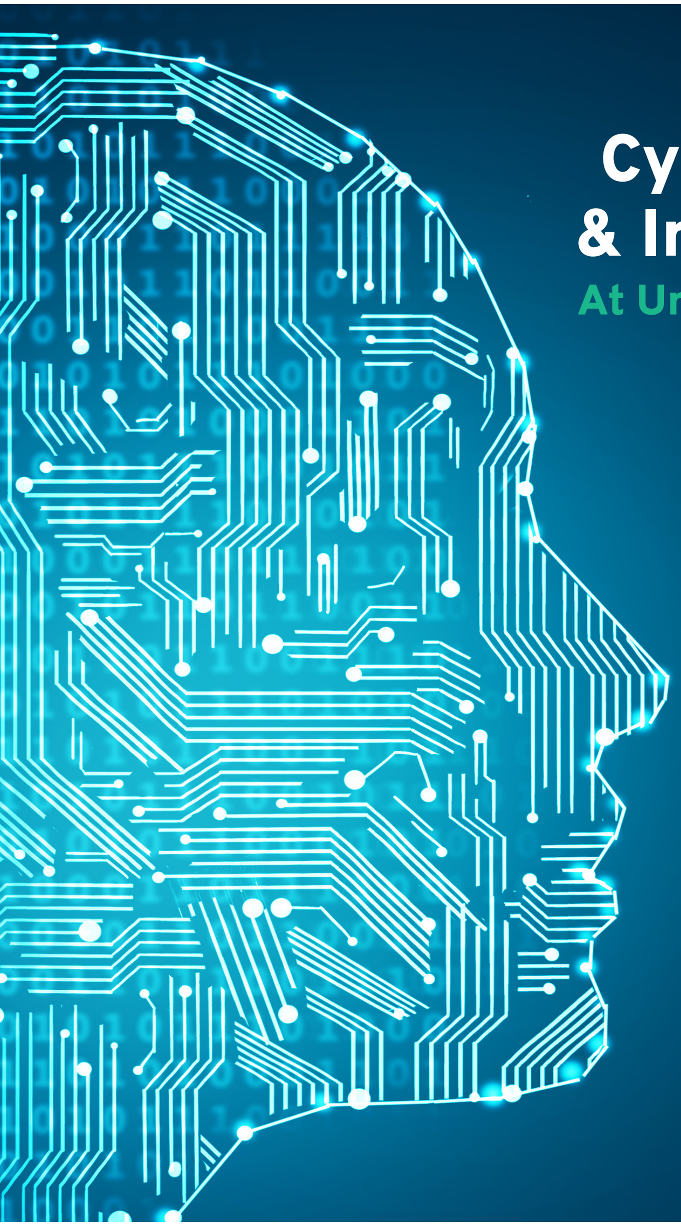
ATTACKING THE ROOTS OF

CYBER(IN)SECURITY

THE ROLE OF EDUCATION



Cyber Center for Education & Innovation Fall Symposium

At University of Maryland University College

Thursday, November 8, 2018

8 am–5:30 pm

College Park Marriott Hotel
& Conference Center

umuc.edu/cyberINsecurity

CYBER CENTER FOR
EDUCATION & INNOVATION
HOME OF THE NATIONAL CRYPTOLOGIC MUSEUM

UNIVERSITY OF MARYLAND
University College
STATE UNIVERSITY • GLOBAL CAMPUS

MARYLAND STATE DEPARTMENT OF
EDUCATION
PREPARING WORLD CLASS STUDENTS

NATIONAL CRYPTOLOGIC
MUSEUM FOUNDATION

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

SYMPOSIUM CHAIR MESSAGE

Welcome!

We are pleased that you have joined us for “Attacking the Roots of Cyber(In)Security: The Role of Education,” the fall symposium of the Cyber Center for Education & Innovation—Home of the National Cryptologic Museum (CCEI-NCM).

A new report, just released in draft by the National Security Telecommunications Advisory Committee recommends that the United States undertake a “Cybersecurity Moonshot” to harness the power of government, industry, and academia to “fundamentally transform the security of our digital landscape” and attack the roots of cyber insecurity. The draft report calls out STEM and cybersecurity education as one of the pillars of the strategic framework of the Moonshot initiative noting the shortage of skilled cyber professionals in the workforce.

The cybersecurity skills gap, its persistence, and its implications for the nation are well documented. The urgent question is: Why does this state of affairs exist? Normally, the market solves labor shortages through rising wages and educational institutions respond by offering programs that increase the supply of in-demand workers. In response to the demand, students are drawn to and prepared for these careers. Over time, the market reaches a dynamic equilibrium where supply meets demand. But this does not seem to be happening in the cyber workplace. If anything, the cybersecurity skills gap is growing both in terms of an insufficient number of new professionals and their level of skills.

Hosted by University of Maryland University College, this symposium will focus on some of the fundamental challenges of cybersecurity education and workforce development and how they might be addressed. It includes the perspectives of senior industry leaders, policy makers, employers, faculty, and students, who will focus on how powerful new technologies might be used to boost the talent pipeline, meet the demand for cybersecurity professionals, and help the nation achieve a sustainable equilibrium.

All of today’s sessions will be recorded and made available to the public at **umuc.edu/cyberINsecurity**. The proceedings resulting from this symposium will contribute greatly to the knowledge and understanding of the broad and evolving field of cybersecurity.

Very respectfully,

MG Roderick Isler (U.S. Army, Ret.)
Vice President, CCEI-NCM Campaign

Thursday, November 8, 2018

9:00 am Opening Program

Master of Ceremonies
Mr. Mark Loepker
Senior Advisor, Education Lead, CCEI-NCM

Welcome
President Javier Miyares
University of Maryland University College

Symposium Honorary Chairman
MG Roderick Isler (U.S. Army, Ret.)
Vice President, CCEI-NCM Campaign

9:30 am Morning Keynote

GEN Dennis Via (U.S. Army, Ret.)
Introduced by MG Roderick Isler, U.S. Army, Ret.)

Dennis Via is an Executive Vice President and Defense Fellow with Booz Allen Hamilton in McLean, Virginia, where he is a member of the Global Defense Leadership Team. He recently retired from the U.S. Army as a four-star general. In his last assignment, he led the largest global logistics command in the U.S. Army and Department of Defense (DoD), comprising 120,000 military and civilian employees in 38 countries and 41 states, with an annual budget of $50 billion.

As the commander of Army Materiel Command (AMC), he was directly responsible for all logistics, information technology, foreign military sales, and industrial base operations for the U.S. Army.

Prior to his promotion and assignment as the AMC commander, he was assigned as the command's deputy commander, where he deployed to Southwest Asia in October 2011 to manage the strategic integration of the retrograde of equipment and materiel out of Iraq after the conclusion of combat operations. Prior to this appointment, he was assigned as a director on The Joint Staff, Pentagon, where he was a direct report to the Chairman Joint Chiefs of Staff for all policies, plans, and programs for DoD communications, information systems, and cybersecurity.

General Via served 12 years as a general officer and is the first Signal Corps Officer in U.S. Army's 242-year history to achieve the rank of four-star General. He is a member of the Council on Foreign Relations, the Association of the United States Army, and the Armed Forces Communications—Electronics Association.

10:30 am Break

10:45 am Panel 1: Building the STEM Pipeline: The Student Perspective

A recent study by the National Cyber Security Alliance explored the talent shortfall in the global cybersecurity industry and found that a fundamental problem was the lack of even a basic awareness of potential opportunities in the field. Most students learn about careers during their formative high school years and, unfortunately, many do not receive any insight on how to pursue a cyber career. Most haven't met or spoken with a practicing cybersecurity professional or have any real knowledge of what these individuals do.

In discussing initiatives to address this problem, we often hear from educators and academics who develop policy and design courses, but what are the perspectives of the students who actually participate in these STEM tracks? In this panel we will hear from students from both high school and college who engaged in STEM-related courses of study and explore their motivations, experiences, and recommendations for improvement.

Moderator

Dr. Karen Salmon
Superintendent, Maryland State Department of Education

Panelists

Ms. Ipshita Bhatnagar
Senior, Damascus High School, Montgomery County

Mr. Antwan King
UMUC Alumnus (MS, Digital Forensics and Cyber Investigation)

Mr. Daniel Liscinsky
Bachelor's Degree Student in Computer Science (Cybersecurity Minor),
University of Maryland, College Park

Mr. Khari Thomas
Associates Degree Student, Howard Community College

Ms. Selena Xiao
Senior, Wootton High School, Montgomery County

12:00 pm Luncheon

Buffet lunch available in the Main Foyer

CCEI and the National Cryptologic Museum

MG Roderick Isler (U.S. Army, Ret.)
Vice President, CCEI-NCM Campaign

Mr. Larry Castro
Chief Operating Officer, CCEI-NCM

Education Week Research Center/Consortium for School Networking Survey

Mr. Benjamin Herold
Staff Writer, *Education Week*

1:15 pm Break

1:30 pm Panel 2: The Labor Market is Talking. Is Education Listening?

It is well known that the shortage of cybersecurity professionals is a significant and growing problem. A recent study by Integrated Computer Solutions (ICS) concluded that there will be a global shortage of 1.8 million cyber professionals by 2022, while it is elsewhere estimated that U.S. employers alone are struggling to fill almost 300,000 cybersecurity positions this year. One recent survey indicated that cybersecurity salaries are twice the national average and 9 percent more than other IT jobs. With this demonstrated market-driven demand, why isn't our education enterprise doing a better job of meeting it?

In response to the need for cybersecurity professionals, colleges and universities have launched degree programs at all levels, and in an effort to directly address industry requirements, many schools have formed industry advisory boards and have aligned curricula with national initiatives. The National Security Agency Centers of Academic Excellence program shapes cybersecurity degrees and research at more than 230 colleges and universities and the NIST Cybersecurity Workforce Framework—the result of an ongoing collaboration of government, industry, and academia—identifies cybersecurity functions, specializations, and job roles, and related knowledge, skills, and abilities. More recently, a collaboration of universities and the major computing societies has referenced these initiatives while defining cybersecurity as an academic discipline and developing curricular guidelines for academic programs.

Despite these efforts, supply still lags demand. Why? In a market-driven supply-and-demand economy, we normally expect rising prices and increasing demand to result in more supply. So why are we not producing more cybersecurity professionals? Additionally, employer surveys continue to suggest that a significant percentage of new cybersecurity graduates are not "qualified" or "job ready." Does industry's assessment of new college graduates reflect inherent weaknesses in cybersecurity degree programs, or does it signal a misunderstanding of what a college STEM graduate brings to the workplace and a failure to invest in more employee training? Could the cybersecurity workforce shortfall represent a deeper problem? Are the inherent problems with our cyber infrastructure so basic and systemic that there will never be enough qualified and trained workers to fill industry's needs?

This panel of experts will explore the supply and demand sides of the cyber-shortage issue and discuss whether we have a problem that is solvable on our current track or whether some new and revolutionary approach is required.

Moderator

Dr. William E. "Brit" Kirwan
University System of Maryland Chancellor Emeritus

Panelists

Ms. Candy Alexander
President, International Board, Information Systems Security Association (ISSA)

Dr. Diane Burley
Executive Director and Chair of the Institute for Information Infrastructure Protection (I3P) and professor of Human and Organizational Learning at The George Washington University

Ms. Mary Ann Davidson
Chief Security Officer, Oracle

Ms. Michele Mullen
Executive Director, Canadian Committee on National Security Systems (CCNSS) and External Compliance

2:45 pm Break

3:00 pm Panel 3: New Technology, STEM Education, and the Cybersecurity Moonshot

Given our current state—described by the two previous panels and speakers—what is the future of cybersecurity education? As we increase the size of the educational pipeline, how can we make it more efficient? New technology tools such as artificial intelligence (AI), big data, the cloud, and augmented reality (AR) are becoming powerful forces in other areas and might be applied to help address problems in K–20 education, including science, technology, engineering, and mathematics (STEM). Google has already demonstrated the ability of natural voice AI "assistants" to simulate human-to-human interactions, and AR can place students in realistic settings that enable hands-on or project-based learning. Big data and the cloud make enormous amounts of information available to students and teachers. As technology develops, these tools will inevitably become more powerful, flexible, and less expensive to use—and thus more attractive to the educational enterprise. If our nation commits to a recently announced presidential "Cybersecurity Moonshot," how might advanced technology improve STEM and cybersecurity education and, in turn, attack the roots of cyber insecurity? This panel of experts will discuss how they view the future of education and the ways in which technology might be leveraged to improve such effective personalized learning—both in the classroom and online.

Moderator

Dr. MJ Bishop
Inaugural Director, Center for Academic Innovation,
University System of Maryland

Panelists

Dr. Matt Gaston
Director, Emerging Technology Center,
Software Engineering Institute, Carnegie-Mellon

Mr. Benjamin Herold
Staff Writer, *Education Week*

Dr. Dee Kanejiya
Founder and CEO, Cognii

Ms. Rachel Zimmerman
Deputy Commissioner, CyberPatriot

4:20 pm Closing Keynote

Ms. Cindy Widick
Chief, Cybersecurity Operations Group
NSA/CSS Cybersecurity Operations Mission Manager (CSOMM)
Introduced by MG Roderick Isler, (U.S. Army, Ret.)

Ms. Cynthia L. Widick is chief of the National Security Agency/Central Security Service's (NSA/CSS) Cybersecurity Operations (CSO) Group in the Operations Directorate where she leads integrated cybersecurity operations to enable high impact operational efforts in the cyber domain and deny adversaries the ability to influence, exploit, or threaten cyber and information infrastructure domains within the bounds of our authorities.

Ms. Widick enlisted in the U.S. Army in 1975 as a Russian voice intercept operator with the Army Security Agency and was stationed in Germany until 1978 when she separated from active duty. After completing her college degrees, she was commissioned in 1983 as an ensign in the U.S. Navy via Officer Candidate School, Newport, Rhode Island as a cryptologic officer. Her assignments included staff, headquarters, sea, and shore tours. Her last six years on active duty, she was assigned to NSA where she worked with the Information Assurance team and Computer Network Operations.

In January 2010, Ms. Widick joined NSA/CSS's Defense Intelligence Senior Executive Service as NSA/CSS Threat Operations Center (NTOC)'s chief of operations where she established its Operations Center, a dynamic, 24/7/365 national-level cyber-focused operation, working in partnership with the U.S. Cyber Command, FBI, DHS, and other U.S. government agencies. In 2013, Ms. Widick became the SID chief of staff until 2015 when she was appointed the director of NTOC until implementation of NSA21 in August 2016, when she became the chief for Cybersecurity Operations.

Ms. Widick attended Southern Illinois University, receiving a BA in Russian Language (1981) and a Master of Business Administration (1982).

5:20 pm Closing Remarks

SYMPOSIUM ORGANIZERS

The Cyber Center for Education & Innovation (CCEI), Home of the National Cryptologic Museum (NCM) is a private-public partnership of the National Cryptologic Museum Foundation (NCMF) and the National Security Agency, formed under federal legislative authority. The NCMF is engaged in a campaign to finance, build, and equip the CCEI-NCM, scheduled to open in 2021 subject to funding availability. In addition to holding the exhibits, papers, and artifacts of the cryptologic community, the CCEI-NCM will offer a state-of-the art conference and meeting venue and will conduct a range of educational programming related to cybersecurity and cryptology. University of Maryland University College (UMUC), a leader in cybersecurity education, has been selected by the NCMF to lead the facilitation, coordination, and development of CCEI-NCM education and training initiatives.

About NCMF

The not-for-profit National Cryptologic Museum Foundation (NCMF) and the National Security Agency (NSA) established a private-public partnership under federal legislative authority to create the Cyber Center for Education & Innovation (CCEI), Home of the National Cryptologic Museum (NCM) facility at Fort Meade, Maryland. The CCEI-NCM will launch a cross-sector enterprise encouraging governments, industry, and academia to share insights, knowledge, and resources to strengthen cybersecurity protection across U.S. critical infrastructure.

About UMUC

University of Maryland University College (UMUC) was founded more than 70 years ago specifically to serve the higher education needs of working adults and U.S. military servicemembers. Today, UMUC continues that tradition online and on-site, offering more than 90 degrees, certificates, and specializations backed by the reputation of a state university and the University System of Maryland. For more information, visit umuc.edu.

SUPPORTING ORGANIZATIONS

Maryland State Department of Education

National Cryptologic Museum Foundation (NCMF)

National Initiative for Cybersecurity Education (NICE)

National Security Agency (NSA)

The CCEI Fall Symposium is an affiliated event of CyberMaryland 2018.

SYMPOSIUM COMMITTEE

Symposium Chair

MG Roderick Isler (U.S. Army, Ret.)
Vice President, CCEI-NCM Campaign

Program/Organizing Committee Chair

Lt. Gen. John Campbell (U.S. Air Force, Ret.)
Senior Advisor, CCEI-NCM

Symposium Program Committee

Dr. Lynne Gilli
Assistant State Superintendent for the Division
of Career and College Readiness,
Maryland Department of Education

CAPT William Gravell (U.S. Navy, Ret.)
President, Diogenes Group, LLC

RADM Betsy Hight (U.S. Navy, Ret.)

Mr. Robert Lentz
President and Chief Executive Officer,
Cyber Security Strategies

Lt. Gen. Harry D. Raduege Jr. (U.S. Air Force, Ret.)
Senior Counselor to the Cohen Group

Mr. Marcus Sachs
Chief Security Officer
Pattern Computer

Mr. Richard C. Schaeffer Jr.
President, National Cryptologic Museum Foundation

Dr. Gregory Von Lehmen
Special Assistant to the President, Cybersecurity, UMUC

Symposium Organizing Committee

Ms. Kat Bugg
Assistant Vice President, Communication & Events, UMUC

Mr. Larry Castro
Chief Operating Officer, CCEI-NCM

Mr. Sheran Fernando
President, Fernando Partners

Mr. Michael Freedman
Senior Vice President, Office of Communications, UMUC

Mr. Alex Kasten
Media Relations Specialist, UMUC

Mr. Mark Loepker
Senior Advisor, Education Lead, CCEI-NCM

Mr. Bob Ludwig
Assistant Vice President, Media Relations, UMUC

Mrs. Carol Stromberg
Executive Administrator, CCEI-NCM

Additional thanks to Jordan Schneyer, Christopher Spriggs, Chip Cassano, Angela Hutchison, Angela Grant, Jillian George, Avi Feinberg, Marquita Friday, Scott Nichols, and Lena Thompson for their expertise and support of this symposium.

umuc.edu/cyberINsecurity

Cyber Center for Education & Innovation Fall Symposium

At University of Maryland University College

CYBER CENTER FOR
EDUCATION & INNOVATION
HOME OF THE NATIONAL CRYPTOLOGIC MUSEUM

UNIVERSITY OF MARYLAND
University College
STATE UNIVERSITY • GLOBAL CAMPUS

MARYLAND STATE DEPARTMENT OF
EDUCATION
PREPARING WORLD CLASS STUDENTS

NATIONAL CRYPTOLOGIC
MUSEUM FOUNDATION

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA