Professionalizing the Army's Cyber Officer Force

Todd Arnold, Rob Harrison, Gregory Conti

Department of Electrical Engineering & Computer Science
United States Military Academy
West Point, NY 10996
{todd.arnold, rob.harrison, gregory.conti} @usma.edu

Vol 1337 No. II
23 November 2013

ACC
Army Cyber Center

Abstract

The emergence of cyberspace as an operational domain, accompanied by the Army's realization that cyber operations are both a critical vulnerability and a massive opportunity, drives the need for an integrated and fully qualified Army cyber officer workforce to meet these challenges and opportunities.[1]

In this paper, we argue for a revolutionary step forward: the creation of a unified cyber branch that brings together the best from each of the stakeholder communities, fills critical gaps not currently provided by the current stakeholders, and discards vestigial remnants from cold-war era organizations, personnel structures, and human resource management approaches. We seek to design a cyber career path that is best for the Army while setting aside near-term parochial concerns for preservation of the status quo. This objective directly supports other transformational Army initiatives including the proposed formation of a Training and Doctrine Command (TRADOC) Cyber Center of Excellence (CCoE), the Army Cyber Center at West Point, Cyber Mission Forces, and Army Cyber Command (ARCYBER).[2]

We propose an actionable way forward to realize a professional cyber force by describing current obstacles, exploring multiple options for the creation of such a force, and finally proposing an accession-based branch and officer career progression which covers the entire career of a cyber leader from college undergraduate to post-retirement.

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

[2] Joe Gould. "New center, school to bring signals, cyber, EW together." Army Times, 1 July 2013 p. 18.

1 Introduction

The need for a unified cyber career path is driven by operational necessity and a demand for efficiencies: our nation faces a critical national threat in cyberspace while today's disparate cyber stakeholders duplicate resources, induce friction, and lack the strength of a unified team. In order to properly face the numerous threats in cyberspace, the Army needs to invest in the development of leaders with the technical acumen and strategic vision to build and lead its cyber forces.

This is not the first time the Army has faced the challenge of integrating a revolutionary technology that demands changes to its force structure, personnel management, and doctrinal foundations. In 1912, the Army experimented with integrating aviation assets as part of the Signal Corps. At the time, Army leaders considered the new, yet inchoate capability relevant only for direct support to ground troops. The limitations of the Army's aviation vision were exposed immediately when deployed to support an actual combat mission – Pershing's expedition against Poncho Villa. In this expedition, aviation assets, as conceived and employed by traditional Army leadership, failed to function on a rudimentary level. Meanwhile, our future allies during World War I were learning the importance of air power during the early years of that conflict. This learning process introduced to our European friends the effects that air power could provide to land conflict – effects that were not at all appreciated by contemporary Army leadership. After witnessing the lethal effects air power can offer, a few Army leaders returned from their experiences in WWI with insights into how aviation assets might be integrated into the next land conflict. LTC Billy Mitchell fervently appealed to his contemporaries and tried to convince them that aerial warfare was equivalent to warfare on land and sea and should be made its own service.[3]

Similarly, the Army now looks to expand its capabilities in cyberspace as it once expanded its presence in the skies. These transformational efforts benefit from the absence of concurrent open hostilities between sovereign nations, which would only blur the lines between *normative* solutions to the cyber problem and *timely* solutions that might yield some immediate tactical or operational gain.[4] Despite the myriad and disparate efforts intended to propel the Army towards successful cyber capabilities, the current patchwork efforts run counter to Billy Mitchell's argument that, "only an independent organization manned by airmen could develop the full potential of aeronautics,"[5] which should be applied to developing an effective and sustainable fighting force in cyberspace.

The Army and the greater Department of Defense's (DoD) experience with the Air Force seems to intimate the need to create a fourth branch of service to be given primacy over the cyber domain.[6] However, we contend that the creation of service specific cyber components is only one possible future step in the maturation process of operating in a new domain. Following the Air Force example, the Air Force serves as the primary component for air operations within combatant commands,

[3] Alfred F. Hurley, "Billy Mitchell: Crusader for Air Power", Indiana University Press, 1975.

[4] Although some would argue that a cyber war has already begun, such as Bob Violino in "Unseen, all-out cyber war on the U.S. has begun"(available at `http://www.infoworld.com/d/security/unseen-all-out-cyber-war-the-us-has-begun-211438`, there is no official declaration of hostilities from any of the parties allegedly involved.

[5] Hurley, pg 47

[6] Gregory Conti, John "Buck" Surdu, "Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of the Military?," *Information Assurance Newsletter*, Vol. 12, No. 1, Spring 2009, pp. 14-18, `http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf`

even though the Army, Navy, and Marines all maintain their own service specific air assets. Previously, the Army and the Navy each had a separate air component for roughly 35 years until the Air Force was established out of the Army Air Corps. Similarly, the Special Operations community developed out of service specific components and has progressively transformed into a functional combatant command; a process that took approximately 25 years.[7] Within the DoD, each of the services is trying to retain as much control as they can over operations in cyberspace, but if we are to realize the full potential this new domain, we will need to rise above inter- and intra-service priorities.[8]

Regardless of the final outcome of incorporating cyber operations, there will be a requirement for officers who are competent and well versed in cyber, who we will collectively refer to as 'cyber leaders.' In order to make the case for the development of cyber leaders, we must first define the domain in which these leaders will operate. For the purposes of this paper, we define cyber as: the engineering and construction of computer networks, computer network defense (CND), computer network exploitation (CNE) and attack (CNA), electronic warfare (EW) activities, information (or influence) operations(IO),[9] and collecting, processing, producing, and disseminating signals intelligence (SIGINT).[10] Naturally, we consider the ability to develop targets, plan operations, and integrate actions across all the aforementioned subdomains an integral component to cyber. However, these aspects are neither endemic nor exclusive to the cyber domain itself, rather they are common across all operational domains, and as such are omitted from the preceding list.

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.

In the following sections, we will discuss challenges hindering the Army's efforts to establish a professional cyber force, compare possible courses of action to place the Army on a sustainable way ahead towards developing a cyber force, further refine our definition of cyber and cyber leaders, lay out a potential career path for officers within the Army's cyber force structure, recommend actions to bootstrap the process of creating a cyber force, examine current efforts to develop a cyber force, and discuss future work based on our recommendations.

[7] We are basing this off the the establishment of the Army Special Forces in 1962 to the creation of Special Operations Command (SOCOM) in 1987, U.S. SOCOM, "History of SOCOM 1987 – 2007", `http://www.fas.org/irp/agency/dod/socom/2007history.pdf`

[8] James Stavridis, "The New Triad: It's time to found a U.S. Cyber Force", Foreign Policy, June 20, 2013, `http://www.foreignpolicy.com/articles/2013/06/20/the_new_triad`

[9] Addendum K - Cyberspace: Army Cyber Command and Cyberspace Operations. 2012 Army Posture Statement, United States Army.

[10] U.S. Army Publishing Directorate, "Department of the Army Pamphlet 600-3: Commissioned Officer Professional Development and Career Management", February 1, 2010.

2 Challenges

In combat arms branches, the Army accepts nothing less than 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. To develop this level of mastery, an ideal cyber leader must be proficient in four areas: technical expertise, leadership, operational fluency, and intelligence/targeting.

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

In this section, we will discuss the current obstacles preventing the Army from consistently and reliably producing leaders capable of achieving these ideals.

2.1 The Changing Nature of Communications and the Military

Traditionally, doctrine emerges from innovation by the operational force, where it is codified over time into doctrine by experts in their fields with years of operational experience. Even with the Army's current standard of reviewing doctrine every 18 months to determine the doctrine's currency,[11] the development of cyber doctrine is lagging. In an era where the rate of change of technology is rapid, we need an agile doctrine development process that can integrate cutting-edge technology into cyber operations. Without leaders who understand cyber operations writing doctrine, this goal will remain elusive.

The exponential pace of technological change is also causing massive doctrinal shifts in existing forces. Continued advances in communications technology may drive many traditional Signal Corps functions into extinction. During the past century, communicators built battlefield networks with a wide variety of bulky communications assemblages with constrained bandwidth; today, most people carry always-on, 3G+ smart phones in their pockets. Austere, dynamic conditions will continue to necessitate battlefield communications personnel, but a smart phone in every soldier's pocket remains a real possibility in the near future. Senior Signal Corps leaders have framed their future strategy with this in mind as demonstrated in the 2011 "Micro-cyber" initiative which sought to "serve more people with smaller systems and to do all this with the same staffing levels and no funding increase"[12]

Army training paradigms are facing similar challenges. By design, Training and Doctrine Command (TRADOC) develops objectives, standards, and courses to adequately prepare our warfighters to perform their battlefield functions. Traditionally, these products are slow to evolve once established. However, in the cyber domain training ages quickly as new technologies, tactics, techniques and procedures (TTPs) develop or expire. Additionally, many cyber technologies and TTPs

[11] U.S. Army Publishing Directorate, "Army Regulation 25-30: The Army Publishing Program", March 27, 2006.

[12] Capabilities Development Integration Directorate, U.S. Army Signal Center of Excellence. "Micro-cyber: Future of Signal Regiment," Army.mil News Archive, 24 June 2011.

are developed outside of the Army and the greater military as a whole; adopting and integrating these external resources can be slow and goes against traditional Army methodology.

2.2 Nominal Transformation

While doctrine is being developed at the Department of the Army level, some communities within the force are making a superficial effort to stake out their own territory in the new cyber domain. In an attempt to defer or avoid necessary change and maintain nominal relevance, some military organizations have appended the term "cyber" to label job titles and training courses without substantive alteration commensurate with the title. An equally ineffective strategy is used to attract additional resources. As a result of this phenomenon, one really cannot trust that a course, job, or organization is actually relevant to the cyber fight just because it is branded "cyber."

These trends in faux-branding belie efforts by cyber leaders to build a foundation of trust with the kinetic warfighting community. Commanders are already integrating cyber capabilities into their operations.[13] However, if some cyber organizations exist in name only we risk overselling these capabilities to the tactical warfighter, who demands, and should expect, reliable and timely cyber effects. Additionally, the Army is not at a point where it can easily integrate cyber effects into kinetic operations.[14]

2.3 Personnel and Force Structure Issues

2.3.1 Lack of a Unified Team Effort

The integration of cyber operations with the traditional kinetic force requires a team effort between the warfighting community and all of the cyber stakeholders. However, there exists a lack of unity between all of the communities who own a fraction of the overall cyber fight. Qualified cyber officers and true cyber 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 defined as cyber and within which the preponderance of cyber leaders exist.

Allowing isolated pockets of expertise to head in different directions reduces efficiency, creates unnecessary friction, and wastes resources. For instance, personnel conducting offensive and defensive cyber operations are not on the same team right now.[15] Traditionally, Signal Corps and Military Intelligence SIGINT communities have executed defensive and offensive cyber operations, respectively. However, there is a significant cultural and technical divide between these two communities despite their similarities. Rather than building diverse and flexible teams based on individual specialized talents, existing cyber units currently group homogenous pockets of Signal Corps or Military Intelligence personnel across the spectrum of build, operate, defend, exploit, and attack operations. For example, current efforts to create Cyber Protection Teams primarily focus

[13]Raphael Satter, "Afghanistan Cyber Attack: Lt. Gen. Richard P. Mills Claims To Have Hacked The Enemy", Huffington Post, August 24, 2012, http://www.huffingtonpost.com/2012/08/24/afghanistan-cyber-attack-richard-mills_n_1828083.html

[14]Matthew Miller, Jon Brickey, and Gregory Conti. "Why Your Intuition About Cyber Warfare is Probably Wrong." Small Wars Journal, November 29, 2012, http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong

[15]Nicole Blake Johnson. "Cyber Command Seeks To Close Gaps in Offensive, Defensive Skills" Defense News, 1 August 2013.

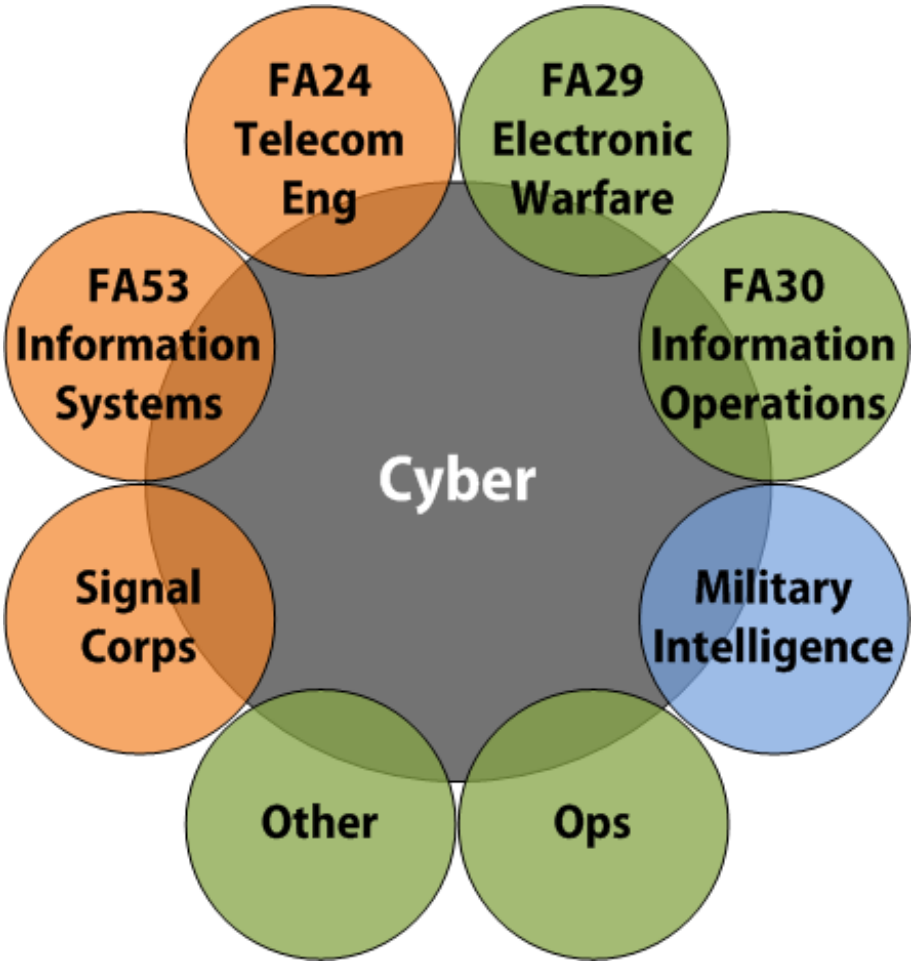

Figure 1: We defined cyber as building and operating networks, CND, CNA, CNE, EW, IO, and SIGINT. In this figure, we can see the different branches and functional areas which perform a portion of cyber operations as well as the existing gap covered by no existing career specialty.

on defense only, and the supporting billets consist primarily of Signal Corps Officers.[16,17] These efforts do not overcome the traditional divide between stakeholders; rather they widen the divide and strengthen the barriers between them. One would not expect to train Infantry officers in only the defense or only the offense and then assign them to defensive-only or offensive-only Brigade Combat Teams. Similarly, our efforts in cyberspace should not be fractured in such a deleterious way either.

2.3.2 Personnel Management

The number of different players in the cyber domain causes friction within the personnel system as well. Assignment officers are well equipped to manage general personnel requirements that fall

[16]"7th Cyber Protection Teams are looking for you", Fort Gordon PAO, available at `http://www.ftgordonsignal.com/news/2013-07-12/Community_Events/7th_Cyber_Protection_Teams_are_looking_for_you.html`

[17]"Army to have two cyber protection platoons in place this summer", Defense Systems Staff, available at `http://defensesystems.com/articles/2013/06/04/netcom.aspx`

within well-established norms. They are ill-equipped to manage specialized requirements at the fringes of existing branches. The problem is exacerbated by coarse grained personnel tracking databases that do not provide mechanisms to track technical certifications, security certifications, or specialized training outside of the Army system.[18]

Personnel managers handle the complexity of manning the force by coding billets in organizations for a particular military occupational specialty. However, since there is no cyber career field, leaders are forced to choose from a pool of limited existing career fields. Unfortunately, once a particular slot is coded for a given specialty, the rest of the force is effectively excluded, including officers with cyber skills who did not happen to choose the correct branch or functional area. While generalist billet codes (such as 01A) exist, assignment in these positions is often detrimental to traditional career paths and filled as a last resort by assignment officers. Dynamically recoding billets is not a practical option with today's personnel management systems.

2.3.3 Disservice of Permanent Change of Station

The detriment of Permanent Change of Station (PCS) moves was precisely described by the current Command Sergeant Major (CSM) of ARCYBER, CSM Harris, whose background is as an Infantry soldier:

> "The Army has some programs that say if you stay in the same place for four to five years and you don't get promoted, you're probably going to be looked at for promotion stagnation and maybe get separated from the Army. And initially, that's what's happened. We've thrown some of our soldiers out because we require them to be in cyber for five to 10 years in order to be really effective. It's exactly the opposite of what the Army thinks is right, but in terms of a cyber soldier, it's 100 percent right."[19]

PCS norms create additional hurdles. Soldiers are typically forced to move every 2-3 years. Successful careers usually result from rotating through assignments at a variety of locations that are a center of gravity within a leader's particular career field. Failure to seek assignments at multiple centers of gravity is considered "homesteading" and is detrimental to a career. The challenge arises because the vast majority of cyber assignments are in the Washington, D.C. metro area. With only limited rotation possibilities elsewhere, Soldiers can appear to be homesteading when in fact they are gaining the experience, expertise, and career development necessary for a cyber leader.

2.3.4 Confusion and Discontent in the Next Generation of Cyber Leaders

The lack of a dedicated career path leads future leaders to make poor choices about which career field to enter. Cadets and junior officers with the requisite skills who seek to serve the Army as a cyber leader are often mismatched between their passion and skills and their best guess at an appropriate branch. The lack of a clear choice leads to discontent and disillusion. Such discontent

[18]The Army is attempting to rectify this problem by allowing certain certifications to be tracked on the Army's Officer Record Brief (ORB), but the certifications that can be tracked have limitations and are restricted to a small and specific list. For instance, even if course is on the accepted list it is not allowed to be added if the officer paid for and attended the course on their own initiative.

[19]CSM Rodney Harris, ARCYBER CSM, interviewd 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`

and the inability of an officer to serve in a relevant position until after branch qualification as a senior captain poses serious retention issues. This point is being made simultaneously at both the most senior and junior ranks:

> "We have to have a way to manage the talent in this because it takes a long time to train them, and we can't just put them in a regular unit or we lose them."[20]

> "The Army loses a lot of its cyber ability because talented junior officers who possess deep technical skills for the Army get told they must wait until they are mid-to–senior level captains."[21]

Senior leaders are making a concerted effort to pull some of the most talented individuals into cyber assignments. While this effort is a positive step, these junior officers who take the assignments do so without a clear career path. If we do not provide this path for them, they will likely find themselves at a severe disadvantage when competing for promotion at a time when the Army is desperately seeking to expand its cyber talent pool while simultaneously reducing its number of personnel. In addition, officers who may not be best qualified to lead cyber organizations, but are successful in traditional career paths may find themselves put into a position of leadership in a rapidly growing cyber force, disadvantaging successful operations and their soldiers.

2.4 Lack of Career Long Cyber Expertise Development

One of the greatest strengths of our Army is the career-long professional development of combat arms officers. These officers proceed from successive assignments of increasing complexity, and approximately every five years receive substantial professional military schooling ranging from six to twelve months. During an officer's career, they will likely receive broadening experiences outside their specialty, which might include Joint service, Training With Industry (TWI), or advanced civil schooling. As a result, the U.S. Army's combat arms leaders are among the best in the world.

Unfortunately, the same is not true for those seeking to specialize in cyber operations. In the current human resources environment, an officer may receive support in pursuing a single tour in a relevant cyber position. Rarely will an officer be permitted to chain together multiple assignments in the cyber domain which is completely opposite from the combat arms world where officers are actively sought out by organizations following an officer's successful performance in a key leadership position. In some cases, assignment officers may assign those coming out of cyber positions into punitive assignments because some cyber positions are considered to be "taking a knee" time away from the "real Army." Clearly, this philosophy needs to change in order to grow cyber leaders rather than drive those prospective leaders out of the Army. The Army should be attempting to grow cyber leaders who are as respected in their tradecraft as combat arms officers are in theirs. Figure 2 compares the career development of combat arms leaders versus leaders who wish to pursue a career in cyber operations.

[20] LTG Edward Cardon, ARCYBER Commander, interviewed by Joe Gould in "Official: Army needs better cyber management," Army Times, November 7 2013, http://www.armytimes.com/article/20131107/NEWS04/311070029/Official-Army-needs-better-cyber-management

[21] Anonymous USMA cadet on his decision to cross commission into the Air Force to pursue a career in cyber.

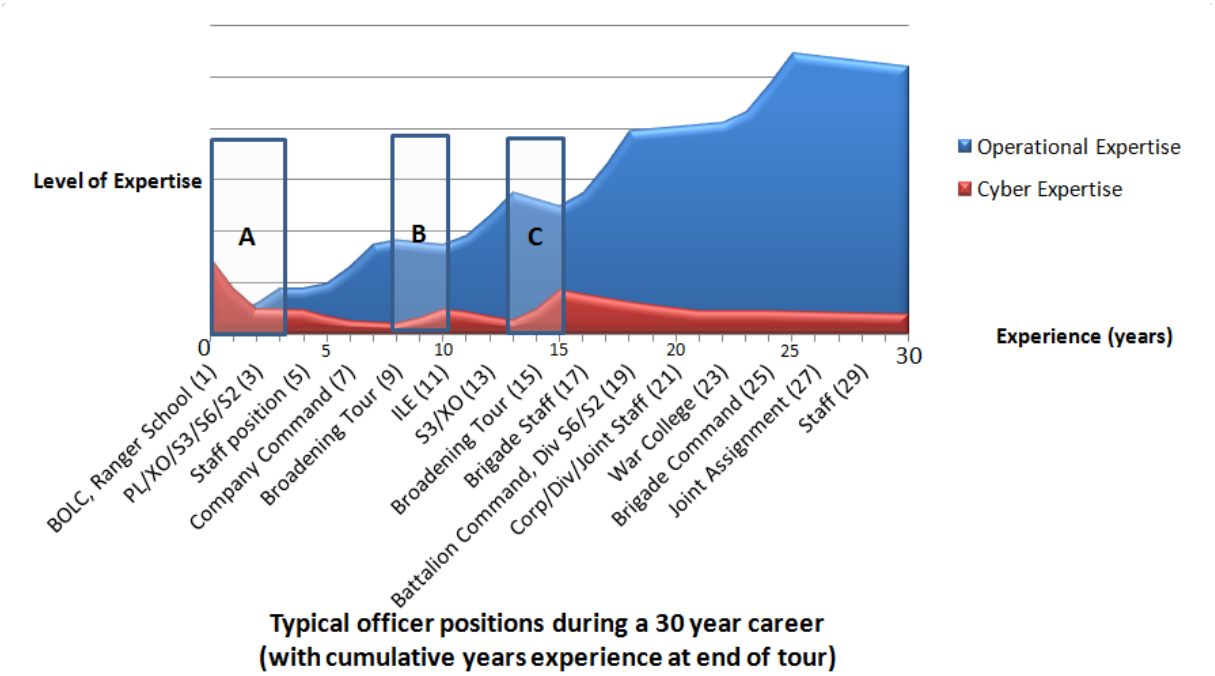

Figure 2: A visual representation of the career expertise and experience gained by combat arms officers (represented in blue) who enjoy consecutive tours in their domain buttressed by kinetic warfare-centric professional military education. Officers who focus in cyber (depicted in red) are typically forced out of a cyber position after a single tour. 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 expertise during their time away from troops, such as on a broadening tour; these are one of the few times a cyber focused officer can focus in his area and gain cyber expertise.

Lack of expertise hampers the ability of senior leaders to discriminate between reality and snake oil when assessing proposed contracts, evaluating the performance of contractors, or understanding the effectiveness of cyber weaponry. While a certification may serve as an indicator of potential capability, the certification alone is unlikely to be sufficient to judge an individual's merit. A leader might believe that the Certified Information Systems Security Professional (CISSP) certification is indicative of an elite level of expertise, where in reality the CISSP is more at the Journeyman level. Some of the best security and technical practitioners in industry eschew certifications and avoid organizations that rely too heavily upon certifications in their hiring processes. The overreliance on certifications is rightfully believed by these individuals to be an indicator of a potentially dysfunctional personnel structure.

2.5 Generalist Leaders

A common misconception is that a good leader can lead any type of unit. However in order to command a maneuver unit, an officer is expected to follow a branch-specific, career-long development-model depicted in Figure 2. Similarly, the Army should expect its cyber leaders to possess a commensurate expertise in their chosen field as that required from combat arms officers. However, some of the most qualified cyber leaders reside in Functional Areas 24 and 53, but these

COA	Solution	Description
1	Skill Identifier(s)	Assign formal skill identifiers to personnel with cyber-specific training or experience.
2	Creation of Functional Area(s)	Create a new functional area or areas that cover gaps in existing specialty fields.
3	Creation of a Career Field	Create a career field, akin to the Maneuver, Fires and Effects (MFE) career field composed of all cyber related Branches and Functional Areas. Service members compete for promotion against this population.
4	Creation of a Branch / Career Management Field (CMF)	Create a cyber branch, akin to Infantry, Aviation, or Military Intelligence that incorporates all branches with cyber related functions. Service members compete for command opportunities and promotion against this population.
5	Creation of a Special Forces like Branch within the Army	Create a branch with rigorous assessment criteria, incorporates only the cyber related functions of existing branches, and is able to fill the gaps in existing requirements.
6	Creation of a separate Cyber Service	Create a entirely new military service, peer to the Army, Navy, and Air Force for Cyber.[22]

Table 1: Potential COAs for managing cyber expertise within the Army.

officers are ineligible for Centralized Selection List (CSL) command. Further, the officers from FA24, FA29, FA30, and FA53 are all encumbered by a glass ceiling at the rank of Colonel. To date, only two officers from this population, an FA53 and an FA30, have reached general officer ranks. To some extent, this promotion record may indicate the maturity of the functional areas assessed to flag grade. Regardless, these results clearly substantiate the existence of a glass ceiling for some of our most technically skilled officers.

3 Paths Towards an Army Cyber Force

The challenges we have described are substantial, but they are not insurmountable. We believe that each of the issues mentioned can be ameliorated or corrected through a viable 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 is critical to the long term success of the Army in cyberspace. In our analysis, we considered six courses of action (COAs) to overcome these challenges, each with varying degrees of effectiveness and requisite change. A brief description of each COA can be seen in Table 1.

[22] James Stavridis, "The New Triad" Foreign Policy, 20 June 2013.

3.1 COA 1: Skill Identifier(s)

The easiest COA to implement is the creation of multiple skill identifiers that allow the Army to track individuals with given skill sets. We see this today in skill identifiers for Soldiers that complete the three week Airborne School.[23] This solution is relatively easy to implement and integrate into current personnel management systems. However, this solution does not clarify the management and assignment of skilled cyber operators and the skill identifier system is too coarse grained to handle specific talents.

3.2 COA 2: Cyber Functional Area(s)

In the 1990s, the Army underwent significant change in the management of officer careers with the enactment of Officer Personnel Management System XXI (OPMS XXI), which presciently created important new functional areas, such as FA40 (Space), FA30 (Information Operations), and FA24 (Network Engineer), and revitalized others, including FA53 (Information Systems Management).[24] Similarly, the Army could do the same with cyber. Efforts are already underway exploring this possibility; for example, the Signal Corps proposed incorporating aspects of FA53 and FA24 into an inchoate functional area FA26 dedicated to cyber security.

While the Army benefited from these earlier changes in officer management, this COA would not address one of the major shortfalls discussed in Section 2.3.1: the lack of a team effort. An existing stakeholder branch would likely become the proponent for a cyber functional area, thus perpetuating the lack of a unifying effort. Worse yet, if multiple functional areas were created across existing branches, then the segregation between offensive and defensive specicialties could become more ossified and difficult to overcome.

3.3 COA 3: Cyber Career Field

The creation of a Cyber Career Field as a peer to the current Maneuver, Fires, and Effects (MFE), Operations Support (OS), and Force Sustainment (FS) career fields would better organize the disparate specialties and partially increase fair promotions and command selection, but again would do little to build a unified team or overcome gaps in technical expertise.

3.4 COA 4: All Encompassing Cyber Branch

The next option would be the creation of a separate Cyber branch as a peer to Infantry, Armor, Field Artillery, etc. This "mega" branch could be an entirely new construct, which would assimilate the Army's cyber-related branches and functional areas as well as expand to fill existing gaps. This COA brings disparate cyber-related branches and functional areas into a single cohesive team. However, incorporating all members of existing cyber-related branches and functional areas into a new Cyber Branch could create a cumbersome branch that is consumed by internal conflict as traditional cultures posture for priority.

[23] U.S. Army Publishing Directorate, "Department of the Army Pamphlet 611-21: Military Occupational Classification and Structure," January 27, 2007.

[24] OPMS XXI Task Force. OPMS XXI Final Report. United States Army, July 9, 1997.

3.5 COA 5: Special Forces-like Cyber Branch

This would also create a cyber branch, but it would be constructed using a Special Forces-like model with rigorous entry requirements and the ability to recruit and select highly qualified individuals from existing branches and functional areas. This COA could consolidate the relevant,qualified personnel into the appropriate billets currently spread across many disparate branches and functional areas. The force structure could optionally expand to a Special Operations Command-like construct allowing greater control over mission requirements, training, and resources.

This option would require more time to develop and grow than other COAs and would likely require the creation of new units and additional resources. Also, without proper support, existing branches and functional areas would try to retain cyber functions which would cause existing stovepipes to remain.

3.6 COA 6: Cyber as a Military Service

The final option we consider is the creation of a separate military service for cyber, as a peer to the Army, Navy, and Air Force. This COA would provide the new service the ability to build a community and culture from scratch and incorporate personnel and force structure from the separate services. However, in the current resource-constrained environment in the DoD, a new service is unlikely to emerge short of a catastrophic national-level cyber event.

3.7 Recommendation

After careful analysis,[25] we recommend COA 5, creation of a Special Forces-like cyber branch, and believe it will provide the most long-term benefit to the Army. This choice should be supplemented with ideas from other COAs. For instance, we suggest coupling this COA with the establishment of skill identifiers to better identify qualified personnel with the necessary skills in cyber operations. Additionally, sub-specialties in the cyber branch can indicate specific fields of concentration or expertise. This is akin to how the Military Intelligence branch denotes officer specialties such as 35D (Tactical Intelligence), 35G (Signals Intelligence), and 35F (Human Intelligence), etc.

4 The Cyber Corps Officer

In order to develop leaders of a cyber force with a level of expertise commensurate with the Army's combat arms officers, a holistic approach is required. A proper career path will consist of a carefully crafted series of training courses, education programs, broadening experiences (including industry engagement), and cyber operations assignments of increasing responsibility.[26] In the following sections, we outline an idealized career path for Cyber Corps officers following from COA

[25] Lawrence Nunn, presentation to the ARCYBER Proponency Office, "Proposed Model for Officers in the Cyber Workforce," June 2012, Fort Meade, MD.

[26] 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.

5, described in Section 3.5. Figure 4 provides a succinct depiction of the career path we describe in the following section.

4.1 Cyber Corps, Military Intelligence, and Signal Corps Differentiation

The current major stakeholders in the cyber domain each own a piece of the puzzle to creating a unified cyber branch in the Army which we call the Cyber Corps.[27] Taken altogether, these pieces seem to imply the existence of a Cyber Corps within the Army already. However, unless these pieces are put together, along with other pieces not currently owned by any of the stakeholders, in a coherent manner, the Army's efforts to project power in cyberspace will languish. While consolidating all of the functions and personnel that comprise cyber operations will initially cause some angst amongst the stakeholders, the primary missions of the Signal Corps, Military Intelligence, and the Functional Areas would still continue to subsist. System and network administration will still need to occur and the Signal Corps, FA24, and FA53 should continue to provide these functions. Tactical communication support is still a legitimate requirement. However, advanced functions such as cyber Opposing Forces (OPFOR) (an online attack force during exercises),[28] red teams (penetration testing),[29] blue teams (assist admins with improving their security),[30] and hunt teams (actively look for computer viruses and malware)[31] are obvious choices that should be culled from traditional branches and be manned by Cyber Corps soldiers.

Likewise, providing timely and accurate intelligence to commanders remains a critical requirement and should continue to be the primary mission of Military Intelligence. Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), Open Source Intelligence (OSINT), and Counter Intelligence (CI) roles should remain unchanged and fall within purview of MI.[32] However, CNO, the offensive nature of CNE, Electronic Warfare, and Information Operations all lie outside the traditional role of MI. MI has been performing these functions to varying degrees due to exigent mission needs, however these functions are inherently cyber in nature and should fall under the purview of a Cyber Corps.

Additionally, within SIGINT, Communications Intelligence (COMINT) should be performed by the Cyber Corps, but the other sub-components of SIGINT (Electronic Intelligence (ELINT) and Foreign Instrumentation Signals Intelligence (FISINT))[33] should remain within the purview of Military Intelligence. Please see Figure 3 for a visual representation and a more comprehensive division of responsibilities between the Cyber Corps, Signal Corps, and Military Intelligence.

We acknowledge that the lines we draw between the related functions may not be as clearly defined as we depict and they challenge existing constructs, roles, and authorities as mandated

[27] We will use the terms cyber branch and Cyber Corps interchangeably hereafter.

[28] LTG Rhett Hernandez, testimony to Congress, "Digital Warriors: Improving Military Capabilities for Cyber Operations", July 25, 2012, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg75668/html/CHRG-112hhrg75668.htm

[29] Zachary Fryer-Biggs, "Building Better Cyber Red Teams", Defense News, Jun 14, 2012, http://www.defensenews.com/article/20120614/TSJ01/306140003/

[30] SANS Institute, "Blue Team", http://www.sans.org/cyber-guardian/blue-team

[31] Gerry J. Gilmore, "Intense Challenge" of Cyber Security", American Forces Press Service http://www.defense.gov/news/newsarticle.aspx?id=65988

[32] "Joint Publication 2-0: Joint Intelligence", October 22, 2013, http://www.fas.org/irp/doddir/dod/jp2_0.pdf

[33] Ibid.

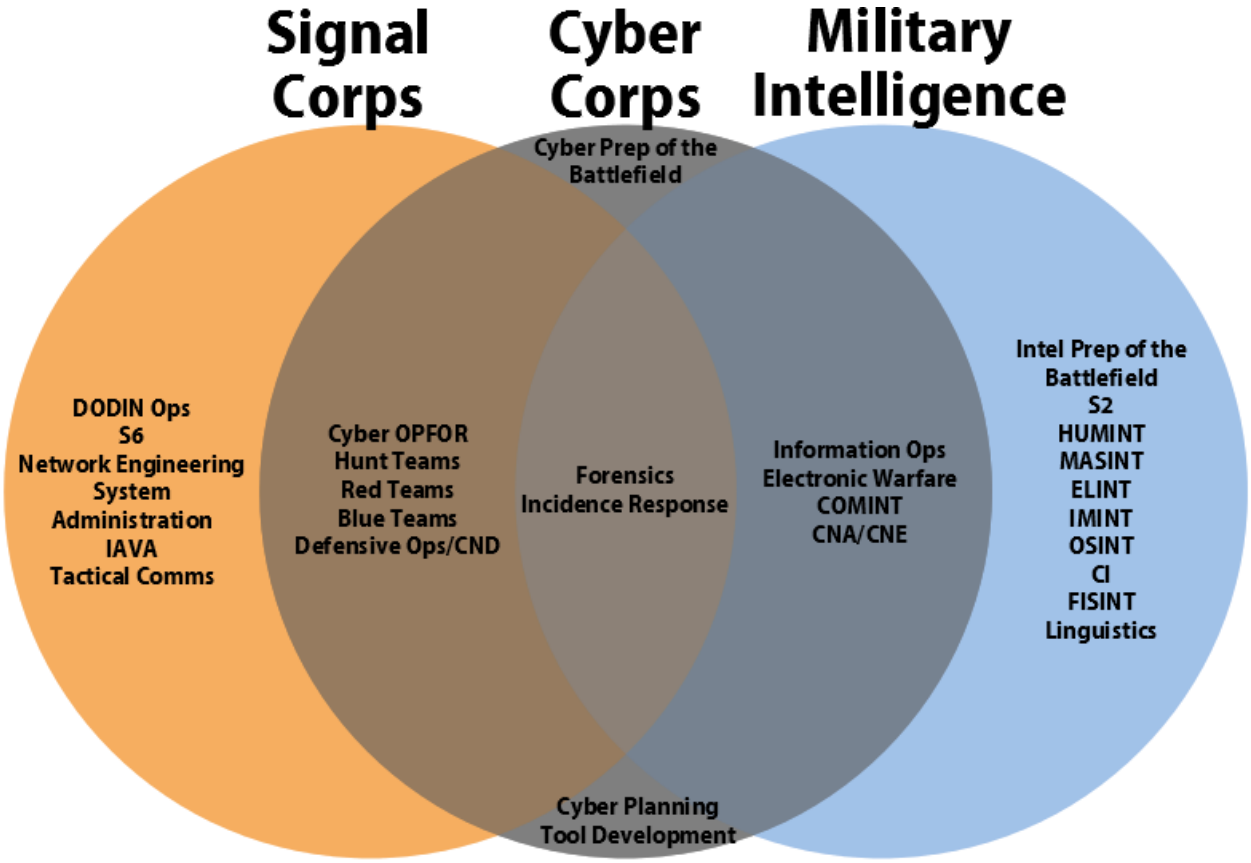

Figure 3: A visual representation of the division of roles between the Cyber Corps, Signal Corps, and Military Intelligence may be delineated. The roles remaining in MI and SC are at the far sides of the diagram, while those roles that are MI, SC, or both that should be in the Cyber Corps are depicted towards the middle. New roles are depicted at the top and bottom of the center of the diagram.

by Congress. Current legislative frameworks justify certain functions of cyber operations being allocated to particular branches in the Army. However, the mere existence of this distribution of capabilities and authorities, does not imply the correctness thereof. In order to create a Cyber Corps, new legislative frameworks that allocate authorities in an appropriate way may be required, but are outside the scope of this paper. We believe that these frameworks should be reviewed and likely updated to reflect the new realities of conducting operations in cyberspace by a unified Cyber Corps.

4.2 Pre-Commissioning

For officers in the Cyber Corps to become experts in their domain, the selection of an undergraduate major is critically important as it lays the foundation for understanding the fundamental aspects of the cyber domain. Prospective officers must study in a cyber related discipline, such as Electrical Engineering, Computer Science, Math, Information Technology, or another closely related discipline. Such a linkage provides the officer a four year or more head start by capitalizing on, rather than disregarding, their undergraduate studies. Students should focus their studies within these disciplines to include courses in cyber security, networking, programming, and operating sys-

tems. Ideally, social science and law courses would also be required as foundational courses for effective service in the Cyber Corps. Students will be able to leverage this technological foundation to teach themselves new technologies, solve ill-defined problems, work through ethical challenges, and communicate technical subjects effectively to nontechnical audiences. Few would argue that a future Army Doctor should choose an undergraduate major other than Pre-Medical, Biology, or a related discipline. Likewise, we believe that the knowledge and skills required to operate in the cyber domain demand a thorough education in a relevant discipline.

Classroom study is only part of the equation; out of classroom activities are equally important. In the future, quality institutions with ROTC programs could provide student internships in cyber-related activities with government agencies (such as NSA, NRO, etc.) and commercial businesses, increasing the student's professional contacts, developing expertise, and providing opportunities to apply classroom lessons in a real world environment. These internships provide an opportunity for students to obtain Top Secret clearances, and to experience cyber operations first-hand prior to commissioning.

Undergraduate study also provides an opportunity to conduct research on cyber-related problems and publish the results. Such research activities will be of great value later in their career as a Cyber Corps officer must solve difficult and ill-defined problems sometimes at the edge of current technology. Finally, collegiate opportunities to participate in cyber competitions, such as cyber defense exercises and capture the flag events abound. Institutions with robust cyber education programs are increasingly supporting competitive cyber teams. These teams meet regularly and participate in very intense cyber competitions. The U.S. Air Force Academy and West Point both host such teams.[34]

Academic institutions already incorporate many of these requirements, such as teaching the fundamental topics relevant to cyber and supporting extracurricular activities geared towards developing cyber skills. What does not exist is a method for identifying, tracking, and determining the technical competence required of each potential Cyber Corps candidate. We recommend the Army Cyber Center (ACC), Cadet Command, and stakeholder proponents collaborate to develop a formalized method (referred to from this point as the Cyber Leader Development Program (CLDP)) for performing these tasks as well as for generating an Order of Merit List (OML) to be taken into consideration during accession, which is explained in the next section. The identification and tracking of qualified Cyber Corps candidates is critical to filling the ranks of the branch and to properly assess officers at appropriate points in their careers.

4.2.1 Scholarship Opportunities

Since deep knowledge in a discipline relevant to cyber operations is what would lend credibility to Cyber Corps officers, we believe that Cyber Corps candidates should be afforded the opportunity to apply to graduate programs directly following their undergraduate studies. This concept is supported by existing Army programs such as the Expanded Graduate School Program (EGSP) and partially funded scholarships, grants, or fellowships offered to USMA and ROTC cadets for graduate study (i.e. Rhodes, Marshall, Truman, Hertz, East-West, Rotary, Gates, Mitchell, Levy,

[34]Don Branum, "Cadet Cyber Team Competes on World Stage" U.S. Air Force Academy Public Affairs, October 5, 2011, `http://www.usafa.af.mil/news/story.asp?id=123274898`

and Fulbright).[35,36] Further, a centrally managed branch could create new scholarship opportunities that best serve its own interests with candidates that might fulfill an immediate or future need.[37]

4.3 Selection and Assessment

Proper assessment and selection is critical to achieve the desired caliber of cyber officers. The requisite knowledge, skills, and abilities (KSAs) required to serve in a cyber branch are under development.[38] As KSAs and other desirable attributes of cyber warriors evolve, they can be used to refine the assessment and screening process to ensure an optimal match between the individual and the requirements of the branch. We suggest a recruiting and assessment process similar to the Special Forces model, but with slight modifications to their vetting frameworks, where applicable, to facilitate assessment and selection in the cyber domain.[39]

Our model provides several opportunities to enter the cyber branch:

- Limited direct accession via traditional commissioning sources, including ROTC, USMA, and OCS for highly qualified lieutenants.
- Branch details, which will allow officers at time of commissioning to select an initial branch in which they will serve their first assignment and, importantly, will be guaranteed re-designation as a cyber officer after their first tour.
- Accession into the Cyber Corps between three and seven years of service. In order to fill out the ranks of the cyber branch at all levels, assessment should initially be allowed as an opportunity across a wide range of ranks, from junior to senior, but over time we anticipate officers will accede into the Cyber Corps earlier in their careers, and at more senior ranks only by exception.

4.3.1 Direct Accession as a Basic Branch and Branch Detail

The initial opportunity for accession will occur towards the end of a student's undergraduate education while part of the CLDP. Candidates for the Cyber Branch will be assessed on their performance and participation in the CLDP as well as their technical knowledge and abilities. The initial assessment and selection process for the Cyber Corps should be exacting and rigorous.[40]

[35]U.S. Army Publishing Directorate, "AR 621-1: Training of Military Personnel at Civilian Institutions," August 28, 2007.

[36]U.S. Army Publishing Directorate,"AR 350-100: Officer Active Duty Service Obligations," August 8, 2007.

[37]The Army has multiple existing scholarship opportunities. A recently released MILPER Message established an ARCYBER scholarship program for senior captains and majors. See `http://www.army.mil/article/70802/`.

[38]Mike Milford, "Leader Development, Education and Training in Cyberspace," Army.mil, August 1, 2012.

[39]Jim Tice, "Spec Ops Board to Screen Junior Officers for Transfer," Army Times, July 23, 2013.

[40]As an initial measure, we suggest heavily weighting a candidate's degree in a cyber-related discipline towards assessment into the Cyber Corps. A relevant degree is an indicator of potential in the Cyber Branch, helps alleviate future training requirements, and demonstrates a baseline level of knowledge the branch requires. For example, the U.S. Navy recently changed their policy and now requires officers working as Cyber Warfare Engineer's to have a bachelor's degree in Computer Science or Computer Engineering from one of NSA's Centers of Academic Excellence. See `http://www.navy.com/careers/information-and-technology/cyber-warfare-engineer.html`, last accessed 10 September 2013.

Candidates who pass the initial screening assessment should be awarded a skill identifier to indicate their potential for accession into the Cyber Branch. Failure to pass the initial assessment does not preclude candidates from trying again at a later point.

In the event there are more candidates who pass the initial screening than existing billets for lieutenants in the Cyber Corps, those qualified candidates who do not receive a billet will retain the skill identifier and will have opportunities to become a Cyber Corps officer later in their career. These individuals are ideal candidates for branch detail programs. Likewise, if a qualified candidate decides that they do not want to branch into the Cyber Corps, via direct branching or branch detail, that candidate will retain the skill identifier and still have opportunities to become a Cyber Corps officer later. The skill identifier will exempt the candidate from having to pass the initial ability screening later in their career. We realize an individual's skills can atrophy over time, but self development can keep these skills sharp.[41] Self development will also prepare the qualified candidates for the Cyber Corps Transition Course (Section 4.4.5), which will provide a refresher for their skills and an opportunity to assess how well they have maintained their skills.

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 gained from experience in line units. Clearly, this would be the case for officers who directly accede into the Cyber Corps. However, officers who qualify for direct accession into the Cyber Corps do so because they possess extremely relevant technical knowledge in a particular facet of cyber operations, which a truly professional cyber force necessarily requires. While we concede that officers who directly accede into the branch will lack operational understanding initially, we do not suggest that cyber units and the Cyber Corps as a whole should lack an 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. As we show in Figure 4, and later in this section, direct-accession officers have opportunities to gain valuable operational experience with line units in a variety of ways.

4.3.2 Later Accession

Between three and seven years of service, officers should be permitted to apply for accession into the Cyber Corps. Officers who received the cyber skill identifier during their pre-commissioning years should be accepted and attend the Cyber Corps Transition Course. There will likely be officers who possess the requisite KSAs and undergraduate degree requirements for accession into the Cyber Corps but did not go through the process for obtaining the skill identifier during pre-commissioning. These officers should not be excluded from applying, but as part of the assessment process for accession into the Cyber Corps they will have to demonstrate the same competency required to obtain the skill identifier. After attending the transition course, these officers will stand shoulder to shoulder with officers who acceded directly into the branch. Failure to pass the screening assessment or the transition course will result in the officer being returned to their basic branch.

The organization responsible for managing the CLDP should still be responsible for performing the screening assessment of officers who wish to obtain the cyber skill identifier at this point in

[41] 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

their career and accede into the Cyber Corps.

4.3.3 Initial Accession for Building the Cyber Corps

To initially build the Cyber Corps, officers at all points in their career should 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 officers the opportunity to apply. The degree prerequisite and technical ability should not be lowered during this time; a technical screening assessment should still be given to the initial round of Cyber Corps officers. This would be similar to the Navy's effort to populate the senior levels of the Information Dominance Corps.[42]

One important near-term issue is the current Active Duty Service Obligation (ADSO) associated with the Army's Volunteer Transfer Incentive Program (VTIP) which allows officers to branch transfer into cyber related career specialties. The current VTIP program requires officers to incur an additional three years of active duty military service in exchange for the transfer.[43] We strongly recommend the VTIP ADSO be waived for all initial assessments into the Cyber Corps until it is fully developed and supported by the Army personnel system, particularly the ADSO for mid-career and senior officers with existing ADSOs.

4.3.4 Exceptional Cases

Despite the stringent requirements we recommend, there should be the possibility for individual exceptions on a case by case basis. For example, there may be individuals whose formal education is in another a discipline totally unrelated to cyber operations, but who still possess the requisite KSAs required to pass the assessment tests and serve with distinction in the Cyber Corps. These individuals should not be excluded from the accession process, so the organization responsible for CLDP should develop a method for handling and granting such exceptions.

4.4 Company Grade (Lieutenant - Captain)

Officers should begin their company grade time with a solid foundation of the nature of cyberspace and during their company grade years learn the TTPs of cyber operations, including mission planning, execution, and post-mission assessment of cyberspace-only and hybrid cyber/kinetic operations. These officers will have the opportunity to progress through a series of increasingly challenging leadership and technical positions that allow them to develop an appreciation of cyber Soldiers and how to lead them most effectively.

Company grade Cyber Corps officers serve in leadership positions and as technical advisers. They are all cleared to the Top Secret level and many have completed an appropriate polygraph exam. 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.

[42] 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`

[43] DesiRee Pavlick. "Voluntary Transfer Incentive Program Now Accepting Applications for Branch Transfer" Army.mil, August 26, 2011, `http://www.army.mil/article/64386/`

4.4.1 Key Development

Lest officers be hurriedly funneled into and out of Key Developmental (KD)[44] positions and career progression devolves into a "check the block" mentality, we deliberately define KD positions broadly to include any position coded for a Cyber Branch officer.[45] Educating Army promotion boards regarding cyber KD positions is important to avoid confusion.[46]

4.4.2 Training and Education

To keep pace with rapidly advancing technology and cyber operations innovation, training and education opportunities need be revisited frequently throughout the career of a Cyber Corps officer. If properly screened during accession, Cyber Corps officers will possess an undergraduate degree in a cyber related discipline as well as a passion for lifetime learning. This foundation allows initial training at Cyber BOLC and the Cyber Captains Career Course to be conducted at a much higher level, rather than simple introductory or overview courses. We also anticipate many officers will be offered the opportunity to pursue a Master's Degree in a cyber-related discipline during their company grade time. Finally, we advocate creation of a rigorous Cyber Ranger School which is the cyber analog to the crucible-like leadership experience of kinetic Ranger School. Graduation from Cyber Ranger school should not be required, but could be a standard all Cyber Corps officers should aspire to achieve.

4.4.3 BOLC-B

Upon initial entry into the Cyber Corps, direct-accession Cyber Corps officers attend the Cyber Basic Officer Leaders Course (BOLC-B) and immediately begin service in Cyber Corps assignments.[47] Because Cyber Corps lieutenants will be required to pass an initial screening assessment and already understand the technical fundamentals of operating in cyberspace, rather than being an introductory course, Cyber BOLC should be an in-depth and challenging course that will focus students on cyberspace operations within the Army and DoD, with a large amount of time focused on current U.S. cyber policy, planning, and executing cyber operations. The capstone event could have teams face off against one another in an attack and defend exercise where each team must defend their own critical resources while attempting to gain access to the resources of other teams.

Cyber Corps lieutenants may also receive additional training based on the requirements of their initial assignment. However, the initial assignment should be matched to a Cyber Corps officer's

[44] 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 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.

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

[46] 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 Corps officers cannot be protected by promotion boards that properly understand various KD positions, this use of combat arms unit nomenclature should be considered.

[47] A candidate model for BOLC-B by David Raymond in "A Proposed Information Dominance Officer Education Model," ACC Report 1337.1, September 30, 2013.

talents. This concept would be similar to the Signal Corps S6 course or the Military Intelligence SIGINT course. We suggest designating different MOS qualifiers to indicate Cyber Corps officers as trained in a particular area of expertise. It should be possible for an officer to obtain multiple qualifiers.

4.4.4 Lieutenant Positions

Upon graduation from BOLC-B and any additional training, Cyber Corps lieutenants can serve in four main positions: cyber team/platoon leader, cyber team operator, analyst, or capabilities developer. These different areas will provide opportunities for cyber lieutenants to gain leadership, operational, and technical experience. Possible locations for Cyber Corps lieutenants to serve as a team/platoon leader and learn the fundamentals of cyber operations is as team lead for one or more of the color teams the Army is fielding to help defend our networks. The red, white, blue, green, hunt, and OPFOR teams provide an ideal blend of technical and leadership challenges for a lieutenant to gain experience.[48,49,50] Additionally, serving as platoon leader within a Cyber Brigade would provide lieutenants an insight into Army-level cyber operations, leadership experience, and hands-on technical experience.[51] The lieutenants who choose to focus on SIGINT collection and analysis will attend a SIGINT planning and analysis course, based on the MI course, and serve in SIGINT positions, likely within a SIGINT unit or Cyber Brigade as an analyst or an analysis team lead. The final lieutenant job option is to serve as a developer for cyber tools and capabilities. Once again, likely locations are within a Cyber Brigade or with the different cyber teams.

4.4.5 Cyber Corps Career Course and Cyber Transition Course

At the three to five year point an officer will attend the Cyber Corps Captain's Career Course. Those officers who started their careers in a different basic branch or served in a branch detail will be required to attend the Cyber Corps Transition Course in conjunction with the Career Course. As with the other courses within the Cyber Corps, attendance of the course does not mean an individual will pass. The transition course will emphasize the skills an officer who has not been in a technical field may need to sharpen to be at the same level of competency and expertise as an officer who acceded directly into the branch. The career course will be grounded in the fundamental skills all Cyber Corps officers are expected to possess, but geared towards the jobs of increasing responsibility an officer will be assigned to as a captain. For example, cyber operations planning should be more strongly emphasized.

4.4.6 Captain Positions

After the career and transition courses are complete, an officer will be given an assignment within one of the core areas of cyber, similar to lieutenant jobs with one addition; officers at this

[48] Gerry J. Gilmore, " 'Intense Challenge' of Cyber Security," American Forces Press Service, November 7, 2011, http://www.defense.gov/news/newsarticle.aspx?id=65988

[49] "Incorporating Cyber into Training Exercises", ARCYBER via AFCEA, http://www.afcea.org/events/tnlf/east12/documents/8IncorporatingCyberintoArmyTrainingandExercisesFinalPR.pdf

[50] Joe Gould, "ARCYBER on the attack on paper, in training," Army Times, December 10, 2012, http://www.armytimes.com/article/20121210/NEWS/212100314/

[51] 780th MI Brigade Welcome, http://www.inscom.army.mil/MSC/780MIB/

level should be technically competent enough and possess sufficient operational experience to serve as advisers to senior leaders. Once again, we deliberately define KD positions broadly to include any cyber coded billet.

Some of the positions a captain can serve in after completion of the course(s) are division cyber team lead or operator, cyber capability developer, ACC member, faculty member in the Department of Electrical Engineering & Computer Science (EECS) USMA, BCT Cyber Technical Advisor (one or two year assignment depending on how low cyber operations are integrated within the kinetic force), or analyst (possibly at the division level as well).[52] Cyber company command will be manifested in several forms, but when serving as a company commander (similar to platoon/team lead), the commander will be expected to maneuver his or her elements with technical mastery in the cyber domain similarly to how kinetic maneuver, fires, and effects (MFE) commanders maneuver their forces with tactical mastery in the land domain. For instance, if an officer leads a company of color teams, then he/she should be giving a task and purpose to sub-elements based on a thorough mission analysis and technical understanding of the overall teams' and sub-elements' core compentencies. The commander should not just be relegated to managing administrative, Uniform Code of Military Justice (UCMJ), and morale, welfare, and recreation (MWR) activities for the unit. Additionally, competent assignment officers at HRC should be equipped with an understanding of the competencies and qualifiations of these officers in order to effectively manage them. Assignment officers should themselves be experienced cyber corps officer.

4.5 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 the necessity of understanding the larger context, including legal and policy aspects, as well as Joint, Interagency, and International collaboration, relationships, and partnering.

4.5.1 Technically Focused Officers

At this point in their career, a Cyber Corps officer would possess a level of experience and expertise few outside of the military would be able to achieve. The talents of these officers should be leveraged and allowed to expand, rather than being culled from the Army at the rank of Major or Lieutenant Colonel. Within FA24, FA53, FA29, and FA30, there exist similar career paths for an officer to achieve the rank of Colonel while remaining technically focused throughout their career. We believe this is an essential component of the Cyber Corps, whether it be in tool development, reverse engineering, cyber operational planning, targeting, etc.

4.5.2 Selection of Individuals for Leadership and Advisory Positions

The organizational structure and size of the Cyber Corps is beyond the scope of this paper. Regardless of its final structure, the Cyber Corps will require senior officers to serve in command and staff positions. 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

[52] Another possible model is these teams be managed at the strategic level and deployed in time of need and during training exercises to allow greater skill development, avoid misutilization, and facilitate optimal operational impact.

and only Cyber Corps officers should be considered to fill these billets. We believe there will be no shortage of qualified officers who seek command and leadership opportunities within the Cyber Corps.

Also, by this point in their career a Cyber Corps officers will have enough experience to serve as an adviser or liaison officer to senior combat arms commanders. The integration of cyber operations into kinetic warfighting will likely continue to evolve and field grade Cyber Corps officers should serve as primary staff positions 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 how to bring true utility to the kinetic warfighting community.

4.5.3 Key Development

As with company grade Cyber Corps officers, field grade KD assignments will be broadly defined to cover all billets coded for Cyber Corps officers. These assignments would include field grade command of cyber formations, cyber staff officer positions, technical advisers, cyber mission planners, and duty with sister-service and Joint cyber organizations and agencies. However, officers should still be required to serve in technical positions between serving in command and staff positions to ensure they maintain their technical competency. For example, an officer should not serve only in command positions during their entire time as a lieutenant colonel and let their understanding of current technology atrophy.

4.5.4 Training and Education

Rigorous training at the field grade level will continue to be important. Specialized training such as (but not limited to) U.S. Cyber Command's (CYBERCOM) Joint Advanced Cyber Warfare Course (JACWC) would be recommended. Due to the inherent interconnection between the military and the private sector, we believe a TWI assignment to a private or public organization in a cyber-related role should be considered a mandatory Field Grade developmental requirement.

Until there exists a Cyber Command and General Staff College and Cyber War College, Cyber Corps officers will complete the Army's existing CGSC Schooling (Major) and War College (Senior Lieutenant Colonel - Colonel) programs with the expectation that Cyber Corps officers will complete as many cyber-elective offerings as possible while attending the courses. We also expect most Cyber Corps 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 cyber operations.

4.5.5 Major Positions

Command and staff opportunities at the rank of major would be to serve as a Cyber Battalion XO or S3, Cyber Team Lead, or as a Division Cyber Advisor. The technically focused positions in which an officer could serve would be Division Cyber Planner, Army/Joint Network Engineer, Army/Joint Cyber Capability Developer, Army/Joint Development Team Lead, Army Cyber Center SME, Faculty EECS USMA, Army/Joint Cyber Analyst, Cyber Operational Planner, or Cyber Center of Excellence Instructor.

4.5.6 Lieutenant Colonel Positions

Command and staff opportunities at the rank of lieutenant colonel would be to serve as a Cyber Battalion Commander, Cyber Brigade XO, S3, or Deputy Brigade Commander, Army/Joint Cyber Policy Advisor, Army Cyber Doctrine Developer, or Army Cyber Center Deputy Director. Technically focused positions in which an officer could serve would include Army/Joint Technical Director, Army/Joint Cyber Capability Developer, Army/Joint Cyber Analyst, Army Cyber Center Senior SME, Faculty EECS USMA, or Army/Joint Cyber Operational Planner.

4.5.7 Colonel Positions

Command and staff opportunities at the rank of colonel would be to serve as a Cyber Brigade Commander, Cyber Corps Proponency Officer, Cyber Center of Excellence Chief of Staff, Army/Joint Senior Cyber Policy Advisor, Deputy Commander of the Cyber Corps, Army Cyber Center Director or Chief of Operations. For a Cyber Corps officer in the rank of colonel, the technically focused positions in which an officer may serve would include Army/Joint Command Cyber Technical Advisor, Army/Joint Staff Technical Advisor, Army/Joint Senior Cyber Operational Planner, Army/Joint Senior Developer, Army/Joint Senior Analyst, Faculty EECS USMA, or Army Research Lab Senior Advisor.

4.6 General Officer

Just like aviation, infantry, armor, or engineers, we believe the best officers to be in charge of the strategic vision and guidance of the Cyber Corps would be officers who rose through the ranks of the Cyber Corps, the way division commanders are the products of 25+ years of service and experience in kinetic warfighting.

There are several positions in which a Cyber Corps general officer billet would be beneficial. One potential brigadier general position would be to serve as the commander of a Theater Cyber Command, similar to a theater signal command if the organizational structure supports such a construct. Another example is a brigadier general to serve as the senior technical adviser to the ARCYBER Commander, perhaps as the ARCYBER Deputy for Research and Development. This should be a Cyber Corps officer who served in significant technical positions. This will provide the adviser with an unmatched level of knowledge with regards to cyberspace operations, tools, and capabilities.[53] Other positions for brigadier generals could be ARCYBER G3 and ARCYBER DCG. At the rank of major general, one potential billet would be to serve as the Chief of the Cyber Corps and Commander of the Cyber Center of Excellence. We believe Cyber Corps officers should also be considered for other general officer billets, especially within cyber-related and technical divisions and organizations, at the joint level. It may take years, but it will likely be desirable to have the ARCYBER Commander be an officer raised from the ranks of the Cyber Corps, as well as CYBERCOM Commander when an Army officer is selected to command this joint organization.

[53]This position would be similar to Scientific & Senior Level Positions within the Government's Senior Executive Service program. See `https://www.opm.gov/policy-data-oversight/senior-executive-service/scientific-senior-level-positions/#url=Overview`

4.7 Post-Service and Post-Retirement

Some Cyber Corps officers will elect to leave service prior to retirement, while others will stay for 20 or more years. Given that the screening process seeks individuals passionate about technology and cyber operations, many leaving the service will continue to pursue these fields in private industry or as entrepreneurs and remain dedicated to serving the nation. These individuals should not be forgotten. A robust network of Army Cyber Corps alumni could help recruit talent, serve in future Cyber Reserve Units, sponsor cadet internships and officer TWI experiences, provide mutually trusted interfaces between the Army and industry (particularly in time of critical national need), and better develop commercial technologies to support mission requirements, among numerous other benefits.

5 Discussion

Overcoming the cultural divide between the larger kinetic warfighting community and the cyber warfare community requires work and mutual respect from both sides. In our model, cyber officers, particularly early in their career, may serve in tactical units. Similarly, kinetic warfighting leaders may serve in cyber organizations as broadening assignments. This cross fertilization will increase awareness of kinetic and cyber realities among all parties.

In the kinetic warfare specialties, such as Infantry, we see officers who fall in love with tactical operations and work at the lowest level possible. Typically, this means Brigade or below. Our model allows officers to gain, maintain, and grow true expertise in cyber operations. We anticipate a similar scenario, officers who do not desire moving from tactical cyber up to higher-level staff work. Some, but importantly not all, can choose this path. However, like their kinetic comrades, some officers need to be willing to step away from tactical operations and serve in higher level leadership roles.

If our model is adopted, flexibility in assignments is particularly important during the initial phases. Army manning documents are notoriously slow to evolve and a mismatch between career field identifiers should not prevent assignment of the right person into the right job at the right time. We also advocate a broad definition of what defines KD positions, which would prevent the herding of officers into and out of a few select positions.

We also advocate careful study of the role of Warrant Officers in the Cyber Corps. Warrant Officers are the Army's technical experts and to a large extent are exempt from the need to leave their technical discipline in order to serve as an administrative leader. Warrant Officers in Signal and Military Intelligence have served with distinction, carefully balancing their role as technical experts, but still growing commissioned officers that are well versed in technology and cyber operations is very important. We do not believe the current model of Warrant Officers advising general purpose commissioned officers who dabble in cyber operations to be sufficient. We owe the warrant officer and our enlisted Soldier communities better.

A sound foundation of ethics is a critical underpinning of a cyber leader. In all but the most egregious, and illegal, cases we do not see kinetic leaders conducting rogue operations. However, the anonymity provided by the cyber domain combined with the relative ease with which rogue operations might take place makes illicit cyber operations a possibility. Such activities cannot be tolerated. Ethical grounding and respect for privacy and civil liberties must be baked into cyber

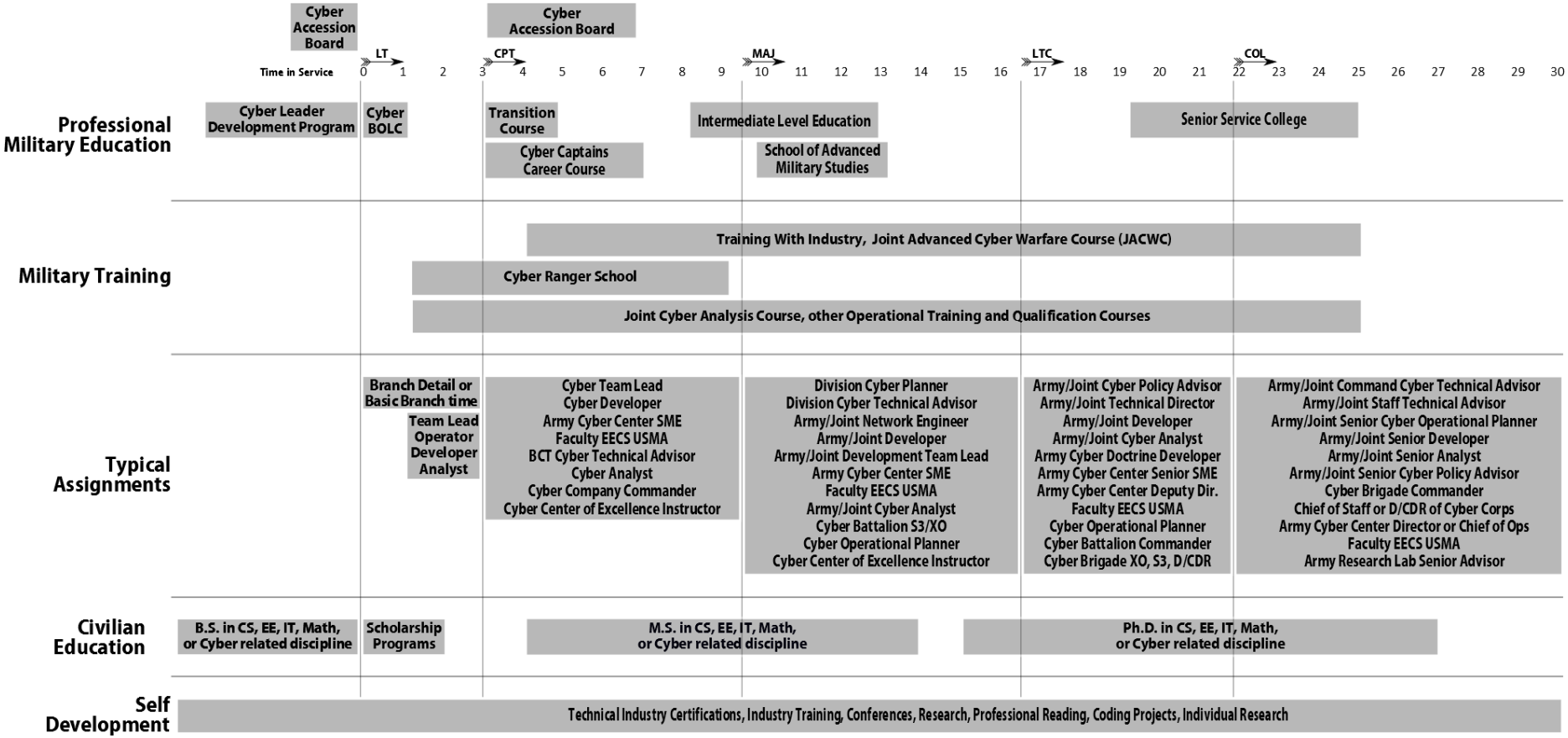

Figure 4: The Cyber Corps officer career progression timeline, from pre-commissioning through colonel.

leader development at all levels.

Improvements to cyber education, training, and professional development should be done in parallel at all officer ranks starting with key points across the entire professional military education spectrum. There is no need to execute change serially.

We must be on guard for the use of industry cyber certifications as a screening mechanism for cyber talent. While such certifications may be an indicator of potential, a certification is not a guarantee of proficiency. Many of the world's experts eschew such certifications. An optimal path likely includes a mixture of traditional classroom education (graduate and undergraduate degrees), operational experience, training and industry certifications, and self-taught learning. The various weightings individuals place on these aspects above a requisite common baseline will provide important diversity in the cyber force.

The career path we suggest must grow cyber leaders who are adept at leading what is effectively 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 cyber mission and those you are leading.[54]

We must recruit cyber leaders judiciously. To do otherwise risks diluting the potential of the cyber forces.[55] Leaders must be able to teach themselves and be lifetime learners passionate about the cyber domain. Classroom training is necessary, but will never be sufficient. Technical experience is also a critical component to developing sound cyber leaders capable of truly leading cyber operations.

Over time, homegrown cyber General Officers will come. Today, at all levels, officers are coming to the cyber domain from a variety of backgrounds. These officers, including the authors, have strengths and weaknesses due to the nature of their upbringing. Currently, it is impossible to come up through the ranks purely in the cyber domain. In the future, with the correct career pipeline combined with rigorous recruiting standards, training requirements, and cyber operations experience, we will grow leaders at all levels better than us. We need not be afraid of this, it is our key contribution to the future Army.

Figure 5: Notional branch insignia for an Army Cyber Corps.

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

[55]Gregory Conti and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," Small Wars Journal, July 29, 2010.

6 Recommendations

This section provides an actionable list of recommendations to move toward a professionalized cyber officer force.

- Generate clear and unambiguous directives from senior Army leadership establishing a Cyber Branch that assimilates the cyber relevant elements of MI, SC, EW, and other cyber-related specialties.
- Establish a Cyber Leader Development Program that will assess junior officers and individuals in their pre-commissioning phase and prepare them to be the initial foundation of junior Cyber Corps officers.
- Create a pilot Cyber Captains Career Course and BOLC, along with specialized follow-on training, if necessary.
- Create a pilot transition course, similar to the MI or SC officers transition course, taken just prior to the Cyber Captains Career Course to aid officers coming into the cyber branch from other specialties.
- Given the significant investment in the Signal Corps and Military Intelligence schools, seek to leverage existing training in cyber relevant topics. One model may involve providing Cyber BOLC in one location and the Cyber Captains Career course at another. Initiate a long-term realignment study, to include analysis of joint efficiencies, to reduce overlap and redundancy.
- Establish a Cyber assignments branch at Army Human Resources Command. These assignment personnel should be empowered to flexibly assign officers from any branch given the individual has appropriate cyber expertise and potential. Ideally this branch would be overseen by a colonel from the Cyber Corps.
- As an interim measure, create a cyber "branch immaterial" position code akin to 01A, branch immaterial, and 02A, combat arms generalist, positions.[56,57]
- Actively work to build a team amongst assimilated branches and functional area personnel. We advocate building a new identity that respects the rich history and contributions of the past, but paints a bold path to the future. This includes creating new branch insignia and iconography, see Figure 5.
- Consider creation of a regimental affiliation.
- Provide clear guidance to promotion and retention boards about the importance of cyber education, training, and assignments. Develop metrics to monitor board treatment of cyber officers.

[56]U.S. Army Publishing Directorate, "Department of the Army Pamphlet 611-21: Military Occupational Classification and Structure," January 22, 2007.

[57]U.S. Army Publishing Directorate, "Army Regulation 611-1: Military Occupational Classification Structure Development and Implementation," September 30, 1997.

- Link branching into cyber branch to undergraduate degrees in cyber-related disciplines and expertise.
- Create pilot program for Lieutenants to serve initial assignments in cyber units. Also, allow Lieutenants to serve in other branches during initial assignment, but have a guarantee of cyber branch designation in conjunction with the Cyber Captains Career and Cyber Officers Transition Courses, via a branch detail program.
- Adopt the Air Force Basic, Senior, and Master cyberspace operations badges for Army cyber personnel. Utilize the Army Space Community's adoption of the Air Force Space Badge as a model.
- Revise and update existing Army skill identifiers for cyber-related expertise. Delete outdated identifiers, some of which date back to the 1990s or earlier. Consider development of higher resolution talent management program, such as the Army's "Green Pages" initiative to better track and assign cyber personnel.[58]

7 Related Work

When we consider the creation of a unified Cyber Branch, it is useful to examine the current status of cyber-related officer military occupational specialties in other branches of service.

The Air Force was the first branch to truly recognize cyberspace as an operational domain when it changed its mission to "fly, fight and win... in air, space, and cyberspace."[59] The new mission set was then aligned under the 24th Air Force by incorporating large portions of the Air Force's intelligence units for network warfare along with the communications units.[60] Career paths, career fields, and training were created in order to consolidate the career specialties that were relevant to cyberspace operations. In a move affecting 43,000 airmen, communications specialties were shifted to new specialties under the 3D series and the 1B series (for enlisted), and the 17 series for officers.[61] New schools and training programs were established for the new and modified career fields. For example, the Intermediate Network Warfare Training is training cyber operators to become Cyberspace Basic Mission Qualified.[62]

The Navy, in a similar vein to the Air Force, moved to align its operations, forces, and career fields in cyber space to a single command. The 10th Fleet Cyber was created[63] and the Information

[58] Casey Wardynski, David Lyle, and Michael Colarusso. "Towards a U.S. Army Officer Corps Strategy for Success: Employing Talent," Officer Corps Strategy Series, U.S. Army Strategic Studies Institute, May 2010.

[59] Mitch Gettle, "Air Force releases new mission statement," Air Force Print News, January 7, 2010, http://www.grissom.afrc.af.mil/news/story.asp?id=123182694

[60] "Air Force Cyberspace Mission Alignment," Chief of Staff, US Air Force, available at http://www.24af.af.mil/shared/media/document/AFD-111003-054.pdf

[61] Michelle Tan, "12 AFSCs to comprise cyber career path," Air Force Times, April 3, 2010, http://www.airforcetimes.com/article/20100403/NEWS/4030343/

[62] Kinder Blacke, "Intermediate Network Warfare Training up and running," Air Force Space Command Public Affairs, March 3, 2011, http://www.afspc.af.mil/news/story.asp?id=123245023

[63] Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," Fleet Cyber Command/10 Fleet Public Affairs, http://www.navy.mil/submit/display.asp?story_id=50954

Dominance Corps was created to align elements of intelligence, communications, and information and cyber operations.[64] Within the Information Dominance Corps, the officers are separated into specialty areas of Information Professional, Information Warfare, Intelligence, Cyber Warfare Engineer, and Meteorology/Oceanography.[65] The focus of these designators are highly technical, so officers must obtain a degree in a relevant scientific or engineering field (with the exception of Intelligence) before they can be considered for designation.

The current state of cyber in the U.S. Army includes Military Intelligence Officers (35G) for the SIGINT specialty, Signal Corps Officers (25A) with general purpose communications knowledge, Information Systems Management officers (FA53) with information technology and management knowledge expertise, Telecommunications Systems Engineering officers (FA24) with in depth network engineering expertise, Information Operations officers (FA30) who conduct information operations, and Electronic Warfare officers (FA29) with electronic warfare and EM spectrum management expertise. In the Fall of 2011, the Office of the Chief of Signal announced the conversion of FA24 officers to FA26A (Cyberspace Networks Engineer) and FA53 officers to FA26B (Information Systems Engineer) as well as the creation of a new functional area FA26C (Cyberspace Defense Engineer).[66] We believe the FA26C position to be particularly innovative, but hampered by the focus on defensive versus full spectrum aspects of cyber operations. We are not aware of a firm implementation date for these conversions.

8 Future Work

A cyber career path for officers is only one component of a larger framework, there remain significant open problems and opportunities to seize. Similar cyber career paths need to be constructed for the enlisted, warrant officer, and Department of the Army civilian ranks. Parallel career paths must also be constructed for the National Guard and Army Reserve. All of which must complement and nest within the larger Joint force structure. Development of specialized awards and decorations for those conducting cyber operations would also serve as an enabler.[67] Our understanding of the desirable attributes of cyber warriors is still at an early stage, we recommend further study to define and characterize these attributes. We believe formation of a United States Cyber Academy, a Joint entity, parallel to the United States Military Academy, United States Naval Academy, and United States Air Force Academy merits careful consideration. Such an entity could greatly aid recruiting, highly develop expertise in the cyber domain, and graduate officers into any military service. Another potential opportunity is the creation of a Cyber War College, a joint entity, that provides Military Education Level - 1 and Joint Professional Military Education - Phase

[64] "Information Dominance Corps (IDC)," http://www.idcsync.org/about/idc

[65] "Navy Information and Technology Careers", http://www.navy.com/careers/information-and-technology.html

[66] Office of the Chief of Signal, "Signal Military Occupational Specialty structure set to change," Army Communicator, 2011, http://www.signal.army.mil/ArmyCommunicator/2011/Vol36/No3/2011Vol36No3Sub03.pdf

[67] We acknowledge the initial attempt at a medal for cyber operations did not go well. See Sean Gallagher "Distinguished Warfare Drone and Cyber Medal Shot Down," Ars Technica, 16 April 2013. However, appropriate awards, decorations, and badges should continue to be developed, despite this initial setback.

II qualifications but with the clear objective of creating cyber-savvy senior leaders.[68,69] In the long term, an entirely new military service, may be necessary to best create the culture and operational capability required to fight and win wars in cyberspace.[70]

9 CONCLUSIONS

Solving cyber in the Army is fundamentally a human resources problem. With the right people, properly trained, educated, organized, motivated, and resourced, everything else follows. However, today's functional and cultural gaps between existing communities threatens overlap, causes infighting, wastes resources, frustrates team effort, and ultimately degrades operations. We need to grow people better than us. A bold, revolutionary solution is called for to fix the situation. We believe the time has come to create a unified cyber career path for Army Officers. One that converges the relevant functions from Signal, MI, IO, and Electronic Warfare and repeatedly grows professionalized and highly qualified leaders because of the system, not despite the system.

[68]"Professional Military Education" Title 10 U.S. Code Chapter 107, 15 January 2013.

[69]For an interesting report on the current status of cyber education at U.S. Military War Colleges, see Francesca Spidalieri's "Joint Professional Military Education Institutions in an Age of Cyber Threat," Pell Center Report, 7 August 2013.

[70]Gregory Conti and John "Buck" Surdu. "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military" Information Assurance Newsletter, Vol. 12, No. 1, Spring 2009, pp. 14-18.

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 serving in the G33 of Army Cyber Command and two tours in Operation Iraqi Freedom (OIF) with the 22d Signal Brigade.

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, both 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.

Colonel Gregory Conti is a Military Intelligence Officer and Director of the Army Cyber Center 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 CYBERCOM Commander's Action Group (CAG), as Officer in Charge of a deployed CYBERCOM Expeditionary Cyber Support Element, and co-developed CYBERCOM's Joint Advanced Cyber Warfare Course. He served in the Persian Gulf War and in Operation Iraqi Freedom.