A Year of Cyber Professional Development

By MAJ Natalie Vanatta | January 23, 2015

The nation that will insist upon drawing a broad line of demarcation between the fighting man and the thinking man is liable to find its fighting done by fools and its thinking by cowards.

– Sir William Francis Butler, 19th-century British Lieutenant General

After more than a decade at war, the Army is not the same institution that I joined before the 9/11 terrorist attacks. Traditions that bound generations of service members together have been forgotten and institutional knowledge has vanished. The development of leaders in a fiscally constrained environment is one of the key skills that has been lost. With military budgets shrinking now, the art of developing leaders prepared to handle diverse situations seems a daunting challenge. We have relied on mobile training teams, scripted rotations in the box[1], and deployments in sustained bases to train Soldiers and Leaders to handle typical scenarios. All of which incur expenses that are no longer sustainable, while none of them truly focus on stretching leaders' skills and capabilities to handle the unknown.

According to Army Doctrine, "leader development is the deliberate, continuous, sequential, and progressive process – founded in Army values – that grows Soldiers and Army Civilians into competent and confident leaders capable of decisive action"[2]. Leaders must be prepared to execute decisive action on today's battlefields but also in future armed conflict situations. However, to do that – we need to train our leaders to think critically and creatively to prepare to fight and win the next battle. How? Well, a professional reading program has been a keystone of leader development for hundreds of years; it is a keystone because it works. It educates about the unknown in order to prepare ourselves to operate there.

This article discusses a leader development program that was instituted in the U.S. Army's 509th Signal Battalion[3] using reading and critical thinking as a foundation. This program focused on educating leaders (both military and civilian) about the future of our Army. It was a grass-roots effort to revive Army traditional formats of leader development in today's environment on a modern topic. That topic was cyber. To paraphrase a 60s hit[4], "This is the dawning of the age of Army Cyber". We, as leaders, need to either learn about it or be left behind.

Concept

Development and broadening of the mind is a critical aspect of the true warrior's preparation for battle.

– General James F. Amos, 35th Commandant of the Marine Corps

Cyber was the over-arching theme for our 2014 leader development program. Why was this theme picked for the program? First, the word 'cyber' means different things to different people. This lack of common understanding of what the word means creates a wealth of topics to discuss, analyze, and explore. For if technically minded individuals cannot agree on what cyber is, how can we expect troops on the ground to decipher the mystery of cyber? It just becomes a scary topic with no "right" answer or concrete solutions. This program attempted to de-mystify cyber. Second, cyber has many facets to explore which kept the program vibrant and non-repetitive. Many of these aspects are described later in this article. Third, cyber touches everyone – no matter the military branch or job description. From the bagger at the Commissary to the NSA analyst, we all have a part to play. The fact that this theme intrigues a multitude of people increased the diversity of those that participated.

The fourth reason that cyber was chosen as the theme for the leader development program is that cyber requires critical thinking. This is an important principle of Army leader development. Cyber in its infancy gives us the opportunity to stretch our minds and hone our thinking skills. Finally, the cyber theme was selected because it is very relevant to the operational Army. In today's Army, everything is networked and associated with a computer-based system. It is the Achilles heel of the modern military. Commanders must understand the threats to these systems, how to protect them, and most importantly, how to train their subordinates to operate without them. They should also be aware of available cyber effects they can leverage within their battlespace and how to maximize their potential. Therefore, cyber is not just a microcosm of the Army but a mainstream concern from the foxhole to the Pentagon.

There were two components to this leader development program. The first component was the reading program. In a traditional reading program a hard-copy book is selected, chapters assigned, and discussion questions explored. Books are typically chosen if they are interesting, rich in ideas, and thought provoking. The 509th leader development program was a traditional reading program with a modern twist. Yes, a handful of hard-copy books were used, but other mediums were explored. Traditional books were supplemented with on-line articles, blogs, and videos. Not only did this approach relieve some of the stress of reading full books each month but a significant amount of quality, up-to-date information about cyber has not been traditionally published. The purpose of a reading program is to stretch participants' minds and exercise their thinking skills. Professional reading programs are essential to self development in the kinetic warfare domain. The cyber domain is no different.

The second component of the leader development program focused on dialogue opportunities. These sessions provided an opportunity for participants to discuss various viewpoints about cyber with individuals and organizations outside our area of operations. In fact, various representatives from the military, government, industry, and partner nations were invited to participate in discussions on how cyber impacts and/or influences their environment. The schedule of speakers was developed to allow for the exploration of different perspectives about what constitutes cyber. These sessions were conducted via video-teleconferencing systems (recall the shrinking military budgets comment at the start of the article) and were patterned after a graduate level seminar series.

The leader development program met monthly, scheduled around operational needs, throughout 2014. In general, the program switched back and forth between the two components in order to keep the program fresh and the participants engaged. More importantly, the sessions were designed to build on each other enabling very complex topics to be examined. Additionally, varieties of different sources were used to provide a breadth of perspectives to the conversations. Invitations to the sessions were distributed to Signal community, Military Intelligence community, Fires community, and the Legal community across Italy. This translated into participation from 173rd Infantry Brigade Combat Team (Airborne), United States Army Africa, United States Army Garrison – Vicenza, and (of course) 509th Signal Battalion.

Sessions

The problem with being too busy to read is that you learn by experience . . . i.e. the hard way. By reading, you learn through others' experiences, generally a better way to do business, especially in our line of work where the consequences of incompetence are so final for young men. Thanks to my reading, I have never been caught flatfooted by any situation . . . It doesn't give me all the answers, but it lights what is so often a dark path ahead.

—General James N. Mattis, USMC

Cyber was illuminated in our first session as it set the stage for the entire program. The Army Cyber Command (ARCYBER) G5/7 section[5] facilitated a discussion to create a foundation for understanding how the Army defines cyber. This was held at the SECRET level in order to reference various classified Army doctrinal manuals and publications on cyber. In fact, materials from 1st IO Command's Executive Computer Network Operations (CNO) Planner's course were used to help participants visualize many of the concepts. The session also covered the action arm of Army Cyber – the Cyber Mission Forces. Ultimately, this opening session enabled the participants to better understand the strategic and operational levels of cyber. Creating a shared understanding of basic terms and doctrine on cyber was essential to the success of the program.

The February session expanded the foundational knowledge of cyber by exploring how individuals attack, defend, and exploit systems and networks. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson[6] was the reading assignment. Not only is this book on most cyber reading lists but General Alexander was also known to give a copy of this book to his fellow general officers so that they could gain an understanding of the basic tools used in the cyber domain and their ethical application. This "How-to" guide contained a multitude of examples that not only explain how our enemies operate against us but also clearly demonstrates how easily it is done. This reading sparked discussion on how to get into a hacker's OODA (observe, orient, decide, act) loop[7], how the methodology of cyber attacks mimics the steps of the military decision making process (MDMP), and finally how the commander's visualization in planning military operations is no different than how a hacker combines elements of art and science in his orchestrated attack. This session was able to clearly show how typical Army planning doctrine was also applicable to planning highly-technical cyber missions.

After the basics of cyber were covered, the leader development program began to branch out to the different aspects of cyber. The third session focused on the current cyber threats to the United States. This threat discussion was led by a member of the ARCYBER G2[8]. While only limited specifics could be divulged at the SECRET level, the discussion was still eye-opening and engaging. During this session, participants were introduced to the Military Intelligence perspective on cyber, giving them an opportunity to contrast it with the communications (Signal) perspective that they had been previously exposed to. They also learned about basic threat detection and classification methods within the cyber domain. Finally, actual infiltrations and cyber events on our military networks were discussed. These concepts led to a thought-provoking conversation on how to detect threats in the future, both more quickly and more accurately, and how to motivate the typical user to change their behavior in order to better defend our key terrain. This session opened many participants' eyes to the reality of how our enemies are actively using the tools/techniques, previously discussed in the February session, against us today.

The April leader development session focused on another well-known book, "Cyber War: The Next Threat to National Security and What to do about it" by Richard Clarke[9]. This non-technical book was used to facilitate a discussion on how the United States government creates cyber policy and how the various aspects of national power can be used against adversaries in the cyber domain. This was a great introduction to the complexities of engaging the cyber domain at the strategic levels of government. The group also discussed the division of cyber-security responsibilities between various federal agencies and departments. The debate on what role an individual should be forced to take to secure their portion of cyberspace was especially engaging. The participants walked away with a renewed understanding of how actions taken within the cyber domain have ripple effects across all other domains of traditional warfare.

In June, the leader development program focused on the issue of rights – predominantly, the right of privacy within cyberspace. The discussion revolved around the idea of where to draw the line between actions taken to protect our rights and actions that just take them away. An amazing literary work of fiction was used to highlight the issue, "Little Brother" by Cory Doctorow[10]. In this book, the United States Government suspended portions of the Bill of Rights in order to protect the population from terrorism. This sparked an interesting discussion about when, as military leaders, it would be appropriate to stand up against the government as we swear our Oath of Allegiance to the Constitution, not to a political leader. Debating when that point is reached yielded a diverse set of answers from the participants. This summer session challenged participants to better understand their oaths, explore the greater good theory, and take a peek at motivations within the hacker sub-culture.

Using a group of on-line journal articles[11], in August we discussed the difficulties with planning cyber operations. On this topic, challenges existed in two flavors – educating individuals capable of planning military cyber operations and educating commanders in cyber capabilities/effects. The main issue was captured by Jason Bender in his article – "'mouth-breathing-knuckle-draggers' versus the 'pocket-protector-and-horn-rimmed-glasses-wearing-geeks'". These two stereotypical groups sometimes have great difficulty communicating with each other, which results in an inability to create a shared understanding. The group discussed how to establish a learning culture in their organizations with importance placed on self study about cyber. They also debated on the key skills and attributes that a cyber planner should have in order to be successful. Results from dialogues after this session sparked increased participation from senior-level operational planners in future professional development sessions.

The Army Cyber Center of Excellence (CCoE)[12] facilitated the next session within the leader development program. Up until this point, most of the discussions

The Army Cyber Center of Excellence (CCoE)[12] facilitated the next session within the leader development program. Up until this point, most of the discussions revolved around the strategic or operational aspects of cyber. Therefore, we needed to explore the Army Training and Doctrine Command (TRADOC) perspective on cyber and the new Army Cyber branch. The conversation revolved around the DOTMLPF (Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities) aspects of cyber with the greatest emphasis on the development of personnel, leaders, and doctrine. Senior warrant officers from the CCoE explained how the Cyber branch was designed and how it would be filled with qualified Soldiers. Another important discussion topic was where the differentiation between Signal, Military Intelligence, and Cyber lies for the Army. Participants left the session with a new appreciation of the complexity of beginning a new branch within the Army and how to support it in the future.

In October, the leader development program incorporated another book, "Worm: The first Digital World War" by Mark Bowden[13]. This book facilitated a discussion on war and the requirements for a conflict to become a war. The group used the writings of Clausewitz and Jomini along with Joint and Army doctrine to discuss Mr. Bowden's claims that the Conficker Worm created a digital war. Discussion subtopics included: How do we know we are at cyber war? What is victory in this type of conflict? and When can cyber war be declared complete? Additionally, many ideas were presented on how to get civilians to have "skin in the game" with regards to cyber-security. The session ended with a great discussion on the importance of having a well-defined and accepted end state before starting a conflict –independent of domain.

The 509th leadership development program finished the 2014 series in November with a session covering the legalities of cyber. A cyber lawyer from the Army Cyber Institute (ACI) led our discussion as we explored how the Law of Armed Conflict applies to actions within the cyber domain. Special attention was paid to discussing the Tallinn Manual which interprets international law with respect to cyber operations and cyber warfare. Concepts like 'use of force', 'proportional response', and attrition were explored within the context of the cyber domain. Additionally, Title 10 and Title 50 responsibilities and legalities were explained. This winter session created a basic understanding of legal terminology and concepts that will be built on in the new year.

End State

For time and the world do not stand still. Change is the law of life and those who look only to the past and the present are certain to miss the future.

– President John F Kennedy, 35th President of the United States of America

The primary goal of this leader development program was to develop individuals' critical and creative thinking skills using the broad topic of cyber. The secondary goal of this program was to enable individuals to have an increased understanding about cyber operations and apply that knowledge in their everyday approach to enhancing cyber security.

There were many challenges in developing this leader development program. First was the challenge of finding time in the work-day to execute the sessions. As most organizational leaders will attest, there are never enough hours in the day to complete the main mission – let alone add new things to the schedule. Gaining command approval and support for the program was essential. My conversations with unit leaders focused on the intellectual benefits their employees would receive if they participated in these hour+ sessions. Additionally, to support scheduling concerns, I scheduled the sessions six to eight weeks in advance so participants and their supervisors could plan around them. As the program progressed and participants became more interested in the topics it was easier for individuals to gain approval from supervisors ,and our numbers increased. Finally, it should be noted once more that command support was essential to making the program work. If leadership feels the program is important, then the program will be successful.

Another challenge was the development of session topics. Other than knowing I wanted to start the program covering basics (to make it accessible to all), I was unsure how to start. In the early days of planning, I reached out to the leadership of ACI and ARCYBER for ideas. BG Nakasone, then ARCYBER G3, supported the concept and provided introductions to various ARCYBER staff elements to assist. It was in these follow-on conversations and brainstorming sessions that the framework of the program was developed. With the support of ACI, ARCYBER leadership and my personal working relationships across the community, I was able to sell the various session topics to organizations/individuals to garner participation. Each session was designed to last approximately one hour. Once the concept was explained, all of the Subject Matter Experts (SME) were enthusiastic to assist and many provided ideas on future session topics to explore.

Deciding on the reading material to use in the professional development program was also a challenge. There are already a few good reading lists on the topic of cyber. As I was developing the program, I reviewed lists from the following military organizations: U.S. Strategic Command[14], U.S. Air Force Chief of Staff[15], and Joint Special Operations Command[16]. I also talked to COL Conti, director of ACI, for his recommendations[17]. Other sources include Rick Howard's, CISO of Palo Alto Networks, Cybersecurity Cannon[18] and Intelink's compiled cyberspace reading list[19]. I wanted the program to use a mixture of books (both fiction and non-fiction), on-line journal articles, and videos to support the various cyber topics. The worst thing that could happen to the program is for participants to get bored because every session used the same medium. Finally, not only did ACI provide ideas for reading material but they were also able to cover some of the costs of purchasing books for active participants. Fortunately the balanced mixture of materials and subject matter experts kept the sessions interesting and made for fluid transitions.

Sessions are already planned for the opening months of 2015. In January, the group will explore the legal and ethical implications of utilizing cyber tools on foreign soil. The case study will be the STUXNET virus and the participants will be playing the role of the individual that must decide whether to unleash it or not. We will analyze the virus against the Law of Armed Conflict to determine the legality of executing the mission along with the projected collateral effects of its use. Then we will discuss the ethical implications of making the decision to use the tool. This is extremely relevant in today's environment as the President must currently decide the appropriate response to the cyber terrorists' campaign against Sony and the movie "The Interview." Additionally, early 2015 sessions will include examining the Coast Guard's unique perspective on cyber, Kevin Mitnick's hacking successes, current Chinese Cyber doctrine, and cyber crime as a threat to national security.

Based on input from participants, some future sessions will be designed to also count as continuing education credits towards required IT certifications (i.e. CompTia Security+). This will assist individuals in justifying their participation with their supervisors and provide truly quantifiable value in their professional development. Ultimately, 2014 focused mainly on the military's perspective of cyber operations – therefore, 2015's program will strive to include other federal agencies and their perspective on their portion of cyberspace responsibility and the challenges that they face. Some of these sessions could include participation from the Department of Homeland Security, Department of State, Federal Bureau of Investigation, and the Central Intelligence Agency.

So, did we make it to the desired end state? Was the program worth it? Absolutely. The individuals that participated grew and developed as leaders and professionals; minds were opened, thinking skills were honed, and understanding about cyber was increased. While information is out there about all the topics that we covered,

participants found it more exciting and engaging when the information was presented by an individual from within the infrastructure. This led to great conversations where information was shared and knowledge gained. Being in the remote location of Italy, it is not easy to have access to programs, conferences, and courses that our stateside counter-parts may be able to attend. Therefore, this program filled a niche that has been neglected for our workforce due to our geographical limitations. For a grass-roots effort, this program was a resounding success.

In truth, it is a shame that this program has to be a grass-roots effort. Developing agile and adaptive leaders is a key mission within the Army. These competent and capable individuals are the reason that the United States Army is the best in the world. Determining ways to continue to grow proficient leaders ready for tomorrow's battle while adhering to fiscal constraints should be every commander's concern. This inexpensive (in terms of funding) program harnessed techniques from the past and modernized them. I believe cyber has a huge role to play in modern and future warfare. We need to educate leaders at all levels across the force about cyber. The Army recognizes the importance of developing cyber capabilities – the Army leadership should also remember that our strongest capability is our people. Through programs like this we can create a better trained cyber force, more agile cyber personnel, and leverage new relationships between diverse organizations to more effectively operate within and defend our cyberspace.

Appendix

[1] Units (Brigade size and larger) transport personnel (~4,000-~10,000 individuals) and equipment (~400-450 railcars) to the Mojave Desert for a 28-day rotation to conduct live fire attack and defense against a scripted enemy. These scripted scenarios are typically based on their upcoming deployment mission.

[2] U.S. Army Publishing Directorate, "Army Regulation 350-1: Army Training and Leader Development", August 19, 2014.

[3] 509th Signal Battalion is located in Vicenza, Italy.

[4] The Fifth Dimension, *The Age of Aquarius*, Soul City Records, 1969.

[5] The G5/7 section is responsible for long-term planning, policy development, and coordination with outside agencies.

[6] Patrick Engbretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, (New York: Syngress, 2013).

[7] The OODA loop was developed by U.S. Air Force pilot COL John Boyd based on his experiences in the Korean War. More information can be found in the John Boyd Compendium, provided by the Project on Government Oversight at http://dnipogo.org/john-r-boyd/.

[8] The G2 section is responsible for conducting analysis and planning to tailor intelligence capabilities to support the mission.

[9] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Ecco, 2010).

[10] Cory Doctorow, *Little Brother*, (New York: Tor, 2008).

[11] Matthew Miller, Jon Brickey, and Gregory Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong", Small Wars Journal, 2012. Jason Bender, "The Cyberspace Operations Planner", Small Wars Journal, November 5, 2013. Scott Applegate, "The Principle of Maneuver in Cyber Operations", (paper presented at the 4th International Conference on Cyber Conflict, Estonia, 2012).

[12] The Cyber CoE is the U.S. Army's force modernization proponent for Cyberspace Operations, Signal/ Communications Networks and Information Services, and Electronic Warfare (EW) and is responsible for developing related DOTMLPF solutions. (http://cybercoe.army.mil/)

[13]Mark Bowden, *Worm: The First Digital World War* , (New York: Atlantic Monthly Press, 2011).

[14] http://www.stratcom.mil/reading_list/

[15] http://static.dma.mil/usaf/csafreadinglist/index.html

[16] http://jsou.libguides.com/c.php?g=83707&p=538565

[17] Gregory Conti, et al, "Self-Development for Cyber Warriors", Small Wars Journal, November 10, 2011.

[18] https://www.paloaltonetworks.com/content/campaigns/lp/cybercanon/index.html

[19] https://intellipedia.intelink.gov/wiki/Cyberspace_Reading_List only for Federal personnel as it is CAC-protected