SMALL WARS JOURNAL

TRAINING FUTURE CYBER OFFICERS: AN ANALYSIS OF THE US ARMY ROTC'S EFFORTS TO PRODUCE QUALITY JUNIOR CYBER OFFICERS

Mad Science

Sat, 09/10/2016 - 6:52am

Training Future Cyber Officers: An Analysis of the US Army ROTC's Efforts to Produce Quality Junior Cyber Officers

Andrew Schoka

The emergence of cyberspace as a recognized warfighting domain has heralded monumental changes in the US Army's mission, focus, and structure over the past several years. Currently, the US Army is moving to field the next generation of cyber warfighters, and the need to identify, train, and develop these cyber professionals is becoming increasingly critical. Bearing the responsibility for leading these cyber warfighters, the training and development of the Army cyber officer corps remains at the forefront of issues facing the effectiveness of the Army cyber branch. With the first groups of officers being assigned directly to Army cyber units, the importance of properly preparing and developing the leaders of the Army cyber force is an issue that requires the continued attention of Army leaders in order to ensure the long-term viability of the Army's warfighting efforts in the cyber domain. The duty of commissioning substantial numbers of these cyber officers falls to the Army's Reserve Officers' Training Corps (ROTC), as does the unique developmental, academic, and professional requirements associated with producing junior cyber officers capable of succeeding in a highly complex and technically demanding field. This paper is intended to provide an analysis of the

current developmental framework used by the Army ROTC to train, develop, and select its future cyber officers, and propose specific, actionable steps to be taken in order to address the current lack of a formalized system for performing this critical function.

The Army ROTC exists, principally, to commission officers into the Regular Army, the Army Reserve, and the Army National Guard. Following the completion of their junior year of college, all Cadets nationwide compete for selection into one of the 17 Army branches available for accessions[i]. The substance of ROTC training is designed to assess Cadets' leadership potential through training in basic soldiering skills and small unit infantry tactics. Cadets also have the opportunity to receive more specialized training and development through Cadet Command programs specifically aligned with their intended branch of choice. This includes training programs such as Cadet Troop Leadership Training[ii] (CTLT), and Cadet Command-sponsored internships with Army contractors and industry partners, all serving to provide valuable, hands-on experience and development to future junior officers. Additionally, the ROTC accessions scheme uses the Cadet Talent Management[iii] system to evaluate the aggregation of a Cadet's academic background, extracurricular experiences, training opportunities, and personal interests in order to select Cadets for the branch in which they are most likely to succeed, and to remain in.[iv] Among the various criteria considered by the Cadet Talent Management system, branch-specific Cadet training opportunities are factored in favorably for accession to that particular branch.

Cadets interested in assessing into a combat arms branch can elect to participate in a number of additional training opportunities designed to prepare junior officers to commission into a specific branch. Training through military science courses, practical leadership labs, and field training exercises culminates in attendance at the Cadet Leaders' Course[v] (CLC) after junior (MS III) year. In addition to this baseline level of required training, Cadets interested in branching combat arms can also compete for training opportunities at Airborne, Air Assault, Mountain Warfare, or Northern Warfare schools.[vi] These cadets can also complete training assignments with combat arms units as a part of CTLT. Cadets following this model advance through a progressive development cycle in the form of Military Science classes and practical Leadership Labs for each Military Science level. This model of progression can differ for individual Cadets, and is only meant to illustrate an archetypical model for a Cadet's training opportunities; training opportunities are funding-dependent and the number of available slots available varies from year to year.[vii] However, it is most common to see Cadets attend Airborne, Air Assault, the Cultural Understanding and Language Proficiency Program[viii] (CULP), or other training schools after MS I or MS II year, and to attend CTLT after MS III year and completion of CLC. Additionally, by participating in ROTC-sponsored activities such as the Ranger Challenge[ix] team, the Society of American Military Engineers[x], Combat Dive preparatory teams, or special operations preparatory organizations, Cadets can gain valuable developmental experience in their intended field of service. This progression, while not mandated by an ROTC contract, represents the typical "pipeline" that Cadets who are interested in combat arms or combat support branches will follow, and offers progressive, iterative development pertaining to that Cadet's intended branch.[xi]

However, the current framework for the selection and development of Cadets specifically interested in the cyber branch exists on a strictly notional level. In practice, there is little formalized guidance for developing Cadets into junior cyber officers through programs and opportunities similar to the ones previously discussed. There is currently no systematic pathway for ROTC Cadets to follow in order to gain the requisite domain knowledge needed for success as junior cyber officers. Further, there is no established set of best practices for Cadets or their corresponding ROTC units to follow. At present, the extent of guidance given to Cadets interested in serving as cyber officers is to select a major in Computer Science, Engineering, Math, or Information Technology. More succinctly, *there is currently no formalized system implemented within ROTC for the development and selection of junior cyber officers*. Compared to the resources available for preparing combat arms officers, and considering the highly technical and domain-specific requirements of the cyber branch, this issue represents a significant detriment to the ability of the Army cyber force to recruit, prepare, and select qualified junior officers, and to build a mission-capable, highly effective cyber force over the long term[xii].

Outside of ROTC, a structured “pipeline” similar to the one detailed above is already used as an extremely effective tool for developing USMA Cadets interested in branching into the cyber force. Administered by the Army Cyber Institute, the Cyber Leader Development Program[xiii] (CLDP) is a program designed to fulfill the need for a progressive system of development for future junior cyber officers commissioned out of the US Military Academy. The program provides guidance in the form of assigned mentors and extensive opportunities for academic and professional development training events.[xiv] One of the strengths of the CLDP is the level of industry cooperation and participation that the program encapsulates, affording Cadets the opportunity to attend professional cybersecurity and information technology conferences, and the ability to participate in internships with groups, units, and companies working in the cybersecurity sector. The CLDP website states that participating Cadets engage in over 800 hours of extra-curricular developmental experiences over the course of the program through the aforementioned conferences, internships, events, and training.

While the existing CLDP timeline and checklist was designed specifically for USMA Cadets, the CLDP site does provide guidance for ROTC Cadets to participate by signing up for the CLDP e-mail distribution listserv and by selecting a mentor on the ROTC branching webpage. However, this is the extent of the program’s implementation for the majority of ROTC programs, and there exists minimal visibility into this program across Cadet Command[xv]. Cadets selected for cyber operations training through the ROTC Cyber Operations Internship Program (RCIP) were unaware of the benefits of participating in the CLDP and lacked the resources and support to enter the program. Many ROTC programs are similarly uninformed regarding the CLDP, leaving Cadets who would otherwise benefit from participation in the program unaware of its existence. There is currently minimal support from Cadet Command to implement the CLDP for ROTC detachments and, consequently, the vast majority of programs will continue to focus on their core competency, which in most cases is training future combat arms officers. This is a critically underutilized developmental resource subject to absence of visibility and a lack of infrastructure to support the program within

Cadet Command.[xvi] The CLDP is a proven system that is successfully developing and training USMA Cadets to become outstanding Cyber officers, and currently, ROTC is failing to implement the program in an equally effective manner.

In lieu of placing the burden of administering and resourcing the CLDP on the ROTC units of host schools, an alternative solution would be to leverage the existing infrastructure of the joint National Security Agency and Department of Homeland Security Centers of Academic Excellence[xvii] (CAE) program. Many of the host schools for ROTC units are designated by the NSA and DHS as CAE institutions in Cyber Defense and/or Information Assurance as a part of the CAE program.[xviii] These schools already have outstanding academic research and coursework in the field of cybersecurity, and provide excellent opportunities for cyber-interested students, whether Cadet or civilian, to take classes and participate in projects relating to a variety of cybersecurity topics. The integration of the CLDP with the CAE program would require cooperation between a school's ROTC office and relevant academic departments to provide support and mentorship to cyber-interested Cadets. By requiring CAE institutions to provide support to their institution's respective ROTC programs, Cadets could be given the opportunity to complete academic projects, conduct research, and participate in conferences as a part of the CLDP. CAE accreditation is renewed every five years, and the requirement for CAE institutions to support their school's CLDP program could be implemented as a reaccreditation requirement, rather than immediately imposing the stipulation on CAE universities. Additionally, the range of CAE designations across ROTC host schools would ensure a broad range of specialties and backgrounds within the Army cyber force in the future.

By definition, CAE-designated institutions already possess the requisite level of infrastructure to administer a rigorous academic program for graduate and undergraduate students. Formalizing this partnership would be as simple as designating an ROTC cadre member to liaise with that school's CAE faculty members to track and assist participating Cadets. A proof of concept for a joint ROTC-CAE effort for the CLDP already exists in the form of the CyberCorps Scholarship for Service[xix] (SFS) program, administered by the Office of Personnel Management. This program leverages academic grants from the National Science Foundation to sponsor undergraduate and graduate students majoring in academic disciplines relevant to the cyber domain.[xx] The SFS program uses the CAE accreditation process to approve institutions for participation in the program, and while universities with equivalent programs may still apply for the SFS, CAE accreditation is a crucial distinguishing factor for schools applying to the program. SFS participants incur a federal employment obligation equal to the number of years of funding provided by the program, and go on to work at various government agencies supporting the national cyber mission. By following a nearly identical model to the SFS program, ROTC could utilize the infrastructure of CAE-accredited universities to implement a solution uniquely tailored to ROTC Cadets that capitalizes on established resources to provide the academic and professional development framework to implementing an ROTC CLDP.[xxi]

Additionally, fledgling programs are already being executed to place ROTC Cadets with cyber mission units as a part of CTLT training, or as an internship training assignment[xxii], meeting one of the most important requirements of the CLDP. This summer, twelve ROTC Cadets, representing universities from across the country, were selected as the inaugural participants in the first

implementation of an ROTC Cyber Operations Internship Program (RCIP). These Cadets were assigned to participate in the National Security Agency's 12-week Cyber Summer Program[xxiii] (CSP), a rigorous academic program intended to provide real-world experience in cyber-related topics. Around thirty additional Cadets were also selected to participate in 4-week RCIP assignments at the NSA, 780th MI BDE, and other locations. The program's stated goal was to provide Cadets with mission-oriented experience working with groups and units operating in the cyber domain.

The execution of the CSP mission changed due to a backlog of security clearance investigations (TS//SCI is required for the CSP)[xxiv], requiring Cadets to be reassigned to alternative organizations. Of the original twelve Cadets, seven were reassigned to locations at the NSA not tied to the CSP, FBI, Boeing, and other groups in the Ft. Meade area, and five Cadets were reassigned to the Army's Space and Terrestrial Communications Directorate[xxv] (S&TCD) under the Communications-Electronics Research, Development, and Engineering Center[xxvi] (CERDEC) at Aberdeen Proving Ground, Maryland. Cadets who were originally selected to participate in 4-week RCIP assignments were assigned to a host of different locations at CERDEC, Ft. Meade, and USMA.

As Cadets began their RCIP assignments, it quickly became apparent that the criteria used for selecting participants had been applied with a significant degree of variability across the Brigades. While all Cadets selected to participate in the RCIP had academic backgrounds in Engineering, Math, or Science, not all had experience in cyber-related fields or an interest in cyber operations.[xxvii] Several of these Cadets elected to instead participate with groups more aligned to their areas of study, such as the CERDEC Command, Power and Integration Directorate[xxviii] (CP&I) and the Aberdeen Testing Center[xxix] (ATC). This incongruity with the RCIP's mission to provide future cyber officers experience in their intended branch of service highlights a lack of information provided to ROTC host institutions regarding the Army cyber mission, a shortfall that could be easily addressed through integrating the RCIP initiative as an element of an ROTC-specific CLDP.

CERDEC employees, both military and civilian, worked hard to provide the resources, support, and mentorship that resulted in a deeply beneficial training experience as a part of the RCIP. In future years, the experience provided through participation in the RCIP could be significantly augmented by implementing the RCIP as an element of a more progressive, multi-year structured training system similar to USMA's integration of Advanced Individual Academic Development[xxx] (AIAD) programs with the CLDP. Establishing a formalized internship program that enables Cadets to participate in a structured academic and developmental program would provide both valuable exposure and experience in the cyber domain. While the intention of the RCIP initiative is spot-on, the execution of this training opportunity's first iteration speaks to the imperative for greater formalization of the process for training future cyber officers. As it stands, the RCIP is largely a stand-alone effort, and could be dramatically improved by folding these programs into the formalized structure of the CLDP in order to integrate these experiences with a rigorous, multi-year academic development program in the cyber field.

There is no question regarding the critical importance of identifying, training, and selecting top-quality officers to serve in the Army cyber force. The Army as a whole has a vested interest in successfully matching future officers with the branch that best suits their talents and interests; this notion forms the impetus for the implementation of the Cadet Talent Management System. The insufficiencies of the current paradigm for training, developing, and selecting these officers through ROTC do not offer a sufficient foundation upon which to build for the development of greater numbers of cyber officers in future year groups, and are stunted by a widespread lack of backing, support, and awareness. Cadet Command should work in tandem with efforts already untaken by USMA and the Army Cyber Institute to establish a more rigorously defined framework for the development of Cadets selected as cyber officers. With the massive potential for both success and vulnerability in the field of cyber operations, the US Army Cadet Command has the opportunity to become a recognized leader in producing top-quality Army cyber officers. This is an opportunity that Cadet Command, the Army, and the nation must address today in order to field a force capable of succeeding in the battlespace of tomorrow.

End Notes

[i] Only Cadets selected for Active Duty will compete for branch assignment. According to Cadet Command-published statistics, the FY16 cohort consisted of 5580 Cadets, of which, 3016 were selected for Active Duty.

[ii] Useful summary of CTLT located at http://www.cadetcommand.army.mil/training/ctlt.aspx (http://www.cadetcommand.army.mil/training/ctlt.aspx).

[iii] Overview and description of Cadet Talent Management located at https://branching-rotc.army.mil (https://branching-rotc.army.mil). Talent Management was rolled out as a pilot program with the FY 16 accessions cohort, and will be fully integrated into accessions for the FY 17 year group.

[iv] Cadet Talent Management was created to address poor long-term retention rates of officers, attributed to dissatisfaction with branch assignments. In 2011, Professor Tayfun Sönmez of Boston College authored an evaluation of the effectiveness of the ROTC Branching Model as it contributed to long-term retention rates for Army officers. Located here: http://www.bc.edu/content/dam/files/schools/cas_sites/economics/pdf/workingpapers/wp783.pdf (http://www.bc.edu/content/dam/files/schools/cas_sites/economics/pdf/workingpapers/wp783.pdf)

[v] Useful description and overview located at http://clc.futurearmyofficers.com/ (http://clc.futurearmyofficers.com/)

[vi] Some other, rarer, school assignments are available in certain years. Cadets have also participated in WHINSEC, SFCDQC, Sapper Leader Course, and other similar assignments. In general, these assignments are geared towards Cadets intending to branch into combat arms. Detailed at: http://www.cadetcommand.army.mil/training/cadet-practical-field-training.aspx (http://www.cadetcommand.army.mil/training/cadet-practical-field-training.aspx)

[vii] The University of Kentucky's Army ROTC page has an informative description of the timeline of Cadet summer training opportunities here: https://armyrotc.as.uky.edu/army-schools (https://armyrotc.as.uky.edu/army-schools)

[viii] CULP is a language and cultural immersion program which sends teams of Cadets to engage with foreign military hosts. Detailed here: http://www.cadetcommand.army.mil/culp/ (http://www.cadetcommand.army.mil/culp/)

[ix] Rensselear Polytechnic Institute's Army ROTC program has a helpful description of Ranger Challenge, located at https://www.rpi.edu/dept/armyrotc/challenge.html (https://www.rpi.edu/dept/armyrotc/challenge.html)

[x] SAME site: http://www.same.org/ (http://www.same.org/)

[xi] CLC is currently the only mandatory course of the summer training events depicted in the diagram. For a full listing of commissioning requirements as a part of the ROTC program, see AR 145-1, Senior Reserve Officers' Training Corps Program: Organization, Administration, and Training.

[xii] Francesca Spidalieri makes a similar argument for the importance of improving cyber-related education in the context of Joint Professional Military Education Institutions in a 2013 paper published by Salve Regina University. Paper located at: http://salve.edu/sites/default/files/filesfield/documents/JPME_Cyber_Leaders.pdf (http://salve.edu/sites/default/files/filesfield/documents/JPME_Cyber_Leaders.pdf)

[xiii] The Army Cyber Institute at USMA has a page detailing the CLDP, found at http://www.westpoint.edu/acc/SitePages/CLDP.aspx (http://www.westpoint.edu/acc/SitePages/CLDP.aspx)

[xiv] Francesca Spidalieri and Jennifer McArdle argue for the inclusion of stronger cybersecurity academic programs in officers' undergraduate education in a 2016 paper published by the Cyber Defense Review. Their work focuses on the programs at service academies, and includes an in-depth description of the cybersecurity program and the CLDP at USMA (pages 152-155). Located at: http://www.cyberdefensereview.org/wp-content/uploads/2015/01/CDR-SPRING2016.pdf (http://www.cyberdefensereview.org/wp-content/uploads/2015/01/CDR-SPRING2016.pdf)

[xv] The University of Cincinnati is, as far as I can tell, is the only ROTC host institution that has established an effective CLDP initiative at an NSA/DHS CAE-designated university. Their website is located at: https://www.uc.edu/armyrotc/opportunities/cldp.html (https://www.uc.edu/armyrotc/opportunities/cldp.html)

[xvi] The authors of "Professionalizing the Army's Cyber Officer Force" cite the need for extensive collaboration between Cadet Command, USMA, and Army Cyber Command to develop a rigorous CLDP. The CLDP would be used with the express purpose of developing and identifying Cyber officer candidates, a critical task to filling the ranks of the branch.

[xvii] More detail on the CAE program here: https://www.iad.gov/NIETP/aboutCAE.cfm (https://www.iad.gov/NIETP/aboutCAE.cfm)

[xviii]

[xviii] Universities can also be designated with other focus areas, listed at: https://niccs.us-cert.gov/sites/default/files/images/cae_ia-cd_focusareas.pdf (https://niccs.us-cert.gov/sites/default/files/images/cae_ia-cd_focusareas.pdf)

[xix] Program site located here: https://www.sfs.opm.gov/default.aspx (https://www.sfs.opm.gov/default.aspx)

[xx] NSF grant information is located at their site, here: http://www.nsf.gov/ (http://www.nsf.gov/)

[xxi] Nearly identical in structure, at least. SFS is expensive, requiring over $50k per student, per year, in order to fund tuition, fees, health insurance, books, and other expenses. The level of funding required to support an ROTC Cadet attending cyber-related programs, internships, and training opportunities would cost substantially less. SFS costs listed at: https://www.sfs.opm.gov/StudFAQ.aspx?#num6 (https://www.sfs.opm.gov/StudFAQ.aspx?#num6)

[xxii] In previous years, internship programs such as the Cyberspace Internship Program (CIP), the Advanced Cyber Education Internship (ACE), and the World Class Cyber Opposing Force Program (WCCO) have placed Cadets in Cyber-related internship roles on an individual basis. The site that describes available internships is located at http://www.cadetcommand.army.mil/training/cadet-internships.aspx (http://www.cadetcommand.army.mil/training/cadet-internships.aspx).

[xxiii] Overview and description of the CSP is located at https://www.intelligencecareers.gov/icstudents.html?Agency=NSA (https://www.intelligencecareers.gov/icstudents.html?Agency=NSA)

[xxiv] Cadets selected for the 12-week COP were identified by early October, and completed TS//SCI requests were due by the beginning of November. Favorable adjudication was not completed until mid-July.

[xxv] S&TCD site: http://www.cerdec.army.mil/inside_cerdec/stcd/ (http://www.cerdec.army.mil/inside_cerdec/stcd/)

[xxvi] CERDEC site: http://www.cerdec.army.mil/ (http://www.cerdec.army.mil/)

[xxvii] This point is not intended to minimize the notion that different academic backgrounds can leverage varying areas of expertise to tackle cyber-related problems. A Systems Engineering and Data Analytics double-major, I certainly agree with this position. Instead, the issue at hand here is the level of interest in the field of cyber operations, and the Army cyber branch.

[xxviii] CP&I site: http://www.cerdec.army.mil/inside_cerdec/cpi/ (http://www.cerdec.army.mil/inside_cerdec/cpi/)

[xxix] ATC site: http://www.atc.army.mil/ (http://www.atc.army.mil/)

[xxx] The USMA Department of Electrical Engineering and Computer Science has a description of the AIAD program at their site, located here: http://www.usma.edu/eecs/SitePages/Summer%20Opportunities.aspx (http://www.usma.edu/eecs/SitePages/Summer%20Opportunities.aspx)

Categories: Mad Scientist (/taxonomy/term/306)

About the Author(s)

Andrew Schoka (/author/andrew-schoka)

Andrew Schoka is an Army Cyber Operations Officer currently assigned to the 780th Military Intelligence Brigade (Cyber) at Fort Meade, MD. He is a 2017 graduate of Virginia Tech with a Bachelor’s Degree in Systems Engineering.