CAE in Cybersecurity Symposium

November 8th-9th, 2018
Hyatt Regency
400 SE 2nd Ave
Miami, FL, 33131

Welcome to the annual CAE in Cybersecurity Symposium!

Message from the Community

Tony Coulson
Director, Cybersecurity Center
California State University, San Bernardino

Cybersecurity educators are facing demands from government and industry to produce more graduates to fill the current and future workforce needs. Each year the Centers of Academic Excellence (CAE) in Cybersecurity Community assembles to discuss the workforce problem as well as to discuss issues unique to our community including faculty shortages, bridging the skills gap, and career pathways.

Five years ago, the CAE in Cybersecurity met for the first time in Gaithersburg, MD to discuss our progress as CAE designated institutions. Since then, the CAE in Cybersecurity Symposium has traveled to Columbia, MD, San Diego, CA, Kansas City, KS, Dayton, OH , and now Miami, FL to discuss changes in the CAE program, receive updates from the community, network with other members, and discuss pressing issues within the community.

To help drive conversation among the community, today's symposium will include fastpitch talks and presentations meant to highlight important contributions from the CAE in Cybersecurity Community as well as important updates from the NIETP Program Office.

Navigate the Symposium Booklet

Symposium Schedule, Thursday

Thursday, November 8th, 2018

8:00am	🟣	Welcome and Logistics
8:10am	🟣	CAE in Cybersecurity Community Updates, Tony Coulson
8:20am	🟣	NIETP Program Office Updates, Lynne Clark
9:20am	🟣	Other Program Updates, Dan Stein (DHS), Rodney Petersen (NICE), Susanne Wetzel (NSF), Carolyn Renick (DOL)
10:10am	🟣	Morning Break
10:20am	🟣	CAE Virtual Career Fair, Tony Coulson
10:30am	🟣	CAE Spotlight, Wayne Pauli
11:00am	BR	Research Presentations 🟣 🟢 🟠 🔵
12:30pm	🟣	Working Lunch (Resources for the Community)
1:30pm	BR	CRRC Breakout Sessions 🟣 🟢 🟠 🔵
2:50pm	🟣	Afternoon Break
3:00pm	🟣	Fastpitch Session
4:10pm	🟣	Discussion
5:00pm	🟣	Evening Break
5:10pm	BR	National Cybersecurity Curriculum Project
7:00pm		Dismissal

Use these icons to navigate the CAE in Cybersecurity Symposium.

🔴	Fastpitch Icon, Red	🔵	Orchid B, Sky Blue
🟡	Presentation Icon, Yellow	🟠	Orchid C , Orange
🟣	Ballroom Icon, Purple	🟢	Orchid D, Green

Presentation Agenda

Time	Room	Presentation Title
11:00am	🖐	Infusing Risk Management into Cybersecurity Education
11:00am	📂	Mapping Hands-on Cybersecurity Labs to CAE Knowledge Units and the NICE Framework
11:00am	🔍	Cyber Up! Digital Forensics and Incident Response (DFIR) project at Coastline College
11:00am	🐴	Teaching Cybersecurity Across the Disciplines
11:30am	🖐	Adapting Security Through Community Engagement
11:30am	📂	Lessons Learned in Cybersecurity Outreach Pre-Engineering Workshops at Polytechnic University of Puerto Rico
11:30am	🔍	A Comparison of Online Course Designs for Cybersecurity Education
11:30am	🐴	The ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education: The CSEC2017 Cybersecurity Curricular Guidelines
12:00pm	🖐	The Centrality of Adversarial Thinking for Cybersecurity Education
12:00pm	📂	Introducing Cyber Labs into Engineering Courses and Developing Curriculum Leading to a Specialization
12:00pm	🔍	Reach To Teach
12:00pm	🐴	Hands-on Learning Experiences for Cyber Threat Hunting Education

CRRC Breakout Sessions

> You have the opportunity to meet with your Regional CRRC to learn more about activities going on in your region. Below you will find the CRRC meeting schedule with meeting times and rooms.

CAE Regional Resource Center Meeting Rooms

Time	Ballroom 🐴	Orchid B 🖐	Orchid C 📂	Orchid D 🔍
1:30pm	National Capital Region	South Western Region	Central Eastern Region	North Central Region
2::10pm	North Eastern Region and South Eastern Region	South Central Region	Northwest Region	Mid-Western Region

Fastpitch Agenda

3:00pm	🐴	CLARK: A Living Cybersecurity Digital Library
3:10pm	🐴	An Exploratory Analysis on Cybersecurity Ecosystem using NICE Framework
3:20pm	🐴	Understanding Workforce Attributes by Exploring Empirical Career Pathways of Cybersecurity Industry Professionals
3:30pm	🐴	The University of Arizona Cyber Virtual Learning Environment (VLE)
3:40pm	🐴	An Innovative and Successful Model to Promote Cybersecurity Education
3:50pm	🐴	Bridging the Gap: Developing Innovative Minds Early On for Cybersecurity
4:00pm	🐴	PASS using Blockchain Technology and its Risks and Challenges
4:10pm	🐴	Introducing the CSUSB Society of Women in Cybersecurity (SWiCS)

Symposium Schedule, Friday

Friday, November 9th, 2018

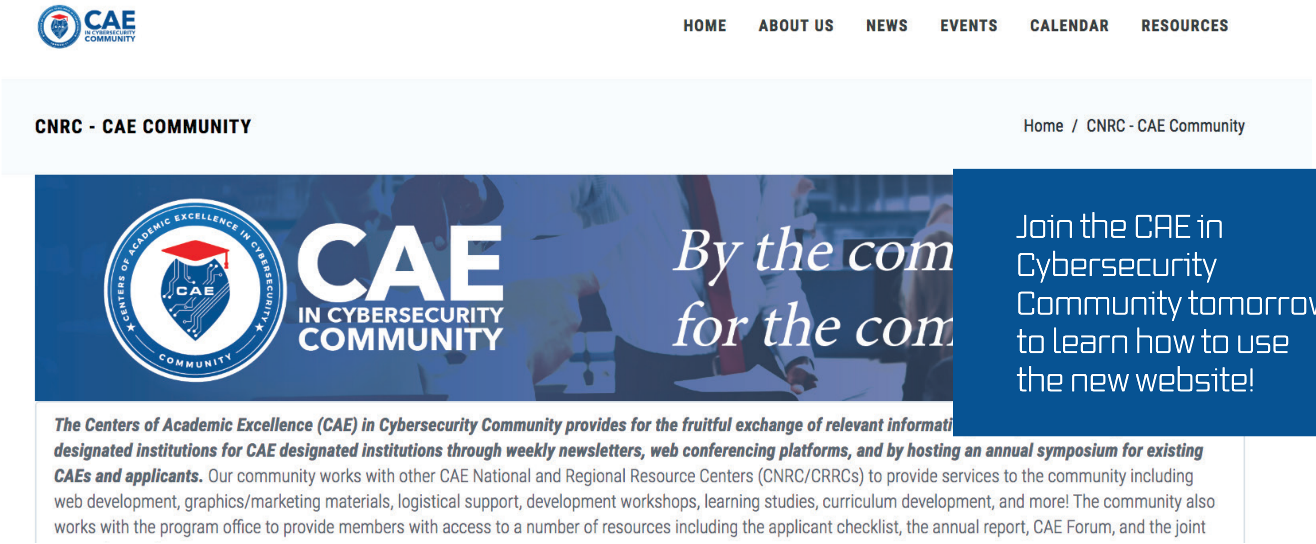
	Orchid B ✋	Orchid C 🧩
8:00am	NICE Challenge Project	CAE in Cybersecurity Community Website Overview
9:00am	CAE-CDE 2019 Knowledge Units	
10:00am	DoD Cybersecurity Scholarship and CAE Cybersecurity Grant Boot-Camp	Southeast CAE Community Collaborative Projects: Working Session
11:00am		
12:00pm	Lunch Break (On Your Own)	Lunch Break (On Your Own)
1:00-4:00pm	Mentor/Peer Reviewer Training	

Use these icons to navigate the CAE in Cybersecurity Symposium.

🔥 Fastpitch Icon, Red	✋ Orchid B, Sky Blue
🖥 Presentation Icon, Yellow	🧩 Orchid C , Orange
🐴 Ballroom Icon, Purple	👁 Orchid D, Green

CAE in Cybersecurity Community Updates

This year the CAE in Cybersecurity Community launched the redesigned community website and held a series of user trainings during Summer 2018. The new website comes with many of the features the community has enjoyed in the past including news, events, and faculty opportunity postings. In addition, the community website is home to the CAE Forum as well as the CNRC and CRRC landing pages.


CAE IN CYBERSECURITY COMMUNITY
HOME
ABOUT US
NEWS
EVENTS
CALENDAR
RESOURCES
Home / CNRC - CAE Community
CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY COMMUNITY
CAE
CAE IN CYBERSECURITY COMMUNITY
By the com
for the com

CNRC - CAE COMMUNITY

The Centers of Academic Excellence (CAE) in Cybersecurity Community provides for the fruitful exchange of relevant informati designated institutions for CAE designated institutions through weekly newsletters, web conferencing platforms, and by hosting an annual symposium for existing CAEs and applicants. Our community works with other CAE National and Regional Resource Centers (CNRC/CRRCs) to provide services to the community including web development, graphics/marketing materials, logistical support, development workshops, learning studies, curriculum development, and more! The community also works with the program office to provide members with access to a number of resources including the applicant checklist, the annual report, CAE Forum, and the joint

Join the CAE in Cybersecurity Community tomorrow to learn how to use the new website!

Initiatives From Community Members

CAE VIRTUAL CAREER FAIR SPONSORED BY CWW AND NSF

On October 5th 2018, the second CAE Virtual Career Fair, sponsored by CyberWatch West and the National Science Foundation, took place between 9:00am-1:00pm PT. This year the CAE Virutal Career Fair was not only free for students/alumni of CAE in Cybersecurity deisgnated institutions, but also free for CAE designated institutions seeking faculty. A total of 17 employers and 8 CAE designated institutions participated in the career fair. A total of 1,198 students/alumni participated in the virtual career fair.

CAE IN CYBERSECURITY SPOTLIGHT: DAKOTA STATE UNIVERSITY

Each year, the community highlights one CAE designated institution that exceeded expectations providing resources, programs, or workshops to the community. This year, the community is recognizing Dakota State University (DSU). DSU has long been a leader in the community acting as a CAE Regional Resource Center for the North Central Region. However, DSU also provided all CAE designated institutions with the opportunity to participate in faculty professional development workshops.

Speaker Biographies

DEBASIS BHATTACHARY

Dr. Debasis Bhattacharya is currently an Assistant Professor at the University of Hawaii Maui College, and program coordinator for the Applied Business and Information Technology (ABIT) baccalaureate program. He has been working in the software industry for 30 years, having worked for large corporations such as Oracle and Microsoft for 15 years. A resident of Hawaii since 2002, he has been actively researching the information security needs of small businesses since 2008. He holds degrees from MIT, Columbia University, University of Phoenix and NW California University School of Law. Research interests include computer science education, cybersecurity, crypto currencies and deep learning.

DIANA BURLEY

Diana L. Burley, Ph.D. is Executive Director and Chair of the Institute for I3P, Associate Dean for Research and External Relations and Professor of Human & Organizational Learning at George Washington University. She has publications on cybersecurity, information sharing, and IT-enabled change; testified before Congress; conducted international cybersecurity awareness training on behalf of the US State Department; served on a cybersecurity advisory committee. She participates in global initiatives to develop cybersecurity workforce, and critical infrastructure protection.

Z CHEN

Dr. Z Chen is a professor and the Chair of the Department of Mathematics and Computer Sciences in Mercy College. His research interests are on student centered learning environment, data exploration and data security. A senior member in the IEEE and ACM, he has published 40 peer reviewed papers. He got PhD/MS from the University of Pittsburgh and MA/BA from Shanghai Jiao Tong University. Dr. Chen has worked for IBM Research over six years and Mercy College over 15 years.

SAM CHUNG

Sam Chung, Ph.D., is a Professor and the Information Security Program Director of Technology Institute at City University of Seattle (CityU). He earned his Ph.D. in Computer Science from the University of South Florida (USF) in Tampa, Florida and has two MS degrees in Computer Science from George Washington University (GWU) and the Korean Advanced Institute of Science and Technology (KAIST). Dr. Chung worked at Southern Illinois University (SIU) in Carbondale, IL and the University of Washington (UW), Tacoma.

SIMON CLEVELAND

Simon Cleveland, Ph.D., is an Associate Dean and the Executive Director of Technology Institute at City University of Seattle (CityU).

DEANNE CRANFORD-WESLEY

Dr. Deanne Cranford-Wesley is currently Department Chair Davis iTEC/Cyber Security Center at Forsyth Technical Community College. She also leads efforts for the Center of Academic Excellence Regional Resource Center where one of her initiatives focuses on the K-12 cybersecurity pipeline. She has design curriculum for K-12 programs as a consultant and is a member of the Chamber of Commerce Workforce Executive Board. Dr. Cranford -Wesley is a cybersecurity professional and has appeared as a subject matter expert on Fox8 and Time Warner News discussing innovations in cyber security and cyber-attacks. She also teaches information security, computer forensics and networking courses in the Business Information Technology Department with the Davis ITEC Cyber Security Center.

Speaker Biographies

RAM DANTU

Dr. Ram Dantu has worked for Cisco, Nortel, Alcatel, and Fujitsu and was responsible for advanced technology products. He is currently a Professor in the Department of Computer Science and Engineering, University of North Texas (UNT). He was also the founding director of the Network Security Laboratory, and the Center for Information and Computer Security at UNT. He has received several NSF awards in collaboration (lead PI) with Columbia University, Purdue University, University of California at Davis, Texas A&M University, and Massachusetts Institute of Technology.

JASON DENNO

Jason Denno is the Director of Cyber Operations at the University of Arizona. Mr. Denno's experience includes designing, developing, deploying, and operating intelligence and cyber systems across the globe. His experience includes senior level positions in defense contracting companies, the Director of the Battle Command Battle Lab for Fort Huachuca, and former US Army Infantry and Signals Intelligence officer. Mr. Denno possesses a Master's of Science in Cyber Operations, MBA, BA in Political Science, and multiple GIAC certifications in Cyber Operations.

EMAN EL-SHEIKH

Dr. Eman El-Sheikh is Director of the Center for Cybersecurity and Professor of Computer Science at the University of West Florida. Eman has expertise in cybersecurity education, research and workforce development and received awards related to cybersecurity education and diversity. She leads UWF's efforts as the NSA/DHS National Center of Academic Excellence Regional Resource Center for the Southeast U.S. She teaches and conducts research in Artificial Intelligence, Machine Learning and Cybersecurity.

WALEED FARAG

Waleed Farag is a professor of Computer Science at IUP. He received his PhD in CS in 2002. Dr. Farag's research interests include cybersecurity education, e-learning, and multimedia security. Dr. Farag has an established record securing funds to support his research. He is the PI of several federally funded grants. He has numerous publications in his areas of interest. Furthermore, he is serving in the TPC and as a reviewer for several international journals/ conferences including the ACM TOCE, FIE, and InfoComm.

BARBARA FOX

Barbara Fox is a cybersecurity educator and research scientist for the Georgia Tech Research Institute (GTRI). Ms. Fox specializes in professional education encompassing cybersecurity, insider threat, and cyber risk management. Her rich experience combines technology, educational principles, and over 25 years of classroom experience. She holds credentials including: CISSP, ISSO, M.S. in Applied Computer Science/Information Assurance, Ed.S. in Educational Leadership, and serving on an Information Security Fundamentals Standards Panel for creating competency-based cybersecurity curriculum on a national scope.

SETH HAMMAN

Seth Hamman is the Director of the Center for the Advancement of Cybersecurity at Cedarville University and an Associate Professor of Computer Science. He received a B.A. in religion from Duke University, an M.S. in computer science from Yale University, and a Ph.D. in computer science from the Air Force Institute of Technology. He is passionate about developing tomorrow's cyber leaders in the classroom and contributing to the growth and development of cybersecurity education in the academy.

ESSIA HAMOUDA

Dr. Essia Hamouda is currently an Assistant Professor at the JHBC of Business, University of California San Bernardino (CSUSB). Her research interests are on the areas of computer networks and performance evaluation, data analytics and data security. She has several refereed publications and working papers. She is the founder and advisor of the Society of Women in Cyber Security at CSUSB. She earned her Ph. D in computer Science from UC Riverside and her BS and MS in Engineering from the Ohio State University and the University of Florida respectively.

Speaker Biographies

SHELLY HELLER

Shelly Keller is the Professor of computer science at The George Washington University and the interim chair of the department. The author of numerous books and papers in computers in education, she is the co-recipient and co-principal investigator of eight significant National Science Foundation sponsored grants. Dr. Heller is currently the editor of Computers & Education: An International Journal, a leading peer reviewed journal that regularly publishes issues and papers related to the computer and educational communities.

LANCE HOFFMAN

Lance Hoffman is a member of the Cyber Security Hall of Fame, Professor of Computer Science, Co-Director of the Cyber Security and Privacy Research Institute at The George Washington University, and the author of articles and books on computer security and privacy. Professor Hoffman developed the first course on computer security at UC Berkeley after serving on the Advisory Committee to the California Assembly Committee on Statewide Information Policy. Dr. Hoffman institutionalized the ACM Conference on Computers, Freedom, and Privacy.

DAN KIM

Dan J. Kim is professor at University of North Texas. His research interests are in multidisciplinary areas including information security and privacy, information-assurance and trust in electronic commerce. His research work has been published in more than 150 papers in refereed journals and conference proceedings including ISR, JMIS, IJEC, DSS, etc. His publications have been cited more than 7,000 times over the last five years. He serves or served as a guest, senior, and associate editor for several top journals including MISQ, ISM, and ISF.

SIDD KAZA

Dr. Sidd Kaza is the Chairperson of the Computer and Information Sciences department at Towson University. He received his Ph.D. degree in Management Information Systems from the University of Arizona. His interests lie in cybersecurity education, data mining, and application development and he is a principal investigator on several cybersecurity education projects (http://towson.edu/cyber4all). He is also on the ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education that produced the four-year cybersecurity curricular guidelines (http://cybered.acm.org). Dr. Kaza's work has been published in top-tier journals and conferences and has been funded by the National Science Foundation, National Security Agency, Department of Defense, Intel, and the Maryland Higher Education Commission.

YAIR LEVY

Dr. Yair Levy is a Professor of IS and Cybersecurity, College of Engineering and Computing, Nova Southeastern U. He is an Aerospace Engineer by training and during the mid to late 1990s, he assisted NASA to develop e-learning systems. He holds an MBA with MIS concentration and a Ph.D. in Information Systems (His CV is available via: http://cec.nova.edu/~levyy/). His research areas: Social Engineering, Cybersecurity KSAs, User-Authentication, & Privacy. He heads the Levy CyLab (http://CyLab.nova.edu/) that conducts innovative research related to his research areas.

HERBERT MATTORD

Herbert J. Mattord, Ph.D., CISM, CISSP, and CDP, is Associate Professor of Information Security and Assurance, Department of Information Systems, Coles College of Business, Associate Director, Center for Information Security Education, and Director of Education, Institute for Cybersecurity Workforce Development at Kennesaw State University. He has published articles and textbooks, with his colleague Dr. Whitman, on information security and cybersecurity that have reached students worldwide. He currently teaches courses in cybersecurity and information systems.

Speaker Biographies

KALYAN MONDAL

Kalyan Mondal earned his PhD in Electrical Engineering from University of California at Santa Barbara. He has 25 years of R&D experience in the communication industry. He teaches courses in Digital Signal Processing, VLSI Design, Integrated Circuit Devices, Microcontroller System Design, Power Systems, and Object-oriented Programming. He is the PI of the NSA CNAP Project No. H98230-17-1-0321. As the Founding Director of FDU Center for Cybersecurity and Information Assurance, he oversees various activities. He was involved in getting FDU designated as CAE/IAE & CAE-CDE.

WAYNE PAULI

Wayne is a Professor in the Beacom College of Computer and Cyber Sciences at Dakota State University. A South Dakota native, Dr. Pauli holds a PhD in Organization and Management from Capella University of Minneapolis, MN, a master's in Information Systems from Dakota State University and a bachelor's degree in Business Administration from Northern State University in Aberdeen, SD.

CHRIS SIMPSON

Chris Simpson is the Director of the National University Center for Cybersecurity and is the Academic Program Director for National University Bachelor of Science and Master of Science Cybersecurity programs. He has developed innovative curriculum and labs in ethical hacking, pentesting, and incident response. Chris retired from the U.S. Navy in October 2009 after 27 years of service. He has extensive experience as an Information Assurance Manager, including a tour as the Information Assurance Manager (IAM) for the Commander, Combined Forces Command Afghanistan.

MARK THOMPSON

Dr. Thompson has been teaching in the computer science field with a special interest in cyber security. He is affiliated with the Center for Information and Computer Security (CICS) at UNT. Before joining the faculty at UNT, he taught at Northwestern State University of Louisiana. He has experience at Bell-Northern Research, the research and development arm of Nortel Networks, on all phases of development as a senior programmer and systems architect on large, real-time telecommunications systems, focusing primarily on military and other security-based technologies.

COSTIS TOREGAS

Costis Toregas is the Director of the Cyber Security Policy and Research Institute. He has taught graduate courses in Public Policy/ Public Administration regarding the management challenges (including cyber security, privacy and transparency) of public managers. He is also a senior advisor of the National CyberWatch Center, a network of over 200 universities and community colleges dedicated to improving the quality and quantity of cyber security professionals. He is the Finance Director of the National Cyber League, and provides collegiate students development with their cybersecurity skills.

LUIS M. VICENTE

Luis M Vicente received Ph.D. in Electrical and Computer Engineering at the University of Missouri-Columbia (2009). From 1990 to 2003 Dr. Vicente worked at the Aerospace Division, SENER Group, Spain. Also, at Voyetra Inc., New York, and at SIEMENS, Madrid. From 2003 to 2009 he became Assistant Professor at the Polytechnic University of Puerto Rico. In 2012 he was promoted to Associate Director. His research interests include signal processing and Cybersecurity. He is finishing a Graduate Certificate in Digital Forensics.

TOBI WEST

Tobi is Department Chair of CIS/CST/DGA, teaching cybersecurity and networking courses. Tobi has a passion for cybersecurity education. She focuses on developing career pathways for students to achieve their goals as a cybersecurity professional. In addition to teaching, she coordinates CyberTech Girls events for middle and high school girls to develop their interest in cybersecurity and technology. She coordinates the Cybersecurity Apprenticeship Program for Coastline students to develop their cyber skills for apprenticeship roles in cybersecurity.

Presentation Abstracts

A COMPARISON OF ONLINE COURSE DESIGNS FOR CYBERSECURITY EDUCATION
SAM CHUNG AND SIMON CLEVELAND, CITY UNIVERSITY OF SEATTLE

The purpose of this presentation is to compare existing online course designs and propose new pedagogical approaches to improve cybersecurity education. For this purpose, we chose three institutes that deliver online courses - one in WA and two in IL. The institute in WA delivers online MS in Cybersecurity (CSEC). The institutes in IL provides both online and on-campus courses for BS in Information Technology (IT) and Master of Business Administration (MBA). Campus visits and interviews were conducted for data collection purposes. The three institutes use different Learning Management Systems (LMS), yet all of them have distance learnings to support and maintain online course development initiatives.

The following criteria were compared during the study: ownership of the course contents in a LMS, openness of the courses to future students, involvement of instructional technology experts, support from media production experts, use of learning analytics for retention and prediction, use of active learning methods for student engagement such as Just-in-Time Teaching (JiTT) and Flipped Classroom (FC), and diverse learning models such as social learning, competency-based learning, and project-based learning. Data revealed that one of the institutes has significant growth in enrollment with highly qualified students. Recommendations for future studies are provided.

ADAPTING SECURITY THROUGH COMMUNITY ENGAGEMENT
MARK THOMPSON AND RAM DANTU, UNIVERSITY OF NORTH TEXAS

Based on the growing number of security and data breaches that are occurring on a daily basis, as well as the impact they are having on our lives, security is no longer working, so as a community of users, we must take charge and reestablish control of our own security and privacy. Unfortunately, due to these frequent occurrences, people now bear a mindset that security is too complex and seem resigned to the fact that security breaches are just a part of their daily lives as they know it. For the most part, they are correct! If security professionals, who have been trained and certified to work on these systems, cannot fully secure them, then how can an average person with little or no computer experience be expected to do so? Rather than attempting to change the behavior of potential attackers, this discussion takes the approach that everyone is responsible for security and what we must do to develop an environment where everyone's own personal background and experience can be used in sharing the responsibility for security, just as a Neighborhood Watch program does for a local community.

CYBER UP! DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) PROJECT AT COASTLINE COMMUNITY COLLEGE
TOBI WEST, COASTLINE COLLEGE

To increase national security for the U.S. and meet its workforce needs, cybersecurity education must develop new knowledge and skills. To address this need, the Cyber Up! Digital Forensics and Incident Response (DFIR) project at Coastline Community College in California will research, create, adapt, adopt, and implement a suite of course content that supports a Certificate of Achievement and an Associate of Science degree. The three-year project will run 10/2018-09/2021 (NSF ATE Award #1800999).

The project will focus on the development of curricula that will teach students and professionals the cybersecurity knowledge and skills of digital forensics and incident response, which need to be deployed in real-time and are dynamic to changing situations during, and in response to, cyberattacks. Through the DFIR program, the project intends to create adoptable educational resources; form academic, government, and industry partnerships; and prepare qualified cybersecurity technicians and professionals for entry into, or advancement within, the U.S. workforce.

The DFIR distance education modalities will be designed for a national reach and assist in preparing students for successful employment. The project will also develop virtual labs and faculty resources. Because of the adoptable, modular content, other institutions can benefit through adoption into their programs, creating pathways to greater skills and knowledge for students and professionals. Increasing skills and knowledge in diverse and underrepresented populations in cybersecurity will help to assure increased participation of women, minorities, and special populations in science, technology, engineering, and mathematics (STEM) education.

Presentation Abstracts

HANDS-ON LEARNING EXPERIENCES FOR CYBER THREAT HUNTING EDUCATION
DEANNE CRANFORD-WESLEY, JINPENG WEI, BEI-TSENG CHU AND JAMES BROWN
FORSYTH TECHNICAL COMMUNITY COLLEGE

Cyber threat hunting has emerged as a critical part of cybersecurity practice. However, there is a severe shortage of cybersecurity professionals with advanced analysis skills for cyber threat hunting. Sponsored by NSA, the University of North Carolina at Charlotte (UNC Charlotte) and Forsyth Technical Community College (Forsyth Tech) have been developing hands-on teaching materials for cyber threat hunting that will expand our current strong educational programs in cybersecurity. UNC Charlotte is designated as a Center of Academic Excellence in Information Assurance Education-Cyber Defense, and a Center of Academic Excellence in Information Assurance Research by NSA and DHS, and has an NSF funded IUCRC in Configuration Analytics and Automation.

Since 2001, UNC Charlotte has run the Carolina Cyber Defender Scholarship Program, one of the largest such programs in the United States, with funding from NSF and NSA. Forsyth Tech was awarded the Center of Academic Excellence (CAE 2Y) Cyber Defense designation in June 2015. In this effort, Forsyth Technical Community College has established the Davis ITEC Cyber Center. We are developing freely-available, hands-on teaching materials for cyber threat hunting suitable for use in two-year community college curriculum, 4-year universities curriculum, as well as for collegiate threat hunting competitions. Our project fits nicely into the NICE 2018 theme of "Innovations in Cybersecurity Education, Training, and Workforce Development," with a focus on "Accelerate Learning and Skills Development" defined by the NICE Strategic Plan.

INFUSING RISK MANAGEMENT INTO CYBERSECURITY EDUCATION
BARBARA FOX, GEORGIA INSTITUTE OF TECHNOLOGY

Cybersecurity education often feels fragmented because of its broad spectrum which includes theoretical principles, cyber hygiene, board-level decision-making, and highly specialized technical skills. Workforce and academic training will benefit from cybersecurity instructors who position multi-faceted topics through the single lens of risk management. Effective programs do not seek to eliminate cyber risk, but to manage it appropriately. Helping students approach cybersecurity challenges from a risk management perspective will provide direction and confidence instead of fear and information overload. The National Centers of Academic Excellence (CAE) program seeks to reduce vulnerability in our national information infrastructure by promoting the development of professionals with appropriate expertise. Technical cyber professionals need help in communicating more effectively with decision makers. Non-cyber professionals need greater awareness of the importance of applying cybersecurity principles to non-IT-based roles. Introducing cybersecurity from a risk management perspective accomplishes both of these needs.

INTRODUCING CYBER LABS INTO ENGINEERING COURSES AND DEVELOPING CURRICULUM LEADING TO A SPECIALIZATION
KALYAN MONDAL, FAIRLEIGH DICKINSON UNIVERSITY

This presentation first discusses the introduction of cyber labs into existing graduate embedded systems and undergraduate microcontroller system design courses. A Raspberry-PI based platform was used to develop a set of six labs for the graduate embedded systems course required to be taken by all MS in Electrical Engineering and MS in Computer Engineering students. Additionally, Python as the programming language, Linux as the operating system, and concepts of security are introduced in the graduate course.

A mapping of existing courses in the engineering programs showed that an Embedded Systems specialization is feasible by adding a few topics into existing graduate courses and developing a new course module on wireless sensor networks. On the other hand, the undergraduate course needs a more simplistic platform where pin level programming is feasible. As such, Micropython based Pyboard was chosen as the platform. The undergraduate microcontroller system design course is taken by electrical engineering, electrical engineering technology, mechanical engineering and mechanical engineering technology majors. Changes to the existing C based undergraduate course requires introducing Python as another programming language in the undergraduate engineering program.

A proposed sequence of such undergraduate curriculum changes will allow introducing cyber and data science concepts into existing undergraduate engineering programs.

Presentation Abstracts

MAPPING HANDS ON CYBERSECURITY LABS TO CAE KNOWLEDGE UNITS AND THE NICE FRAMEWORK
CHRIS SIMPSON, NATIONAL UNIVERSITY

Hands on labs are a critical component of any cybersecurity program. Schools can develop labs internally, outsource labs to a provider, or utilize free grant resourced labs, or use free and open source labs. Many externally provided labs aren't mapped to CAE Knowledge Units or the NICE Framework, especially the open source labs. This makes it challenging for schools to identify the right labs for their program and requires extensive efforts to map the labs to meet these different requirements. There is duplicated effort as different institutions map the same labs and in many cases will map them to the same knowledge units and NICE KSA's. This presentation will discuss National University's efforts to map labs from external providers and open source labs to knowledge units and to the NICE Framework. A proof of concept portal that will allow schools to share their mappings will be demonstrated.

REACH TO TEACH
SHELLY HELLER, LANCE HOFFMAN, AND COSTIS TOREGAS, THE GEORGE WASHINGTON UNIVERSITY

It is a well published concern that in order for the United States to maintain and expand its capabilities in the world of cybersecurity. Currently there is a capacity issue: students cannot readily be added to the education system, especially at the community college level, because trained faculty are scarce. The weak link in the cybersecurity workforce supply chain is often finding faculty who can be effective and provide the proper encouragement to students to join the cyber workforce. Our answer: Tapping into cybersecurity experts as adjunct faculty. Cybersecurity experts in the workforce have the potential to fill the need for part-time cybersecurity faculty at the community college level. By tapping into the pool of working cybersecurity experts and retired individuals from government positions whose background fits the typical qualifications listed above, a viable long term strategy can be developed. Currently the Reach To Teach project is exploring these possibilities through a research effort and a pilot "REACH TO Teach" onlinecourse (See Figure 1) funded by the U. S. Defense Department .

Introduction to Community Colleges, Ethics and general structure of a course
The typical Community College student, Faculty codes, Crafting goals and objectives
Teaching concepts – moving from concrete to abstract
Teaching concepts – using group work in your class
Teaching concepts – using case studies in your class
Teaching concepts – using discussions during a class
Figure 1: Cybersecurity Teaching Corps Course Content

TEACHING CYBERSECURITY ACROSS THE DISCIPLINES
DEBASIS BHATTACHARYA, UNIVERSITY OF HAWAII - WEST OAHU

Cybersecurity has become a prevalent topic in many colleges, but how it should fit into the overall educational process is still not fully understood. A cybersecurity project at the University of Hawaii Maui College (UHMC), funded by the NSF SFS program, spans multiple disciplines and targets women and minorities. The goal of this project is to ensure that a broad audience of faculty, students and practitioners get trained in the fundamentals of cybersecurity.

THE CENTRALITY OF ADVERSARIAL THINKING FOR CYBERSECURITY EDUCATION
SETH HAMMAN, CEDARVILLE UNIVERSITY

The field of cybersecurity is predicated on the existence of humans who deliberately attack computer systems. In other words, without cyber adversaries, there is no cybersecurity. Therefore, adversarial thinking, which is the study of cyber adversaries, is central to a cybersecurity education. However, the learning outcomes associated with adversarial thinking are not well-defined, making it difficult for cybersecurity educators to confidently instruct students in this crucial area. This presentation aims to advance cybersecurity education by rigorously defining what it means to "think like a hacker." The proposed definition highlights the primary learning outcomes associated with adversarial thinking, and it will help educators see more clearly the big picture of a cybersecurity education. This presentation will also promote the CLARK curriculum repository where cybersecurity educators can find materials to help develop the adversarial thinking abilities of their students.

Presenation Abstracts

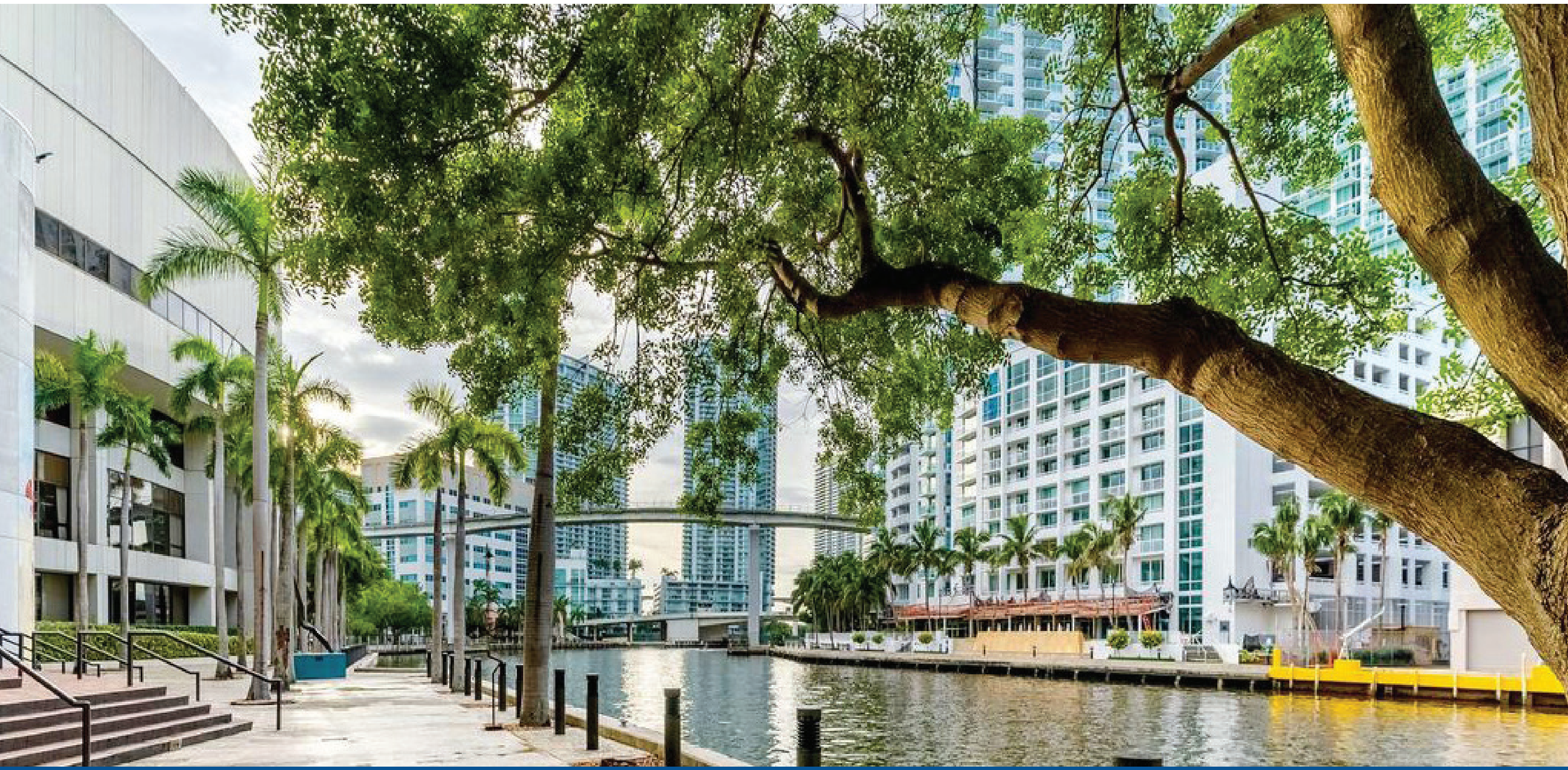
THE ACM/IEEE/AIS/IFIP JOINT TASK FORCE ON CYBERSECURITY EDUCATION: THE CSEC2017 CYBERSECURITY CURRICULAR GUIDELINES

YAIR LEVY, DIANA BURLEY AND HERBERT MATTORD, NOVA SOUTHEASTERN UNIVERSITY

The Joint Task Force (JTF) on Cybersecurity Education (http://cybered.acm.org/) was launched in September, 2015 as a collaboration between major international computing societies: ACM, IEEE Computer Society, AIS's Special Interest Group on Security (SIGSEC), and IFIP. The purpose of the JTF on Cybersecurity Education was to develop comprehensive model curricular recommendations for undergraduate program in cybersecurity education that will support future program development, and associated educational efforts. Prior ACM-lead JTFs that have worked to produce model curricula recommendations (www.acm.org/education/curricula-recommendations) for undergraduate degree programs, included:

- The ACM/IEEE CE2004 for Computer Engineering
- The ACM/AIS IS2010 for Information Systems
- The ACM/IEEE CS2013 for Computer Science
- The ACM/IEEE SE2014 for Software Engineering
- The ACM/IEEE IT2017 for Information Technology (under development)

Similarly, this JTF has been working to achieving the proposed curricular guidelines for undergraduate degree programs in cybersecurity (CSEC 2017). This presentation will start with an overview of JTF, the work that the JTF conducted, and Working Groups activities, including the thought model using the cross-cutting ideas, the knowledge areas, knowledge units, and topics outlined. Following, a discussion will be provided about the final report itself, the recommendation usage of the CSEC 2017 curricular guideline, issues related to the scope of the field of cybersecurity, along with challenges of defining the program outcomes. Discussion about the opportunities to be engage in the Exemplary Programs will be provided, and its role in ABET accreditation for cybersecurity programs.



All materials for the CAE in Cybersecurity Symposium will be available on the community website following the conference. For more information visit www.caecommunity.org.

Fastpitch Abstracts

AN EXPLORATORY ANALYSIS ON CYBERSECURITY ECOSYSTEM USING NICE FRAMEWORK
DAN KIM , UNIVERSITY OF NORTH TEXAS

Within the past few decades, cybersecurity has grown from individual concerns to a national-level issue. With such an explosive growth, there has been a discrepancy between the increasing demand for a better cybersecurity knowledge base and cybersecurity workers who are struggling to keep up. Government, academia, and the private sector have taken initiatives in order to fulfill these discrepancies with varying methods and levels of success. Additionally, considerable amount of research for each sector spanning across multiple disciplines have been conducted. However, there is a lack of a holistic view on cybersecurity knowledge among these three sectors and the relationships that exist between them. This research paper aims to explore the current cybersecurity ecosystem in order to allow future researchers and practitioners to understand and broaden the full scope cybersecurity knowledge. In order to achieve our research goal, we use an ontological network and identify key relationships that exist within all three sectors.

AN INNOVATIVE AND SUCCESSFUL MODEL TO PROMOTE CYBERSECURITY EDUCATION
WALEED FARAG, INDIANA UNIVERSITY OF PENNSYLVANIA

This proposal reports on the success and lessons learnt of an innovative and interdisciplinary project (funded by the NSA) with the objective of enhancing Cybersecurity education in western PA. This project implemented six different services that worked collaboratively to identify and address challenges facing Cybersecurity education. A focus of this funded project was to implement a novel program to enhance communications skills (soft skills) of Cybersecurity students and those aspiring to enter this promising field. Our ultimate objective was to propose an innovative and successful model that can be easily replicated in other schools and/or environments. These services and activities are briefly described below:

1. Designed and implemented quantitative and qualitative research studies to identify challenges facing Cybersecurity education.
2. Employed results from the above-mentioned research studies and from extant published research as the basis for designing a comprehensive program for delivering individualized instruction to Cybersecurity students.
3. Offered three weekend Cybersecurity skill enhancement workshops that provided very engaging sessions on various aspects of Cybersecurity.
4. Worked on building a Cybersecurity community that invited students, teachers, business owners, NGO's, and government organizations to come together to increase Cybersecurity awareness, practice, and education by pooling resources, collaborating in teaching and learning, and creating an integrated network for cyber education.
5. Offered a successful and well attended Cybersecurity skill enhancement summer camp (modeled after GenCyber camps).

BRIDGING THE GAP: DEVELOPING INNOVATIVE MINDS EARLY ON FOR CYBERSECURITY
MARK THOMPSON AND RAM DANTU, UNIVERSITY OF NORTH TEXAS

Forecasters are predicting a catastrophic shortage in workers to fill open positions in cybersecurity by 2020. We are not developing enough qualified candidates for this field, but by the time students enroll in a higher education institution, it may already be too late as many students are unable to handle the complexity and continually changing environment in cybersecurity. We propose starting a discussion on a new pedagogical approach to cybersecurity education based on our past strength in innovation. America has long been considered a nation of innovators, but with rapidly changing technology, we have to up our game by making innovation a part of growing up. Innovation should start from elementary school and promote thinking outside of the textbook. by making an investment to educate teachers and parents to encourage and sustain innovation. This presentation will discuss some initial steps needed to create a culture of innovation by educating teachers and parents to encourage and sustain innovation early on.

CLARK: A LIVING CYBERSECURITY DIGITAL LIBRARY
SIDD KARA, TOWSON UNIVERSITY

It is clear that in order to address the cybersecurity education and workforce crisis, the challenges are not just numerous but also inextricably linked. The least of which include a greater number of prepared faculty, effective curriculum, and infrastructure to host, use, and disseminate the curriculum. There is a demonstrated need for a cybersecurity digital library (DL) that will help address these challenges. The Cyber DL is similar to other curricular digital libraries in some respects (material quality, uptake, etc.) and unique in others (national security concerns, presence of damaging material – malware, material integrity issues, etc.). We have been working on the design and implementation of CLARK – The Cybersecurity Labs and Resource Knowledge-base. CLARK is a prototype curriculum management platform that hosts diverse cybersecurity learning objects. This submission introduces the system and highlights its capabilities as a tool that is much needed in the cybersecurity education community.

All materials for the CAE in Cybersecurity Symposium will be available on the community website following the conference. For more information visit www.caecommunity.org.

Fastpitch Abstracts

INTRODUCING THE CSUSB SOCIETY OF WOMEN IN CYBERSECURITY (SWICS)
ESSIA HAMOUDA

In this talk we will present the Society of Women in Cybersecurity (SWiCS), a less than one year old club. SWiCS is energized and ran by CSUSB students of The Jack H. Brown College of Business. The main aim of the club is to attract women to the technical field and especially to cybersecurity. SWiCS is a community of students (all genders) supporting each other through every step of their career, from school duties to job hunting. The aim of the club is to supplement classroom curricula through study groups, workshops, mentoring, networking, and internship/job placement assistance. Though one year old, the club members have doubled in number, attracting not only females but also males.

PASS USING BLOCKCHAIN TECHNOLOGY AND ITS RISKS AND CHALLENGES
Z CHEN, MERCY COLLEGE

It this fast pitch, blockchain technology and its potential applications are presented. We will explore so called decentralized transparent immutable yet secured applications using the blockchain technology and will describe a novel approach of "proof of X" such as proof of identity, proof of college degree and proof of academic achievements. The project prototype of a personal archive service system (PASS) is demonstrated. Personal archive is defined as a collection of various artifacts that reflect personal portfolio as well as personal unique identifications. Personal portfolio is in addition to a simple statement of personal achievement. It is an evidentiary document designed to provide qualitative and quantitative chronically documentation and examples.

The pitch moves on to focus on security concerns, risks and challenging. Blockchain technology has been bringing cryptography to individuals who are in turn as value investors in the internet with a clear time sequence, not just any information consumers. But, it is also coupled with various threats and concerns. We will discuss issues inherited from the current blockchain technology such as scalability, efficient and block sizes. We will also talk over a possibility of altering blocks even without over 50% mining power, low resource eclipse attacks and other forms of cheating. We will also present in the end a challenging case of cleaning poisoned blocks.

THE UNIVERSITY OF ARIZONA CYBER VIRTUAL LEARNING ENVIRONMENT (VLE)
JASON DENNO, UNIVERSITY OF ARIZONA, TUCSON

The University of Arizona, to enhance the learning experience of online, hybrid, and face-to-face students in the Cyber Operations degree program, has designed, built, and implemented a Cyber Virtual Learning Environment (VLE). Built upon a hybrid cloud architecture, students can log in to their classes from anywhere there is internet access, and safely complete hands-on learning exercises in a synthesized environment with no fear of damaging or interfering with current, live, computer networks. This provides a cost-effective option for students wishing to pursue their degree, paired with the geographic flexibility students may need.

The VLE is made up of several components which students will use throughout their courses. This vast array of components keeps students challenged and provides a depth of experience in the Cyber realm not readily available elsewhere. Our students, regardless of learning modality, leave the program with the knowledge, skills, and abilities to work immediately in the Cyber field upon graduation. Through the VLE, they will attack and defend the businesses, individuals, and governmental offices of CyberApolis, our virtual city. With 15,000 highly developed virtual citizens, CyberApolis is a thriving city with its own social media, hospital, bank, businesses, and organized crime. Our Internet of Things lab devices are being increasingly integrated into CyberApolis to allow students to interact with these everyday devices that may be watching, listening, or interfering with our homes and businesses. And the Malware Sandbox provides a safe environment in which to reverse engineer malware, with no threat to current computers or networks.

UNDERSTANDING WORKFORCE ATTRIBUTES BY EXPLORING EMPIRICAL CAREER PATHWAYS OF CYBERSECURITY INDUSTRY PROFESSIONALS
DAM KIM , UNIVERSITY OF NORTH TEXAS

The purpose of this research is to glean insight into the taxonomy or differentiation methods used in cybersecurity employment. In addition, the research will identify the career paths have experienced professionals such as executives and senior managers taken to reach their current positions. Considering both top-down and bottom-up approaches, we can better identify what current KSAs and cybersecurity certifications are predominantly obtained by current cybersecurity professionals and what types of KSA are missing. More specifically, we expect that the results of this analysis provide several important outcomes such as current cybersecurity career paths, a cybersecurity certification and KSA map, and a cybersecurity knowledge units mapping. As a result, we can improve future workforce efficiency by identifying what experience, education and certifications are needed and encouraged to pursue.

This study will provide insights of the practical utilization of the knowledge and skills in the cybersecurity industry that provide the greatest impact it contemporary employee needs. It explains the directions that successful employees have taken to reach their current positions. It also provides perspective into the priorities of industry leaders by outlining their backgrounds, and the industries and fields in which they were previously employed.

Special Interest Group Abstracts

CAE-CD 2019 KNOWLEDGE UNITS

This Session is an opportunity for current CAEs and CAEs in the Candidate Program to become more familiar with the CAE-CD 2019 Knowledge Units. Attendees will have the opportunity to ask questions and learn more about the KU requirements.

CAE IN CYBERSECURITY COMMUNITY WEBSITE

In June 2018, the CAE in Cybersecurity Community annouced the launch of the newly redesigned community website. While much of the functionality remains the same, there are some new features we would like to show you how to use. At this talk you will learn how to use the website, specifically posting content, faculty opportunities, as well as events. Additionally, we will go over some of the new community pages and discuss how they can be of use to your institution.

DOD CYBERSECURITY SCHOLARSHIP AND CAE CYBERSECURITY GRANT BOOT-CAMP

General information to include updates and changes about the scholarship program. Also, learn what is required to apply for CAE cybersecurity grants. This event is open to all. Attendees will leave with a DoD CySP checklist/FAQ sheet as well as tips and suggestions on how to submit a concise grant proposal. Other NSA grant programs (GenCyber / CAE Cyber Operations / Cyber Curriculum) will not be discussed. Please refer questions on those grants to respective Program Directors.

NICE CHALLENGE PROJECT CAE STATUS REPORT 2018

Over the course of 2018 the NICE Challenge Project has reached some incredible new usage milestones, increased our systems capacity four-fold, and released some of our best content yet. This session will be an in-depth walkthrough of 2018 at the NICE Challenge Project including a live demo of one of our newest challenges. The session will also cover what the NICE Challenge Project has planned for 2019, how educators can get access to the challenges, and how new and current users alike can get involved in the development process. For more information please go to https://nice-challenge.com/.

SOUTHEAST CAE COMMUNITY COLLABORATIVE PROJECTS: WORKING SESSION

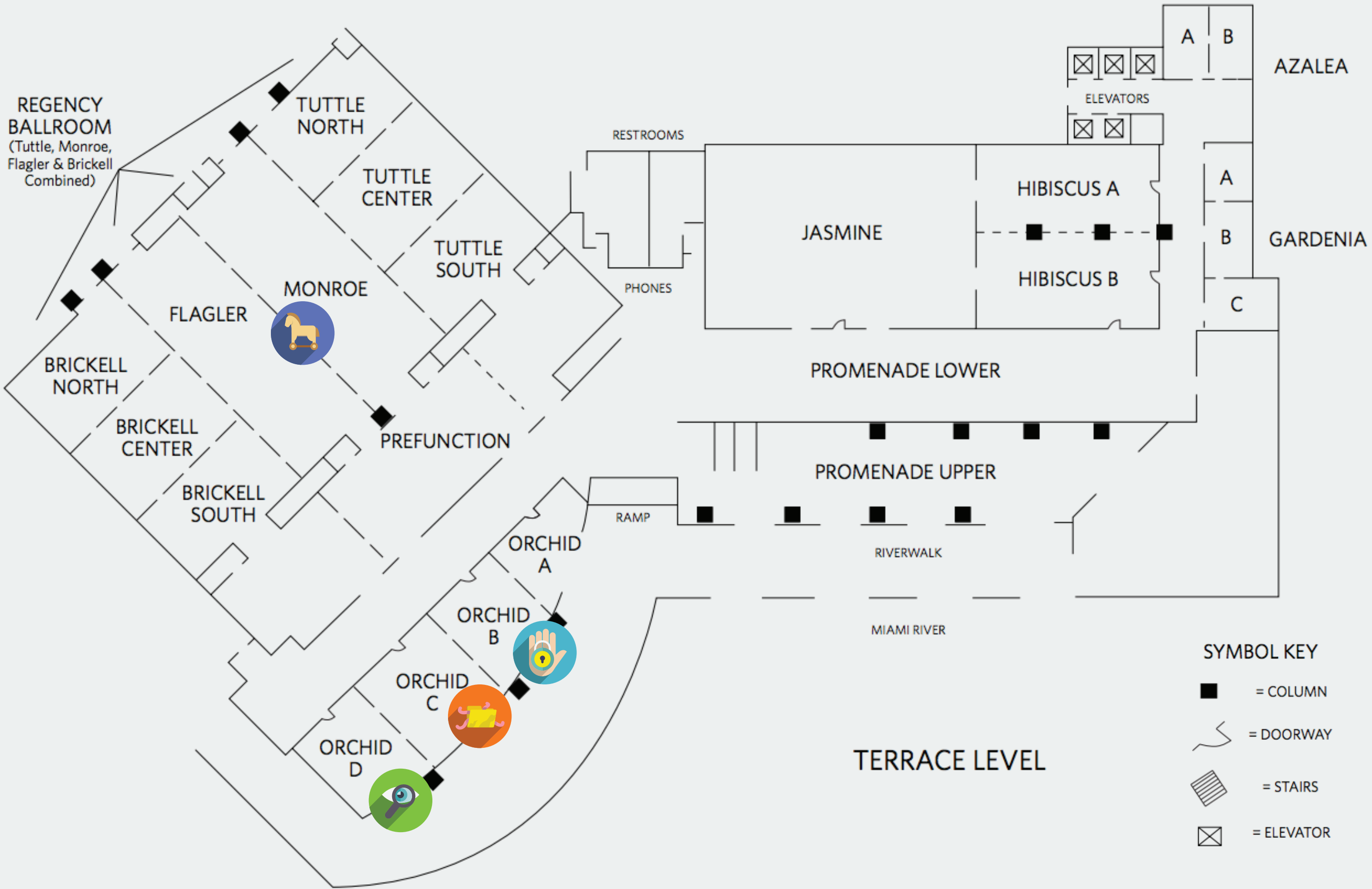
The Southeast CAE Regional Resource Center will facilitate a working session to discuss and develop collaborative projects and proposals. All faculty from CAE institutions in the Southeast region are invited to participate.

2018 Designated CAEs

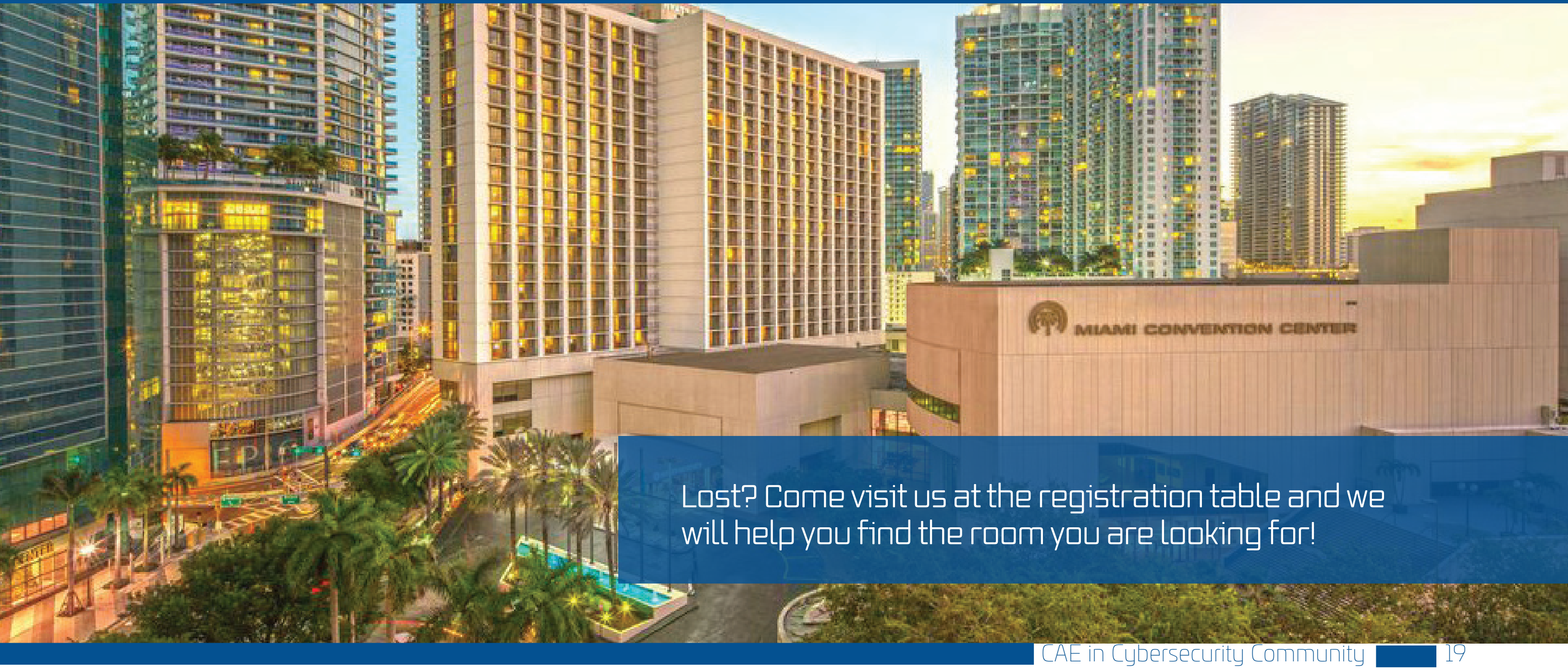
> Welcome to the CAE in Cybersecurity Community! Below is the list of all the designated as Centers of Academic Excellence in Cybersecurity for 2018.

American Public University
Augusta Technical College
Calhoun Community College
Clemson University
College of Southern Nevada
Community College of Rhode Island
Cypress College
ECPI University
El Paso Community College
Fayetteville Technical Community College
Florida State College at Jacksonville
Grand Rapids Community College
Green River College
Indian River State College
Laredo College
Leeward Community College
Lehigh Carbon Community College
Liberty University
Lincoln Land Community College
Long Beach City College
Marquette University
Metropolitan Community College
Metropolitan Community College - Kansas City
Northeast Community College
Oakland University
Pennsylvania Highlands Community College
Pikes Peak Community College
Portland Community College
Regent University
Roosevelt University
Southern Utah University.
Texas State Technical College in Harlingen
University at Albany, State University of New York
University of North Carolina, Wilmington
University of Virginia
Valencia College

Symposium Map



Hyatt Regency Miami Hotel Map



Lost? Come visit us at the registration table and we will help you find the room you are looking for!

Thank you for attending the CAE in Cybersecurity Community Symposium!

All materials from the symposium will be available to view and download on the CAE in Cybersecurity Community Website. If you have any questions, comments, or concerns please contact us at info@caecommunity.org.