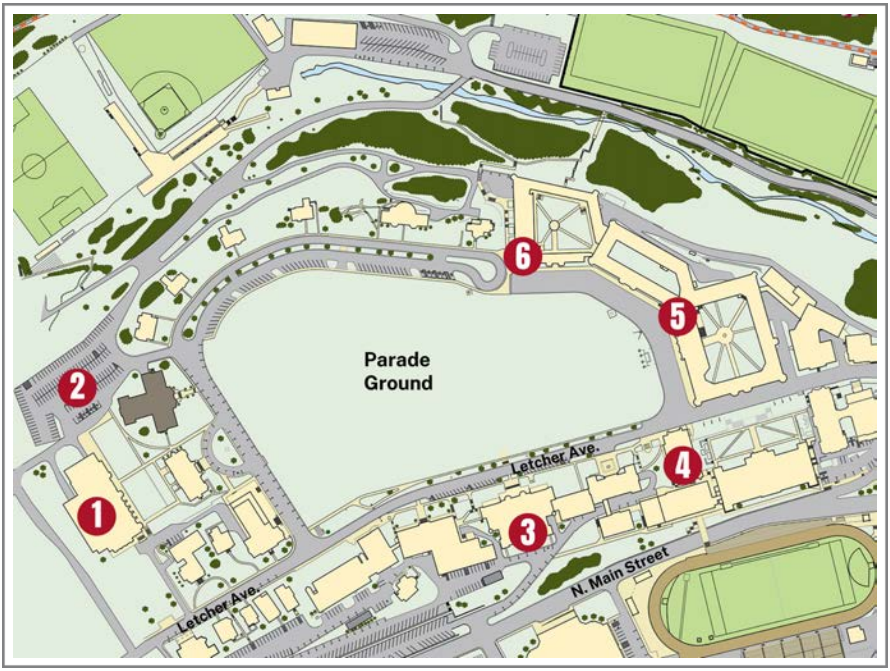
VIRGINIA MILITARY INSTITUTE

CENTER FOR LEADERSHIP & ETHICS



WELCOME TO VMI

1. Marshall Hall, Center for Leadership & Ethics
2. Marshall Hall Parking Lot
3. Preston Library
4. VMI Museum
5. Barracks
6. PX Food Court & VMI Bookstore

PARKING

Please refer to our website for the latest parking announcements. Weather will affect some locations. Main parking is location (2). Follow signs and attendants once arriving on post.

Questions? Please call: Center for Leadership & Ethics at (540) 464-7361

SCHEDULE

MONDAY, AUGUST 2, 2021

7:15 - 7:30 AM ..... Van Shuttles from Hotel to VMI
8:00 - 8:45 AM ..... Registration & Full Breakfast
8:45 - 9:15 AM ..... Welcome & Introductions
9:15 - 10:00 AM ..... Keynote Speaker
10:15 - 11:15 AM ..... Expert Panel
11:15 - 11:30 AM ..... *BREAK*
11:30 AM - 12:30 PM ..... Enabling IoT Vulnerability Analysis
12:30 - 1:15 PM ..... *LUNCH*
1:15 - 5:15 PM ..... Decision Making Exercise
5:15 - 5:30 PM ..... *BREAK*
5:30 - 6:00 PM ..... Competition Instructions
6:00 - 7:00 PM ..... Post Tour by VMI Cyber Captains
7:00 PM ..... Dinner in Downtown Lexington
8:30 PM ..... Van Shuttles back to Hotel

TUESDAY, AUGUST 3, 2021

6:45 - 7:00 AM ..... Van Shuttles from Hotel to VMI
7:00 - 8:00 AM ..... Full Breakfast
8:00 - 12:00 PM ..... CTF Competition
* *Concurrent challenge for observer students during this time*
9:00 - 10:30 AM ..... Faculty Roundtable
* *Moderated discussion on issues, challenges, solutions in cybersecurity education at SMC's*
12:00 - 1:00 PM ..... *LUNCH*
1:00 - 1:30 PM ..... Review of Competition
* *Announcement of Winning Teams*
1:45 PM ..... Van Shuttles from VMI to Airport

SUPERINTENDENT
VIRGINIA MILITARY INSTITUTE

Dear Guests,

Welcome to Lexington and the Virginia Military Institute! We are honored to host the inaugural Senior Military College Cyber Fusion event.

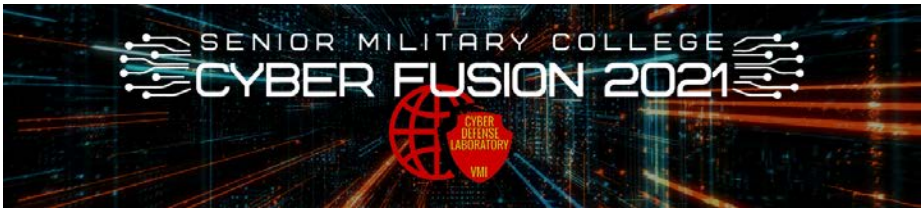
This event is the result of great collaboration. VMI's Cyber Defense Lab, its Department of Computer and Information Sciences, VMI's Center for Leadership and Ethics staff, the Virginia Cyber Range, and the Norwich University Applied Research Institutes have all worked together to produce an event that is truly a fusion of technology and awareness of societal and political forces on cyber security.

I urge each of you to take full advantage of this forum to encourage greater student interest in cyber fields. Enjoy networking with others from our peer institutions who are engaged in the rapidly-developing, transformational technologies that are shaping our society.

We hope you enjoy this event and exploring the many facets of cyber technology. Please take the opportunity to build connections that will serve you now and well into the future.
Again, I wish you a warm welcome and a most productive visit to the Institute.

Best regards from the Institute,

Maj. Gen. Cedrick T. Wins
U.S. Army (Retired)



PARTICIPATING SCHOOLS

NORWICH UNIVERSITY

THE CITADEL

UNG
UNIVERSITY of NORTH GEORGIA
THE MILITARY COLLEGE OF GEORGIA

VIRGINIA MILITARY INSTITUTE

VIRGINIA TECH

KEYNOTE SPEAKER

Dr. Deborah Frincke, *Associate Laboratory Director for National Security Sciences, Oak Ridge National Lab*

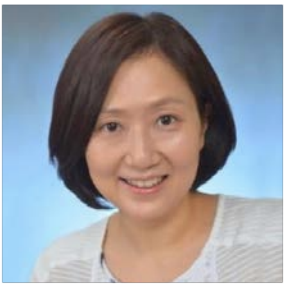
Keynote Speaker

For over two decades, Dr. Frincke has led security-related research and development within organizations both public and private, including two U.S. Department of Energy national labs and the National Security Agency (NSA). She currently guides Oak Ridge National Laboratory's efforts to solve complex threats to America by developing new science as well as leveraging the Lab's broad scientific portfolio, especially cyber, cybersecurity, nuclear and uranium science, high-performance computing, analytics, materials science, and advanced manufacturing. A founding member of the NSA Board of Directors, Dr. Frincke has served on the Intelligence Community Steering Committee for Artificial Intelligence and co-chaired the White House Committee on Economic and National Security Implications of Quantum. She is a U.S. representative to the NATO Emerging and Disruptive Technologies Advisory Board and is an Association of Computing Machinery Fellow. She has received the NSA Distinguished Civilian Service Medal and the USA Presidential Rank Award for Distinguished Executives.

EXPERT PANEL

Panel Moderator

Stephanie Travis is the Director, Senior Military College Cyber Institute at Virginia Tech University. Before her current position, Stephanie spent 10 years on Active Duty in the United States Air Force where she focused small enclave and Air Force-wide cyber security before coordinating cyber security operations across 46 unique Department of Defense organizations. Additionally, Stephanie spent three years as a cyber warfare operations instructor at the US Air Force Weapons School where she focused on cyber tactical integration across all Air Force mission sets. In addition working at Virginia Tech, Stephanie continues to serve in the Maryland Air National Guard.



Expert Panelist

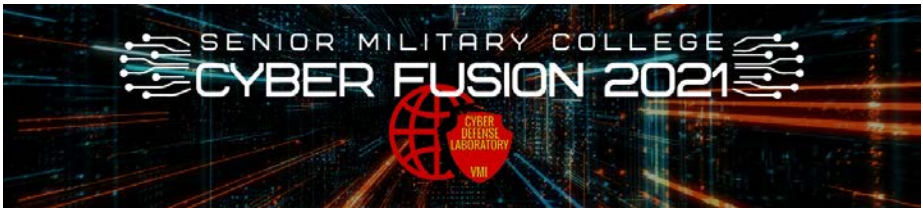
Dr. Jin-Hee Cho is currently an associate professor in the Department of Computer Science at Virginia Tech, since Aug. 2018, and a director of the Trustworthy Cyberspace Lab. Before joining Virginia Tech, she worked as a computer scientist at the U.S. Army Research Laboratory (USARL), Adelphi, Maryland, since 2009. Dr. Cho has published over 150 peer-reviewed technical papers in leading journals and conferences in the areas of trust management, cybersecurity, metrics and measurements, network performance analysis, resource allocation, agent-based modeling, uncertainty reasoning and analysis, information fusion/credibility, and social network analysis. In 2016, Dr. Cho was selected for the 2013 Presidential Early Career Award for Scientists and Engineers (PECASE), which is the highest honor bestowed by the US government on outstanding scientists and engineers in the early stages of their independent research careers. Dr. Cho is currently serving on the editorial board as an associate editor in The Computer Journal, IEEE Transactions on Network Services Management, and IEEE Transactions on Services Computing. She is a senior member of the IEEE and a member of the ACM.

Expert Panelist

Gloria Curry is a cybersecurity professional with 20 years' experience working in DoD. Gloria is currently the Endpoint Team lead within Joint Force Headquarters DoD Information Networks (JFHQ-DODIN). Previously she led the Net Defense team at Army Cyber Command (ARCYBER), and also worked within the Cybersecurity Program Manager's office within US Army Europe (USAREUR). Gloria has also played and coached semi-professional soccer and football. Currently, she is a member of the coaching staff for the Baltimore Nighthawks, a semi-professional women's tackle football team.

FACULTY ROUNDTABLE

Experts from the SMCs will discuss means to incorporate new developments in the field into the classroom. They will



Competition Rules

The Senior Military College Cyber Fusion Capture-the-Flag (CTF) competition is a Jeopardy-style CTF in which teams solve individual challenges of various point values across different categories to score points. The team with the highest point total at the end of the competition will be the winner. If two teams finish with equal point values, the team that first reaches the highest point value will be winner.

- The competition will use a web-based CTF engine hosted by the Virginia Cyber Range. Players will receive instructions on how to self-register on the CTF site and join their team before the competition begins.

- Team members should bring their own laptop computers for the competition and may use any open-source or properly licensed software that they bring with them for the contest.

- Teams will have full internet access for the duration of the competition, and they may use internet searches to help solve challenges. Teams can bring a hot spot, if desired.

- Teams may not ask for external assistance or otherwise contact individuals that are not on their team for help on any challenge.

- Teams will also refrain from attacking the CTF infrastructure, either by attempting to gain unauthorized access or by interfering with other teams' access to the CTF site or to the competition network.

- Violation of these rules will result in a team’s immediate disqualification from the competition.

ABOUT THE CYBER RANGE

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth's public high schools, colleges, and universities.

The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

The Virginia Cyber Range was proposed by Governor McAuliffe in spring 2016 as part of his vision to boost Virginia's cybersecurity industry through strategic educational investments. The cyber Range is led by an executive committee representing public institutions that are nationally recognized centers of academic excellence in cybersecurity within the Commonwealth.

VIRGINIA
CYBER RANGE

ABOUT NUARI and DECIDE

NUARI has executed command and control decision making exercises with organizations of all sizes, from thousands of participants spread across numerous international locations, to fewer than 30 participants in a local municipal initiative. NUARI is a 501(c)(3) non-profit that serves the national public interest through the interdisciplinary study of critical national security issues with a focus on strengthening and protecting critical infrastructure.

NUARI 1819
Norwich University Applied Research Institutes

DECIDE(R) - Distributed Environment for Critical Infrastructure Decision-making Exercises

DECIDE(R), a cybersecurity exercise platform, simulates cyber-attacks for organizations and their partnership stress and test incident response plans, resulting in after action reports to improve strategic communication, compliance, risk, and overall resilience. Initially conceived and started independently by NUARI and developed with funding from the Department of Homeland Security, the DECIDE platform has been a trusted cybersecurity live exercise solution for more than ten years.

decide® PLATFORM

VIRGINIA MILITARY INSTITUTE

CENTER FOR LEADERSHIP & ETHICS

CYBER DEFENSE LABORATORY VMI

Notes & Contacts

Notes & Contacts

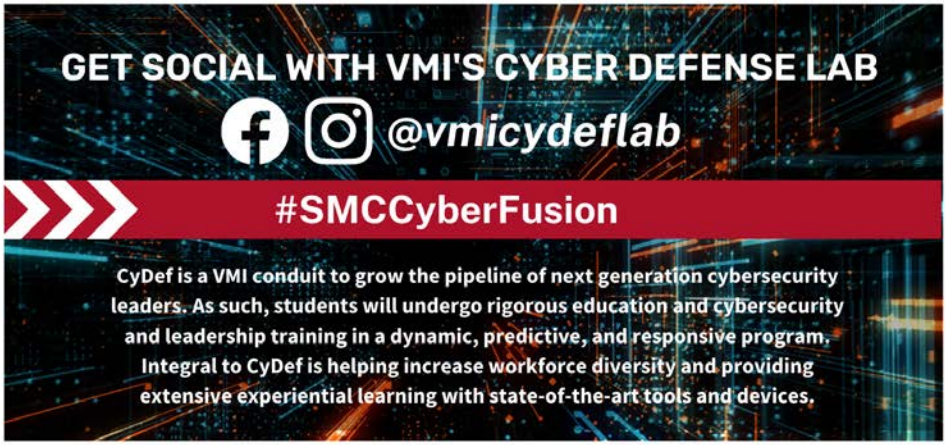
ENABLING IoT VULNERABILITY ANALYSIS

Given the rapid spread of IoT devices and the heavy reliance on its feedback and remote smart controls, IoT became a very attractive target for attacks. Recent attacks demonstrated how buggy and vulnerable IoT devices can be, particularly due to rapid software development that leads to serious security issues. In this experiment, we will explore IoT firmware emulation for exploit development and vulnerability analysis. Relying on open-source emulators, wrappers, and tools we will explore how IoT ARM architecture can be emulated using a containerized framework with easy IoT firmware porting. The experiment will demonstrate hosting an IoT camera as a case study. The experiment will also demonstrate a brief experiment for vulnerability discovery and exploitation. The goal is to enable easy software testing and vulnerability analysis in a portable software-based controlled environment.

A talk by Dr. Azab

Dr. Mohamed Azab is an assistant professor at the Department of Computer and Information Sciences at Virginia Military Institute. Mohamed received his Ph.D. in Computer Engineering in 2013 from The Bradley Department of Electrical and Computer Engineering at Virginia Tech. He has multiple provisional patents, book chapters, and over 80 publications in archival journals and respected conference proceedings. His research interests lie in the area of cybersecurity and trustworthy engineering ranging from theory to design and implementation. His recent research crosscuts the areas of Software Defined Networking (SDN) architectures and protocols, high performance and cloud computing, ubiquitous Internet of Things (IoT), and Cyber-Physical Systems (CPS). He has served on steering committees for conferences, workshops, and archival journals.

On June 7th – 11th, 2021 the VMI Cyber Defense Laboratory hosted its first ever CyberSmart Workshop. This workshop was for local high school students from Rockbridge and Augusta County. With almost 30 students in attendance, students learned about topics such as social engineering, python, and cryptology. Students had the opportunity to participate in hand-on activities such as building an Internet of Things Device. This year's CyberSmart workshop was the first of many. In the years to come, middle and elementary school students will be involved.



Thank you for attending!

CYBER DEFENSE LABORATORY

(CyDef)

Sponsored by the

DEPARTMENT OF DEFENSE

CENTER FOR LEADERSHIP AND ETHICS

VIRGINIA MILITARY INSTITUTE

EDUCATE, ENGAGE, INSPIRE

www.vmi.edu/cle