 35Q belongs to Military Intelligence. Other structural changes are under development and consideration.

• **Cyber Mission Forces:** The concept of an initial structure for the DoD's CMF was publicly disclosed in 2013.[vii] Even before the force's structure was disclosed, the Army recognized the emerging need and created the 780th MI Brigade to perform intelligence collection and, when called upon, to perform offensive operations.[viii] The Army has also created a unit primarily focused on defensive activities within the past year, now called the Cyber Protection Brigade,[ix],[x] and a one-star headquarters to oversee the two brigades known as the Joint Forces Headquarters-Cyber.[xi] The DoD is expanding its number of personnel within cyberspace operations to 6,000, with the Army tasked to create 41 of the 133 teams within the CMF structure.[xii],[xiii]

Figure 3: Notional branch insignia for an Army Cyber Branch.

The Cyber Operator

While the aforementioned progress certainly addresses some of the challenges facing the Army in developing a professional cyber officer force, the absence of a traditional branch will continue to marginalize cyber officers as outliers of traditional branches and stymie the career progression of capable and talented cyber officers. Such a branch would develop and cultivate capable officers in a proper career path consisting of an effective assessment paradigm as well as a carefully crafted series of training courses, education programs, broadening experiences (including industry engagement), and operational assignments of increasing responsibility in the cyber domain.[xiv] Figure 5 provides a succinct depiction of the career path we describe in this section.

Existing Stakeholders and a Cyber Branch

Currently, several major stakeholders in the cyber domain each own a piece of the puzzle required to create a unified cyber branch in the Army (see Figure 3 for a notional branch insignia). Unless these pieces are consolidated, and gaps filled, the Army's efforts to project power in cyberspace will languish. While consolidating all of the functions and personnel that comprise cyber operations will require transformation amongst the historical stakeholders, the primary missions of the Signal Corps, Military Intelligence, and several Functional Areas would continue once a cyber branch is established. Figure 4 depicts a comprehensive division of responsibilities between Cyber, Signal Corps, and Military Intelligence branches. We acknowledge that the lines drawn between the related functions may not be as clearly defined as depicted and they may challenge existing constructs, roles, and authorities as mandated by Congress and Executive actions. In order to create a Cyber Branch, new legislative frameworks and orders that allocate authorities in an appropriate way may be required, but are outside the scope of this paper.

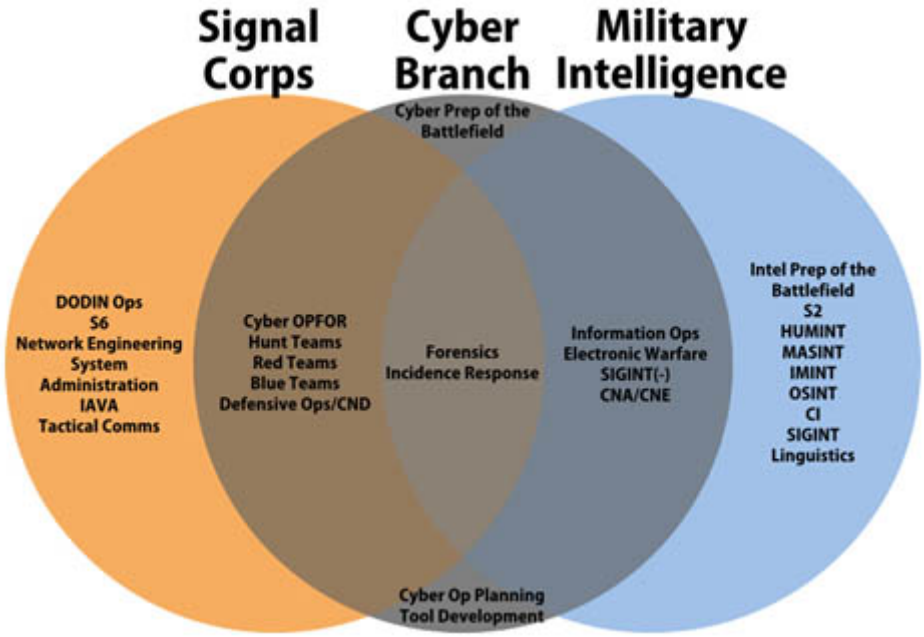

Figure 4: This diagram shows a proposed division of labor between Cyber, Signal Corps, and Military Intelligence branches. The roles shown in the extremes of the diagram would remain served by the traditional branches while those shown in grey would be subsumed by a Cyber branch.

Pre-Commissioning

For officers in the Cyber branch to become experts in their domain, the selection of an undergraduate major is vitally important as it lays the foundation for understanding the fundamental aspects of the cyber domain. Prospective officers should study in a discipline related to cyberspace operations, such as Electrical Engineering, Computer Science, Mathematics, Information Technology, or another closely related discipline. Such a foundation provides the officer a four year head start by capitalizing on, rather than disregarding, their undergraduate studies upon commissioning. Ideal candidates would take specialized courses in security, networking, programming, operating systems, cyber law, and cyber policy. Additionally, a proponent will need to develop the standards of technical competence, method of identifying, and process of vetting for potential Cyber branch candidates. We recommend Cadet Command, West Point, and the Army Cyber Institute collaborate to develop a formalized program (referred to from this point as the Cyber Leader Development Program (CLDP)) for performing these

tasks.

Selection and Assessment

Given the Cyber branch's somewhat unique requirements, we propose an accession model for a cyber branch that follows a combination of the functional area and Special Forces models, in which most officers will accede into the branch as senior first lieutenants or junior captains.**[xv]** However, due to the expertise an individual may possess prior to commissioning, we believe there should also be a limited number of direct accession allocations for highly qualified second lieutenants. While the requisite knowledge, skills, and abilities (KSAs) to serve in a cyber branch are still under development,**[xvi]** proper assessment and selection of officers that possess those KSAs is critical to achieve the desired competence of a cyber branch. As KSAs and other desirable attributes of cyber operators evolve, they can be used to refine the assessment and screening process to ensure an optimal match between individuals and requirements of the proposed branch. Our model provides several opportunities**[xvii]** that balance technical skill, leadership, operational Army experience, and force management:

> • Limited direct accession via traditional commissioning sources, including ROTC, USMA, and OCS for highly qualified lieutenants.
>
> • Branch details combined with assessment.**[xviii]**
>
> • Open accession into the Cyber branch between three and seven years of service.**[xix]**

Despite the fact that individual skills in the cyber domain atrophy notoriously quickly, we believe that a branch detail model can still be a viable path to accession.**[xx]** We envision the creation of a transition course for newcomers to the cyber branch. The course will be taken prior to the captain's career course, which will provide an opportunity to assess how well individuals have maintained their skills as well as subsequent refresher training.

An obvious criticism of our proposal would center around the lack of understanding direct-accession officers would have for the application of conventional land power as well as troop leadershipt gained from experience in line units. Clearly, this would be the case for officers who directly accede into the Cyber branch. However, officers who qualify for direct accession into the Cyber branch do so because they possess extremely relevant technical knowledge in a particular facet of cyberspace operations, which a truly professional cyber force necessarily requires. While we concede that officers who directly accede into the branch will lack this operational understanding initially, we do not suggest that cyber units and the Cyber branch as a whole should lack a greater understanding of Army operations – such a proposition is a recipe for disaster and irrelevance. The technical skills of the direct-accession officers will complement the line experience of branch detailed officers, and officers who accede later (see Figure 5). Further, our development model affords these direct-accession officers later assignment opportunities to serve with distinction in line units and gain better operational understanding.

"Bootstrapping" Initial Accession to Build a Cyber Branch

In our model, we recommend that initially, officers at all points in their career be allowed to apply for accession. The initial recruiting window will likely need to last for two to three years in order to allow all eligible and qualified officers the opportunity to apply. The degree prerequisite, aptitude, and skillset requirements should not be lowered during this time; a screening assessment should still be given to the

initial round of Cyber branch officers. Such a process would be similar to the Navy's effort to populate the senior levels of the Information Dominance Corps.[xxi]

Exceptional Cases

Despite the stringent requirements we recommend, the possibility for individual exceptions, on a case-by-case basis, should exist. For example, there may be individuals whose formal education is in a discipline totally unrelated to cyberspace operations, but who still possess the requisite KSAs required to pass the assessment tests and serve with distinction in the Cyber branch. These individuals should not be excluded from the accession process, but they should face the same rigorous assessment as other candidates.

Key Development

Lest officers be hurriedly funneled into and out of Key Developmental (KD)[xxii] positions wherein career progression devolves into a "check the block" mentality, we deliberately define KD positions broadly at all ranks to include any position coded for a Cyber branch officer.[xxiii] Educating Army promotion boards regarding KD positions within cyberspace operations is important to avoid confusion. [xxiv]

Company Grade (Lieutenant - Captain)

Officers should begin their company grade time with a solid foundation in the nature of cyberspace and during their company grade years learn the TTPs of cyberspace operations, including mission planning, execution, tool development, and post-mission assessment of cyberspace-only and hybrid cyber/kinetic operations. Initial assignments will cover all aspects of cyber operations: learning to engineer, defend, exploit, or attack networks and systems as well as the creation, analysis, evaluation, and detection of tools that perform those tasks. Company grade officers would spend the majority of their time performing the roles mentioned above and serving in leadership positions within the Cyber National Mission Teams, Cyber Combat Mission Teams, and Cyber Protection Teams.[xxv]

Field Grade (Major - Colonel)

While company grade development should include a sound foundation in the technical and tactical aspects of cyberspace operations, field grade development should prepare officers for greater responsibility and larger context of executing cyber operations, including legal and policy aspects as well as Joint, Interagency, and International collaboration. While the final organizational structure of a Cyber branch is beyond the scope of this paper, we assume that senior officers will need to serve in command and staff positions[xxvi] as well as in adviser/liaison roles to senior combat arms commanders.[xxvii] Additionally, at this point in their careers many officers within the cyber branch will possess a level of experience and expertise in cyberspace operations few outside of the military would be able to achieve.[xxviii] The talents of these officers should be leveraged and retained. Within FA24, FA53, FA29, and FA30, there exist similar career paths for officers to earn the rank of Colonel while remaining technically focused throughout their career. We believe this technical focus is an essential component of the Cyber branch, whether it be in tool development, reverse engineering, cyber operational planning, targeting, EW, etc. [xxix]

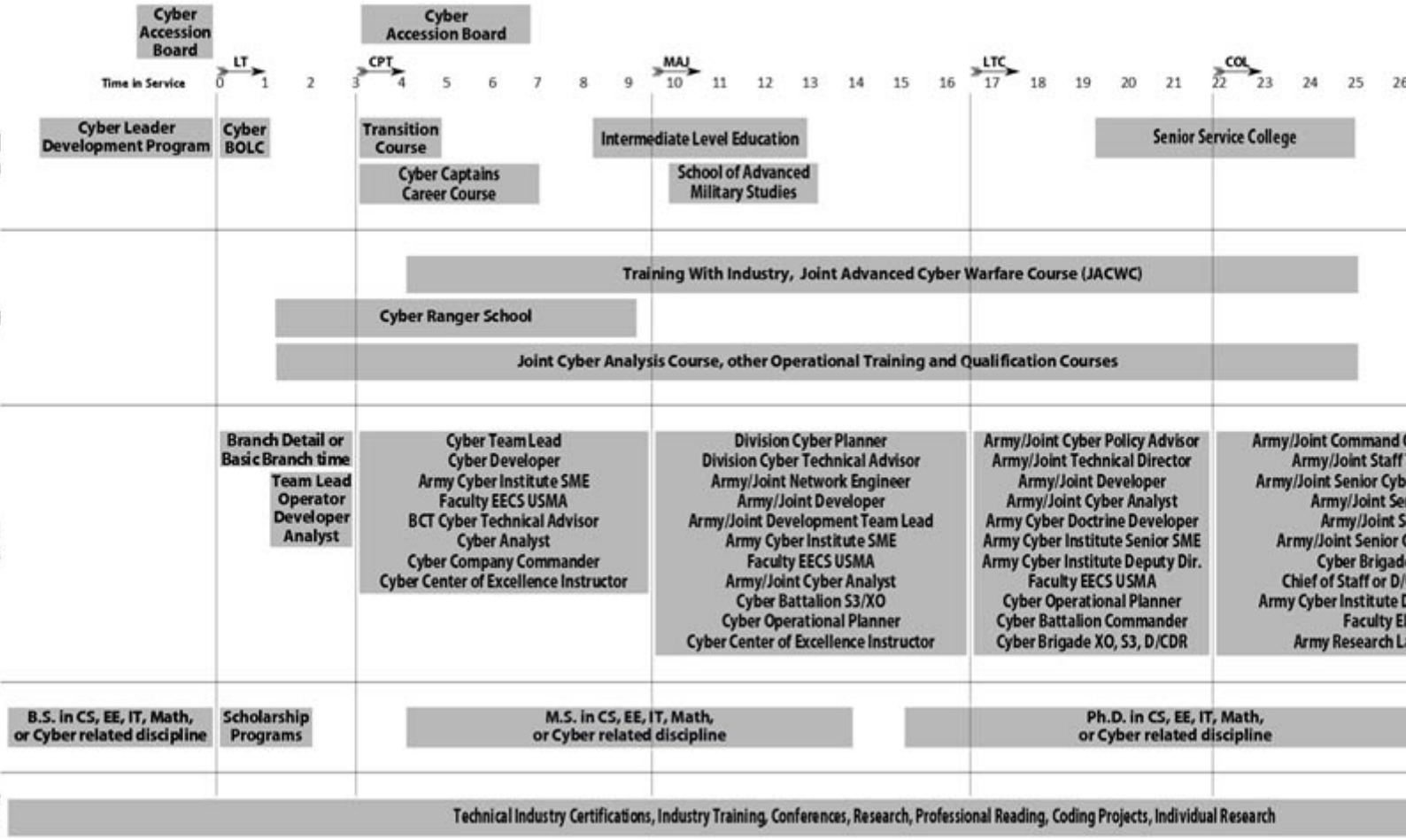

Figure 5: The Cyber branch officer career progression timeline, with deliberately generalized position titles, from pre-commissioning through colonel.

Conclusions

A viable career path must grow cyber leaders who are technical experts adept at leading a different breed of operator. We believe traditional leadership principles, such as “know yourself and seek self improvement,” and “be technically and tactically proficient,” absolutely apply, but the means by which one leads must be adapted to the nature of the missions in cyberspace and the skills of those whom one is leading.**[xxx]** Technical experience and a deep understanding of the nature of cyberspace are critical components to developing sound leaders capable of truly leading operations in cyberspace. While these bedrocks form the basis of our proposal, officers from a variety of backgrounds are currently being assigned into leadership positions in the cyber domain at all levels. These officers, including the authors, have strengths and weaknesses due to the nature of their upbringing – an upbringing that was tailored to the needs of something other than cyberspace operations. Without a purposeful, cohesive, and unified career path like the type that we have described, the Army will continue to find itself lacking the leaders it needs to fight and win on battlefields of the future. Over time, “homegrown” Cyber branch officers will come**[xxxi]** and we will develop leaders of cyber operations at all levels that are better than us. Regardless of our traditional backgrounds, we need not be afraid of these developments; we will rely on these future officers to keep our ever-increasingly technologically-reliant Army relevant and protected from the

unknown threats of the 21st century.

The views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, Army Cyber Command, the Department of the Army, US Cyber Command, the Department of Defense, or the US Government.

End Notes

[i] Jonalan Brickey, Jacob Cox, John Nelson, and Gregory Conti, "The Case for Cyber," Small Wars Journal, September 13, 2012.

[ii] For the purposes of this paper, we define cyberspace operations as: computer network defense (CND), computer network exploitation (CNE) and attack (CNA), electronic warfare (EW) activities, information (or influence) operations (IO), and some aspects of signals intelligence (SIGINT). We acknowledge this is a broad definition, but only by bringing together all of these intersecting and mutually supporting domains into a single cohesive team can we create a functional cyber force. Following directly from this definition, we will define cyber leaders as a select group of officers that are currently dispersed amongst several functional areas (FA) and branches: Signal Corps, Military Intelligence, FA 24 (Telecommunications Engineer), FA 29 (Electronic Warfare), FA 30 (Information Operations), and FA 53 (Information Systems). Not every officer within these fields should be considered a cyber leader, nor should we exclude officers from other branches or fields. We are starting with this definition because the preponderance of existing cyber leaders reside in these fields.

[iii] Todd Arnold, Rob Harrison, Gregory Conti, "Professionalizing the Army's Cyber Officer Force," November 23, 2013, Volume 1337.2, Army Cyber Institute. Available at http://www.usma.edu/acc/SiteCollectionDocuments/FULL\%20PACOF.pdf

[iv] LTC Chevell Thomas, "Human Resources Command stands up Cyber Branch," March 24, 2014, www.army.mil. Available at http://www.army.mil/article/122456/Human_Resources_Command_stands_up_Cyber_B

[v] Ibid.

[vi] CSM Rodney Harris, ARCYBER CSM, interviewed by Jared Servu in "Army ponders proper shape, size of cyber workforce", Federal News Radio, October 28, 2013, available at http://www.federalnewsradio.com/1195/3492533/Army-ponders-proper-shape-size-of-cyber-workforce

[vii] Allysa Sternstein, "Pentagon Plans to Deploy More Than 100 Cyber Teams by Late 2015," March 19, 2013. Available at http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948/

[viii] Tina Miles, "Army Activates First-of-its-Kind Cyber Brigade," December 9, 2011, 780th MI Brigade. Available at http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/

[ix] Siobhan Carlile, "Army recruiting highly qualified Soldiers, DA civilians to serve on new specialized Cyber Protection," October 8, 2013, 7th Signal Command (Theater) Public Affairs, Army.mil. Available

at
http://www.army.mil/article/112793/Army_recruiting_highly_qualified_Soldiers__DA_civilians_to_serve_on_new_speciali

[x] Cyber Protection Brigade, available at https://cpb.army.mil

[xi] Joe Gould, "Army Cyber Command names Fort Gordon as new headquarters," December 19, 2013, Army Times. Available at http://www.armytimes.com/article/20131219/NEWS04/312190018/Army-Cyber-Command-names-Fort-Gordon-new-headquarters

[xii] Chuck Hagel, Retirement Ceremony for General Keith Alexander, March 28, 2014, available at http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1837

[xiii] Michael O'Connel, "Army CyberCom meets challenge of recruiting cyber warriors," October 23, 2013, Federal News Radio. Available at http://www.federalnewsradio.com/398/3489371/Army-CyberCom-meets-challenge-of-recruiting-cyber-warriors

[xiv] The U.S. Army's canonical guide to officer development and career management is "Department of the Army Pamphlet 600-3: Commissioned Officer Professional Development and Career Management," February 1, 2010. We used this document as a template for the following sections.

[xv] Todd Arnold, Rob Harrison, Gregory Conti, "Professionalizing the Army's Cyber Officer Force," November 23, 2013, Volume 1337.2, Army Cyber Institute. Our original analysis of a way forward for an officer career path considered six COAS, each with varying degrees of effectiveness and requisite change. The analysis is available at http://www.usma.edu/acc/SiteCollectionDocuments/FULL\%20PACOF.pdf

[xvi] Mike Milford, "Leader Development, Education and Training in Cyberspace," Army.mil, August 1, 2012. Available at
http://www.army.mil/article/84754/Leader_development__education_and_training_in_cyberspace/

[xvii] We considered direct commissioning for officers, similar to the Navy's program for direct commissioning of recent college graduates as Ensigns into Information Warfare (see http://www.navycs.com/officer/informationwarfareofficer.html), but that option should be limited if traditional commissioning sources are permitted to commission officers directly into a Cyber branch.

[xviii] According to Army Pam 600-3: "When required, some lieutenants are branch detailed to a combat arms branch for 3 or 4 years, or until their life-cycle or cyclic units are in a reset period. Under the branch detail program, officers attend the company grade level education at the school of the branch to which they are detailed. Company grade officers in the 4-year detail program receive transition branch training in conjunction with their enrollment in the captain's level education."

[xix] These officers should have to demonstrate the same level of competence required for direct accession. Failure to pass the screening assessment or the transition course will result in the officer being returned to their basic branch or functional area.

[xx] Gregory Conti, James Caroland, Thomas Cook, and Howard Taylor; "Self-Development for Cyber Warriors;" Small Wars Journal, 10 November 2011, http://www.rumint.org/gregconti/publications/893-

conti.pdf

[xxi] Ed Barker, “Information Dominance Warfare Officer ’Grandfather’ Qualification Available on Navy eLearning,” Naval Education and Training Command Public Affairs, October 6, 2010, http://www.navy.mil/submit/display.asp?story_id=56425

[xxii] Key Developmental (KD) positions are mandatory positions in which an officer must serve in order to remain competitive for promotion. If constrained to only a single or very few positions, this will incentivize officers to aggressively seek out these positions – typically company command for Captains and Battalion Operations Officer (S3) or Battalion Executive Officer (XO) for Majors. Officers typically queue up to rotate into and out of these positions, resulting in a high turnover rate and sometimes a poor match between an individual’s experience and the mission of a unit. This approach creates a “check the block” career progression model.

[xxiii] Our suggested approach parallels that of many functional areas, where service in a position coded in a functional area is all that is required to accomplish the KD requirement for promotion.

[xxiv] Some traditional Army branches have deliberately constructed their organizational structure to mirror combat arms units, i.e. as companies, battalions, and brigades to better mirror the expectations of promotion boards. If Cyber branch officers cannot be protected by promotion boards that properly understand technical KD positions, this use of combat arms unit nomenclature for jobs should be considered.

[xxv] For a more comprehensive and detailed list of potential positions, please see our prior work.

[xxvi] Following the FA24/FA53/FA29/FA30 models, we believe only the officers who volunteer for these positions should be considered for centralized selection list (CSL) billets and only Cyber branch officers should be considered to fill cyber CSL billets.

[xxvii] The integration of cyber operations into kinetic warfighting will likely continue to evolve and field grade Cyber branch officers should serve as primary staff officers within Army and Joint level tactical formations. This broadening assignment to a traditional kinetic Army formation would be highly beneficial to maintain an awareness of current Army operations and an understanding of how to bring true utility to the kinetic warfighting community.

[xxviii] We also expect most Cyber branch field grade officers will achieve some level of graduate level education, ideally completing a Masters and possibly a Ph.D., in a discipline relevant to cyberspace operations.

[xxix] For a more comprehensive and detailed list of potential positions, please see our prior work.

[xxx] Gregory Conti and David Raymond. “Leadership of Cyber Warriors: Enduring Principles and New Directions,” Small Wars Journal, July 11, 2011.

[xxxi] This year, for the first time ever six graduating USMA second lieutenants are being assigned directly to one of the brigades within the CMF. These individuals represent the first opportunity for an

Army officer to rise through the ranks serving exclusively in cyberspace operational assignments. See http://www.businessweek.com/videos/2014-05-26/cyber-cadets-west-point-graduates-hackers

About the Authors

Todd Arnold

Major Todd Arnold is an FA24 and former Signal Corps officer. He is a research scientist in West Point's Cyber Research Center and an Assistant Professor in the Department of Electrical Engineering and Computer Science (EE&CS). He holds an M.S. from the Pennsylvania State University and a B.S. from West Point, both in Computer Science. His previous assignments include two tours in Operation Iraqi Freedom (OIF) with the 22d Signal Brigade, serving in the G33 of Army Cyber Command, and developing, testing, and analyzing CNO capabilities in support of current and future contingency operations for NSA and USCYBERCOM.

Rob Harrison

Major Rob Harrison is an FA24 and current Assistant Professor in the Department of EE&CS at the United States Military Academy. He holds an M.S.E and B.S. from Princeton University and the United States Military Academy, respectively, in Computer Science. Rob has completed three combat tours in support of OIF with both conventional Signal Corps and Special Operations units in a variety of capacities.

Gregory Conti

Colonel Gregory Conti is a Military Intelligence Officer and Director of the Army Cyber Institute at West Point. He holds a Ph.D. from the Georgia Institute of Technology, an M.S. from Johns Hopkins University and a B.S. from West Point, all in computer science. He has served as a senior adviser in USCYBERCOM Commander's Action Group (CAG), as Officer in Charge of a deployed USCYBERCOM Expeditionary Cyber Support Element, and co-developed USCYBERCOM's Joint Advanced Cyber Warfare Course. He served in the Persian Gulf War and in Operation Iraqi Freedom.

Available online at : http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers

Links:
{1} http://smallwarsjournal.com/author/todd-arnold
{2} http://smallwarsjournal.com/author/rob-harrison
{3} http://smallwarsjournal.com/author/gregory-conti-0

{4} http://www.army.mil
{5} http://www.army.mil/article/122456/Human_Resources_Command_stands_up_Cyber_B
{6} http://www.federalnewsradio.com/1195/3492533/Army-ponders-proper-shape-size-of-cyber-workforce
{7} http://www.nextgov.com/defense/2013/03/pentagon-plans-deploy-more-100-cyber-teams-late-2015/61948/
{8} http://www.army.mil/article/70611/Army_activates_first_of_its_kind_Cyber_Brigade/
{9} http://www.army.mil/article/112793/Army_recruiting_highly_qualified_Soldiers__DA_civilians_to_serve_on_new_speciali
{10} https://cpb.army.mil
{11} http://www.armytimes.com/article/20131219/NEWS04/312190018/Army-Cyber-Command-names-Fort-Gordon-new-headquarters
{12} http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1837
{13} http://www.federalnewsradio.com/398/3489371/Army-CyberCom-meets-challenge-of-recruiting-cyber-warriors
{14} http://www.army.mil/article/84754/Leader_development__education_and_training_in_cyberspace/
{15} http://www.navycs.com/officer/informationwarfareofficer.html
{16} http://www.rumint.org/gregconti/publications/893-conti.pdf
{17} http://www.navy.mil/submit/display.asp?story_id=56425
{18} http://www.businessweek.com/videos/2014-05-26/cyber-cadets-west-point-graduates-hackers