



# CAE

## in Cybersecurity Community Symposium

Leading The Way To Tomorrow's Cybersecurity Education

---

Symposium Guide  
Schedule, Speaker Biographies, and other resources

November 9, 2017

Hosted at: Crowne Plaza Dayton,  
33 E. 5th Street, Dayton, OH 45402














## Welcome to the annual CAE in Cybersecurity Symposium!

Each year the CAE in Cybersecurity Community gathers to talk about changes in the program, receive updates from the community, network with other members, and listen to pressing issues in the community. This year, we want to know how you are helping lead the way to tomorrow's cybersecurity education since becoming a CAE designated institution.

To help start the conversation, today's symposium will include fast-pitch talks and presentations meant to highlight important contributions from the community as well as important updates from the program office. You will also receive some updates from the CAE in Cybersecurity Community regarding some of the changes you have already seen and the changes yet to come.

# Symposium Schedule

Welcome and Logistics Tony Coulson		8:00-8:15
CAE in Cybersecurity Community Updates Tony Coulson		8:15-8:45
NIETP Program Office Lynne Clark		8:45-9:15
Other Program Updates NSF- Susanne Wetzel NICE- Rodney Peterson DHS- Daniel Stein		9:15-10:00
Morning Break		10:00-10:15
CAE Virtual Career Fair Corrinne Sande & Tony Coulson		10:15-10:45
CAE Spotlight Eman El-Sheikh		10:45-11:15
Presentations (Breakout Rooms)    		11:15-12:00
Lunch/ Web Development		12:00-13:00
Appointments		
CRRC Breakout Sessions   		13:00-14:45
Afternoon Break		14:45-15:00
Fast Pitch 		15:00-16:15
Closing Ceremonies		16:15-17:00



Use the following icons to help you navigate. CRRC breakout sessions and the Speaker agenda are available on page 4. Speaker bios are located on pages 6 through 8. Fast Pitch and Presentation abstracts are located on pages 8 through 10. Fast Pitch and Presentation abstracts will use these icons. Please note Fast Pitch and Presentation icons come in two colors (blue and black).



Presentation Icon, Blue/Black



Ballroom Icon, Orange



McKinley Icon, Green



Fast Pitch Icon, Blue/Black






Harding Icon, Purple













Harrison Icon, Sky Blue

# 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 times, rooms, and discussion topics. A regional map is provided for your reference on page 11.

Times	 McKinley	 Harding	 Harrison
13:00-13:35	North Eastern Region CRRC	National Capitol Region CRRC	East Central Region CRRC
13:35-14:15	South East Region CRRC	Mid-Western Region CRRC	North Central Region CRRC
14:15-14:45	North Western Region CRRC	South Central Region CRRC	South Western Region CRRC

## Presentation/Fast Pitch Agenda

Capturing Their Attention: Utilizing Capture-The-Flag (CTF) Competitions In The Classroom		11:00-11:20
Cybersecurity Programs at a Premier HSI Polytechnic University of Puerto Rico (PUPR)		11:00-11:30
Leveraging Federal Agencies' Assistance to Inspire Youth to Pursue Cybersecurity Education and Career Path at a CAE in Florida		11:00-11:30
CA Cybersecurity Apprenticeship Program at Coastline Community College		11:00-11:30
Standards Based Integration of Security Operations Center Experiences into a Four Year Undergraduate Cyber Security Program		11:20-11:40
Cyber Security Resiliency Engineers for Cyber-Physical Systems		11:30-12:00
Developing Hands on Cyber Threat Hunting Exercises		11:30-12:00
CyberTech Girls - A Hands-on Workshop for MS/HS girls		11:30-12:00
Ethical Thinking in Cyber Space		11:40-12:00
Closing the Gap in Cybersecurity Talent: Another Approach		15:00-15:10
A Video-Based Course Package for Community Colleges on Cybersecurity Advanced Research Topics		15:10-15:20
Hardware for Hacking and Defending		15:20-15:30
An Interdisciplinary, Multifaceted Approach to Enhance Cybersecurity Education in Western Pennsylvania		15:30-15:40
Cyber-Leadership and Threat Gamification Engineering		15:40-15:50
Recap of CAE NE Region Workshop on Virtual Platforms and Exercise Design for Cyber Competitions		15:50-16:00
Pilot Schools Wanted: Competency-Based Curriculum for Information Security Fundamentals		16:00-16:15



# CAE in Cybersecurity Community Updates

The CAE in Cybersecurity Community was involved in a number of different initiatives this year including the CAE Virtual Career Fair, Hands-On Learning Study, and updating the community website. In addition, many of our members held professional development workshops, NIETP Program Office Planning Meetings, as well as regional meetings to discuss CAE membership.



## WEBSITE REDESIGN

The CAE in Cybersecurity Website is currently under redevelopment. We are in the process of opening up membership to include academia, industry, and government. In addition, we are also redesigning the website with the community in mind, making it more user-friendly, creating custom content for the CNRCs and CRRCs as well as adding more communication platforms.

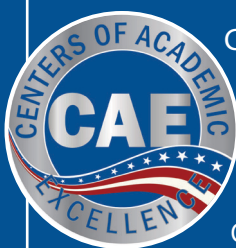


## NEW CAE IN CYBERSECURITY LOGO

Along with the website redesign the community redesigned the CAE in Cybersecurity Community logo. Our new logo accentuates our identity as cybersecurity educators and professionals, as well as our commitment to produce qualified cybersecurity graduates that will protect and defend as part of the cybersecurity workforce.

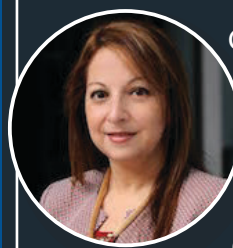


Members of the CAE in Cybersecurity Meeting met with the NIETP Program Office to discuss plans for the next year.



## CAE Virtual Career Fair Corrinne Sande & Tony Coulson

On October 13, 2017, the National Centers of Academic Excellence held its first Virtual Career Fair, sponsored by our friends at Cyber Watch West and the National Science Foundation. The job fair connected students from CAE designated schools to employers looking to fill internships, part-time positions, and full-time positions. Students in Cyber Security degrees from schools designated as Centers of Academic Excellence in Cyber Security (CAE-C), Cyber Defense (CAE-CD), Cyber Operation (CAE-CO) participated at no cost.



## CAE Spotlight Eman El-Sheikh

Since becoming a CAE, the University of West Florida has quickly become a leader in the CAE in Cybersecurity Community.

Not only is the University of West Florida a very active member of the community, but it also hosts numerous events for its region. Eman El-Sheikh, Director of the Center for Cybersecurity, will talk about the many great things she has done for the community and her region since becoming a CAE designated institution.

# Speaker Biographies



## 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.

## ROBERT MILLS

Dr Robert Mills is a Professor of Electrical Engineering at the Air Force Institute of Technology. His research interests include security in cyber physical systems, insider threat mitigation, and convergence of cyber/electronic warfare. He has authored/co-authored over 120 articles on a variety of security-related topics.



## NANCY JONES

Nancy is the Dean of Instruction for Career and Technical Education including the disciplines of Accounting, Business Computing, Business, Building Codes, Computer Information Systems, Computer Networking, Emergency Management, Paralegal Studies, Process Technology, Real Estate, and Management and Supervision. In addition, She oversees the STAR program that is a fast-track 3 primary semester and one summer transfer degree program developed using the C-ID AS-T templates. Other areas of interest include: Articulation, Programs of Study, Course Alignment and Student Success.

## BEI-TSENG "BILL" CHU

Bill Chu is Professor at the Department of Software and Information Systems, University of North Carolina at Charlotte. He is associate director of the Center for Configuration Analytics and Automation. His research interest includes Cyber Security Education, Software Security, Cyber Threat Intelligence, and Security Analytics. He is the point of contact for UNC Charlotte's NSA/DHS recognized Center of Academic Excellence in Information Assurance Education-Cyber Defense, and Center of Academic Excellence in Information Assurance Research. He is the PI of the Scholarship for Service program at UNC Charlotte. He has received several cybersecurity education grants from both NSA and NSF.



## JANE BLANKEN-WEBB

Jane Blanken-Webb is a Postdoctoral Research Associate with the Information Trust Institute at the University of Urbana-Champaign, where she is researching cybersecurity ethics and education. She is a co-principal investigator on an NSA funded project entitled: Ethical Thinking in Cyber Space (EthICS). She also works closely on the Illinois Cyber Security Scholars Program, funded by the NSF. Her work has been published in numbers journals including Educational Theory, Philosophical Inquiry in Education, and Philosophical Studies in Education. She holds a PhD in Philosophy of Education from the University of Illinois at Urbana-Champaign and has prior experience as a K-12 educator.



## KYLE JONES

Kyle Jones is the Chair & Assistant Professor at Sinclair's College. Mr. Jones holds a Security+ Certification and a master's degree in Information Assurance and Security. He is a CAE2Y Principal Investigator and serves as the coordinator and the curriculum specialist. In addition, Mr. Jones has been featured as a public speaker on cybersecurity topics. Most recently he participated in a roundtable hosted by the Dayton Business Journal on cyber security, and he was featured on WDTN Dayton-Channel 2 about "Good Cyber Hygiene." His previous work experience ranges from working for small PC repair shops to Fortune 500 Datacenters.



## BO YUAN

Bo Yuan, Ph.D., is a professor and chair in Department of Computing Security at Rochester Institute of Technology. He joined RIT in 2003 and has been in cybersecurity education since. Dr. Yuan is the PI of multiple cybersecurity educational grants including the five years, \$3.9 million CyberCorps® Scholarship for Service grant funded by National Science Foundation (NSF). He has a Ph.D. from Binghamton University, a BS and an MS from Shanghai Normal University. Before joining RIT, Dr. Yuan was a scientist at Manning & Napier Information Services for six years.



## 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 and Dissemination, E-learning, Assessment, Multimedia Security, and Multimedia Indexing and Retrieval Techniques. Dr. Farag has an established record securing funds to support his research. He is currently the PI of several active federally funded grants. In addition, he has numerous publications in his areas of interest. Furthermore, Dr. Farag is serving in the technical program committees and as a reviewer for several international journals/conferences including the ACM TOCE, IEEE FIE, Springer, and IEEE InfoComm.

# Speaker Biographies

## CASEY O'BRIEN

Casey W. O'Brien is the Executive Director and Principal Investigator of the National CyberWatch Center, a cybersecurity education and research consortium focused on advancing cybersecurity education and strengthening the national cybersecurity workforce. Casey has more than 20 years of industry experience in information security and large-scale IT implementation and project management in challenging and cutting edge computing environments that include both the public and private sectors.



## TREZ JONES

Dr. Jones is the assistant director of the Texas A&M Cybersecurity Center and a faculty member at Sam Houston State University. He comes to academia from 25 years of private and public sector experiences in network engineering, database administration, system administration and IT project management. His research interests focus on cybersecurity andragogy, digital forensics and chain-of-custody issues, and exploring cyber-leadership.



## MAJOR LOGAN MAILLOUX

Maj (Dr) Logan Mailloux is an Assistant Professor of Systems Engineering at the Air Force Institute of Technology. His research interests include secure systems engineering, architecture analysis, modeling and simulation, and test/evaluation of systems operating in contested environments. He has authored/co-authored 20 journal papers, 11 conference papers, and 3 book chapters on these topics. He has also contributed to the development of NIST Special Publication 800-160 for systems security engineering.



## JOSH STROSCHIN

Dr. Stroschein is a subject matter expert in malware analysis, reverse engineering and software exploitation. He is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis, reverse engineering, software exploitation and other related security topics. Dr. Stroschein is also an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon and Hack-In-The-Box (Amsterdam). He is also the Director of Training for a Cyber Protection Team (CPT) for the Air National Guard in Des Moines, IA.



## TOBI WEST

Tobi is Department Chair at Coastline Community College in Garden Grove and is adjunct faculty in the CIS Department at Cal Poly Pomona. With a passion for cybersecurity education, Tobi focuses on developing career pathways for students to achieve their goals as a cybersecurity professional. In addition to teaching security related courses, she coordinates local training and competition for middle schools and high schools in CyberPatriot and CyberTech Girls at Coastline Community College.



## WILLIAM BUTLER

Bill has worked in the networking and IT industries as a network engineer and consultant for over 20 years. Bill also served as a joint qualified communications information systems officer in the U.S. Marine Corps and retired as a Colonel with 30 years of service (active and reserve). Bill is very active in various working groups such as the National Institute of Standards and Technology Cloud Computing Security Forum Working Group (NIST CCSFWG), Cloud Security Alliance (CSA) Big Data and Mobile Computing Working Group, and the National CyberWatch Center Curriculum Taskforce and the National Cybersecurity Student Association Advisory Board.



## ALFREDO CRUZ

Dr. Alfredo Cruz holds two PhD degrees. He has been working with graduate students in projects and papers related to IA and Computer Security. Dr. Cruz is the Director and founder of the Center for Information Assurance for Research and Education (CIARE) and has also been the key to obtaining the CAE IA/CD designation. Dr. Cruz has developed seven academic programs in computer science and computer engineering, and two Graduate Certificates in IA that are at the forefront of education in this field. He has a proven track record, and has outstanding leadership and experience in managing grants and proposals.



## ANDREW KRAMER

Mr. Andrew Kramer serves as an instructor of computer science and cyber security at Dakota State University. His previous experience includes roles as a cyber security intern at Johns Hopkins Applied Physics Lab and a penetration test engineer. Andrew is a subject matter expert in hacking methodologies, reverse engineering and software exploitation.





# Speaker Biographies



## DEANNE WESLEY

Dr. Deanne Cranford-Wesley is currently Department Chair Davis iTEC/Cyber Security Program Director at Forsyth Technical Community College. She is the POC for the Center of Academic Excellence and Co-PI for the Scholarship for Service program at Forsyth Technical Community College. Dr. Cranford-Wesley is a cybersecurity professional and has appeared as a subject matter expert on Fox8 and Time Warner News discussing recent advances in cyber security vulnerabilities and mitigating attacks. She has received several cybersecurity grants from the NSA/NSF. She also teaches information security, computer forensics and networking courses in the Business Information Technology Department with the Davis ITec Center. Additionally, Dr. Cranford-Wesley sits on the Board of the Colloquium of Information System Security Education Conference (CISSE) and has presented at various conferences including several presentations at The Colloquium Information System Security Education Conference.



## ANTON DAHBURA

Anton Dahbura has served as the Executive Director of the Johns Hopkins University Information Security Institute in Baltimore since 2012. He received the BSEE, MSEE, and PhD in Electrical Engineering and Computer Science from the Johns Hopkins University in 1981, 1982, and 1984, respectively. From 1983 until 1996 he was a researcher at AT&T Bell Laboratories, was an Invited Lecturer in the Department of Computer Science at Princeton University, and served as Research Director of the Motorola Cambridge Research Center. From 1996-2012 he led several entrepreneurial efforts in the areas of printing, professional baseball operations and commercial real estate.




## JAKE MIHEVC


Jake Mihevc serves as Associate Dean of Business, Cybersecurity, and Computer Sciences at Mohawk Valley Community College (MVCC), a CAE2Y in Upstate NY. Jake is also the Director of the Northeast Regional Resource Center for the CAE program. Jake is also a co-founder of the Central New York Hackathon, a regional cybersecurity competition that brings over 100 students from eight cybersecurity programs together each semester to test their skills.

# Presentation Abstracts


## CAPTURING THEIR ATTENTION: UTILIZING CAPTURE-THE-FLAG (CTF) COMPETITIONS IN THE CLASSROOM JOSH STROSCHIN & ANDREW KRAMERI, DAKOTA STATE UNIVERSITY

 Capture-the-flag (CTF) competitions provide dynamic, real-time environments intended to engage and challenge the participants. However, they are often not designed to be educational. Rather, they simply provide a series of progressively more difficult challenges in which the participant must find the flag (answer). As these challenges are typically devoid of any direction, this can lead to participants being unable to progress any further in the CTF and therefore unable to achieve educational goals. This presentation will discuss the process of hosting a CTF, their limitations and common work-arounds. We will then discuss our successes and failures in utilizing existing CTF frameworks in the classroom. Finally, we will introduce a custom designed CTF framework that aspires to solve many of the difficulties inherent in the current CTF space. This framework introduces a novel hint system that allows for customizable help to be built for each challenge within a CTF event. The goal is to allow all to participate and progress through the challenges by providing varying levels of help throughout the competition. This approach maximizes learning and student engagement, opening the utility of such frameworks to the classroom. The framework will be made publicly available upon conclusion of the presentation.

## CYBER SECURITY RESILIENCY ENGINEERS FOR CYBER-PHYSICAL SYSTEMS MAJOR LOGAN MAILLOUX & ROBERT MILLS, AIR FORCE INSTITUTE OF TECHNOLOGY

 This presentation brings awareness to cyber security experts (multiple specialty domains), engineers (of all fields), and supporting personnel (managers, testers, analysts, etc.) on the cyber security and resiliency implications associated with developing and operating complex cyber-physical systems built to operate in highly contested cyberspace environments. In contrast to conventional cyber security thinking (i.e., Confidentiality-Integrity-Availability), cyber-physical systems are often operated in real-time with an emphasis on availability and safety over confidentiality. Moreover, the United States Department of Defense (DoD) is increasingly concerned with successful mission execution and resiliency of advanced warfighting systems such as aircraft, ships, missiles, command and control systems, navigation subsystems, and other combat focused DoD systems. We present and discuss ongoing work which focuses on creating a cyber resiliency knowledgeable workforce.

## ETHICAL THINKING IN CYBER SPACE JANE BLANKEN-WEBB, UNIVERSITY OF URBANA-CHAMPAIGN

 In the rush to prepare the next generation of cybersecurity professionals, it is vital that we maintain a holistic view of the education these professionals need. Along with technological expertise, these professionals require an education that will cultivate and develop wide-ranging capacities, skills, and dispositions that will prepare them to address ethical and technological conundrums that stand to shape the future of society. Innovative approaches to cybersecurity education are needed to equip these professionals to be technologically savvy as well as ethically minded and capable of meeting the heavy burden of responsibility that comes with increased technological skills and access to sensitive data. This presentation will introduce core ideas driving a curriculum development project funded by the NSA entitled: Ethical Thinking in Cyber Space. This case study-based curriculum will immerse students in real-life ethical dilemmas inherent to cybersecurity and engage them in open dialogue and debate within a community of ethical practice. This "hands on" approach to cybersecurity ethics will engage a rich integration of theory and practice, beginning with concrete and richly detailed case studies and examples, and drawing philosophical insights from the analysis of those particulars.



# Presentation Abstracts

## CYBERTECH GIRLS - A HANDS-ON WORKSHOP FOR MS/HS GIRLS TOBI WEST, COASTLINE COMMUNITY COLLEGE

Imagine...Believe...Achieve. Coastline Community College hosts an annual hands-on event in which high school and middle school girls have the opportunity to learn about cybersecurity. The event brings together girls from local schools, industry professionals, and academic leaders to the college campus. This year's event will be presented in collaboration with Fullerton College as part of the Southern CA Cybersecurity Community College Consortium (SoCalCCCC). Students have the opportunity to experience cybersecurity activities, speak to professionals about career interests, and develop an understanding of some of the cybersecurity disciplines. Activities include a crime scene with digital evidence collection from "dead bodies", digital evidence examination, web page development with emphasis on personal cyber wellness topics, and computer assembly/disassembly. This presentation will discuss outcomes and lessons learned from the October 2016 and 2017 events.



## CA CYBERSECURITY APPRENTICESHIP PROGRAM AT COASTLINE COMMUNITY COLLEGE TOBI WEST & NANCY JONES, COASTLINE COMMUNITY COLLEGE

Coastline Community College has a new CA Cybersecurity Apprenticeship Program (CCAP) which provides students with free tuition, textbooks, and industry certification exams to prepare them for the cybersecurity workforce. The program, funded by the State Chancellor's Office, anticipates that apprentices will complete 2,000 hours on-the-job with local employers while Coastline provides training through 7 college-credit courses that align with its Associate of Science in Networking: Cybersecurity. Apprentices are encouraged to prepare for cybersecurity careers through career-readiness workshops, on-campus events, and mentoring. Exam prep courses are offered between each of the 8 week credit courses to ensure that the apprentices are ready to sit for the certification exams. The courses support hands-on learning using Netlab and other remotely accessible labs. Courses include Network+, Security+, Windows Server, Python, Ethical Hacking, Cybersecurity Analyst+, and Computer Forensics.



## LEVERAGING FEDERAL AGENCIES' ASSISTANCE TO INSPIRE YOUTH TO PURSUE CYBERSECURITY EDUCATION AND CAREER PATH AT A CAE IN FLORIDA YAIR LEVY, NOVA SOUTHEASTERN UNIVERSITY

Current cyber-threats are imminent for all organizations as it is evident from the reporting of weekly data breaches. However, shortage for cybersecurity workforce has been well documented, and remains a major concern for future sustainability and resilience of our cyber infrastructure. Since 2012, Dr. Levy has been working to establish relationships with federal agencies (FBI, DHS, NIST, NSA, & USSS) to have their Special Agents and key personnel come to an annual event where over 200 high-school students bused to the university campus for a day full of passion and excitement about cybersecurity education and career path. This presentation will start with an overview of a self-funded "Cybersecurity Day" event that has been successfully running yearly each October, the cybersecurity awareness month, and will also highlight the presentations provided by agency personnel along with feedback notes from the high-school students and teachers who attended the event.



## CYBERSECURITY PROGRAMS AT A PREMIER HSI POLYTECHNIC UNIVERSITY OF PUERTO RICO (PUPR) ALFREDO CRUZ, POLYTECHNIC UNIVERSITY OF PUERTO RICO

PUPR hosts a competitive graduate IA security program under the Master of Science in Computer Science (MS CS) with a specialization in Information Technology Management and Information Assurance (ITMIA), a track in Cybersecurity under the BS CS and BS CpE programs, and two (2) graduate security certificates: 1). Graduate Certificate in Information Assurance and Security (GCIAS); 2). Graduate Certificate in Digital Forensics (GCDF). All these programs service a large, mainly Hispanic, under-represented student population. The MS CS ITMIA covers most of the aspects of Computer Science, IT Management, and focuses on Information Assurance to protect data and information at large. Computer Engineering focuses on software and hardware security, software development, and internet engineering, through an emphasis in cybersecurity. The GCIAS covers both technical and managerial aspects of IA and Security while the GCDF covers the technical aspects of Digital Forensics including knowledge and skills to protect, detect, recover and mitigate data loss and theft.



## DEVELOPING HANDS ON CYBER THREAT HUNTING EXERCISES BEI-TSENG "BILL" CHU & DEANNE WESLEY, UNIVERSITY OF NORTH CAROLINA, CHARLOTTE

Cyber threat hunting has emerged as a critical part of cyber security practice. However, there is a severe shortage of cybersecurity professionals with advanced analysis skills for cyber threat hunting. This presentation presents an effort to develop 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 efforts will be focused on the following two areas. (1) develop hands-on learning experiences that cover two important areas in threat hunting: threat analysis and security data analytics, and (2) build institutional capacity by integrating at least seven hands-on labs on threat hunting into existing curricula at two participating institutions: UNC Charlotte and Forsyth Tech. Our hands-on labs focus on exercising a set of essential technical skills (called the threat hunting skill set) in an enterprise environment and they are modeled after real-world scenarios. Our lab environment contains real threats (e.g., malware) against real software (e.g., Operating Systems and applications), and real security datasets. These labs are designed to help a student learn how to detect active and dormant malware, analyze its activities, and assess its impact. These labs also teach a student how to search and probe for anomalies in a variety of datasets using multiple analytical skills, such as statistical analysis, machine learning, and data visualization. Our labs are designed at different difficulty levels suitable for use by two-year community college students, 4-year university students, as well as for collegiate threat hunting competitions.



## STANDARDS BASED INTEGRATION OF SECURITY OPERATIONS CENTER EXPERIENCES INTO A FOUR YEAR UNDERGRADUATE CYBER SECURITY PROGRAM WILLIAM BUTLER, CAPITOL TECHNOLOGY UNIVERSITY

Capitol will integrate a security operations experience into its Bachelor of Science in Cyber and Information Security and related degree Programs (Computer Science and Management of Cyber Information Technology). These unique operational experiences will better prepare our graduates to protect and defend networks by integrating required tools and technologies into a concept of operation (CONOPS). Students will be trained and mentored by vendors, faculty and alumni knowledgeable of SOC operating tools and techniques. Students will receive industry recognized certifications (forensics, malware analysis, scripting) where appropriate and focused experience with those tools.



# Fast Pitch Speaker Abstracts



## CLOSING THE GAP IN CYBERSECURITY TALENT: ANOTHER APPROACH

BO YUAN, ROCHESTER INSTITUTE OF TECHNOLOGY

It is well-known that there is a tremendous need for cybersecurity talent in the industry and government agencies. According to a recent (ISC)2 report, there will be 1.8 million unfilled cybersecurity positions by 2022. In this talk, we present our approach at RIT to help alleviate the cybersecurity workforce shortfall. It includes our partnerships with industry to provide real world scenarios for students to practice and our MicroMasters in Cybersecurity offering on edX to reach worldwide learners. The preliminary results in increasing diversity and career changing students are encouraging.



## HARDWARE FOR HACKING AND DEFENDING

KYLE JONES, SINCLAIR COMMUNITY COLLEGE

The Cyber Security Faculty at Sinclair pride themselves on hands-on learning. This is no exception for our security classes. The faculty at Sinclair have taken notes from conferences like Defcon to get their students involved in the classroom. Currently, the department uses everything from hardening blade servers as a part of our Securing a Windows Network Environment class to lock picking and WiFi Pineapples in our Network Security course. Recently, Sinclair was awarded funds from the NSA to help improve their hands-on experience. With these funds, Sinclair will be purchasing new blade servers that students will be hardening in teams. Then it will be attacked by other teams in that same class. The funds will also cover Open-Air PC's where students will Create a SCIF style environment in the classroom. Mobile devices and tablets will also be purchased for the Cyber Forensics class so the students can learn hands on mobile forensics. Sinclair College believes that if students get their hands-on hardware for hacking and defending it will ignite a learning passion for Cyber Security.



## A VIDEO-BASED COURSE PACKAGE FOR COMMUNITY COLLEGES ON CYBERSECURITY ADVANCED RESEARCH TOPICS

ANTON DAHBURA, JOHN HOPKINS UNIVERSITY

This talk will describe an innovative approach to cybersecurity education that the Johns Hopkins University Information Security Institute (JHUISI) is developing under a grant from the CAE Cybersecurity Grant Program. The goal of the project is to introduce the latest cybersecurity topics and materials to a broad audience of community college students. This effort is centered on the development of a series of educational video modules and accompanying learning materials that target community-college-level students with an in-depth exposure to the forefront subjects of cybersecurity research. These materials can be delivered in flexible modes, as a complete in-classroom course with reading materials, lectures, and exercises and assignments, as modular components in classes studying cybersecurity, or simply as online resources to improve the awareness and digital hygiene of the interested general public.



## AN INTERDISCIPLINARY, MULTIFACETED APPROACH TO ENHANCE CYBERSECURITY EDUCATION IN WESTERN, PA

WALEED FARAG, INDIANA UNIVERSITY OF PENNSYLVANIA

This proposal describes an ongoing, interdisciplinary project (funded by NSA) to address persistent cybersecurity challenges identified in several national initiatives such as NICE and CNAP. The project proposes a set of activities and services designed with an interdisciplinary perspective to provide effective solutions to such challenges. The proposed project is innovative for several reasons: 1)The project begins with a research component that will guide key steps of the project and add to the body of knowledge in cybersecurity education. 2)It includes collaboration between IUP's Institute for Cybersecurity and the university's Writing Center in order to deliver instruction to students from rural areas and help improve their soft skills. This collaboration puts to work the established expertise of a group of faculty from four different disciplines, see below. 3) It proposes the use of multiple approaches to solve persistent challenges in cybersecurity education including: peer-tutoring, weekend workshops, interactive learning experiences, flexible delivery format, flexible structural design, a summer camp, and the formation of a local cybersecurity consortium. 4)It is easily replicable for other institutions and rural areas. 5)It employs a set of assessment approaches throughout various project execution phases.



## CYBER-LEADERSHIP AND THREAT GAMIFICATION ENGINEERING

TREZ JONES, TEXAS A&M UNIVERSITY

How do we take traditional red team/blue team activities and interpolate a more real-world scenario to create an inclusive experience that gets folks' pulses running? How can we create more "buy-in" from participants in cyber defense and cyber operation activities? This fast-pitch session will take a quick look at methods of generating threat that require cross-disciplinary analysis spanning beyond technical disciplines and takes a holistic look at crisis and incident response.



## PILOT SCHOOLS WANTED: COMPETENCY-BASED CURRICULUM FOR INFORMATION SECURITY FUNDAMENTALS

CASEY O'BREIN, PRINCE GEORGE'S COMMUNITY COLLEGE

This Fast Pitch will highlight a library of adaptive, personalized, performance-based instructional modules designed by National CyberWatch to facilitate developing mastery of Information Security Fundamentals. These materials were created under a Core Curriculum Cybersecurity grant from the National Security Agency. The library will be presented and discussion will include an overview of the process of becoming a pilot implementation site for the Spring 2018 semester.

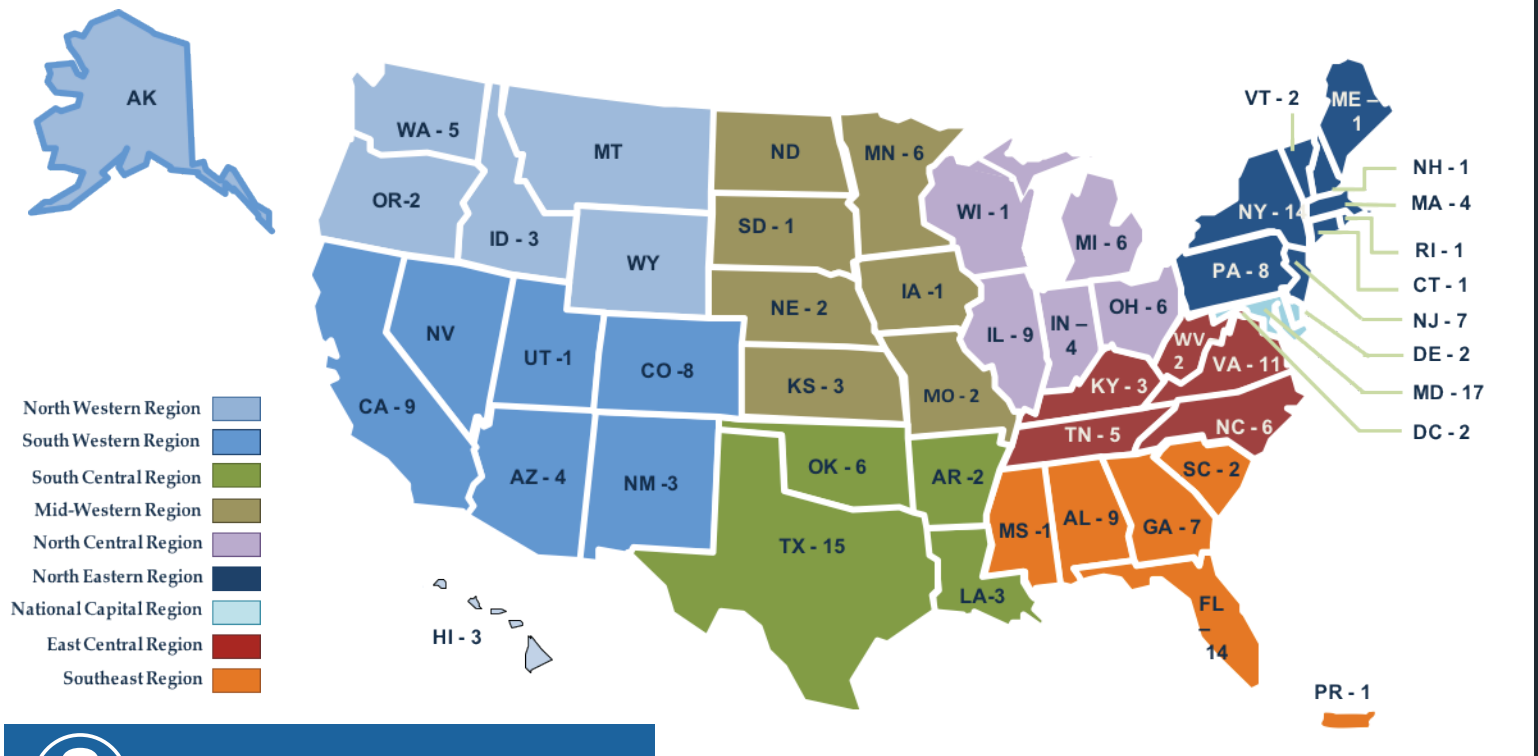


## RECAP OF CAE NE REGION WORKSHOP ON VIRTUAL PLATFORMS AND EXERCISE DESIGN FOR CYBER COMPETITIONS

JAKE MIHEVC, MOHAWK VALLEY COMMUNITY COLLEGE

This presentation summarizes the presentations and discussions at the Northeast Region CRRC workshop on virtual platforms and exercise design for cybersecurity competitions.

# CAE National & Regional Resource Centers



Map prepared by the NIETP Program Office



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

## Symposium Map



Ballroom Icon, Orange



Harding Icon, Purple



McKinley Icon, Green



Harrison Icon, Sky Blue





# 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 see our contact information below.

## CONTACT INFORMATION

909-537-7535

<http://www.caecommunity.org>

[info@caecommunity.org](mailto:info@caecommunity.org)