SMALL WARS JOURNAL

smallwarsjournal.com

Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture

by Lieutenant Colonel Gregory Conti *and* Lieutenant Colonel Jen Easterly

Make no mistake, our nation faces persistent, widespread and growing threats in cyberspace. Across the array of dangerous actors and their capabilities, we've witnessed an evolution from data compromise and loss, to the disruption of information networks to the physical destruction of information systems. Our military forces, in particular, depend heavily on classified and unclassified networks for command and control, intelligence, operations and logistics. These networks – over 15,000 of them – represent a very tempting target, and the number of attacks against them has increased dramatically over the past several years. The United States Government recognized the clear and present danger posed by this increasingly perilous threat environment and created United States Cyber Command.

We are at a unique cusp in history, as we have the first-ever opportunity to create a large-scale organization to fight and win wars in cyber space. This isn't a trivial undertaking; there are myriad details that must be addressed. In this article, we focus on what is arguably the most important – the human dimension, specifically how we attract, develop, and retain a world-class cadre of cyber warriors. By building the best possible team and creating an environment that attracts more, we can lay the foundation upon which we can successfully build Cyber Command. However, while the Defense Department has endorsed Cyber Command, the kinetic warfighting culture generally has not. Positive strides have been made recently to include the development of the Navy's Information Dominance Corps and planned establishment of the Army's Cyber Brigade.

However, building the most effective Cyber Command will require fundamentally changing military culture – specifically how we think about networks and how we manage the talent that we need to leverage these networks for warfighting effects. Uncomfortable, but necessary change will be required, else we risk creating a large bureaucracy, staffed with marginally effective individuals, a "Cyber Command" in name only. This article presents a viable way ahead and suggests actionable solutions for building, developing and retaining a world-class team.

The rise of the cyber domain as the battleground of the 21st Century provides a dramatic new environment in which the current United States military is ill-equipped to operate successfully. Today's military excels at recruiting, developing, and retaining kinetic warfighting expertise, but is ill-suited for recruiting, developing, and retaining creative and intellectual talent on the scale required to successfully operate in the contested cyber domain. Until the end of the 20th Century combat arms expertise ruled the day, but in the 21st Century kinetic combat arms soldiers must learn to co-exist, cooperate, and coordinate with non-kinetic cyber warriors.

Key to creating a formidable force in cyberspace is the recruitment, development, and retention of highly skilled individuals. The dynamics in play are significantly different from traditional military recruiting. The nation faces a severe shortage of information security savvy talent. The pool of candidates dwindles even more when considering such constraints as the ability to receive a Top Secret clearance, possession of U.S. citizenship, desire to undergo repeated drug tests, and, in some circumstances, ability to pass a polygraph exam. The combination of a highly competitive job market and a relatively small pool of candidates require the military to actively create a culture that attracts, not repels, talent. So how do potential cyber warriors perceive the military? It isn't a pretty picture.

Perceptions of the Military by Potential Cyber Warriors

In order to gauge the perception of the military by the technical community we posed the question "How has the military treated you and your technical friends?" on Slashdot.org. Slashdot is arguably the most popular technical news website and is an ideal location to gain a sense of the technical community's perception of the military. The posting drew 415 responses, some quite detailed.[1] The online discussion focused on a variety of themes:

- *Limited creativity* – "The very things that make us valuable -- the ability to think critically, take the initiative, and not be weighed down by conventional thinking is exactly the thing the military seems to weed out."
- *Inflexibility* – "The military is not setup to advance and reward those with technical ability. It is setup to have standard sized cogs."
- *Recognition* – "The military doesn't recognize the existence (or need for) a different type of person to fight their new battles."
- *Unfair pay – "*I looked at the 3 stripes on the arm of the guy flipping my burger. I then looked at the 3 stripes on my own arm, realizing we both get paid the same. At that moment my mind was made up and I chose not to reenlist.*"*
- *Limited meritocracy* – "There is no mechanism for payment or reward based on technical skill level."
- *Lack of a technical career path* – "I think one of the things that the Army did wrong was to completely eliminate that secondary path to advancement. If we're talking about highly technical specialties with little to no relationship to direct combat, then the idea to make everyone a capable sergeant doesn't fit so well."
- *Bias against non-combat personnel* - "In USAF's officer corps, if you don't turn and burn for a living, you're somewhat less than a man."
- *Technically ignorant leadership* – "[The Colonel's] eyes glazed over after 3 or so minutes as he could not follow what I had done at all"
- *Low pay* – "I can walk into any DoD security contractor out there with my DD214 and make 10 times what I did when I was discharged"
- *Danger* – "I hope those guys tell their wives that they are lawful military targets"

[1] "How Do Militaries Treat Their Nerds?" Slashdot.org, 13 March 2009. Available online at http://tech.slashdot.org/article.pl?sid=09/03/13/1336206.

- *Distrust* – “We are talking about handing the keys to America's entire computer security infrastructure over to military intelligence agencies like the NSA”
- *Anti-intellectual bias – “*I attended West Point and was in the top 10% of my class. One of my tactical officers once told me that I needed to get my priorities straight. No one wanted someone who was too smart, he said. He'd rather have someone in his unit who could ace the physical fitness test than someone who studied.*”*
- *Lack of career advancement* – “Its great if you're just in for the college money, sucks later on if you decide to make a career out of it.”
- *Lack of tolerance of alternative lifestyles* – “Many of us live alternative lifestyles and conventional military thinking is that we're a security risk.”
- *Compulsory management responsibilities* – “The system itself isn't designed to handle individuals that have technical ability, but who aren't ready/don't want to command lower level troops.”
- *Misutilization* – “The government sent me to six months training in 29 palms. Yet, when I finally got the chance to deploy, I was a glorified MP.”
- *Hazing (or worse)* – “Nerds were treated with a bar of soap wrapped in a towel, routinely beat on, robbed from, cast out, and had their opinions dismissed.”

Some of those surveyed did voice positive aspects of the military, citing benefits such as travel, education, and early retirement, with a few even praising what others reported as negatives including technically savvy leadership, enjoyment of the structured lifestyle, and respect from peers. The preponderance of the comments, however, were negative. These perceptions are what we must overcome in order to recruit the best possible cyber warriors.

Creating a Successful Cyber Culture

Without attracting the best possible cyber warriors, by definition, we will create a second-rate organization. Fortunately, we are at the birth of Cyber Command; the culture is malleable and thus we have the opportunity to change both perception and reality. The key is to create a culture within Cyber Command, and the larger US Military to the extent possible that respects technical expertise, values diversity, and provides a viable career path from junior enlisted to General and Flag Officer. The importance of the last point cannot be overemphasized; experience gained to date in building the Army Network Warfare Battalion (ANWB) overwhelmingly points to the critical need for a career path to effectively recruit, manage and retain cyber talent.

Perhaps a visit to Google is in order. Google has created a culture which earned the title the “Best Place to Work in America.” Their online recruiting videos receive comments such as “I think I’m in love with Google. Watching this makes me want to go do my homework” or “I’m 13. I plan to become a Google computer engineer one day.” Current Google employees describe the interesting problems they work to solve, the conversations they look forward to within the day, the fact that no two people in the company have the same background, and the freedom they have to explore new ideas during 20% of their time. The result is a global powerhouse with the revenues of a nation-state.

If you walk around companies like Google, you don't see beige walls, battleship gray desks, and workers, like lemmings, heading off to irrelevant and redundant meetings. You see white boards, food that doesn't taste like paste, yoga classes, comfortable small group areas, and bright, creative, and motivated people excitedly collaborating. You see people working long hours, because they believe in what they do and work to accomplish results, a place where talent matters.

Of course Google isn't perfect, nor does Cyber Command share the same cultural freedom as a private company, but Cyber Command has far more room to maneuver than one might expect. There are many existing resources that can be leveraged to craft a successful and mission focused cyber culture within the larger culture of the Department of Defense. We will address these ideas later in the article.

We aren't saying that Cyber Command should be staffed with soldiers with pink Mohawks, but we argue that the current military culture as echoed by the Slashdot audience cannot attract and retain the bright and creative minds required to fight and win in the dynamic and constantly evolving cyber domain. In this respect, it is important to note that Cyber Command does have a good thing going for it in its close partnership with the National Security Agency. The Secretary of Defense set it up this way, directing that the Commander of Cyber Command be dual-hatted as the Director of NSA, to allow Cyber Command to leverage the power of NSA's Cryptologic platform – its cyber intelligence collection capabilities and its information assurance expertise. NSA hosts our nation's greatest concentration of crypto-mathematicians and some of the world's best minds in information technology; roam its basements and you may in fact find a pink-mohawked research engineer or an intricately-tattooed code breaker. This relationship, in which a good portion of CYBERCOM's military forces are embedded in NSA's offices, should help encourage and facilitate the culture of innovation so critical to the development of a successful military cyber force.

However, the culture we seek must not be so distant from the kinetic warfighter that we risk irrelevance. Each cyber warrior will be a member of the Army, Navy, Air Force, or Marines. Perhaps at some point the Nation will create a new branch of service for Cyber, but not for the foreseeable future.[2]. However, we are not without specialized, thriving cultures within the Military. Ask yourself, what would an organization that combined the best attributes of Google and the Special Forces, look like? By answering this question, we will be much closer to an agile and effective culture that will excel in the military, and in cyber war. We should study lifestyles, culture, organizations, and other practices of elite military organizations, because Cyber Command must become an elite organization. Do not misunderstand us, elite doesn't mean exclusionist or an organization filled with prima donnas. To us elite means world class, quiet professionals. To be elite will help us create the right culture, protect our cyber warriors from misuse, and attract the best possible people.

[2] 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.

The Attributes of a Successful Candidate

Cyber Command needs to attract individuals who embody the hacker mindset. The word "hacker" is politically charged, but we use it in its purest sense – someone who is passionate about technology and enjoys creatively overcoming or circumventing limitations.[3] In many ways the hacker mindset runs counter to that of traditional service training which teaches people to follow a simplistic set of cookbook instructions to perform a task. Cyber conflict is a different animal, where creative problem solving in the face of ill-defined problems is essential.

The history of the military is replete with outstanding warfighters, such as Major General "Chesty" Puller, a legend in the Marine Corps and the Nation's most decorated Marine. For those that have paid attention, the computer security community also possesses legendary hackers, see Figure 1. A great example is Dan Kaminsky, who discovered a massive Internet-wide flaw in the system that maps domain names (e.g. www.google.com) to network addresses (e.g. 10.100.15.2). Essentially, Dan found a way to break the Internet. Instead of exploiting the flaw for his own gain, Dan quietly worked with experts to fix the problem and avert an information catastrophe on a global scale.[5]. In the world of cyber warfare, experts such as Mr. Kaminksy are the "Chesty Pullers" of the 21st Century.[6]

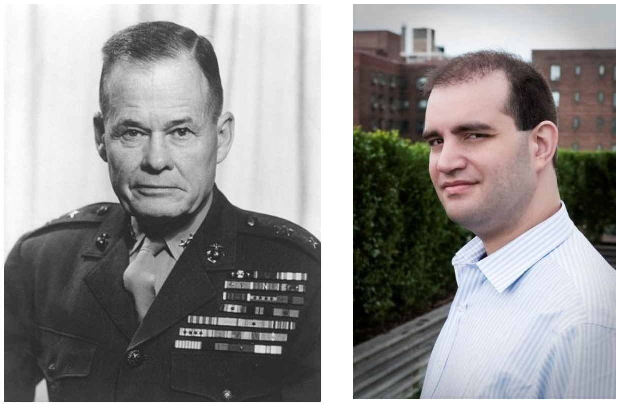

Figure 1: Major General "Chesty" Puller (left), the most decorated Marine in history[4], and Dan Kaminsky (right) a world-class computer security researcher. We argue that such experts as Mr. Kaminsky will be the Chesty Pullers of the 21st Century.

Cyber Command needs digital natives and hackers that are creative, intelligent, innovative, and hungry for knowledge. The best will continually teach themselves to tackle new challenges. Some pick locks, read Security Focus obsessively, write poetry, shoot competitively, compete in triathlons, or use chemistry equipment to cook. We need people who will read books on cryptography as they are in the back of a truck heading to a field exercise or will take an iRobot robotics kit and, over the weekend, build a mobile Nerf rocket launcher controlled wirelessly from a laptop. These people have tech in their DNA. You don't have to overly manage them, just point in the direction you want them to go. You will have to peel them out of the office at the end of the day. To help recruit this type of talent, the military should develop an ASVAB-like recruiting

[3] Gregory Conti. "Why Computer Scientists Should Attend Hacker Conferences." Communications of the ACM, Vol. 48, No. 3, March 2005, pp. 23-24.

[4] Photo of Lieutenant General Lewis Burwell "Chesty" Puller. Source: United States Marine Corps. Public Domain image.

[5] Joshua Davis. "Secret Geek A-Team Hacks Back, Defends World Wide Web." Wired Magazine, Vol. 16, No. 12, November 2008. Available online at http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky

[6] John "Buck" Surdu and Gregory Conti. "Join the Cyber Corps.' IEEE Information Assurance Workshop (IAW), West Point, NY, June 2002.

test for cyber. Such a tool may be built upon the assessment test provided to Soldiers accessing for ANWB. Developed by a group of expert programmers and computer science professors, and borrowing concepts from the GLAT (Google Aptitude Test), it has proven very successful to date in judging innate cyber aptitude. Cyber talent clearly exists, both inside and outside the military, in the numbers necessary to staff Cyber Command, but in addition to finding it, we must also convince the individuals who have it that they and what they can do will be respected. Google succeeded, can we?

Remember that in some cases, these people are interviewing Cyber Command harder than we are interviewing them during the recruiting process. Creating teams of cyber warriors out of such individuals challenges our current culture, but not the core techniques of leadership.[7] However, cyber warriors deserve equally tech-savvy leaders who understand and appreciate their accomplishments; who empower creative problem solving and encourage out of the box thinking; who can empower individual efforts and yet successfully focus these efforts into a cohesive team; we believe Cyber Command should be up to this task. That being said, we need rigor and expertise in making the right hiring calls. Some candidates won't be able to work well on teams, some will focus on only specialized areas of expertise, and some may need ethical guidance or role models to help them learn how to be responsible. As part of the recruiting process, we need to determine what attributes positively add to the diversity of Cyber Command and what attributes are incompatible.

Bootstrapping the Force

Given the recent national and global recognition of the cyber warfare threat, individuals with computer and information security experience are in high demand. In the Fall of 2009, the United States Department of Homeland Security announced its desire to hire 1,000 cyber security experts.[8] They aren't alone, myriad businesses, government agencies, and academic institutions are similarly seeking out large numbers of cyber security experts. Depending on one's definition of "expert," demand far exceeds supply. So, how and where does one find the talent, in appropriate numbers, to work for Cyber Command? The first step is to look inward and closely examine our current force.

The military possesses a unique advantage - approximately 1.4 million Active Duty and 850 thousand Reserve service members. By scouring our existing force we will find much of the talent we need to create the initial core of Cyber Command. Those who have the passion for cyber warfare service have been waiting for an opportunity for a seminal event like the formation of US Cyber Command to occur. Despite Cyber Command's evolving status, many are actively seeking out duty with Cyber Command. As one newly commissioned Lieutenant put it in personal correspondence to the authors, "I would crawl through mud to work at Cyber Command."

[7] TJ O'Connor and Joseph Doty. "We Need Teams of Cyber Warriors." Army Magazine, Vol. 60, No. 1, January 2010. Available online at http://www.ausa.org/publications/armymagazine/archive/january2010/Pages/BuildingTeamsofCyberWarriors.aspx.

[8] Michael Cooney. "Homeland Security to hire 1,000 cybersecurity experts." Computerworld, 1 October 2009. Available online at http://www.computerworld.com/s/article/9138808/Homeland_Security_to_hire_1_000_cybersecurity_experts.

The problem often lies not in the talent or desire of these individuals, but in inflexible military human resource systems. For example, most service members are assigned to a unit based on a career field identifier and their rank. Searching the larger force and identifying appropriate individuals is only half the battle. Many of these individuals do not have the correct career field specialties to be assigned to Cyber Command. Making the appropriate changes to a service member's record or on a unit manning document can take years. In these instances, the military is its own worst enemy. Rare exceptions are possible, but only with the direct intervention of General and Flag Officers.

Where does the desired expertise reside today? It exists primarily in the signals intelligence and communications career fields of the services, other talent also lies hidden in less likely places such as combat arms career fields. Consider the Army. The prescient creation of Officer Personnel Management System (OPMS XXI) in the late 1990's reinvigorated decaying technical careers such as Information Systems Management (FA53) and added several others in Telecommunication Systems Engineering (FA24), Information Operations (FA30), and Space Operations (FA40). Importantly, OPMS XXI created viable career fields through the rank of Colonel. Other programs such as the National Systems Development Program (NSDP), the Junior Officer Career Cryptologic Program (JOCCP) and the NSA Director's Fellowship Program have combined classroom training with immersive operational experiences to develop technical and management expertise for specialized follow-on assignments. The output of these and other enlisted, warrant officer, and officer initiatives have created a valuable source of prepared and ready people for initiating Cyber Command.

There is however a finite pool of talent in these pockets of expertise. The Services will be loathe to release large numbers of their highly trained personnel to serve with Cyber Command, so it is essential that a separate career path be developed for cyber warriors. In the Army's case specifically, initial efforts to create a cyber specialty MOS for enlisted Soldiers and Signal Warrants are encouraging, but what ultimately may be required is the development of a new Career Management Field that serves to break down the stovepipes between the Signal, MI and Information Operations communities. This should include the development of a Functional Area for officers, separate from Information Operations, but potentially incorporating the recently created FA29 (Electronic Warfare). These officers would serve within Cyber Command but would also be embedded at tactical formations down to Brigade level to advise Commanders on integrating cyber into their operations. Embedding Cyber LNO's throughout the force is fundamental to breaking down those cultural barriers and creating an appreciation for cyber within the kinetic warfighting community.

A big question is when to allow personnel to join a cyber warfare force. Should this occur immediately upon joining the service, or at a later point, after the individual has had operational, possibly even combat, experience. We believe the cyber force would be best enriched by allowing both options. Some individual are singularly focused on cyber operations, forcing them to participate in areas outside their passion may mean we lose them altogether. Others however, desire to initially work in a combat unit, perhaps as an infantry platoon leader or surface warfare officer, but wish to be guaranteed an opportunity to later work in a cyber specialty.

The Army has a mechanism in place today that can support this option, “branch detail.” Under the branch detail program, an officer may select an initial assignment in one career field and after approximately 4-5 years is *guaranteed* the opportunity to transition to a new career field. At this point, the officer is given appropriate training to prepare for the transition. Similarly, we should allow some personnel to transition to the cyber force at a later point in their careers. Regardless of entry point, though, care should be taken to select only those with a true passion and capacity for cyber warfare, not those with careerist or other ambitions. Under no circumstances should an individual be forced into a cyber warfare assignment. To fall into any of these traps will certainly create an unhealthy work environment that encourages talent to leave and undermines mission accomplishment. However, if we avoid these pitfalls the result will be a mixture of people with deep cyber warfare experience and others with valuable operational experience.

We need to think broadly across the various ways soldiers join the force, easing the placement of appropriately motivated and prepared individuals in the right officer, warrant officer, and enlisted specialties. For example, if the most talented hacker on the planet decides to join the military and walked into a main street recruiting station, what type of reception and advice will she receive? Without a career field or other tracking mechanism, the individual will, at best, be placed into the nearest match, such as automation or signals intelligence. Importantly, however the individual will then be assigned at the whim of their human resources managers, which will almost certainly result in a disappointing follow-on assignment. Part of the solution to recruiting demands providing clear guidance to military recruiters on how to properly place potential cyber warriors along with the creation of cyber career fields. A recent partnership between the Army Network Warfare Battalion and the US Army Recruiting Command (USAREC) attempts to do just this, with USAREC identifying potential candidates based on aptitude testing and desire and providing these candidates to ANWB for nomination into the unit.

Officer ranks are typically drawn from Service Academies, Reserve Officer Training Corps (ROTC) programs, and Officer Candidate Schools (OCS). In many cases, unfortunately, there is little linkage between the academic degree of an individual and their placement in a career field. As we move forward, Cyber Command must take advantage of the prior experience of incoming personnel, and link it closely with cyber-related career fields rather than the current haphazard approach that wastes years of academic preparation. In addition, we should identify talent as early as possible and track their careers, reaching out to them at an appropriate time. Another tool we must consider using are the Services’ direct commissioning programs which allow the Army, Navy, and Air Force to acquire talented individuals based on specialized backgrounds. In today’s environment direct commissioning is rare, but we should exploit this existing program to bring on board the correct talent to staff the cyber warfare force. We should also creatively consider recruiting appropriate people at later points in their careers, ideally creating win/win solutions. For example, one promising pool is departing Service Academy faculty. These individuals all possess Masters and PhD degrees, but are frequently assigned to unrelated positions after departure from the Academies; many would be a great fit for Cyber Command.

Reservists have a very important part to play in Cyber Command. Because of their role as citizen soldiers, they bridge both the civilian and military worlds. It is from this pool that we can bring in regular infusions of civilian experiences and best practices. For example, the military logistics functions are frequently augmented with Reservists whose day to day job is in the same area. Cyber Command should recruit Reservists from diverse elements of the Information Technology sector, especially those who work in the field of computer security. One current shortcoming is the difficulty which many qualified Reservists face when seeking out how to apply for a Cyber Command assignment. It is critical that we make this path easy, but again we must filter those interested and only select individuals with the right background, capacity, and motivation.

Growing the Cyber Force

Bootstrapping the initial cyber force is a good start, but we will need to reach outside the force to maintain and grow over time. Finding out the details of how to join Cyber Command should be easy, even for those unfamiliar with the military. Recruiting websites are an obvious option, but other new media venues such as Facebook, Linked-In, Twitter, and online video should also be employed.[9] We should also reach out to appropriate communities. For example, if seeking out computer security expertise, Cyber Command could send teams to security and hacker conferences.   Even better would be not to just set up a table at a vendor or job fair, but to become a respected member of those communities. This might mean sending speakers to hacker conferences, competing in network warfare contests, and publishing research papers at academic conferences.

Importantly, these engagements should be impressive. The best and brightest candidates will be attracted to other bright minds who obviously enjoy their work. For example, the Naval Post Graduate School's (NPS) winning Capture the Flag teams at the Defcon hacker conference and NPS faculty member Chris Eagle's exceptional Black Hat and Defcon talks have set the standard for professional cyber warriors and resulted in a world-class reputation for NPS within the corporate and hacker security communities. Cyber Command has the ability to do the same. The end result will be a feedback loop where the best and brightest seek out work with Cyber Command, further fueling its capabilities and reputation. Word of mouth, from public outreach, current members, and alumni will magnify this effect and refer more talent. However word of mouth works both ways. A second rate organization will only attract second rate individuals. All who join Cyber Command should be bettered by the experience and proud of their service.

Retaining and Developing the Cyber Force

Acquiring a talented group of cyber warriors means nothing if they leave at first opportunity. Remember, these are people that could have chosen to work anywhere, so how you treat them makes a big difference. This isn't a plug and play operation. From our experience, it takes six to twelve months on the job for an operator to *begin* to be effective in many cyber specialties. This is a pretty extensive investment in time and training dollars, one that makes it all the more important that we develop creative ways to retain our high-end cyber talent.   While some cyber warriors will continue to serve because of patriotism, others to make a difference, still others because they love the mission, professional development opportunities and career progression are essential.

[9] For a great example see this Google recruiting video http://www.youtube.com/watch?v=JcXF1YirPrQ.

We believe a passion for learning will be an essential trait in the best cyber warriors. It has to be. Those that do not continually seek out new knowledge will find their skills quickly out of date. However, the desired means to acquire new knowledge varies widely. Some will prefer self study, others a short duration, high intensity training course, and still others a semester long college course. Cyber Command should explore training with industry programs as well as establish internship opportunities with companies like Google, Microsoft and NetApp for reenlistment options. There are numerous computer security competitions that can help build technical skills and teamwork. We should take advantage of world-class security training courses offered by the SANS Institute and others, as well as provide personnel access to cutting edge technology. We should leverage tuition assistance programs and the GI Bill to support college education. As people pick-up new skills, we need to place evidence in their online records so we can find appropriately skilled people in the future. As of today, many military record keeping systems do not offer this option.

Of course, no organization has an unlimited training budget, but there are many ways to cost effectively feed the Cyber Warrior's passion for knowledge. Many top-tier universities, such as MIT make their course materials available online for free (ocw.mit.edu). Service members can form lunchtime study groups, rather than attend expensive boot camps, to prepare for professional certification exams. Books and lending libraries are another inexpensive way to facilitate learning. Local guest speakers from government, academia, industry, and the hacker community can help create regular professional development sessions. Cyber personnel can also grow professionally by leading workshops and giving talks for nearby professional groups. Such outreach will also serve to assist recruiting efforts. Where applicable, we should maximize quality on the job training and seek to consolidate redundant service training into Joint and Combined schoolhouses. In short, there are many opportunities for cost-effective professional growth.

Not everyone can or should have the same training, but leaders must ensure that the sum of their cyber warriors' experiences cover the desired skillsets. Care must be taken to not just teach technical skills, but also to develop communication abilities, as Cyber Command personnel will frequently be called upon to communicate technical topics to non-technical audiences. Similarly, we need to grow some individuals who desire to become leaders, but importantly we need to allow some to specialize, without penalty, in technical areas. The Special Forces A-Team model, where individuals are trained in a specialty, but are sufficiently cross trained to provide overlapping coverage, may provide valuable insights.

We cannot build a professional cyber warfare force without viable cyber warfare career fields within each service. Recreating the current model that rotates personnel into and out of cyber assignments is insufficient. It drains training resources, induces skillset atrophy and encourages the departure of our best and brightest. For many specialists, an assignment away from their skill area is reason enough to leave the force. Additionally, we should explore opportunities for medals, awards, tabs, and other means to publically recognize and reward technical accomplishments, a sorely neglected area in today's kinetic-centric service award systems. A career path that inspires others means career progression with promotions based on merit and competitive pay. We will know we have succeeded when we have General Officers, Sergeants

Major, Senior Warrant Officers, Master Chiefs, and Chief Master Sergeants that are products of a pure cyber warfare career.

Conclusions

We are at a very critical time in the formation of Cyber Command. By acting now while the organization is still malleable, we can create the right culture and recruit the right people, who will in turn build the best possible Cyber Command. In this article we have presented actionable suggestions for the way ahead. Central among these ideas are the creation of military specialties in cyber warfare, attracting the best and brightest talent, fostering a hacker mindset, and leveraging existing military personnel programs, but not being afraid to innovate when necessary. The changes that we suggest will be uncomfortable for the old guard kinetic warfighter, but are essential to the creation of an adaptive and agile Cyber Command rather than yet another lumbering bureaucracy. Our success will result in the world's best cyber warfare fighting force, who will deter our enemies, and when necessary strike with precise, effective, and coordinated force in cyberspace.

LTC Gregory Conti is an Academy Professor and Director of West Point's Cyber Security Research Center. He holds a BS from West Point, an MS from Johns Hopkins University and a PhD from the Georgia Institute of Technology, all in Computer Science. He is the author of Security Data Visualization (No Starch Press) and Googling Security (Addison-Wesley) as well as over 40 articles covering computer security, online privacy, and cyber warfare. He is a frequent speaker at leading security conferences including Defcon, Black Hat, RSA, and Shmoocon. He recently returned from a deployment as Officer in Charge of Cyber Command's Expeditionary Cyber Support Element in support of Operation Iraqi Freedom.

LTC Jen Easterly is a member of the US Cyber Command Commander's Action Group (CAG). She served as the first Commander of the Army Network Warfare Battalion from July 08 - July 2010. She holds a BS in International Relations from the United States Military Academy and an MA in Politics, Philosophy and Economics from the University of Oxford.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, United States Cyber Command, the Department of the Army, the Department of Defense, or the United States Government.