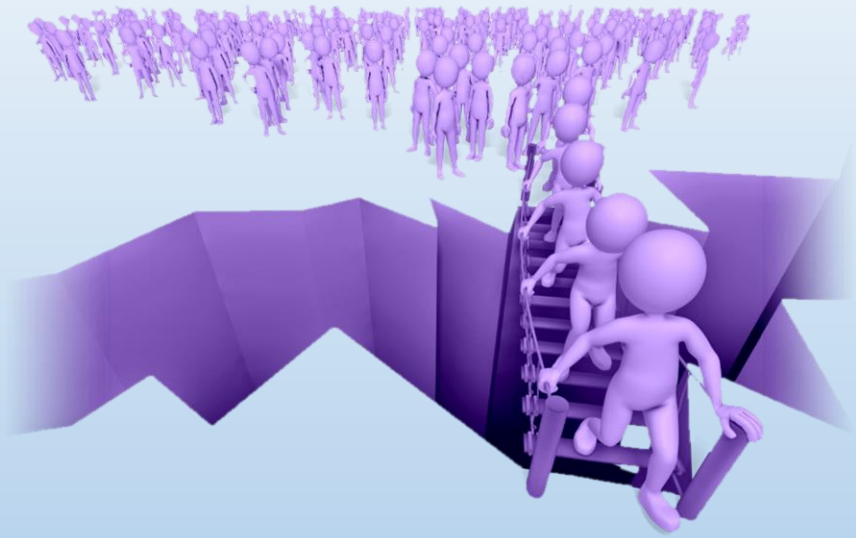
DoD Senior Military College Cyber Institutes



Creating a Pathway for DoD Cyber Careers

Dr. Sharon R. Hamilton
Colonel, US Army, Retired
Assoc VP Strategic Partnerships, Norwich University
PI, NSA Evidencing Competency & DoD SMC Cyber Institute Grants

DoD SMC Cyber Institute Program Goals

Develop

- Develop a DoD focused cyber talent pathway using the power of 6 SMCs

Conduct

- Conduct a pilot program to demonstrate capability and capacity

Employ

- Employ the Cyber Leader Development Program (CLDP) framework leveraging unique strengths of each SMC

Prepare

- Prepare students for DoD cyber work roles by providing incentives, opportunities, experiences, & certifications to develop competencies, confidence, comms skills, and leadership

Enhance

- Enhance the accessibility to and diversity of the DoD cyber workforce

Establish

- Establish a Cyber Institute program of record and several models to export to NCAE-C institutions with ROTC programs

Cyber Mission Force (CMF) work roles

- Data Scientists
- Capability Developer
- Network Operations
- Operational Research Systems Analyst
- Reverse Engineer
- Malware and Exploitation Analyst
- Big Data Analysis/ Data Analytics
- Vulnerability Researcher
- Information Operations Integrators into Cyber Operations
- Forensics Analyst

Cyber Leader Development Program (CLDP)

- Cyber related major/minor - Cybersecurity, Computer Science, Information Systems, Forensics, IA, Engineering, Data Science
- Cyber-related internship (Funded; at least 6 weeks)
- Cybersecurity club/study group (Actively participate for two years)
- Cybersecurity training, competition, certification, or conference
- Cybersecurity project or capstone
- Leadership position/experience

CLDP provides an experiential framework, standards, skills development program, and competency outcomes

How can this framework be applied at your institution?

CLDP four-year academic student cohort program

Freshman

- Provided information on their institution's CLDP
- Invited to join the cybersecurity clubs/study groups, participate in competitions, attend speaker and internship informational programs and resume/ portfolio preparation sessions, and attend DoD internship application workshops

Sophomore

- Invited to the Cyber Summer Immersion programs (2-3 weeks) developed and presented jointly by SMC faculty at various SMC campuses
- Compete for paid intern positions and funded competitions

Junior and Seniors

- Apply to CLDP cohort
- Eligible for at-school and external internship funding, scholarships, research stipends, competition travel, funded research projects, and funded certification preparation and testing

Power of Six

NORWICH UNIVERSITY
CYBERSECURITY RESEARCH IN UNDERGRADUATE PROGRAMS
CYRUP

All 6 SMCs Participated in:

NSA Codebreaker Challenge

NSA Cyber Exercise (NCX)

Norwich Cyber Research Undergraduate program

NSA/DoD Summer internships (51)

Army Cyber Institute Summer research internship

VMI Cyber Fusion

Cyber Summer Immersions

- Taught by Norwich, Citadel, & UNG faculty; attended by students from the six SMCs
- July 18 – 22 (The Citadel): Intro to Cybersecurity, Penetration Testing, Reverse Engineering, Cyber Forensics
- July 24-30 (Norwich) Deepfakes, Information Operations, & Cyber Intelligence

Where do we go next?

- This is a pilot program funded by DoD; if effective, we will export to other NCAE-C universities (with ROTC programs)
- Began Phase II in OCT 21 (Years 2 & 3) focused on joint SMC cyber events, research linked to DoD requirements, and sparking interest in freshmen and sophomores

NSA/DHS CAE-CD Cyber Programs at UNG

UNG is designated by the NSA and Department of Homeland Security as a **National Center of Academic Excellence in Cyber Defense (CAE-CD)** since 2016

- B.S. Computer Science with Information Assurance/ Cyber Concentration since 2004; ABET accredited 2017
- B.A. Strategic Studies w/Cyber Concentration since 2017
- B.S. Healthcare Informatics concentration in Cybersecurity
- B.S. Cyber began in Fall 2018, **390 majors** as of Fall 2021
- Over **1,200 CS/IS/Cyber majors** Fall 2021
- UNG offers **8 DoD Strategic Languages**
- **2023 M.S. C.S. with Cyber Ops** Specialization approved ✓

UNG Institute for Cyber Operations

- 2020-2021 cohort of 20 students
  - 7 female, 13 male: 35% gender diversity
  - 65% racial/ethnic diversity
    - 7 White/Caucasian, 13 racially/ethnically diverse participants
- Summer Language Institute 2021 at UNG in Russian, Korean, Mandarin and Arabic served 5 cyber majors from UNG and Norwich

UNG Institute for Cyber Operations

- 2021-2022 cohort of 20 students
  - 8 female, 12 male: 40% gender diversity
  - 55% racial/ethnic diversity
    - 25% Asian, 20% African American, 10% Latino, 45% Caucasian
  - Includes 3 former **GenCyber** participants (2 female, 1 male)
- Summer Language Institute 2022 serving 11 cyber majors from SMCs

UNG Student Internships

- In 2021-2022, 30 cyber students interned in private industry (IBM, Truist, T-Mobile, Home Depot, FRB Atlanta, Mass Mutual, IHG…)
- Federal Internships: 8 participated in NPS Monterey Phoenix Virtual Internships; 1 intern at Army Cyber Institute; 2 CySP interns at NIWC
- 6 NSA internships, 5 NSA new-hire grads

UNG Student Competition Achievements

- Won 2020 NSA Codebreaker Challenge
- Placed #2 in 2021 NSA Codebreaker, out of 631 schools
- Won 2020 SMC Cyber Challenge
- Won SMC Cyber Fusion 2021 Cup
- Best in Defense at SECCDC, 2nd place overall

University	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Task 7	Task 8	Task 9	Score
University of North Georgia	168	148	139	98	87	89	27	2	0	323,150.00

UNG Student Research Achievements

- In 2021-2022, CLSP Scholars presented **8 papers** and posters at regional to international conferences – but the research emphasis sparked non-cohort **undergraduate** cyber majors to publish
- Cyber majors published and presented more than **25 papers**, including 3 international conferences, 2 book chapters, 3 journal articles, and 5 proceedings, 14 poster presentations (up from two or three total publications in prior years)

Key UNG-NSA Partnerships

1. **NSA Codebreaker Challenge:** Eric Bryant, Julie Dhanraj, Mike Annicharico
2. **Academic Engagement:** Trish Butler, Latoya Harris-Hasket, Michelle Isenhart, Natalie Janiszewski, Betsy Stein, Pamela Jock & Kathy Hutson
3. **CAE Academic Liaison :** UNG's Academic Liaison, Julina Edwards, NSA-G
4. **The NSA/DHS CAE program:** Lynne Clark, Deputy Chief, CAE-CD Program Office
5. **NSA+NSF GenCyber camps**: Ashley Greely, GenCyber Program Manager
6. **DoD CySP scholarships:** Alice Smitley, DoD Cyber Scholarship Program Director
7. **NSA internships:** Shelly Thiess, SAIP/ROTC Cyber Intern Program Manager
8. **NSA Cyber Exercise (NCX):** Shirley McMonigle, NCX Program Manager (and special thanks to our NCX Mentor, Alexander Pearson, NSA-G)
9. **NSA adjunct faculty:** Five NSA faculty/adjuncts teaching online since 2017
10. **PPP collaborations:** Ian Thomas, Public-Private Partnerships, NSA-G

Cyber Advisory Council

UNG | UNIVERSITY of NORTH GEORGIA™

Mission

- To ensure the delivery of **Principled Leaders** for the **Department of Defense** who are educated and trained in **cybersecurity skillset** that is required to join the **cyber workforce** on “day one” after graduation.

Cyber Leaders Development Program (CLDP) at CDCI

THE CITADEL
DEPARTMENT OF DEFENSE CYBER INSTITUTE

- Education
  - BS in Cyber Operations
  - BS in Computer Science with a minor in Cybersecurity
  - BS in Computer Science with a minor in Data Science
- Cyber Competencies
  - Skillset from NSA/DHS Knowledge Units
  - Certifications: Network+, Security+
- Principled Leadership
  - Embedded in 4 Years program
- Service Learning
  - Summer Camp for K-12 Teachers/Students
  - Cybersecurity Awareness Day
- Research
  - Capstone Projects
- Experiential Learning and Professional Development
  - Internship
  - Cyber Club/WiCys Citadel Chapter
  - Cyber Competitions: SECCDC, NCX, NCL, PCDC, NSA Codebreaker Challenge
- Professional Mentorship
  - One-on-one contact with practicing cybersecurity professionals
  - Career Guidance

Cyber Lab at CDCI

THE CITADEL
DEPARTMENT OF DEFENSE
CYBER INSTITUTE

Cyber Lab with NetLab Framework and Vmware vCloud

- Network+
- Security+
- Certified Ethical Hacking (CEH)
- Forensics
- Palo Alto Firewall
- VMware vSphere

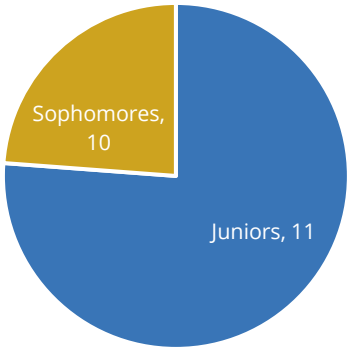
Cyber Lab will be used

- Cyber courses
- Summer Outreach Programs for Middle/High School Teachers/Students
- Summer Training for SC National Guard
- Practice for Cyber Competitions

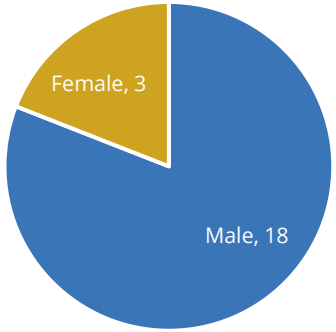
CLDP Cohort for 2022-23

- 21 Students : 20 Cadets, 1 Veteran

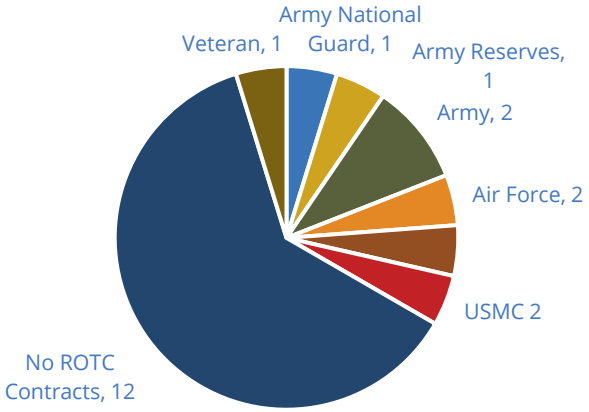
Academic Classification



Gender



ROTC Contracts

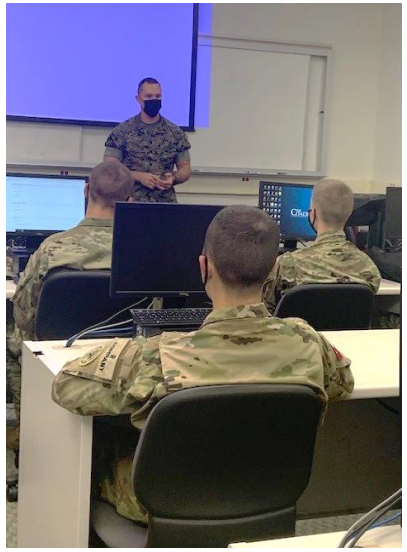


Students Recent Internship/Job Placement in Cyber

THE CITADEL
DEPARTMENT OF DEFENSE CYBER INSTITUTE

Cybersecurity Day in the month of October (National Cybersecurity Awareness Month)

THE CITADEL
DEPARTMENT OF DEFENSE
CYBER INSTITUTE



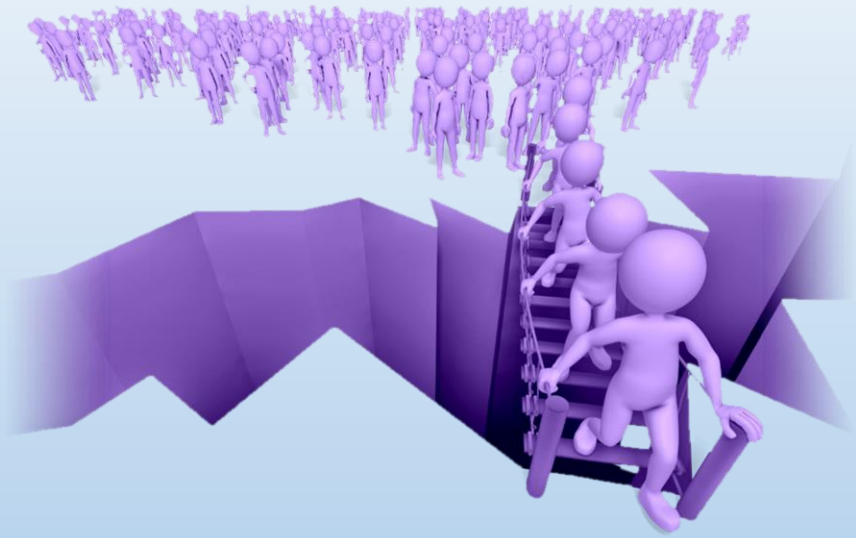
CDCI Summer Program

Citadel Cyber Bootcamp:

SC National Guard and State Guard

- July 10 – July 16
- **30 Soldiers scheduled to attend**
- One week training on **Security+**
- Each soldier received a participation certificate for 40 hrs of training and a **voucher for test certification**

DoD Senior Military College Cyber Institutes



Creating a Pathway for DoD Cyber Careers

Dr. Sharon R. Hamilton
Colonel, US Army, Retired
Assoc VP Strategic Partnerships, Norwich University
PI, NSA Evidencing Competency & DoD SMC Cyber Institute Grants

Backups

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

H. R. 5515—495. SEC. 1640

The Secretary of Defense may carry out a program to establish a Cyber Institute at institutions of higher learning 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.

The Secretary of Defense shall select institutions of higher learning…from among institutions of higher learning that have a Reserve Officers' Training Corps program…the Secretary shall consider the senior military colleges…

Each institute established shall include programs to:

1. 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. Target strategic foreign language proficiency training for such future leaders
3. Relate to mathematical foundations of cryptography and courses in cryptographic theory
4. Include 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. Develop early interest and cyber talent through summer programs, dual enrollment opportunities for cyber, strategic language, data science, and cryptography related courses
6. Incorporate training and education programs to expand the pool of qualified cyber instructors necessary to support cyber education in regional school systems.

Phase I (FY 21) DoD SMC Cyber Institute Lines of Effort

LOE 1: Develop SMC DOD Cyber Institutes

- Hire and Designate SMC Cyber Institute Director and program support (2 full-time employees per SMC)
- Increase cybersecurity/data science/AI faculty (as required by SMC)
- Establish Cyber Leader Development Program (CLDP)

LOE 2: Build governance and assessment framework/processes

- Conduct Assessment reporting and demonstrations
- Establish Government Governance (Senior Steering Group; Steering Group)
- Establish SMC Governance Group (Norwich Program Manager, SMC Cyber Institute Directors)
- Develop SMC Cyber Institute Senior Advisors Board

LOE 3a: Expand and Sustain Cyber Experiential Programs (Internal to SMCs)

- Use Security Operations Centers (SOC) at Norwich/Texas A&M for cyber threat assessment and analysis experience
- Develop exportable SOC module for NCAE-C institutions
- Develop Joint (faculty/students) SMC Cyber Summer Immersions for freshmen and sophomore students

LOE 3b: Expand and Sustain Cyber Experiential Programs (External)

- Develop and Share DoD internship opportunities amongst the SMC Cyber Institutes
- Establish SMC Cyber Institute USCYBERCOM/NSA/CSC Internships
- Support unclassified intern programs at USCYBERCOM DreamPort facility

LOE 4: Entry Level Education programs at SMCs

- Build Capacity for cyber programs – address current and projected skills gaps (People, Process, Technology)
- Incorporate NSA Adjuncts into course development and instruction (Virtual)
- Incorporate Cybersecurity certifications into SMC Cyber Institute cohort
- Link Undergraduate Research Programs to USCYBERCOM Problem Sets and requirements

LOE 5: Recruit, Train and Deploy RC SMC Deputy Directors

Phase II (FY 22/23) DoD SMC Cyber Institute Lines of Effort

LOE 1: Sustain SMC DOD Cyber Institutes

- Develop cybersecurity/data science/AI faculty
- Sustain Cyber Leader Development Program framework

LOE 2: Sustain governance and assessment framework/processes

- Review Assessment reporting and demonstrations

LOE 3a: Expand and Sustain Cyber Experiential Programs (Internal to SMCs)

- Export Security Operations Centers module to NCAE-C institutions (work roles)
- Expand SMC Cyber Summer Immersions to High/Middle School students
- Execute Joint (faculty/students) SMC Cyber Summer Immersions for freshmen/sophomore students
- Develop Degree Capstones and Projects linked to USCYBERCOM requirements

LOE 3b: Expand and Sustain Cyber Experiential Programs (External)

- Expand USCYBERCOM/NSA/CSC Internships and Apprenticeships
- Expand Internships/Expeditionary Corps programs at USCYBERCOM to CSC, DISA

LOE 4: Entry Level Education programs at SMCs

- Link Undergraduate Research programs to USCYBERCOM/ CSC requirements
- Support Cybersecurity certifications for students and faculty
- Establish INSuRE and Hack For Defense Course Modules– Challenges/Research
- Expand USCYBERCOM/NSA/CSC Visiting Professors & Adjuncts (Virtual)

LOE 5: Recruit, Train and Deploy RC SMC Deputy Directors

- Select Reserve cyber personnel for 1-year tours (selected by USCYBERCOM and with duty at SMC)
- Serve as CYBERCOM Liaison Officers and student mentors

LOE 6: Tailored Strategic Retention (one-year Army Cyber Command pilot program)

- Execute pilot program to transition early/mid-career Active-duty Army Cyber soldiers to the Reserve Forces
- Provide focused academic counseling and career transition services

Phase III (FY 24/25) DoD SMC Cyber Institute Lines of Effort

LOE 1: Sustain SMC DOD Cyber Institutes

LOE 2: Sustain governance and assessment framework/processes

- Review Assessment reporting and demonstrations

LOE 3a: Expand and Sustain Cyber Experiential Programs (Internal to SMCs)

- Execute Degree Capstones and Projects linked to USCYBERCOM requirements
- Enhance Security Operations Centers/Security Situation Centers work role competencies
- Expand SMC Cyber Summer Immersions to K-12 and Military/DoD Civilian for development and retention

LOE 3b: Expand and Sustain Cyber Experiential Programs (External)

- Expand SMC USCYBERCOM/NSA/CSC Internships and Apprenticeships
- Execute Internship/Expeditionary Corps programs at USCYBERCOM to CSC, DISA

LOE 4: Entry Level Education programs at SMCs

- Link Undergraduate Research programs to USCYBERCOM/ CSC requirements
- Sustain Cybersecurity certifications for students and faculty
- Sustain INSuRE and Hack For Defense Course Modules– Challenges/Research
- Sustain USCYBERCOM/NSA/CSC Visiting Professors & Adjuncts (Virtual)

LOE 5: Recruit, Train and Deploy RC SMC Deputy Directors

LOE 6: Extend Persistent Cyber Training Environment to SMCs

LOE 7: Develop Export Model for new DoD Cyber Institutes

- Identify candidate NCAE-C and ROTC institutions
- Provide DoD Cyber Institute CLDP process and one on one mentorship from SMC Cyber Institute to candidate institutes