Centers of Academic Excellence in Cyber Security (CAE-C)

Heather Eikenberry
Lori Pfannenstein
National Security Agency (NSA)
March 2016
National Centers of Academic Excellence in Cybersecurity (CAE-C)

- New paradigm for CAE in Cybersecurity (CAE-C)
  - NSA/DHS CAE in Cyber Defense (CAE-CD)
    - CAE in Cyber Defense Research (CAE-R)
    - CAE in Cyber Defense Education (CAE-CDE)
    - CAE in Cyber Defense 2Y Education (CAE-2Y)
  - NSA CAE in Cyber Operations (CAE-CO)
Centers of Academic Excellence (CAE) Purpose

**Creating the workforce our Nation needs**
- Reduce national infrastructure vulnerabilities
- Promote CD higher education & research
- Grow number of professionals with cybersecurity expertise

**CAE in Cyber Defense (CAE-CD)**

**CAE in Cyber Operations (CAE-CO)**

Creating the workforce DoD, IC & NSA need
- Complementary to the CAE-CD program
- Deeply technical, BS/MS level programs
- Offers a 12 week summer internship to gain knowledge of cyber operations topics & to work real world mission related challenge problems.
CAE: Creating Tomorrow’s Workforce

CAE in Cyber Defense (CAE-CD)

- Began in 1999 with seven Institutions designated
- As of 2016, designations:
  - CAE-R: 64
  - CAE-2Y: 40
  - CAE-CDE: 128
- Target: Yearly 10% growth in each designation – continuous community input on standards

CAE in Cyber Operations (CAE-CO)

- Began in 2012 with four Institutions designated
- As of 2015:
  - 14 Designated Institutions
- Target: Around 25 institutions designated – standards continually elevated

Re-designation every 5 years
Increase Info sharing between CAEs SEALs
Common Criteria for CAE-C Institutions

- Robust Program
- Physical or Virtual (hands on) Labs
- Active Faculty in Cyber Research
- Students in Cyber Research & Cyber Activities
- Student Recognition
- Multidisciplinary
- Outreach to Community
- Academic Requirements: Knowledge Units
Common Knowledge Unit Examples

• Mandatory (examples)
  – Networking Concepts
  – Cyber Defense
  – Security Fundamental Principles
  – Legal
  – Programming

• Optional (examples)
  – Secure Software Development
  – Risk Management
  – Forensics
  – SCADA Systems
CAE Cyber Defense Designation

- Promote Higher Education & Research in CD
  - Prepare growing number of CD professionals in various disciplines
  - Reduce vulnerabilities in Nation’s networks & infrastructure

- Broader Technical Skill Set for the Defensive Cyber Space Mission across the Nation
CAE Cyber Defense
Designation Requirements

• Academic Requirement – KU Mapping
  – CAE-2Y: 11 Core
  – CAE-CDE: 17 Core + 5 Optional

• Program Requirement
  – Program Outreach
  – CD Center Establishment & Maintenance
  – Student Curriculum Path & Recognition
  – CD Multidisciplinary Efforts
  – Practice of CD at Institution Level
  – CD Faculty
CAE Cyber Defense Program Outreach

- Shared curriculum or shared faculty
- Student access to CD practitioners
- Articulation/Transfer agreements with other Institutions & high schools
- Sponsorship/participation in Cybersecurity competitions
- Community Outreach
• Cyber Center & Website
  – Program guidance
  – General CD information
  – Cyber competitions, events, & news
  – Journals available to students & faculty
  – Labs & equipment; hands-on learning

• Promotes collaboration & interaction with other students, faculty, and programs
• Cybersecurity degrees, areas of study, track or certificates
• Applied training for students
• CD student recognition
• CD treated as a multidisciplinary science with elements of CD knowledge incorporated into various disciplines
  – CD taught in existing non-CD courses
  – Non-technical/non-CD students are introduced to CD
  – CD programs require non-technical courses of study
  – Non-credit/credit professional development courses in CD
• Institution encourages practice of CD - not merely teaches CD
  – Institution Cybersecurity plan and/or policies
  – Institution designated Information System Security Officer or equivalent
  – Institution encourages CD awareness throughout the campus
• Faculty assigned specifically to teach and/or develop CD courses/curriculum/modules
  – Person with overall responsibility for CD program
  – Additional Cybersecurity faculty teaching CD courses
  – Evidence of faculty qualifications to teach Cybersecurity
CAE Cyber Defense & Cyber Workforce

- PhD
- MA/MS
- BA/BS
- Associates
- CAE R
- CAE CD
- CAE 2Y
- Technical Schools
- Commercial Training
- Certificate Programs
- Military Training
- Advanced High School
64 CAE-R, 128 CAE-CDE, and 40 CAE-2Y, totaling 194 CAEs (40 are both CDE and R) in 44 states + District of Columbia and Commonwealth of Puerto Rico

https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm
CAE Cyber Defense Program Partnerships

NIST
National Initiative for Cybersecurity Education

NICE Interagency WG
NICE WG Collegiate SWG

CAE-CD Institutions

NSA
National Cryptologic School (NCS)
College of Cyber
CAE-CD Program Office

DHS
National Cybersecurity Training & Education Program

EOP / OMB
Cybersecurity National Action Plan (CNAP)

NSF
CyberCorps®: Scholarship for Service (SFS) Program
Advanced Technological Education (ATE) Centers

Industry

CAE Community
CAE Cyber Operations Program Details

• Supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation
  – Furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation

• Academic Requirement – KU Mapping
  ▪ 10 Mandatory Requirements
  ▪ 10 of 18 Optional Requirements

• Deeply technical skill set for the offensive cyber space mission including collection, exploitation, and response

• 2 Part Program
  – CAE-CO Designations and CAE-CO Summer Internship
CAE in Cyber Operations Designees

2012
- Dakota State University
- Naval Post Graduate School
- Northeastern University
- University of Tulsa

2013
- Air Force Institute of Technology
- Auburn University
- Carnegie Mellon University
- Mississippi State University

2014
- New York University
- Towson University
- United States Military Academy
- University of Cincinnati
- University of New Orleans

2015
- University of Texas, Dallas
Impact Examples of a CAE Cyber Operations Designation

“300% enrollment increase”

“Stopped State Funding Cuts”

“Increased opportunities for NSF grants”

“Influencing regional collegiate programs and outreach activities”

“Increased contact from government and industry seeking partnerships”

“Collegiate level Red Team vs. Blue Team exercises between CAE-CO schools”

“Administration support to increase faculty and programs for Cyber Operations curriculum”

“Chosen by State government to consult on Cyber Security Councils”
Unique 12 week summer program

Mission Relevant CAPSTONE + Hands on Education

Topics include Security Fundamentals, Virtualization, Cyber Operations, Digital Forensics, Memory Analysis, Reverse Engineering, SCADA, Cellular/Mobile

Instructors are academic Subject Matter Experts from U.S. Schools
CAE Cyber Ops Summer Internship

<table>
<thead>
<tr>
<th>Year</th>
<th>Interns</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>8</td>
</tr>
<tr>
<td>2014</td>
<td>13</td>
</tr>
<tr>
<td>2015</td>
<td>16</td>
</tr>
</tbody>
</table>

Selection Priority is given to qualified applicants from CAE-CO school programs.

80% of eligible Interns accepted NSA Job Offers!
CAE in Cyber Defense Program Office

• [https://www.iad.gov/NIETP/CAERequirements.cfm](https://www.iad.gov/NIETP/CAERequirements.cfm)
• askCAEiae@NSA.gov 410-854-6206

CAE in Cyber Operations Program Office

• askCAEcyberops@NSA.gov 410-854-6535