

**Testimony before the National Commission on Military, National & Public Service
May 16, 2019 | Washington, D.C.**

Military Service Hearing: Creating New Pipelines to Service and Fostering Critical Skills

**Colonel (U.S. Army, Retired) Sharon R. Hamilton, Ph.D.
Director, Liaison and Military Programs, Institute for Leadership & Strategic Studies
University of North Georgia**

Chairman Heck, Vice Chair Wada, Vice Chair Gearan, and Commissioners,

Thank you for inviting me to testify today on a very important topic to the University of North Georgia, the senior military colleges, and the Nation. I am honored to be here to discuss our initiatives to foster critical skills and create new pipelines to the Department of Defense (DOD) while also increasing the diversity of the DOD workforce, and providing opportunities to under-represented groups.

It starts with a spark. I proudly served this country for 27 years as an active duty Army officer. For me, the spark to serve occurred my sophomore year in college when I was invited to an ROTC canoe trip to find out more about Army scholarships and careers. That one event changed the path of my entire life. **Spark.**

The feasibility and possibility of serving one's country through military and civilian DOD service after achieving a college degree is not widely communicated to most high school and college students, particularly those in rural and minority communities. Elementary, middle school, and high school faculty and administrators are not knowledgeable of DOD military and civilian career opportunities unless they served in DOD, have a close familial connection to DOD, or live in proximity to a military base or post. How do we **spark** the interest of students in rural and under-represented communities to see college as a viable option, to pursue degrees in critical fields, and to consider DOD military or civilian service?

My comments today focus on two areas that seek to foster critical skills and create new pipelines to DOD military and civilian service. First, the DOD Cyber Institute proposal developed by the senior military colleges. Second, the University of North Georgia strategic foreign language and cybersecurity educational initiatives.

Section 1: DOD Cyber Institutes

The supply of cybersecurity professionals has fallen far short of demand, with some estimating the gap being as large as 600,000 professionals needed to meet the Nations demand. Recently, the senior military colleges (SMCs) developed a plan to help meet that need in DOD. The six SMCs are University of North Georgia, Norwich (Vermont), The Citadel (South Carolina), Texas A&M, Virginia Military Institute, and Virginia Tech.

Beginning in the fall of 2017, the University of North Georgia (UNG) coordinated with the other SMCs to develop the senior military college cyber consortium (SMC³) to expand cyber scholarships, increase cyber competition opportunities, increase student applications to DOD

cyber internships, and provide cyber certificate training all while exposing them to the unique and valuable opportunities of DOD careers. The SMC³ vision is to be part of the solution to the DOD's and the Nation's critical shortfall of skilled cyber professionals. We seek to **spark** in high school and college-age students the desire to serve their nation as DOD military or civilian cyber leaders.

The SMCs have a unique and specified Title 10 U.S. Code authority and have consistently provided substantial numbers of highly qualified, long-serving leaders to the Armed Forces. The SMC mission is to develop and educate students to become honorable, self-disciplined leaders by instilling core values in an intellectually challenging, military discipline environment. SMC students focus on academic achievement, teamwork, physical fitness, and service to others. The SMC graduates serve in all components of the Total Force: Active, National Guard, and Reserve. SMC graduates, military and civilian, serve in the Department of Defense (DOD), federal government, intelligence community, state agencies, and in the corporate and private sectors. The consistent and effective SMC focus on leadership permeates our values, curriculum, and activities, and serves to **spark** our students' propensity for service. The six SMCs, out of the 274 Reserve Officer Training Corps (ROTC) programs nationwide, produce over 900 new officers or 12% of ROTC commissions each year.

The SMCs invest deeply in National Security Education and DOD programs critical to recruit, educate, and develop tomorrow's DOD military and civilian leaders. In addition to computer science, the SMCs offer a wide range of academic programs involved in cybersecurity and operations including strategic foreign languages, intelligence, mathematics, data science, supply chain logistics, homeland security, health sciences, international affairs, and geospatial analysis. The six SMCs have the capability and capacity to conduct research and award graduate certificates and degrees beyond the baccalaureate level.

Recruiting and Cultivating DOD Cyber talent: SMC³ DOD Cyber Institute Proposal

The SMCs cooperatively worked with their elected officials to include language in the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) authorizing the Secretary of Defense to establish Cyber Institutes for the *"purposes of accelerating and focusing the development of foundational expertise in critical cyber operational skills for future military and civilian leaders of the Armed Forces and the Department of Defense"* (Enclosure 1).

Acting on the NDAA 2019 authorization, the SMCs developed the institute model and proposed to serve as the initial DOD Cyber Institutes. The SMCs can more readily leverage their scalable, adaptable, and diverse cyber programs to educate, identify, and sustain a ready cyber workforce and to enhance the Nation's cyber talent (Enclosure 2). As National Security Agency/Department of Homeland Security Centers of Academic Excellence (CAE) for Cyber Defense Education/Cyber Operations, the SMCs have already aligned their cyber curriculum and activities with DOD requirements and actively coordinate with NSA to ensure our students are exposed to recent and relevant cyber threats, activities, and requirements (Enclosure 3).

The SMC³ DOD Cyber Institute proposal supports and complements three priorities in the *2018 DOD Cyber Strategy* Line of Effort: Cultivate Talent (Enclosure 4).

Priority 1. Sustain a ready cyber workforce

Build future talent, identify and recruit sought-after talent

- A. Offer Cyber Institute scholarships linked to post-grad DOD work commitment. We propose to fund DOD Cyber Institute scholarships that have a designated post-graduation DOD work commitment. The scholarships linked to post-graduation jobs in DOD will **spark** the interest of Generation Z (born 1995-2010) students who are focused on reducing their student debt while seeking job stability and the opportunity to serve. The scholarships would serve to provide new opportunities to groups currently under-represented in cyber career fields, to include women and minorities. We would leverage existing scholarship administration to reduce costs and increase efficiency to ensure the largest amount possible goes to scholarships. The SMC capacity can greatly expand current DOD cyber scholarship programs.
- B. Develop and offer Summer Cyber Intensive Programs (CIP). We will offer six-week Summer Cyber Intensive Programs (CIPs) modeled on the UNG Summer Language Institute (see Section 2). The CIP participants will earn eight (8) academic credit hours in two accelerated cyber academic courses required for the respective SMC cyber degree programs. The UNG CIP pilot program is scheduled for summer 2019 for hands-on content coding and python (See Section 2, Upward Bound).
- C. Link the DoD Security clearance process to cyber scholarships. Once scholarships are awarded, we propose the security clearance process begins. By starting the lengthy clearance process earlier, we build a pool of students for cleared DOD cyber internships and potentially reduce the amount of time students wait for clearances post-graduation. Currently, graduating students face a wait of 6-12 months for a clearance during which time they are more likely to accept private sector positions that do not require clearances.
- D. Establish and/or expand student cybersecurity organizations at college and high school level. We will establish, expand, and fund annual high school cybersecurity challenges to energize high school students and **spark** an interest in and understanding of cybersecurity. Cyber competition winners could be awarded DOD Cyber Institute scholarships which raises the visibility of this career option to fellow students. We would provide tools, certificate training, and faculty advisors to collegiate and high school cybersecurity clubs to nurture and maintain interest in cyber and DOD careers.

Priority 2: Enhance the Nation's cyber talent.

Promote Leadership, Support STEM-L disciplines, and Expand Cyber-Foreign Language Interdisciplinary focus

- A. Provide incentives for students enrolled in Strategic Foreign Language degrees to pursue cyber minor/double major, and vice versa. The combination of cyber education and strategic language knowledge is what we refer to as the "golden ticket". This rare combination of critical skills is highly sought after in DOD, the intelligence community, and private sector.

- B. Incorporate foreign language elements and translation into cyber competitions and projects to allow students to practice these skills and to spark an interest in students who think they have to choose between studying cyber or a foreign language.
- C. Develop 2-6 week cyber experiential learning opportunities for students with government, military, industry, and partner countries. Experiential learning is key to gaining and retaining Generation Z students and employees.
- D. Integrate undergraduate and graduate military students into applied cyber research programs to develop talent and integrate operational knowledge and research gaps.

Expand K-12 Cyber Education programs

- A. Expand primary and secondary faculty summer and online programs in cybersecurity and computer science to enhance DOD talent pipeline. The more cyber knowledge and experience primary and secondary teachers have the better able they are to **spark** and retain young students' interest in this field.
- B. Build a deeper Educator pool in support of K-12 teacher instruction and curriculum through funded summer cyber intensive programs, labs, and experience based education.

Priority 3: Establish a cyber top talent management program

Provide focused resources and opportunities to develop key cyber skills at DOD Cyber

Institutes

As designated NSA/DHS CAEs for Cyber Defense Education/Cyber Operations, the DOD Cyber Institutes can quickly conceive, develop, pilot, and document cybersecurity and cyber operations curriculum offerings and programs IAW DOD standards and requirements.

- A. Supplement existing SMC Cyber Institute/Center staff with Military Officers (Active, Guard, and Reserve) and DOD civilians with recent cyber operations (or related) experience to bring DOD relevant skills and experience to Cyber Institute academic faculty and students.
- B. Support clearances for qualified academic cyber professionals.

Expand current funding, accessibility, and scope for Cyber Competitions and Simulations

- A. Provide funding for students to attend international cyber competitions (physical and virtual) to gain relevant, real-world exposure to the cyber challenges and to increase their cross-cultural understanding.
- B. Develop cyber competitions between the SMCs, Service academies, and DOD organizations, similar to Collegiate Cyber Defense Competition.
- C. Incorporate leadership decision-making and strategic languages into cyber competitions.

Section 2. Critical foreign language and Cybersecurity educational initiatives at the University of North Georgia (UNG)

What does UNG do to **spark** a student's interest and motivation to not only attend and succeed in college but to also pursue an educational path that supports DOD and national interests? We provide interesting, challenging, and rewarding programs to students who may not have considered college, foreign language, or cybersecurity as options. At UNG, we take innovative

and interdisciplinary approaches to encourage the study of critical languages and cybersecurity to pique student interest in DOD careers.

Summer Language Institute (SLI)

To adequately defend our country and meet the global challenges that face us today we need scholars and leaders that understand the languages of our allies and adversaries. Despite the national trend for fewer students studying foreign languages, the UNG language programs are thriving and expanding. UNG offers 11 foreign language programs including Arabic, Chinese (Mandarin), French, German, Italian, Japanese, Korean, Latin, Portuguese, Russian, and Spanish - eight of which are included on the DOD strategic language list.

Since 2008, UNG has offered the college-level Summer Language Institute (SLI) for Arabic, Chinese (Mandarin), Russian, and Korean. This six-week intensive residential program focuses on incoming freshmen, transient students, and dual-enrolled high school students. From 2008-2018, 729 SLI students received intensive critical language education. Approximately 80% of those attending SLI are funded through the National Security Education Program (NSEP) Project GO grant.

SLI students learn *one year's worth of language and earn eight (8) academic credit hours* upon successful completion of the six-week program. SLI students spend most of the day in the classroom receiving language instruction, engaging in foreign language conversation, and participating in experiential activities. The daily SLI student schedule also includes 1-2 hours in the language lab and 1-2 hours with language tutors. SLI weekends consist of cultural activities, cultural lectures, cooking competitions, movie nights, and a field trip to heritage communities in Atlanta, Georgia. <https://ung.edu/summer-language-institutes/>

UNG STARTALK Chinese and Astronomy Summer Academy

Faculty members in three colleges at the University of North Georgia (UNG) are collaborating on a two-week residential summer camp to teach 24 high school students astronomy and the Chinese language. A STARTALK grant from the National Security Agency (NSA) is making the rare combination of instruction possible. STARTALK's mission is to increase the number of U.S. citizens learning, speaking, and teaching critical languages, with programs for teachers and students from kindergarten through college. The intent of the UNG program is to **spark** students' interest in the value of learning a critical language and demonstrate they can use a foreign language in ways they never imagined.

The UNG STARTALK program is one of only three nation-wide to pair science, technology, engineering, and math topics with languages (STEM-L). The residential camp targets high school students who have no prior knowledge of the Chinese language. The recruitment efforts focused on minority and/or low-income high school youth in rural areas. The content will focus on teaching literacy of Chinese myths about the night sky and the Chinese language to introduce basic knowledge of astronomy. It will be integrated with topics of astronomy selected from the Georgia Performance Standards. UNG's STARTALK camp takes a refreshing interdisciplinary approach that shows students the links between different subjects in a real world context. <https://ung.edu/news/articles/2019/03/summer-camp-will-teach-high-school-students-chinese-and-astronomy.php>

UNG's GenCyber Warrior Academy

In June 2019, UNG will host its fourth GenCyber Warrior Academy (GCWA), funded jointly by the National Security Agency and the National Science Foundation. UNG's GCWA program will prepare students for military, federal service, and civilian cybersecurity career paths with an emphasis on personal, organizational, and national cybersecurity awareness and ethical cyber operations training. The program demand greatly exceeds the amount of students we can currently support. As in past years, we had over 140 applications for the 40 slots for the 2019 program.

The 2019 UNG GCWA will consist of 40 high school students, of which 50% will be female. Priority consideration is given to students who have studied a strategic language (such as Arabic, Farsi, Russian, Mandarin Chinese, Japanese, and Korean) in high school or elsewhere. Priority consideration is also given to students with a high aptitude in math and computer science courses or activities.

Students will attend the fully-funded 9-day residential academy modeled around earning a Certified Ethical Hacker (CEH) certificate. UNG students and Army ROTC cadets studying cybersecurity will serve as the academy tutors. UNG faculty and certified high school faculty members will provide the instruction. The academy includes 80-hours of instructional and extension activities, including 40 hours of hands-on labs in learner-centered classrooms using the CEH iLabs curriculum. The standards-based content will reinforce Cybersecurity First Principles through hands-on exercises. In addition to lab exercises, students will participate in extension activities involving coding in Python, Sphero robotics, Drone programming, 3D printing, car hacking, and capture-the-flag and red-team/blue-team events. Fun athletics and physical fitness activities are part of this program.

<https://ung.edu/cyber-operations-education/national-cyber-warrior-academy.php>

UNG Upward Bound Summer Cyber program

The Department of Education Upward Bound (UB) program provides fundamental support to participants in their preparation for college entrance. The program provides opportunities for participants to succeed in their precollege performance and ultimately in their higher education pursuits. Upward Bound serves high school students from low-income families and from families in which neither parent holds a bachelor's degree.

In the summer of 2019, UNG will expand its previous program and host the first Upward Bound (UB) Cyber program. UNG was able to support this first run through an extension of the current UB grant. This summer, UNG will have 60 students in two 30-student cohorts participate in a no-cost 4-week, 2-day-per-week instruction in Python Programming and Ethical Hacking. This fully funded program will serve as a pilot for the Summer Cyber Intensive Program (CIP) concept in the DOD Cyber Institute proposal. With funding support, we foresee having the capacity in the summer of 2020 to host 4-8 40-student cohorts under a non-credit and/or for-credit model. In 3-5 years, we could potentially host 25 total cohorts of 40 students (1,000 students at full capacity) offering both for-credit and non-credit options.

Conclusion

Thank you for the opportunity to share our ongoing cybersecurity and strategic language initiatives that can serve to **spark** the interest of students in rural and under-

represented communities to see college as a viable option, to pursue degrees in critical fields, and to consider DOD military or civilian service. The end state of these initiatives would be a continuous pipeline of cyber and foreign language prepared students, future cyber and foreign language graduates and professionals, as well as better-educated overall workforce. It all starts with a **spark**.

Enclosure 1. 2019 NDAA Program to Establish Cyber Institutes at Institutions of Higher Learning

H. R. 5515—495. SEC. 1640. PROGRAM TO ESTABLISH CYBER INSTITUTES AT INSTITUTIONS OF HIGHER LEARNING.

(a) PROGRAM AUTHORIZED.—The Secretary of Defense may carry out a program to establish a Cyber Institute at institutions of higher learning selected under subsection (b) for purposes of accelerating and focusing the development of foundational expertise in critical cyber operational skills for future military and civilian leaders of the Armed Forces and the Department of Defense, including such leaders of the reserve components.

(b) SELECTED INSTITUTIONS OF HIGHER LEARNING.—

(1) IN GENERAL.—The Secretary of Defense shall select institutions of higher learning for purposes of the program established under subsection (a) from among institutions of higher learning that have a Reserve Officers' Training Corps program.

(2) CONSIDERATION OF SENIOR MILITARY COLLEGES.— In selecting institutions of higher learning under paragraph (1), the Secretary shall consider the senior military colleges with Reserve Officers' Training Corps programs.

(c) ELEMENTS.— Each institute established under the program authorized by subsection (a) shall include the following:

(1) Programs to provide future military and civilian leaders of the Armed Forces or the Department of Defense who possess cyber operational expertise from beginning through advanced skill levels. Such programs shall include instruction and practical experiences that lead to recognized certifications and degrees in the cyber field.

(2) Programs of targeted strategic foreign language proficiency training for such future leaders that—

(A) are designed to significantly enhance critical cyber operational capabilities; and

(B) are tailored to current and anticipated readiness requirements.

(3) Programs related to mathematical foundations of cryptography and courses in cryptographic theory and practice designed to complement and reinforce cyber education along with the strategic language programs critical to cyber operations.

(4) Programs related to data science and courses in data science theory and practice designed to complement and reinforce cyber education along with the strategic language programs critical to cyber operations.

(5) Programs designed to develop early interest and cyber talent through summer programs, dual enrollment opportunities for cyber, strategic language, data science, and cryptography related courses.

(6) Training and education programs to expand the pool of qualified cyber instructors necessary to support cyber education in regional school systems.

(d) PARTNERSHIPS WITH DEPARTMENT OF DEFENSE AND THE ARMED FORCES.— Any institute established under the program authorized by subsection (a) may enter into a partnership with one or more components of the Armed Forces, active or reserve, or any agency of the Department of Defense to facilitate the development of critical cyber skills for students who may pursue a military career.

(e) PARTNERSHIPS.— Any institute established under the program authorized by subsection (a) may enter into a partnership with one or more local educational agencies to facilitate the development of critical cyber skills.

(f) SENIOR MILITARY COLLEGES DEFINED.—The term “senior military colleges” has the meaning given such term in section 2111a(f) of title 10, United States Code.

Enclosure 2: Cyber Impact and Influence of the Six Senior Military Colleges

The six senior military colleges (SMC) are Norwich, The Citadel, Texas A&M, University of North Georgia, Virginia Military Institute, and Virginia Tech. The six SMCs invest deeply in National Security Education and Department of Defense (DOD) programs critical to developing tomorrow's DOD military and civilian cyber leaders.

- The six SMCs, out of 274 ROTC programs nationwide, produce over 900 new officers or 12% of ROTC commissions each year. The SMC commissionees represent all components of the Total Force: Active, Guard, and Reserve. Guard and Reserve officers employ their leadership and technical skills in the DOD organizations, state agencies, corporate and private sectors.
- Five of the six SMCs are designated National Security Agency / Department of Homeland Security (NSA/DHS) National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) and/or Cyber Operations (CAE-CO).
- One SMC is a National Geospatial Intelligence Agency and U.S. Geologic Survey (NGA/USGS) Center of Academic Excellence in Geospatial Science (CAE GS).
- Five of the six SMCs offer an undergraduate minor in Cybersecurity.
- Two of the six SMCs offer a Bachelor of Science degree in Cybersecurity.
- Two of the six SMCs offer Graduate Certificates in Cybersecurity.
- Five of the six SMCs are Project Global Officer institutions sponsored by the Defense Language and National Security Education Office for strategic languages in Mandarin Chinese, Russian, Korean, and Arabic. One SMC is a ROTC National Language Flagship Program for Mandarin Chinese.
- The SMCs have Cadets enrolled in the Army Cyber Leader Development Program (CLDP) or are developing programs to do so. The CLDP provides cadets interested in cyber careers an assigned mentor, curriculum framework, interaction with industry, and extensive opportunities for academic and professional cyber development training events.
- In addition to computer science, the six SMCs offer a wide range of academic programs involved in cybersecurity and operations including strategic languages, mathematics, data science, supply chain logistics, homeland security, health sciences, international affairs, and geospatial analysis.
- The SMCs have robust international partnerships necessary for collaborative cyber defense, to include relationships with "Five Eyes" higher education and professional organizations.
- The six SMCs have the capacity to conduct research and award graduate certificates and degrees beyond the baccalaureate level. This role exceeds the statutory function and capacity of the Service Academies.

Four SMCs are located in Georgia, Virginia, and Texas, three of the top military host states and collocated with major DOD and Intelligence Community agencies and corporate centers facilitating close collaboration in cyber and national security.

Enclosure 3. NSA/DHS Centers of Academic Excellence Program Overview

The Center of Academic Excellence in Cyber Defense Education (CAE-CDE) and Cyber Defense Research (CAE-CDR) programs are jointly sponsored by National Security Agency and Department of Homeland Security. The Center of Academic Excellence in Cyber Operations program is sponsored by National Security Agency.

These designations recognize academic programs that meet the rigorous and stringent standards set by the NSA and are the de facto accreditations for cyber programs in higher education. Students attending CAE schools are eligible to apply for scholarships, internships, and grants through the Department of Defense.

To be awarded these designations, colleges and universities must satisfy a set of criteria that include:

- establishing academic degree programs and pathways in Cyber Defense / Cyber Operations
- engaging faculty and students in Cyber Research
- teaching hands-on skills in Cyber Defense / Offense using applied labs and assignments,
- integrating Cyber in multidisciplinary courses
- involving students in Cyber Competitions, Conferences, and Certifications
- practicing Cyber Protection at the institution by establishing Institutional Security Plans
- including local/national industry professional in Cyber in the Advisory Board for program guidance
- organizing and hosting Outreach Activities in Cyber for the Community and for K-12 schools.

To achieve CAE status, colleges and universities must map Knowledge Units (KUs) designated by NSA to courses in the academic path of Cyber Defense / Operations programs. The Cyber Defense KUs include **Cybersecurity Foundations, Cybersecurity Principles, IT Systems Components, Cryptography, Networking, Scripting and Programming, Network Defense, Operating Systems Concepts.**

The Cyber Operations KUs include **Software Reverse Engineering, Systems and Embedded Programming, Operating Systems Theory, Networking, Cyber Defense, Security Principles, Vulnerability Assessment, Legal and Ethics.**

Current Designations of SMCs

- University of North Georgia: CAE-CDE
- The Citadel: CAE-CDE
- Norwich University: CAE-CDE
- Texas A&M University: CAE-CDE, CAE-R, CAE-Cyber Operations
- Virginia Polytechnic Institute and State University: CAE-R, CAE-Cyber Operations

All six Senior Military Colleges are pursuing or have already achieved CAE-Cyber Operations designation.

Enclosure 4. 2018 DOD Cyber Strategy “Cultivate Talent” Summary

Line of Effort: Cultivate Talent (p. 6)

Sustain a ready cyber workforce: The Department’s workforce is a critical cyber asset. We will invest in building future talent, identifying and recruiting sought-after talent, and retaining our current cyber workforce. We will provide ample opportunities—both inside and outside the Department—for the professional development and career progression of cyber personnel. We will create processes for maintaining visibility of the entire military and civilian cyber workforce and optimizing personnel rotations across military departments and commands, including maximizing the use of the Reserve Components. The Department will also ensure that its cyber requirements are filled by the optimal mix of military service members, civilian employees, and contracted support to serve mission requirements.

Enhance the Nation’s cyber talent: The Department plays an essential role in enhancing the Nation’s pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors. To that end, we will increase our efforts alongside other Federal departments and agencies to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States. The Department will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.

Embed software and hardware expertise as a core DoD competency: To make it attractive to skilled candidates, the Department will establish a career track for computer science related specialties (including hardware engineers, software developers, and data analysts) that offers meaningful challenges, rotational billets at other Federal departments and agencies, specialized training opportunities tied to retention commitments, and the expansion of compensation incentives for the Cyber Excepted Service (CES).

Establish a cyber top talent management program: The Department will establish a cyber talent management program that provides its most skilled cyber personnel with focused resources and opportunities to develop key skills over the course of their careers. The Department will use competitive processes, including individual and team competitions, to identify the most capable DoD military and civilian cyber specialists and then empower those personnel to solve the Department’s toughest challenges.

Enclosure 5. Cyber Leader Development Program

The Army Cyber Leader Development Program (CLDP) was developed at the Army Cyber Institute at West Point in 2014 and opened to all Army ROTC programs in 2016.

CLDP Goal: to create a framework for cyber enrichment and extracurricular opportunities to holistically develop, grow, and inspire emerging Army leaders to succeed in the technical domain of cyberspace. This program helps the Army grow cyber capacity in all branches and will assist with building cyber leaders for the Nation.

The CLDP prescribes a framework of cyber-related activities, outside the traditional classroom environment, and recognizes Cadets with the C1 Additional Skill Identifier (ASI) upon completion of the program. The ASI allows the Army to track those officers with specific cyber education, training, and experience.

Cadets with a Cyber-related Major or Minor can join CLDP:

- Computer Science
 - Information Technology
 - Electrical Engineering
 - Systems Engineering
 - Math
 - Cybersecurity
-
- The complete the CLDP requirements, students must:
 - Be a U.S. Citizen – with eligibility for a Top Secret security clearance
 - Participate in a cyber-related internship lasting three weeks or more
 - Participate in a Cybersecurity club or study group for two academic years
 - Attend at a Cybersecurity training event or conference
 - Participate in a significant Cybersecurity project or capstone