2017 - 2018 ANNUAL REPORT

NATIONAL CYBERWATCH CENTER

www.nationalcyberwatch.org



ANNUAL REPORT 2017-2018

Cybersecurity Education Solutions for the Nation



Hard copies of this Annual Report can be ordered by contacting us at: *info@nationalcyberwatch.org*. In addition, electronic copies are available here: *library.nationalcyberwatch.org*

TABLE OF CONTENTS

EXECUTIVE DIRECTOR'S MESSAGE	04
MAJOR EFFORTS	05
Culture of Collaboration	05
National Curriculum	05
National Curriculum Standards	05
Competency-Based Education Curriculum	06
Complete Cloud-Based Lab Solution	06
Innovations in Cybersecurity Education	07
2017 Community College Cyber Summit (3CS)	80
Membership	09
Mid-Atlantic Collegiate Cyber Defense Competition	09
2017 National Cyber League (NCL) Seasons	10
Digital Press	11
Webinar Series	11
National Cybersecurity Student Association	12
Scholarship for Service, 2/4-Year Pathways	12
National Centers of Academic Excellence Leadership	13
TOWARD THE FUTURE	13
Programs, Services, and Partnerships	13
Apprenticeships/Residencies	14
Educational, Training, and Assessment Standards	14
Evidence-Based Practices	14
Competency-Based Mastery Learning Curriculum	15
New Certificate Programs	15
NATIONAL CYBERWATCH CENTER TEAM	16

EXECUTIVE DIRECTOR'S MESSAGE



Dear Colleagues,

2017 was a banner year for attackers, who operated without regard for geography, industry vertical, or victim: Ransomware (WannaCry, Petya/NotPetya), leaked government tools (NSA, CIA), continued lack of privacy protections for consumers (Equifax, Yahoo, votor records), campaign hacking (Macron)...the list goes on.

Lawmakers are proposing needed legislation; consumer and corporate awareness is at all-time highs; and advances in Machine Learning and Artificial Intelligence applied to Information Security (IBM Watson for Cyber Security) show promise at decreasing the asymmetric threat.

Amid this fast-moving and evolving landscape, the National CyberWatch Center (NCC) continues to innovate, leverage its 12+ years of experience, and tap into its unique networks and partnerships as the go-to organization for cutting-edge, replicable, and cost-effective educational and workforce development solutions. A sample of these efforts included:

- Development of Cybersecurity Education Curriculum Standards for the new generation of Information Security specialists
- Application of recent advances in Learning Science to innovate the conception, design, and delivery of cybersecurity education
- Creation of skills-based instructional content available in our partnered Cloud-Based Lab platform
- Unveiling of the Innovations in Cybersecurity Education awards and recognition program

These successes would not have possible without the support of our academic network of excellence (over 300+ higher education institutions and faculty), students, industry and government partners, the dedicated NCC team, and the senior leadership team at Prince George's Community College. We are also grateful for the ongoing support of our National Science Foundation Program Officers, Dr. Corby Hovis and Dr. Victor Piotrowski, as well as our National Visiting Committee members.

While the challenges in Information Security remain daunting, rest assured that NCC will do its part to promote and provide educational and workforce planning and development solutions that make a difference. Our evolving programs and services will continue to incorporate "ground truth" practices that increase the maturity of cybersecurity capabilities in individuals and organizations so essential to the reliability and effectiveness of our critical infrastructure and national security.

Sincerely,

Casey W. O'Brien Executive Director & Principal Investigator, National CyberWatch Center

18 Annual Repo

MAJOR EFFORTS

CULTURE OF COLLABORATION

Effective collaboration means developing and maintaining responsive, cooperative, mutually beneficial, and ethical internal and external relationships that nurtures diversity, promotes the success of our partners, and sustains the NCC mission. Representative activities included:

- Partnering with the Dept. of Homeland Security (DHS) during October's National Cyber Security Awareness Month
- Participating in the NSF-funded Regional Center for Nuclear Energy and Training (RCNet) Workshop on Automation: Adapting to the Changing Nature of Work
- Briefing the U.S. Senate Career & Technical Education (CTE) Caucus
- Participating in the 31st IBM Security Summit panel presentation: Opening the Aperture: How New Collar Workers Can Help Enterprises Address Growing Threats and Attack Vectors
- Sponsoring the Women in Cybersecurity (WiCyS) Conference

NATIONAL CURRICULUM

NCC continues to develop and promote its reference curriculum degrees and certificate programs in Cyber Defense, Network Security Administration, Network Forensics, Secure Software Development, and Systems Security Administration, as well as work with academic institutions to implement new programs, or update existing ones.

To view the range of curricular offerings and benefits of adopting this content in both educational and training programs, see National CyberWatch's Information Security Curricula Guide: A Complete Solution for Higher Education Institutions:

https://www.nationalcyberwatch.org/resource/ curriculum-guide

NATIONAL CURRICULUM STANDARDS FOR CYBER EDUCATION

In 2016, the NCC Curriculum Standards Panel was established to identify the learning objectives, concepts, procedures, situational judgments, and intellectual abilities required to develop capability and maturity in cybersecurity foundational principles, techniques, tactics, and protocols. The standards produced by the NCC Curriculum Standards Panel are the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs.

COMPETENCY-BASED EDUCATION CURRICULUM

In 2017, the standards panel architecture and mission were extended to develop course-specific standards panels to advance the models of instructional design used in cybersecurity education. Each standard course panel will develop a competency-based, mastery learning curriculum library. Competency-Based Education curriculum substantively differs from traditional instructional techniques used in most cybersecurity education and training programs today by increasing the cybersecurity capability and maturity of the entrant and incumbent Information Technology workforce. By embedding assessments of capability maturity at each step of the learning process, readiness for instructional material is increased, thereby accelerating and deepening the comprehension or transfer of instructional material.

For more information on these efforts to-date, see the *Mapping of the National CyberWatch Center's Curriculum* to National Workforce Competency Requirements Report: https://www.nationalcyberwatch.org/resource/mappingnational-cyberwatch-centers-curriculum-national-workforce-competency-requirements

COMPLETE CLOUD-BASED LAB SOLUTION

NCC's partnered lab solution provides a hands-on, scalable, and customizable virtual lab platform that supports skill development in any degree, certificate, or training program. The virtual lab platform provides an unmatched turnkey solution with real-world tools and technologies.



Hands-on labs support skill development in the following domains:

- Digital Forensics
- Ethical Hacking & Systems Defense
- Hadoop Administration
- Information Security Fundamentals
- Linux Server I: Linux Fundamentals
- Linux Server II: System Administration
- Networking Fundamentals
- Network Security
- Pentesting & Understanding Vulnerabilities
- Scripting Fundamentals

To learn more, go to: lab.nationalcyberwatch.org

INNOVATIONS IN CYBERSECURITY EDUCATION AWARDS & RECOGNITION PROGRAM

NCC is committed to providing a robust collaboration platform that supports an informed community of interest in cybersecurity education. A symbol of this commitment was the launch of the annual Innovations in Cybersecurity Education program.

Forty-four submissions were received and reviewed last spring by a panel of peers, and five uniquely creative ideas were selected for special recognition at the 2017 Community College Cyber Summit (3CS). All submissions form the foundation of a treasure trove of ideas that will ensure that the proverbial wheel stops being reinvented, that creative ideas are celebrated, and that cybersecurity education keeps up with advances in tactics, techniques, and procedures.

The 2017 Innovations in Cybersecurity Education winning entries were:

- Curriculum Category: Cyber Warrior Princess Cyberher Education for Girls: Rebecca Onuskanich
- Faculty Development Category: Free E-Book: Framework for SCADA Cybersecurity: Stephen Miller
- Lab Activity Category: Network Defender Threat Hunting Honors Project: Andrew Rozema
- Local Partnership Category: Providing Students Hands-on Experience and Volunteerism Through Work with Nonprofits: Denise Pheils
- Student Learning Aid Category: Carefully Combining Strategies has a Big Impact on Cybersecurity Education for the Youngest Learners: Rebecca Hoffart

View the full 2017 Innovations in Cybersecurity Education booklet: https://www.nationalcyberwatch.org/resource/2017-innovations-cybersecurity-education



2017 COMMUNITY COLLEGE CYBER SUMMIT (3CS)

The 3CS provides a forum to share effective practices, eliminate duplication of effort, and coordinate, standardize, and proselytize various educational and training initiatives effectively impacting ever-important workforce challenges. The 3CS also ensures that the community college "voice" is heard in the national dialogue, that the pathways between two-year and four-year programs are aligned, curriculum standards now being shaped have strong community college input, and that the student pipeline is filled and workforce shortages are abated.



The fourth annual 3CS was held June 28-30, 2017 at Prince George's Community College in Largo, MD and the National Harbor. Highlights included:

- Participation from 600+ educators, students, industry representatives, and government partners
- Presentations and hands-on workshops focused on the Summit's theme, Strengthening our Cyber IQ
- Launch of the 3CS Job Fair: a successful first step toward building stronger bridges between community colleges and industry, preparing students more effectively for the workforce, and addressing the national need for a strong cybersecurity workforce
- Unveiling of the Innovations in Cybersecurity Education awards and recognition program

"Informative and fun. Great opportunity for meeting peers." -Jimmy Hargrove **"Great experience and networking opportunities."** -Kimberly Terry

The 2018 3CS will take place August 2-4, 2018 at Mt. Hood Community College in Portland, OR. This year's theme is *Expanding Expertise: Transforming Cybersecurity Programs*.



MEMBERSHIP

NCC members continue to play a unique and powerful role in shaping cybersecurity education, workforce development, and emerging issues in research, assessment, and evaluation. NCC provides varied opportunities for members to engage directly with NCC's staff, programs and events, as well as with established and emerging leaders in Information Security.

Last year saw the launch of a new Membership program for Corporations and Individuals, the adoption of an Association Management Software platform, a Member's only portal, as well as increased growth of the NCC Academic Membership base:

- Current total number of members: 385
- Number of community college (institutional) members: 167
- Number of states with community college (institutional) memberships: 43
- Number of university (institutional) members: 124 (2 international)
- Number of states with university (institutional) memberships: 40 plus District of Columbia

MID-ATLANTIC COLLEGIATE CYBER DEFENSE COMPETITION (MACCDC)

The 12th MACCDC Regional Finals was held March 30-April 1, 2017 at the Johns Hopkins University Applied Physics Lab in Laurel, MD. Teams competed in Man Vs. Machine. An Internet of Things (IoT) middleware development company, We-B-Smart, learned that their network experienced several intrusions over several months. This affected their reputation as a company that develops secure connected applications and smart products. The sources of the intrusions were unknown; however, it was suspected that a competing company, Reds-R-Us, launched a cyber-espionage campaign designed to ruin We-B-Smart's reputation in the industry and obtain control of their intellectual property. It was further speculated that the attacks were orchestrated into a complex system that functioned without human interaction.

2017 Final Regional Team Standings:

- 1. University of Maryland, Baltimore County
- 2. University of Maryland
- 3. Towson University
- 4. Drexel University
- 5. Liberty University
- 6. Wilmington University
- 7. Frederick Community College
- 8. Delaware Technical Community College



The University of Maryland Baltimore County team represented the Mid-Atlantic Region in the National CCDC, April 13-15, 2017 in San Antonio, TX and went on to best nine other teams to win the 2017 National Championship.

2017 NATIONAL CYBER LEAGUE (NCL) SEASONS

Now in its seventh year, the NCL is a defensive and offensive puzzle-based, Capture-the-Flag cybersecurity competition. NCC was a founding sponsor of the NCL and continues to provide support, marketing, and leadership. Its virtual training ground helps high school and college students prepare and test themselves for cybersecurity challenges that they will face in the workforce. All participants play the games simultaneously during the Preseason, Regular Season and Postseason, as both individuals and in teams.

The NCL ran its first full spring season in 2017. Building on past successes from its fall seasons, the spring season mimicked the fall season schedule of events and provided participants opportunities to develop and validate knowledge and skills, year-round.

The 2017 fall season was by far the largest event the NCL has run and included:

- Record numbers of participants (3,449)
- New game challenges
- Integrated preparatory lab exercise platform (AKA NCL Gymnasium) and game environment (AKA NCL Stadium), powered by Cyber Skyline
- New registration system
- Weekly Facebook Live sessions with the NCL Commissioner
- Sample challenges with prizes via NCL Social Media (Facebook, Twitter)
- Individualized Competency Profiles (AKA Scouting Reports) for participants from Preseason and Regular Season play



ACL excited, frustrated and engaged my students to the point they showed up early to class to participate!"

-Donald Wingate, Creekside High School

When you learn this stuff in the lab, it's in ideal conditions. You are given the perfect command to get the perfect result on the perfect target.

Unfortunately, the real world isn't perfect. When you play NCL, you have to apply your skills and knowledge on a less than ideal target. You have to learn, adapt and figure out how to make it work no matter the obstacles. You gain a deeper understanding of what you are doing in a real and applicable situation. I've never understood what the commands I was running would do in a lab, but in NCL I gained a mastery of skills to apply in any situation I encounter while working as a cybersecurity professional."

-Kaitlyn Bestenheider, NCL Player

DIGITAL PRESS

The following publications were published through the NCC Digital Press, which produces and disseminates collections of timely publications related to cybersecurity education:

- Resource Guide: A Guide for Mapping Courses to Knowledge Units (KUs) Version 2, Dr. Fred Klappenberger
- White Paper: Analysis of Third and Fourth Year Undergraduate Cybersecurity Curriculum, Dr. Jim Hoag
- Report: Mapping of the National CyberWatch Center's Curriculum to National Workforce Competency Requirements, Dr. David Tobey
- National CyberWatch's Information Security Curricula Guide: A Complete Solution for Higher Education Institutions, Casey W. O'Brien
- Innovations in Cybersecurity Education booklet



WEBINAR SERIES

Now in its fifth year, the Webinar Series promotes the transfer of innovative, cost-effective, and sustainable cybersecurity education and workforce development solutions.

2017 topics included:

- Jan. 26 Critical Infrastructure Cybersecurity Course
- Apr. 19 Automotive Cybersecurity Module
- Oct. 26 Losing the Privacy War
- Nov. 30 Closing the Cybersecurity Skills Gap

2018 topics include:

- Jan. 25 2030: Building a Diverse Cybersecurity Workforce
- Feb. 22 Cultural Change that Sticks: Driving a Culture of Security Through Design Thinking
- Apr.26 The Relationship Cyber Leader: Because People Do Business with People They Like
- Nov. 29 Machine Learning & Cybersecurity

NATIONAL CYBERSECURITY STUDENT ASSOCIATION

With a focus on growing Student Chapters, forging industry and professional association partnerships, and completing the Member Portal, the National Cybersecurity Student Association continues to fulfill on its vision of cultivating a national community that supports students in their cybersecurity endeavors through extracurricular activities, career opportunities, mentoring, and keeping them at the forefront of cybersecurity trends.

For more on how you can support the National Cybersecurity Student Association, see www.cyberstudents.org

The National Cybersecurity Student Association portal contains lots of technical and business resources for students, as well as a job portal that could help them launch their careers."

-Mark Krzyszkowski, Information Security Instructor Waukesha County Technical College

SCHOLARSHIP FOR SERVICE, 2/4-YEAR PATHWAYS

The Scholarship for Service (SFS) Pathways project has placed NCC squarely in the middle of the discussion between 2- and 4-year academic institutions as they grapple with ways to re-enforce the workforce pipeline through aligned efforts. To-date, results have helped universities understand community college degree programs and ways to encourage exploration of alternate paths beyond the SFS traditional Computer Science degree domain. Going forward, NCC will be an indispensable element in the scholarship discussions of great interest to Congress, as well as a strong starting point for distributed apprenticeship discussions thanks to the experience gained in grant matching and institutional support to both 2- and 4-year organizations. 15 universities and 25 community colleges are participating in the effort; a research workshop was held at the National Harbor, MD in June 2017, and a second is planned for August 2018 in Portland Oregon.



NATIONAL CENTERS OF ACADEMIC EXCELLENCE IN CYBER DEFENSE (CAE-CD) LEADERSHIP

Over the years, NCC has developed a comprehensive support and technical assistance system for institutions that need to re-designate as CAEs, as well as those intending to apply for the first time. In recognition of its leadership role in the CAE program, the NCC was selected by the National Security Agency (NSA) as a CAE Regional Resource Center (CRRC), with the express purpose of continuing to lead efforts to improve and expand cybersecurity education in the National Capital Region (Delaware, Maryland, and Washington, D.C.).

The goal of the National Capital Region CRRC is to reduce vulnerabilities in our national infrastructure by continuing to promote effective practices in Information Security education and workforce development. The continued growth and improvement of academic institutions running cybersecurity programs will result in qualified technicians and professionals. See *crrc.nationalcyberwatch.org* for more information on the Capital Region CRRC goals and activities.

TOWARD THE FUTURE

NCC will continue to pursue initiatives that impact cybersecurity education, training, and workforce development, while continuing to support and grow its network of educators, students, industry leaders, and government organizations that support technical education in the U.S. The following strategic programs and services provide a sample roadmap for future NCC work:

PROGRAMS, SERVICES, AND PARTNERSHIPS DESIGNED TO ATTRACT LARGE NUMBERS OF DIVERSE POPULATIONS

NCC has partnered with the following organizations committed to diversity in both academic and workforce settings:

- International Consortium of Minority Cybersecurity Professionals (ICMCP)
- Institute for Women in Trades, Technology and Science (IWITTS)
- WB&B Executive Search
- Women in Cybersecurity (WiCyS)

NCC and its members benefit directly from these partnerships by getting access to resources that increase the number of female students in cybersecurity programs; scholarship money for underserved students; discounts on national conferences; and effective practices bridging the diversity gap.

APPRENTICESHIPS/RESIDENCIES

"Apprenticeships are a tried and true workforce development strategy that have paid dividends for companies who use the program. Employers who utilize apprentices report higher productivity, higher retention rates, and a substantial return on investment. As the economy continues to grow, business leaders across all industries are in the best position to tell their success stories: that apprenticeships fulfill their need to create a pipeline of skilled workers to help them take their companies to the next level." - Department of Labor

NCC is exploring Apprenticeship/Residency models that allow it to provide access to large numbers of students and faculty from its Academic Member network, while partnering with organizations that offer apprenticeship opportunities. Initial funding for pilots could come from government organizations (e.g., Dept. of Labor, NSF), with industry sponsoring the program as it evolves.

EDUCATIONAL, TRAINING, AND ASSESSMENT STANDARDS

The standards produced by the NCC Curriculum Standards Panel are the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks (e.g., NSA CAE Knowledge Units; National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) Knowledge, Skills, and Abilities (KSAs)), and industry needs.

Curriculum Standards Panel activities include:

- Integrating validated assessments, instruction, practice labs, and challenge scenarios to improve cybersecurity talent management in organizations
- Raising learner capability maturity in foundational cybersecurity concepts, principles, and practices

EVIDENCE-BASED PRACTICES FOR MODEL CURRICULUM DEVELOPMENT

NCC's Cybersecurity Core Curriculum Standards apply evidence-based principles established through the empirical study of effective practices in competency-based learning to continually evaluate, enhance, and develop model curriculum for cybersecurity education. Eleven practices were identified as necessary to design curriculum that is valid and reliable for maturing job- and career-ready capabilities of program graduates. Each of these eleven practices will be applied in producing the NCC curriculum standards. These evidence-based practices will be replicated within each course design process. The result is a multiphase, technology-supported, agile development process that permits simultaneous development of courseware.

COMPETENCY-BASED MASTERY LEARNING CURRICULUM: INFORMATION SECURITY FUNDAMENTALS COURSE

The current project, funded by a grant from the NSA (#H98230-17-1-0287), will apply psychometrically-valid, competency-based instructional design techniques to develop the model domain taxonomy, assessment items, instructional content, and the sequencing plan for that content necessary to overcome constraints to developing mastery of the fundamentals of Information Security.

A prototype implementation of the formative, competency- and performance-based curriculum development process for a single course, Fundamentals of Information Security, is well underway.

For more on NCC's Competency-Based Mastery Learning Curriculum and how you can get involved, see: *https://www.nationalcyberwatch.org/cbe*

NEW CERTIFICATE PROGRAMS

These specialized and stackable certificates allow students to earn multiple academic certificates while pursuing their degrees and to earn industry credentials by sitting for industry-recognized professional certification exams.

Look for new Certificates in the following areas:

- Security Operations
- Cyber Threat Intelligence
- Cloud Security



NATIONAL CYBERWATCH CENTER TEAM

The NCC team has benefited from continuity in leadership over the past 13 years, as well as from recruiting new subject matter experts who bring an infusion of new energy and varied perspectives. The 2017-2018 NCC Team includes:

Casey O'Brien Executive Director & Principal Investigator Prince George's Community College Maryland

Dr. Vera Zdravkovich

Senior Advisor Prince George's Community College Maryland

Dr. Costis Toregas

Senior Advisor Director, Scholarship for Service Four-Year George Washington University Washington, D.C

Dr. Barbara Belón

Director, Member Services Director, Scholarship for Service Two-Year Belón Research & Practice Pennsylvania

Michael Burt

Virtual Lab Manager Prince George's Community College Maryland

Dr. David Tobey

Director, Research & Assessments Co-Principal Investigator Indiana University South Bend Indiana

Dr. Bob Spear Senior Advisor Director, Community College Cyber Summit Prince George's Community College Maryland

Fran Melvin Director, Finance Center Manager Prince George's Community College Maryland

Anita Shelton Administrative Associate Prince George's Community College Maryland

Gus Hinojosa

Director National Cybersecurity Student Association Arizona

Dr. Margaret Leary

Senior Advisor Co-Principal Investigator Northern Virginia Community College Virginia

Lewis Lightner

Director, Operations & Programs Competition Director, MACCDC BrightPath Technology North Carolina

John Sener

External Evaluator Sener Knowledge Maryland

Lynn Dohm Director Marketing & Communications Nelly Group Illinois

Dr. Beth Hawthorne Senior Advisor

Union County College New Jersey

NATIONAL VISITING COMMITTEE (NVC)

The Advanced Technological Education (ATE) program supported by NSF funds projects to improve technological education at the undergraduate and secondary school levels. The goal of the program is to produce more technicians to meet workforce demands and improve the technical skills and content preparation of these technicians and the educators who prepare them. Most of its grants are made to two-year colleges.

Successful applicants for large grants (funded at \$750,000 or more) are required to appoint a NVC. These committees are groups of advisors that work with grantees and NSF to help them achieve their goals and objectives. They assess the plans and progress of the project and report to NSF and the project leadership. Committee members also provide advice to the project staff and may serve as advocates for effective projects.

In general, NVCs are similar to the advisory committees that are already an integral part of higher education institutions. In fact, most state and federally funded programs for these colleges require a local or regional advisory committee. However, there are differences between these committees and the NVCs. For example, local advisory committees report only to the project leadership who, in turn, set the meeting agendas. The NVCs not only report to the project, but also to NSF. Furthermore, NSF appoints the committee members, and the NVC chairperson plays a major role in setting the agenda.

Nicholas M. Cefaratti Information Security Systems Engineer Harris Corporation Florida

Dr. Corby Hovis

Lead Program Director Directorate for Education and Human Resources National Science Foundation Virginia

Elayne Starkey

Chief Security Officer State of Delaware Delaware

Dr. Philip Crager

Associate Professor of Cybersecurity Department of Security Studies and International Affairs Embry-Riddle Aeronautical University Florida

Dr. Victor Piotrowski

Lead Program Director CyberCorps®: Scholarship for Service (SFS) Division of Graduate Education National Science Foundation Virginia

Georgia Weidman

Founder and CTO Shevirah Inc. Virginia **Dr. Gaby Hawat** *NVC Chair Principal* Catalyst Partners Florida

Corrinne Sande

Director & Principal Investigator CyberWatch West Whatcom Community College Washington

WWW.NATIONALCYBERWATCH.ORG





