

# NICE | Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

## DEMYSTIFYING CYBERSECURITY

Integrated Approaches to  
Developing Career Pathways

**FIU** | FLORIDA  
INTERNATIONAL  
UNIVERSITY

 **NEW  
AMERICA**

# The Impact and Role of Academia in Government's Cybersecurity Strategies

**Rita Doerr**

Academic Outreach Lead, Cybersecurity Collaboration Center  
National Security Agency

# The Impact and Role of Academia in Government's Cybersecurity Strategies

Dr. Rita Doerr

Academic Outreach Lead

NSA's Cybersecurity Directorate





# Historical Motivation

- 10+ years ago ...
- NSA Academic Liaisons
- Visit colleges/universities around the U.S.
- Recurrent theme ... “what does NSA do??”
- Need some **\*UNCLASSIFIED\*** problem
  - Codebreaker Challenge (CBC) was born



# What? Codebreaker Challenge

- Annual cryptanalytic & cyber competition
- NSA academic outreach & recruiting effort
- “... to give university students exposure to unclassified problems that simulate the classified work performed at NSA.”



# Why? Codebreaker Challenge

- it provides a realistic, NSA mission-centric scenario that inspires students to develop or master their technical abilities.
- an experiential learning innovation aimed at bolstering available resources for cybersecurity education
- Ultimately a 'recruiting & hiring' tool
  - Teaser – see Impact #3



# Who? Codebreaker Challenge

- **Participants:** open to schools based in U.S. or territories (register with your school email address)
- **Designers / Developers / Deployers:** NSA employees
  - 2013-2020: “other duties as assigned” volunteers/cohort
  - 2021: full-time Operations Lead
  - 2022: full-time Cyber Co-Lead (added)



# When? Codebreaker Challenge

- Runs throughout the fall semester
  - August – December
- Design / Develop / Deploy
  - January - July





# How? Codebreaker Challenge

- **Structured:**

- a series of successively harder “tiers / tasks” that closely mirror the real-world scenarios that NSA analysts deal with every day
- one task gives “hints/insights” into the next 😊

- **Scored:**

- Participants: earn points for each completed task
- Schools: accumulate points from all participants (from the same school)



# CBC by the Numbers

	Total Participants	Total Schools/Districts	Total Solvers
2013		5	
2014		14	
2015	2217	329	54
2016	3325	481	15
2017	3103	539	3
2018	2850	377	18
2019	3777	531	50
2020	3156	452	6
2021	5465	631	38



## CBC Scenarios

- **2013**: Reverse-engineer a program which prompted for a password; needed AES key derived from SHA256 hash
- **2014 & 2015**: International terrorist orgs revised OPSEC procedures to their operatives in the field using a program being used to covertly encrypt messages
- **2016**: Terrorists have developed a new IED making it harder for US military to detect & prevent roadside attacks



## CBC Scenarios (cont.)

- **2017**: DHS has requested NSA's assistance in investigating a potential intrusion into critical US infrastructure.
- **2018**: A new strain of ransomware has managed to penetrate several critical government networks and NSA has been called upon to assist in remediating the infection to prevent massive data loss.



## CBC Scenarios (cont.)

- **2019**: Reverse engineer and develop new exploitation capabilities against TerrorTime, a custom Android secure messaging app
  
- **2020**: Two days ago, a renowned American went missing on an assignment abroad. Local street surveillance cameras recorded footage of incident as well as cell phone of journalist being destroyed.





# Top CBC Solvers

	Schools (# of Solutions)
2013	
2014	
2015	Georgia Institute of Technology (7)
2016	Georgia Institute of Technology (5)
2017	Carnegie Mellon University (2)
2018	Georgia Institute of Technology (3)
2019	University of North Georgia (30)
2020	6-way tie (1)
2021	Georgia Institute of Technology (8)



# 2021 Scenario

- NSA was investigating a foreign cyber actor
- We identified suspicious IP address and captured network traffic going towards it
- We suspect the machine is one of the actor's listening posts



# 2021 Mission

- **Identify** scope of compromise
- **Analyze** actor's comms protocols and tradecraft
- **Gain** access to actor infrastructure
  - Uncover additional tradecraft, tools
  - Swim upstream



# 2021 Tasks

- Tasks 1 – 4: Identify Scope of Compromise
  - Task 1: Which Defense Industrial Base (DIB) companies? (Network Forensics)
  - Task 2: Which user account? (Log Analysis)
  - Task 3: What was the attack vector? (Email Analysis)
  - Task 4: What was compromised? (Powershell, Registry Analysis)



# 2021 Tasks (cont.)

- Tasks 5 – 8: Analyze tradecraft and protocols
  - Task 5: Locate malicious artifact (Docker analysis)
  - Tasks 6 & 7: Reverse engineer malware (RE, Protocol Analysis)
    - Understand comms implementation
  - Task 8: Crack other comms sessions (Cryptanalysis)





# 2021 Tasks (cont.)

- Tasks 9 – 10: Gain access to actor infrastructure
  - Task 9: Connect to LP and identify registered clients (Protocol Analysis, Software Development)
  - Task 10: Expand LP access and identify data exfil path (Exploit Development)



# 2021 Skills Learned

- Forensics (network, host)
- Binary Reverse Engineering
- Protocol Analysis / Reverse Engineering
- Cryptanalysis
- Software Development
- Vulnerability Research and Exploitation



# CBC Impact #1

	Total Participants	High School Participants*
2013		
2014		
2015	2217	5
2016	3325	5
2017	3103	2
2018	2850	13
2019	3777	136
2020	3156	61
2021	5465	185

\* Counted by searching for 'School', then manually filtering; generally can't distinguish between high school and below



## CBC Impact #2

- **One Georgia post-secondary school:**
  - Used [some of] the CBC technical resources as part of their cybersecurity curriculum
- **Another Georgia post-secondary school:**
  - The CBC enabled students to obtain credit for a course's final exam if they successfully solved the entirety of the Challenge.
  - The CBC steers which topics are covered within cyber and computer science courses.



# CBC Impact #3 – the ‘So What’?!

- Since CBC inception in 2013:
  - 965 applicants
  - 432 CJOs
  - 140 FJOs
- **DISCLAIMER:** numbers are lower bounds, where CBC email address = email address on NSA application





# Coming Soon: CBC 2022!!

- **Scenario**: Ransomware
- **Number of Tasks**: 9
- **Launch Date**: early August
- **Visit**: `nsa-codebreaker.org`



# Looking Back ...

- **Participants**: high school students!!
- **Cyber/CS Curriculum**: CBC driving content!!
- **Hiring**: thousands have applied; hundreds offered jobs!!



# Acknowledgements

- Aaron H
- Ben M
- Eric B
- Jess S
- Michelle I
- “One Team; One Mission!!”



# Questions?

## Thanks for your time!



# NICE | Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

## DEMYSTIFYING CYBERSECURITY

Integrated Approaches to  
Developing Career Pathways

**FIU** | FLORIDA  
INTERNATIONAL  
UNIVERSITY

 **NEW  
AMERICA**



# Youth-to-Retirement Approach to Build a Cybersecurity Workforce

**Lynne Clark**

Chief

National Centers of Academic Excellence in the Cybersecurity  
(NCAE-C) Program Office





# NSA Cybersecurity Education Programs

Building a Cybersecurity College Readiness Pathway

# NSA Center for Education, Innovation, & Outreach

- A National Cryptologic University (NCU) organization
- Goal: Alignment of programs to ensure student opportunities and the development of youth to retirement cybersecurity college and career readiness pathways





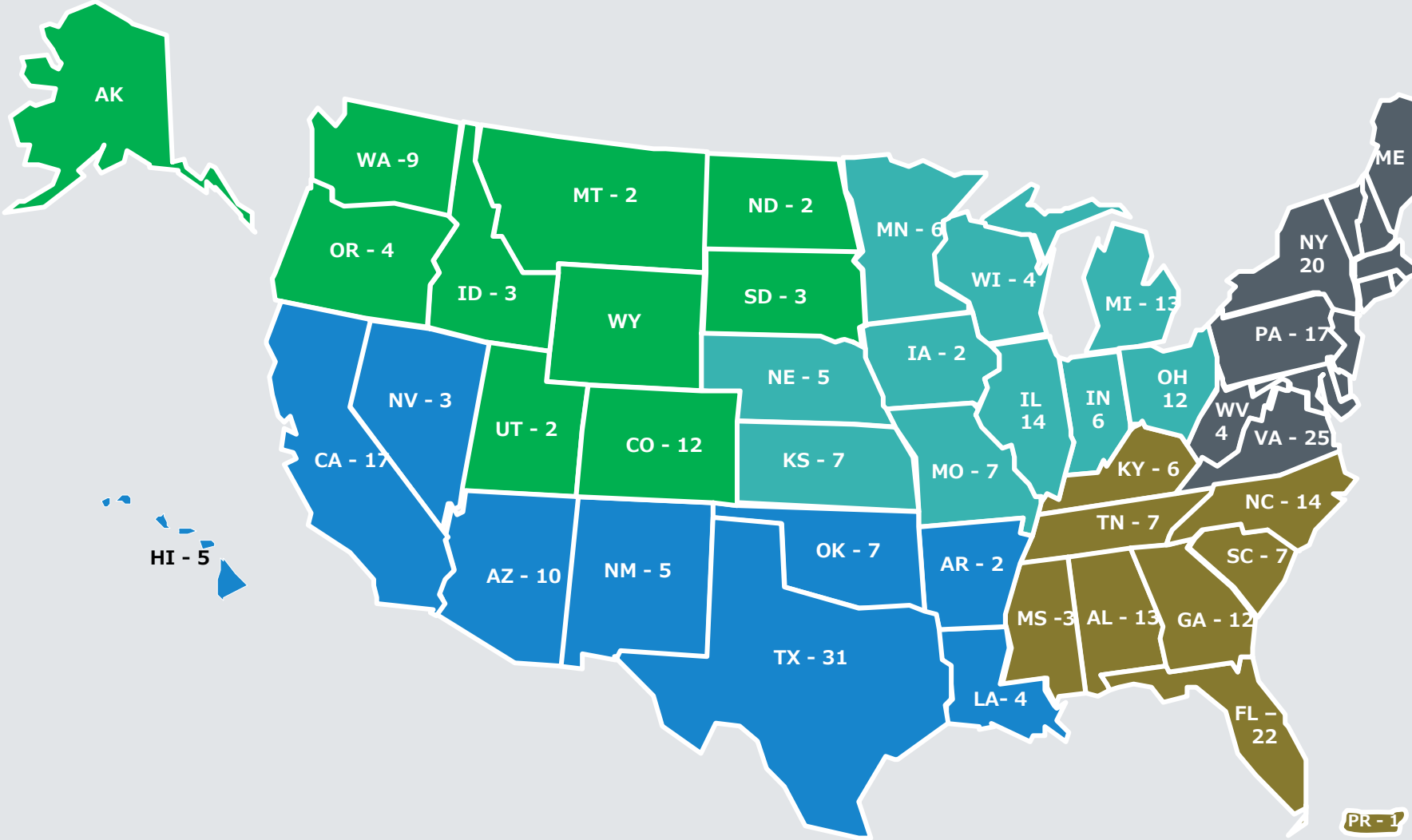
# **Opportunities in Post-Secondary Education**

# National Centers of Academic Excellence in Cybersecurity (NCAE-C)



- Over 370 universities, colleges, and community colleges
- Schools meet NSA-endorsed criterion demonstrating rigor, breadth, and scope in education, research, and outreach activities related to cybersecurity in Cyber Defense, Cyber Operations and Cyber Research
- Goal: improve the cybersecurity posture of our nation by cultivating the next generation of cybersecurity professionals.

# NCAE-C Regions and Designations



- VT - 2
- NH - 2
- MA - 8
- RI - 4
- CT - 2
- NJ - 9
- DE - 2
- MD - 21
- DC - 2

334 Institutions, 402 Programs of Study  
 116 Cyber Defense (Associates)  
 184 Cyber Defense (BA-PhD)  
 80 Research  
 22 Cyber Operations (BA-PhD)

As of Feb 2021

# Current CAE Community Initiatives (FY20)

Faculty  
Development –  
secondary & post-  
secondary  
educators

Evidencing  
Competency –  
documenting  
student  
achievement

Competitions –  
National  
HACKATHON

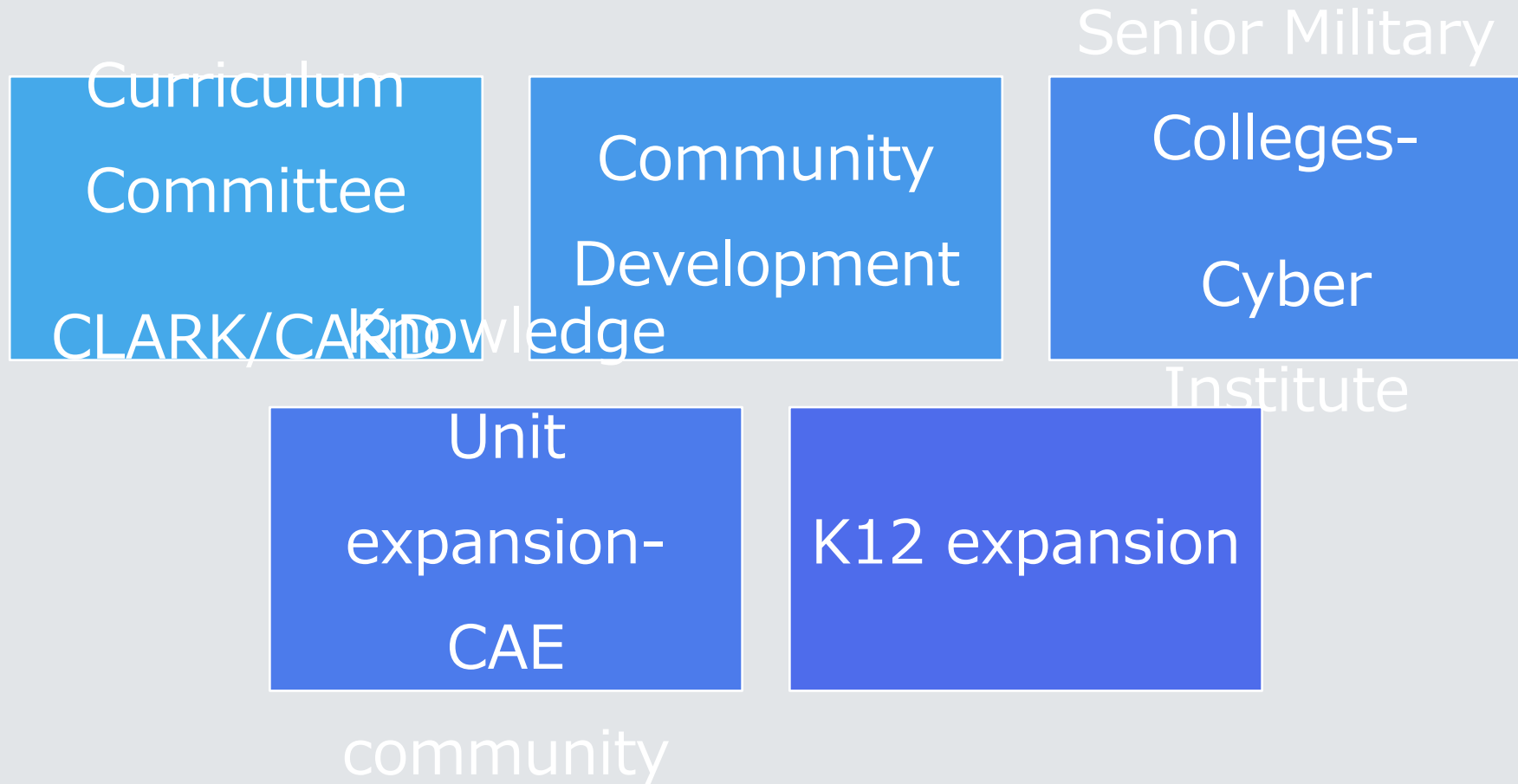
Workforce  
Development –  
academia and  
industry  
collaboration

Cybersecurity  
Education  
Diversity  
Initiative -  
Minority Serving  
Institutions

K-12 RING  
project – student  
pipeline to CAE-C  
designated  
institutions



# Current CAE Community Initiatives (FY21)



# DoD Cyber Scholarship Program (DoD CySP)

## Recruitment Scholarships (Non-DoD Employees):

- US citizens at universities designated as a National Centers of Academic Excellence in Cybersecurity are eligible; must be eligible for security clearance
- DoD Departments and Agencies select students for full-time employment
- Students receive full-tuition, required books and fees/healthcare, a one-time laptop allowance, a stipend
- Students are required to work for the DoD a minimum of one year for each year of scholarship support they receive.

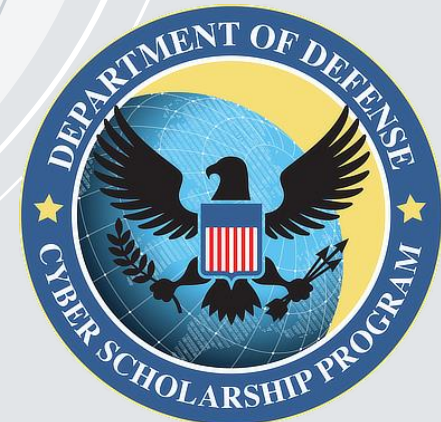


# DoD Cyber Scholarship Program (DoD CySP)

Retention Scholarships (DoD Civilians Employees and Active Duty Military):

- DoD civilian employees and active duty military eligible
- Associates degree at a NCAE-C two-year institution or a Masters/PhD at the Naval Postgraduate School or Air Force Institute of Technology
- Retention Scholars required to perform a period of obligated service at parent organization
- Receive full tuition, required books and fees

Capacity Building: NCAE-Cs who apply with scholarship students





# Youth Education Pathways Opportunities

# NCAE-C RING Project

## Middle and High School Students



### Co-Leads: University of Alabama Huntsville and Moraine Valley CC

- Online cybersecurity course based on the NCMF<sup>1</sup> High School Cybersecurity Curriculum Guidelines & aligned to CAE KUs
- Students: rural, homeschooled & under-resourced
- Development of a Career Awareness Virtual Reality experience
- Curriculum developed by UAH with interactive resources developed by MV for a hands-on user experience
- Additional features: CyberTalk, student honor society, labs, teacher resources
- Release: August 2022

<sup>1</sup>National Cryptologic Museum Foundation



**Website:**<https://caecommunity.org/initiative/k12-ring>

**Email:** [ring@caecommunity.org](mailto:ring@caecommunity.org)



# FY 2022 Education Pathway Projects



- Expansion of RING
- Development of more RING resources (middle school)
- Teacher Professional Development (National Cybersecurity Teacher Academy + Cybersecurity High School Innovations)
- CAE Regional Hubs Collaboration with States Department of Education

**Questions?**

**Email [K12\\_NCAEC@nsa.gov](mailto:K12_NCAEC@nsa.gov)**

# GenCyber



## *Igniting the Next Generation of Cyber Stars*

- Grants program responding to need to develop cybersecurity awareness and teach cybersecurity fundamentals at K-12 levels to both students and teachers
- Institutions work with a target population utilizing a unique, hands-on curriculum based upon foundational concepts and cyber ethics
- Funding Partner(s): National Science Foundation (NSF) and other federal partners on annual basis



## Program Goals



Ignite, sustain, and increase **awareness** of K12 and postsecondary cybersecurity content and **career opportunities** for participants through year-round engagement;



Increase student **diversity** in cybersecurity college and career readiness **pathways** at the K-12 level; and



**Facilitate teacher readiness** in a teacher learning community to learn, develop, and deliver **cybersecurity content for the K-12 classroom** in collaboration with nationwide initiatives.



# GenCyber Summer 2022

- 102 Programs hosted at 74 institutions (15 new) in 37 states + DC
- 70 Student Programs
- 29 Teacher Programs
- 3 Combination Programs
- 2 Capacity-building activities

Spring 2022: Up to date  
information at

[www.gen-cyber.com/camps/](http://www.gen-cyber.com/camps/)

# Structural Changes



- Two-year Period of Performance on all grants; increased funding amounts
- Required pre/post camp outreach with new reporting requirements
- Required administrative support letter for teachers
- GenCyber Concepts + career unit
- Emphasis on community partnerships

## Structural Changes (2)

- Format options: face-face, virtual, hybrid
- Teacher, student, combination camps
- GenCyber Student Language Pilot
- Capacity-building opportunities





# The Future

- GenCyber will continue to serve as both an ignition and a sustainment force in the local K12 cybersecurity ecosystem
- The Program Office continues to work with federal partners to ensure GenCyber fills the void in areas where no other programs exist
- Leveling the playing field for all continues to be a foundational goal of the program



# Resources



- National Centers of Academic Excellence in Cybersecurity: <https://public.cyber.mil/ncae-c/>
- CAE Community [www.caecommunity.org/](http://www.caecommunity.org/)
- DoD Cyber Scholarship Program <https://public.cyber.mil/dcysp/>
- GenCyber [www.gen-cyber.com](http://www.gen-cyber.com)
- K12 RING Initiative <https://caecommunity.org/initiative/k12-ring>
- STARTALK (K14 Language programs): <https://startalk.umd.edu/public/>

# NICE | Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

## DEMYSTIFYING CYBERSECURITY

Integrated Approaches to  
Developing Career Pathways

**FIU** | FLORIDA  
INTERNATIONAL  
UNIVERSITY

 **NEW  
AMERICA**



# Designing a Sustainable Workforce Development Model through Customizable Upskilling and Reskilling Pathways

**Eman El-Sheikh**

Associate Vice President, Center for Cybersecurity  
University of West Florida

**Dr. Guillermo Francia III**

Faculty Scholar, Center for Cybersecurity  
University of West Florida

**Tirthankar Ghosh**

Associate Director and Professor, Center for  
Cybersecurity  
University of West Florida



CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

# Designing a sustainable workforce development model through customizable up-skilling and reskilling pathways, competency-focused curricula, and digital credentialing

**Tirthankar Ghosh, Guillermo Francia III, Eman El-Sheikh**

**Center for Cybersecurity  
University of West Florida**



CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Agenda

- Motivation
- Workforce Development Model
- Industry Engagement
- Curricular Model
- Cybersecurity Pathways
- Stackable Digital Credentials
- Competency Assessment
- Aptitude Assessment
- Conclusion
- Future Directions





CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Motivation

- Approximately 3.5 million job openings, coupled with lack of skilled instructors and limited re-skilling and upskilling opportunities, requires competency-focused need-based learning to train and educate a sustainable workforce
- We need creative educational pathways to address the immediate skills shortage
- Digital micro-credentialing is gaining steam
- Private and public records are slowly being transformed into digital format



CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Workforce Development Model

- Workforce development provides the opportunity for workers to improve and be more productive
- Our Cybersecurity Workforce Development model is guided by best practices that facilitate flexible pathways and verifiable credentials
- We developed a nationally-scalable workforce model that is implemented nationwide with pathways at CAE-C institutions that support various cybersecurity work roles aligned to the NICE Cybersecurity Workforce Framework
- The model provides multiple on-ramps based on participants' aptitude and interests, and off-ramps to recommended cybersecurity work roles aligned with the NICE CWF



CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Industry Engagement

- Industry engagement through employer partnerships and job placements
- Strategic partnerships, between higher education, industry employers, employer associations, recruitment and support organizations, and government partners play a critical role in program and student success
- We established a national Cybersecurity Employers Network to provide valuable employability feedback on our program and share job opportunities
- Employers Network is comprised of two tiers: National Employers, that is large organizations with multiple locations across the country, and Regional Employers, which includes small and mid-sized companies with either a single location or limited regional presence as well as regional branches of national employers

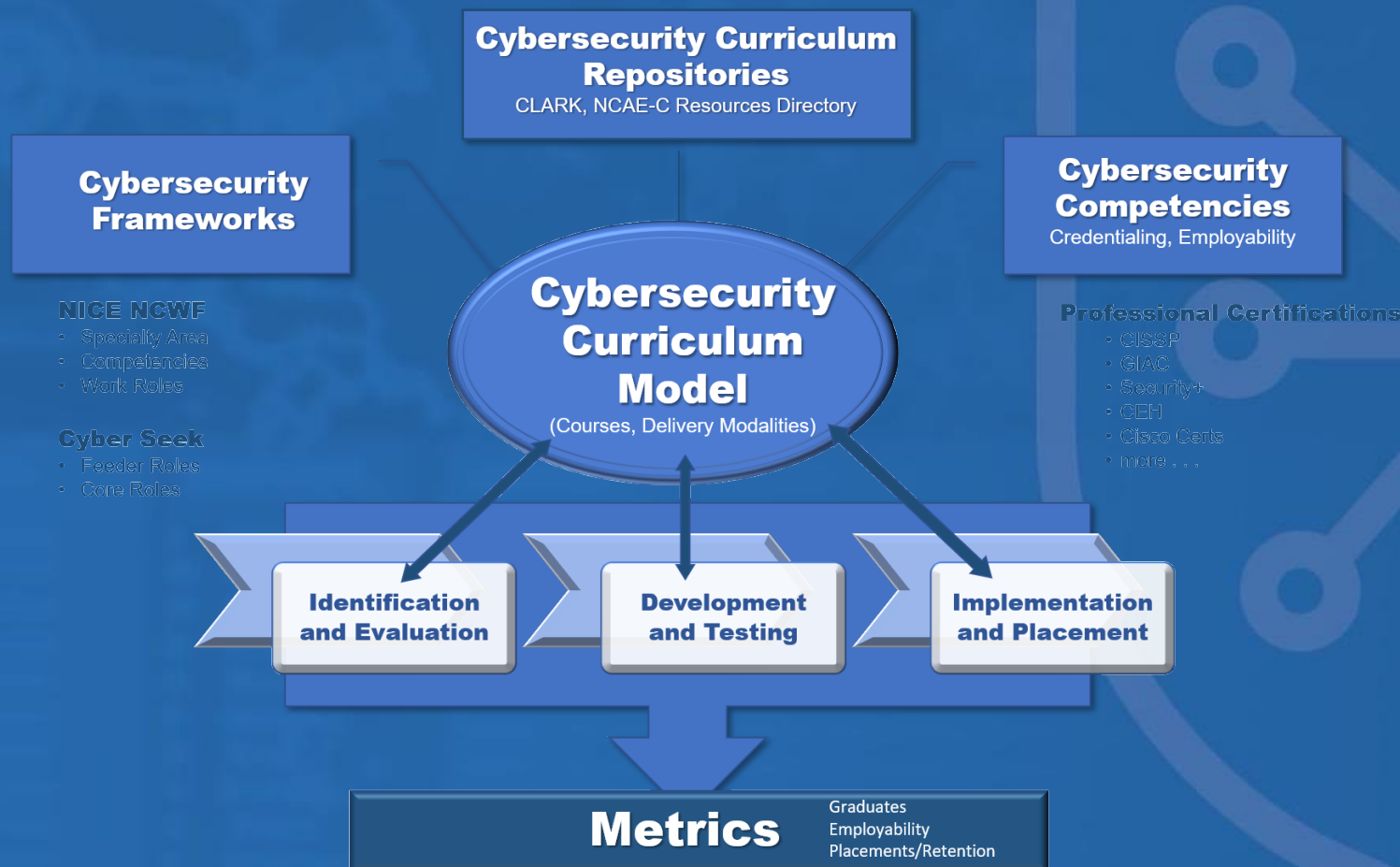


# Curricular Model

The curricular model will ensure that the workforce development materials conform to and align with appropriate external reference models, including:

Inputs: NICE Cybersecurity Workforce Framework work roles, tasks, knowledge and skills (TKS), and proposed competencies, industry certifications, and NCAE-C Knowledge Units

Outputs: CLARK curricular repository, industry certifications, and badging system







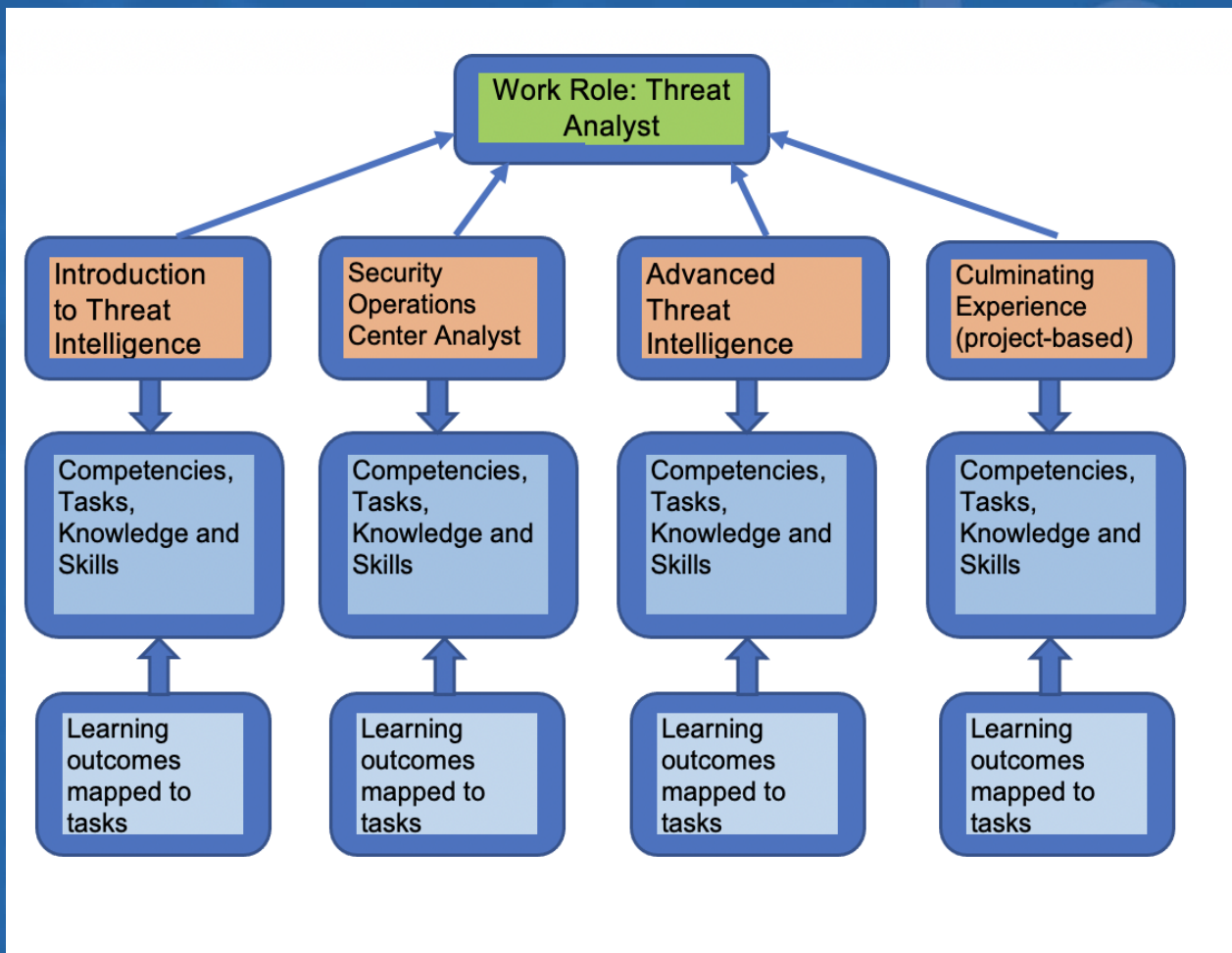
CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Cybersecurity Pathways

- Pathways reflect the needs of our industry partners and are tied to the work roles and competencies in the NICE Cybersecurity Workforce Framework.
- Each pathway has an on-ramp from a previous work role and off-ramp to the next one for upskilling individual participants
- Each pathway is designed to have a sequence of courses that are modular, scalable, and competency-focused
- The learning outcomes of each course are tied to the tasks, skills and knowledge in the NICE Framework



# An Example Pathway







CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Stackable Digital Pathway Credentials and Badges

To enable a shareable and verifiable credentialing and badging system for our Cybersecurity Workforce Development (CWD) Program we adopted the open badge initiative standards

- Participants are provided with digital credentials that are shareable, comprehensible, portable, and, most importantly, verifiable
- Digital badges should be awarded, not solely for course completion but also, for work experiences, college credits, and industry certificates
- Prospective employers should be provided easy access to digital credentials to facilitate talent search and hiring
- The opportunity to expand the CWD Program towards national recognition and adoption could be enhanced with the digital badging system as a driving force.

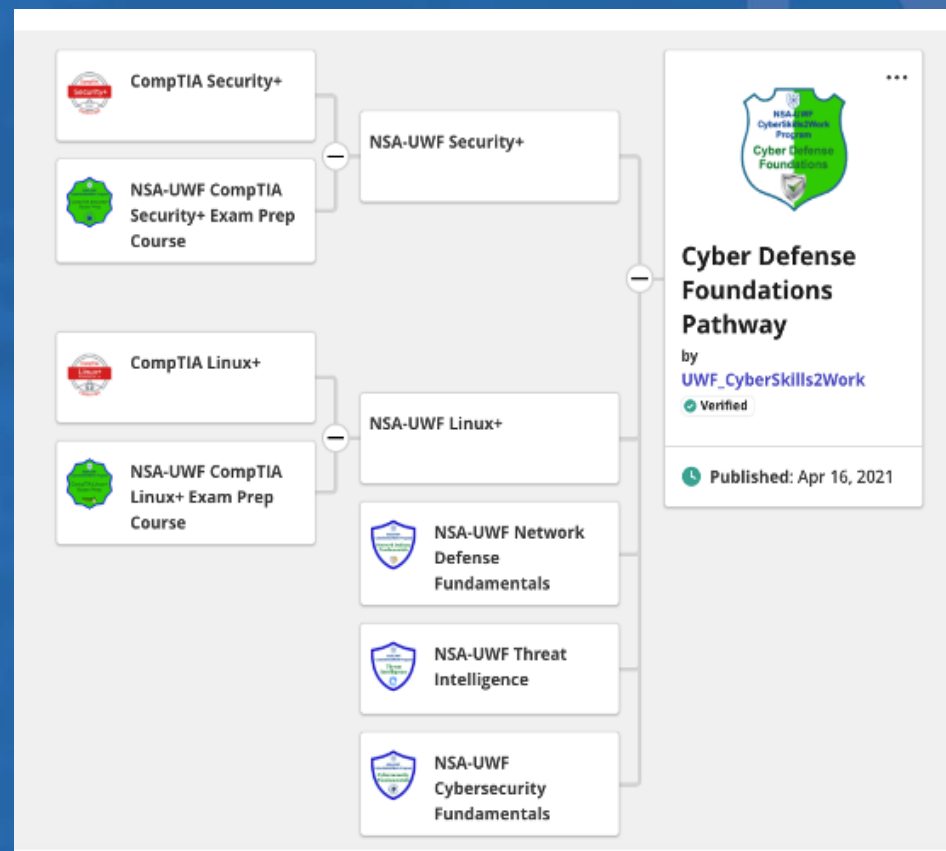


# CENTER FOR **CYBERSECURITY**

AT THE UNIVERSITY OF WEST FLORIDA

## Digital Pathway

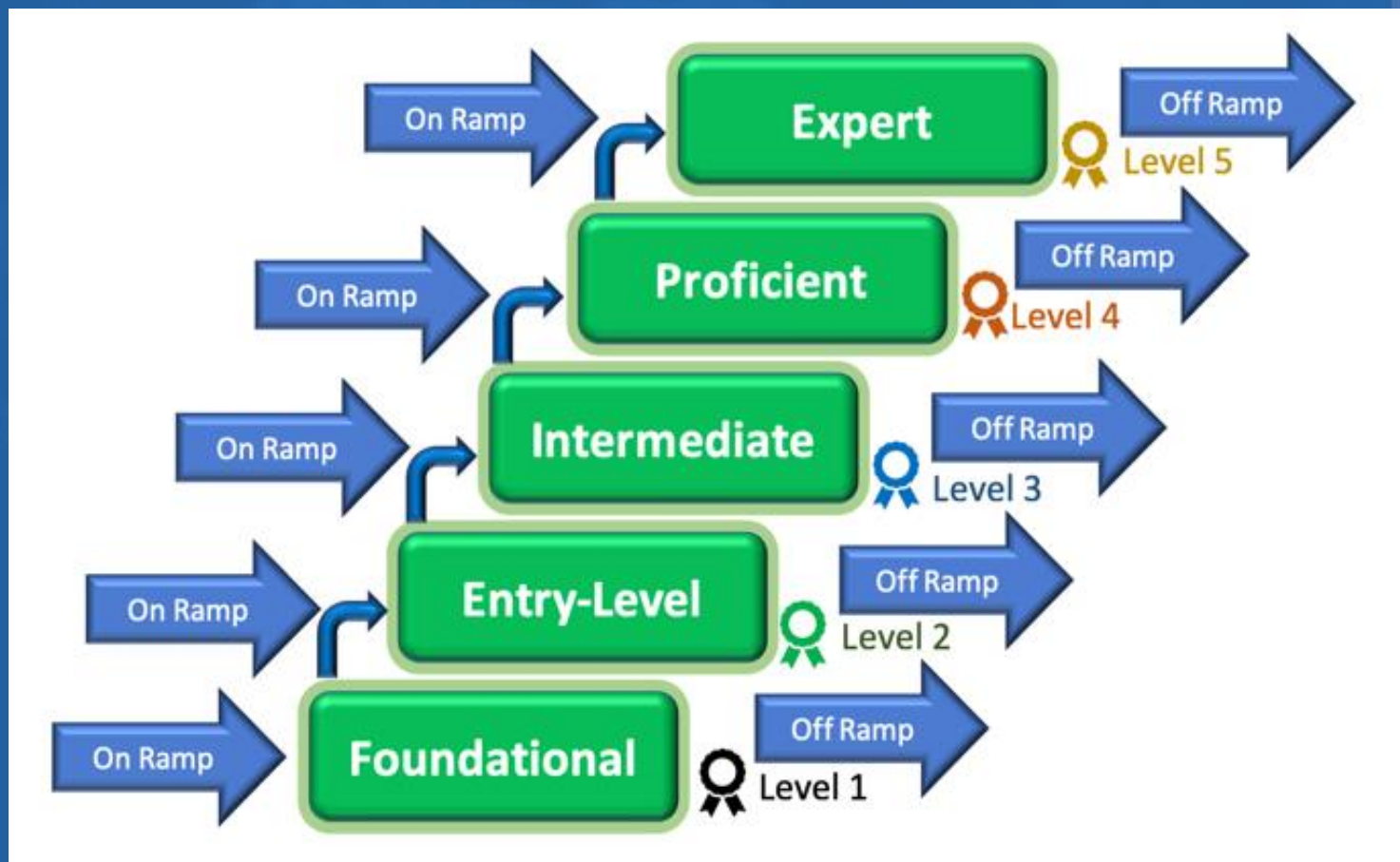
Digital badges are accumulated by the learner into a digital backpack or wallet. The sequence of steps taken to accumulate these badges toward the completion of a certain credential is called a pathway





## Stackable Credentials

- Recruitment
- Diagnostic Assessment
- Career Counseling
- Mentoring
- Monitoring and Intervention



- Post Assessment
- Badging
- Competency Certification
- Professional Development
- Internships and Coops
- Job Placement





CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Competency Assessment

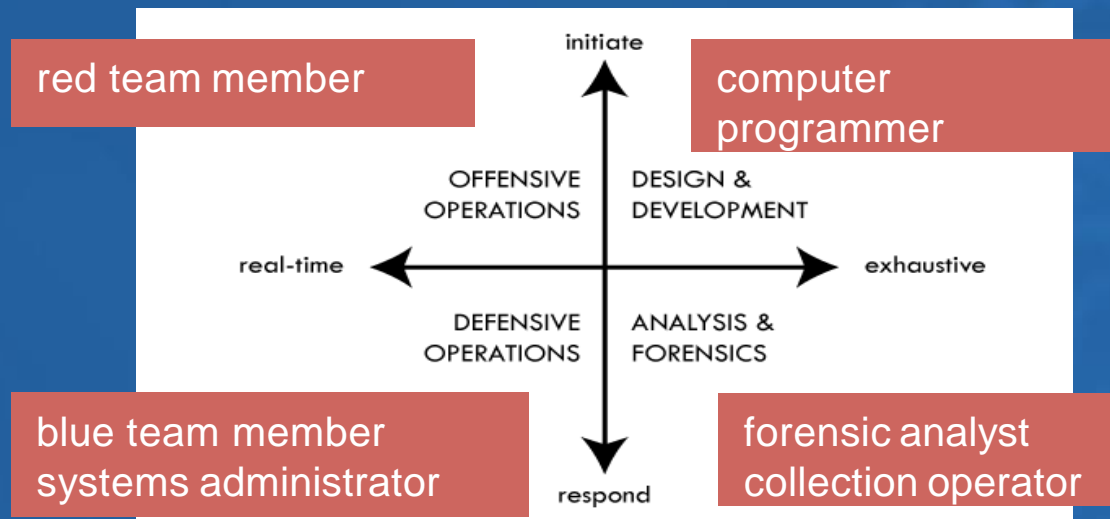
- Start with a work role corresponding to the chosen competency
- We list tasks that are needed for that work role and to achieve the chosen competency, followed by sets of knowledge and skills needed to perform relevant tasks
- Scenarios are designed to guide students through a set of tasks and to impart the knowledge and skills required to perform those tasks
- Creation of assessment rubrics

Ghosh & Francia, *Journal of Cybersecurity and Privacy*. 2021, 1, pp. 539–552. September 2021



## Aptitude Assessment

- Cybersecurity work roles require different knowledge, skills, and competencies
  - A one-size-fits-all solution may leave some people out
- Leverage the Cyber Aptitude and Talent Assessment (CATA) model
  - Determine cognitive skills/abilities associated with NCWF work roles
  - Utilize tests to identify cognitive skills and recommend associated work roles



Quadrants = major tasks with characteristics described on axes

“Defense” → response to problem in real-time

“Development” → initiation of exhaustive solution



CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

## Issues To Address

- What level of granularity should the learning modules address?
- What is the most optimal length of these training courses/modules to make learning most effective while not losing students
- How to develop a dynamic and artificial intelligence-based system that provides an effective learning path that is in line with the learner's abilities and interest
- Can work role pathways be replaced with competency pathways in order to enable a more holistic training objective





CENTER FOR **CYBERSECURITY**  
AT THE UNIVERSITY OF WEST FLORIDA

**Thank you!**

**Questions?**

# NICE | Conference and Expo 2022

JUNE 6 - 8, 2022 | WESTIN PEACHTREE PLAZA | ATLANTA, GA

## DEMYSTIFYING CYBERSECURITY

Integrated Approaches to  
Developing Career Pathways

**FIU** | FLORIDA  
INTERNATIONAL  
UNIVERSITY

 **NEW  
AMERICA**