CyAD
Cybersecurity Across Disciplines

#CyAD2023

2023 CyAD Conference

August 1-2, 2023 • Palos Hills, IL

Hosted at:
Moraine Valley Community College

NCyTE CENTER
National Cybersecurity Training & Education Center

The National Cybersecurity Training and Education Center (NCyTE) is funded by the National Science Foundation grant #2054724.

Organizing Institutions

NCyTE - The National Cybersecurity Training and Education Center (NCyTE) at Whatcom Community College (WCC) is an Advanced Technological Education (ATE) National Center, grant-funded by the National Science Foundation (NSF). NCyTE advances cybersecurity education in the U.S. by supporting technological innovation, creating and disseminating resources, and providing professional development and tools to support faculty, community colleges, and the workforce pipeline of tomorrow. NCyTE is focused on building a comprehensive network of higher education institutions, businesses, and government agencies dedicated to developing and maintaining a robust cybersecurity workforce.

Whatcom Community College is a regionally and nationally accredited college with an accomplished faculty and staff who serve nearly 11,000 students annually. On its 72-acre campus in Bellingham, Washington, and through online courses, Whatcom offers transfer degrees, professional-technical training programs, as well as basic education, job skills, and Community & Continuing Education classes. The college is regularly recognized as one of the nation's top community colleges based on student success. Established in 1967, Whatcom has been accredited by the Northwest Commission on Colleges and Universities since 1976.

Moraine Valley Community College is one of the nation's leading community colleges with a proud tradition of meeting the diverse needs of our students. The college offers more than 140 degree and certificate programs and services specifically designed to help students succeed in their academic, personal and professional pursuits. Students choose Moraine Valley for a variety of reasons, but the most important include excellent faculty, small class size, up-to-date curriculum, equipment and facilities, affordable cost, convenience, and safe environment. Established in 1967, Moraine Valley is accredited by the Higher Learning Commission.

TABLE OF Contents

INFORMATION
Health and Safety

EXPECTATIONS FOR PARTICIPANTS IN THE CYBERSECURITY ACROSS DISCIPLINES (CyAD) CONFERENCE

Preventing Discrimination, Harassment, and Bullying

The organizers of the Cybersecurity Across Disciplines (CyAD) Conference are committed to the principles of diversity, integrity, civility, and respect in all our activities. We look to you to be a partner in this commitment during your CyAD participation by helping us to maintain a professional and cordial environment.

Discrimination and Harassment

Moraine Valley Community College ("the College") is committed to maintaining a safe and healthy educational and employment environment that is free from discrimination, harassment and misconduct on the basis of sex, which includes sexual orientation or gender-related identity. The purpose of these Procedures is to implement the College's Policy Prohibiting Sex-Based Misconduct and the Equal Educational Opportunity Policy (Board Policy 300.1 and Board Policy 300), ensure a safe and healthy educational and employment environment, and meet legal requirements in accordance with: Title IX of the Education Amendments of 1972 ("Title IX"), which prohibits discrimination on the basis of sex in the College's education programs or activities; relevant sections of the Violence Against Women Reauthorization Act ("VAWA"); Title VII of the Civil Rights Act of 1964 ("Title VII"), which prohibits discrimination on the basis of sex in employment; relevant sections of the Illinois Human Rights Act, which prohibits discrimination on the basis of sex or sexual orientation, including gender-related identity; the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act ("Clery Act"), which requires timely warning to the community of certain immediate threats; the Preventing Sexual Violence in Higher Education Act; and other applicable law and local ordinances.

The College has an affirmative duty to take immediate and appropriate action once it knows or its management should know of an act of sex-based discrimination, sexual harassment or other sex-based misconduct in any of its educational or employment programs or activities. The College will promptly and thoroughly investigate any complaints of sexual discrimination, harassment and/or misconduct in accordance with the procedures set forth below.

Electronic and/or Anonymous Reporting

The College maintains an online system for electronic reporting. The reporter may choose to provide his/her identity or may choose to report anonymously. Electronic and/or anonymous reports can be filed at ***https://cm.maxient.com/reportingform.php?MoraineValleyCC***. Where a reporter chooses to provide his/her identity and contact information, the College will respond to the reporter within 12 hours.

Faculty, staff, students, and community members can submit information about Moraine Valley Community College students whose behaviors are disruptive, concerning, or illegal. For emergencies, please first contact the Moraine Valley Police Department by calling (708) 974-5555, and then complete this form.

INFORMATION
ATE Centers

The National Science Foundations Advanced Technological Education (ATE) program supports the development of innovative approaches for educating highly skilled technicians for the industries that drive the nation's economy. ATE Centers occupy a key role in this mission, focusing on a particular subject area and/or geographical region and providing leadership for the ATE community in reaching that audience.

To ensure you have the most up-to-date information about each center, please visit their respective websites. You can find the original source of the information below at ***https://atecentral.net/centers***.

*Centers highlighted in green will be participating in the CyAD conference or are on a conference committee.

ADVANCED MANUFACTURING TECHNOLOGIES

Florida Advanced Technology Education Center for Manufacturing (FLATE)

Executive Director: *Ernie Friend* • ***Institution:*** *Hillsborough Community College, Tampa, FL*
Website: *http://fl-ate.org*

The Florida Advanced Technology Education Center for Manufacturing is dedicated to the creation of a manufacturing education system that offers "technical programs, curriculum development, best practice demonstrations, and student training" required to create a workforce with high performance skills to fill the needs of the ever-growing manufacturing industry.

National Center for Next Generation Manufacturing (NCNGM)

PI: *Karen Wosczyna-Birch* • ***Institution:*** *Education Connection, Litchfield, CT*
Website: *http://www.nextgenmfg.org*

The National Center for Next Generation Manufacturing (NCNGM) addresses the need for highly skilled workers in the manufacturing workplace by building programs that provide resources to educators and students interested in learning new technologies in manufacturing. The NCNGM is directed by the Connecticut College of Technology (CCOT), a virtual organization representing technology curriculum geared toward engineering and technical training offered at Connecticut's 12 community colleges.

National Center for Welding Education (Weld-Ed)

PI: *Monica Pfarr* • ***Institution:*** *Lorain County Community College, Elyria, OH*
Website: *https://www.weld-ed.org*

Weld-Ed, in collaboration with business and industry, improves the quality, quantity and availability of welding technicians through advancement of educational curriculum and instructor professional development. To accomplish the mission, the Center's staff and partners work collaboratively on the development of new and improved curricula in all areas of the materials joining industry. As a result of these efforts, faculty and instructors are provided continuing education opportunities throughout the academic year and in the summer months. These programs are specifically designed to train the next generation of workers for the materials joining industry and to upgrade the skills of existing workers.

INFORMATION
ATE Centers

AGRICULTURAL AND ENVIRONMENTAL TECHNOLOGIES

Advanced Technology Environmental and Energy Center (ATEEC) *[ATEEC is sunsetting. Check out the Environmental And Natural Resources Technology (EARTh) Center.]*

PI: *Ellen Bluth* • ***Institution:*** *Eastern Iowa Community College, Davenport, IA*
Website: *https://ateec.org*

The Advanced Technology Environmental and Energy Center (ATEEC) provides a wide range of environmental and energy technology learning resources for students, teachers, and technicians; the Center does this, in part, through their electronic Environmental Resources Library (eErl) digital library. The Center's objective is the "advancement of environmental technology education through curriculum development, professional development, and program improvement in the nation's community colleges and high schools."

Center for Renewable Energy Advanced Technological Education (CREATE)

PI: *Kenneth Walz* • ***Institution:*** *Madison Area Technical College, Madison, WI*
Website: *http://createenergy.org*

The Center for Renewable Energy Advanced Technological Education (CREATE) aims to address the rapidly changing energy landscape to develop and promote exemplary programs in support of the education of a skilled technical workforce for the American energy sector. The CREATE National Energy Center proposes to become the preeminent source of faculty professional development and instructional materials for energy educators, increase the visibility of energy careers and broaden participation of groups historically underrepresented in these careers, and build academic, industry, and international partnerships to advance energy technician education.

Environmental and Natural Resources Technology Center (EARTh)

PI: *Ellen Bluth* • ***Institution:*** *Eastern Iowa Community Colleges, Davenport, IA*
Website: *https://ourearthcenter.org*

Environmental Technologies (ET) is a career field that applies math, science, technology, economics, engineering, law and communication to manage, protect and sustain natural resources and to ensure human health and safety. Environmental technicians are a part of homeland security in the protection of our country's air, water and soil and an important part of the major environmental issues of global warming and water pollution. ET will also reshape pedagogy and hands-on delivery of learning in the post-COVID new normal, as well as become part of the solution for health and safety issues in the workplace following any other infectious disease pandemic. ET jobs cannot be outsourced and survive economic downturn.

Regional Center For Nuclear Education & Training (RCNET) *[RCNET is sunsetting. Check out the National Electric Vehicle Consortium (NEVC).]*

PI: *Kevin Cooper* • ***Institution:*** *Indian River Community College, Fort Pierce, FL*
Website: *http://gonuke.org*

Indian River State College houses the Regional Center for Nuclear Education and Training (RCNET). It meets the demand for skilled nuclear technicians in the Southeastern United States through a unified and systematic approach. RCNET aims to create a comprehensive curriculum, enhance regional college training programs, offer pathways to higher education and research, and provide remote access to specialized training components. As a training resource, curriculum repository, and industry expert, this center enhances communication and collaboration within the nuclear industry.

INFORMATION
ATE Centers

Viticulture and Enology Science and Technology Alliance (VESTA)
PI: *Michelle Norgren* • ***Institution:*** *Missouri State University, Springfield, MO*
Website: *https://www.vesta-usa.org*

The Viticulture and Enology Science and Technology Alliance (VESTA) is a NSF and ATE funded partnership between the Missouri State University System, two year schools in Iowa, Illinois, Oklahoma, state agriculture agencies, vineyards and wineries with "a 21st century vision for education in grape growing and wine making." The goal of VESTA is to establish programs of study in viticulture and enology through collaborations with educational institutions and government and industry partners that are tailored specifically for the Mid-American region. In addition, VESTA provides opportunities for students to participate in hands-on field experiences through partnerships developed with area vineyards and wineries, thus providing students with laboratory experience in their location.

BIO AND CHEMICAL TECHNOLOGIES

InnovATEBIO National Biotechnology Education Center
PI: *Linnea Fletcher* • ***Institution:*** *Austin Community College, Austin, TX*
Website: *https://innovatebio.org*

The InnovATEBIO National Biotechnology Education Center will address the need to educate highly skilled technicians for the nation's biotechnology workforce. Toward this goal, InnovATEBIO will provide leadership in biotechnology technician education, including support for development and sharing of best practices in biotechnology workforce development. In addition, the Center will promote local and national economic development of the biotechnology industry and help accelerate innovation in biotechnology and associated fields. The Center will focus on biotechnology technician education across the country, with a specific focus on strengthening the connections between high school and community college biotechnology programs.

ENGINEERING TECHNOLOGIES

Building Efficiency for a Sustainable Tomorrow (BEST) Center
PI: *Peter Crabtree* • ***Institution:*** *University of California-Berkeley, Berkeley, CA*
Website: *https://www.bestctr.org*

The BEST Center proposes to serve as a national vehicle for the collection, dissemination, and adoption of responsive, timely, and exceptional educational programs, courses, lab applications, and innovative instructional methods for the education of building systems technicians. This project outlines three goals: 1) Transform the instructional capacity of community colleges in the field of building technician education, with an emphasis on HPBOP and BAS training and certification; 2) Engage industry stakeholders and research partners in a national collaboration with community colleges to support high quality building science instructional programs; and, 3) Strengthen the national STEM pipeline for building technicians, focusing on outreach to both high school students and underrepresented adult learners.

INFORMATION
ATE Centers

ENGINEERING TECHNOLOGIES (cont.)

Center for Advanced Automotive Technology (CAAT)
PI: *Donald Hutchison* • ***Institution:*** *Macomb Community College, Warren, MI*
Website: *http://autocaat.org/Home*

The Center for Advanced Automotive Technology (CAAT) provides educational resources to meet the continuously evolving, technology-driven workforce needs of the automotive industry. The CAAT's technology focus is in the areas of Connected and Automated Vehicles (CAV), Alternative Fuels and Fuel Cells, Material Light-Weighting and Vehicle Electrification. The CAAT partners with industry, education, government, and professional organizations to support local economic development. Through these partnerships, the CAAT identifies funding opportunities for the creation and adaptation of curricula in advanced automotive technology programs.

Laser and Fiber Optics Regional Center (LASER-TEC)
PI: *Natalia Chekhovskaya* • ***Institution:*** *Indian River Community College, Fort Pierce, FL*
Website: *https://laser-tec.org*

The LASER-TEC Resource Center supports the LOPFO technical workforce by providing educational services and materials to secondary, post-secondary, and industry programs. Project aims include: 1) developing a comprehensive website for LOPFO educational products; 2) improving curricular materials; 3) conducting professional development events and creating tailored content for educators and industry members; 4) informing K-12 and college educators about LOPFO resources; and 5) building bridges between industries and colleges offering LOPFO programs.

Marine Advanced Technology Education Support Center (MATE)
PI: *Deidre Sullivan* • ***Institution:*** *Monterey Peninsula College, Monterey, CA*
Website: *https://www.marinetech.org*

The Marine Advanced Technology Education (MATE) Center is a national partnership of organizations working to improve marine technical education and in this way help to prepare America's future workforce for ocean occupations. Headquartered at Monterey Peninsula College (MPC) in Monterey, California, the MATE Center has been funded as a National Science Foundation (NSF) Advanced Technological Education (ATE) Center of Excellence since 1997. On the site, visitors will find a number of resources to support marine advanced technological education, including info about MATE's ROV (remotely-operated vehicle) competition, internships, workshops, curriculum, job listings, workforce info, publications, and more about the center and its industry and educational partners.

National Center for Autonomous Technologies (NCAT)
PI: *Jonathan Beck* • ***Institution:*** *Northland Community & Technical College, Thief River Falls, MN*
Website: *https://ncatech.org*

This ATE National Center aims to serve the national need for developing and maintaining a skilled technical workforce in the field of autonomous technologies. Autonomous technologies have the potential to revolutionize the way people across the globe live, work, travel, and learn. They also have critical implications for the national economy, as well as national safety and security. The National Center for Autonomous Technologies will focus on three areas of autonomous technology: unmanned aircraft systems, connected automated vehicles, and unmanned underwater vehicles.

INFORMATION
ATE Centers

National Center for Supply Chain Automation (NCSCA)
PI: *Valorie Piper* • ***Institution:*** *Riverside Community College District, Norco, CA*
Website: *https://supplychainautomation.com*

A Supply Chain Technician is a person who installs, operates, supports, upgrades or maintains the automated material handling equipment and systems that support the supply chain. The supply chain encompasses every commercial enterprise with a tangible product to move, store or deliver. The National Center for Supply Chain Automation (NCSCA) informs the public and increases the visibility of this high-growth career opportunity that is so crucial to so many different industries. NCSCA's mission is to increase the number of highly-qualified supply chain technicians in the workforce by helping educational institutions across the US establish programs that train supply chain technicians. We accomplish this by providing valuable instructional and technical assistance at no cost.

The Center for Aviation and Automotive Technology Education using Virtual E-School (CA2VES)
PI: *Anand Gramopadhye* • ***Institution:*** *Clemson University, Clemson, SC*
Website: *https://cecas.clemson.edu/cucwd/ca2ves*

The Center for Aviation and Automotive Technological Education Using Virtual E-School is a resource that develops and disseminates e-learning curriculum modules with complimentary virtual reality simulations for aerospace and automotive technological education. Aerospace and automotive industries, faculty from two and four-year colleges and other ATE Centers help to provide content and pilot testing with student users for the modules developed through NSF funding. The modules utilize modern andragogical strategies, including self-directed, mobile learning and formative and summative assessments. All materials are ADA compliant and meet UDL (universal design for learning) standards. The primary target audience is two year college and high school faculty and students.

GENERAL ADVANCED TECHNOLOGICAL EDUCATION

Technological Education Center for Deaf and Hard-of-Hearing Students (DeafTEC)
PI: *Donna Lange* • ***Institution:*** *Rochester Institute of Technology, Rochester, NY*
Website: *https://deaftec.org*

DeafTEC is unique in the fact that its focus is on a particular audience, deaf and hard-of-hearing students, rather than on a technical discipline. DeafTEC is administered by faculty at the National Technical Institute for the Deaf, on of the nine colleges of the Rochester Institute of Technology, and overseen by a National Visiting Committee made up of professionals in academia and industry. Emphasizing career education, Rochester Institute of Technology is a privately endowed, coeducational university with one of the most accessible communities available for deaf and hard-of-hearing students. Over 1,300 deaf and hard-of-hearing students attend RIT and study, live, and socialize with more than 16,000 hearing students in what is widely regarded as the largest "mainstreamed" program in the world.

Evaluation Resource Center for Advanced Technological Education (EvaluATE)
PI: *Lyssa Becho* • ***Institution:*** *Western Michigan University, Kalamazoo, MI*
Website: *https://evalu-ate.org*

The Evaluation Resource Center (ERC) focused on evaluating the work of the ATE program through an annual survey since 2000. The ERC now investigates and responds to the evaluation needs of the ATE projects by assisting current and prospective ATE grantees to develop high-quality evaluations that provide evidence to demonstrate the extent to which the goals of the projects and the ATE program are achieved. The Center provides ATE grantees and evaluators with support to design, conduct and report credible, useful improvement and accountability-oriented evaluations.

INFORMATION
ATE Centers

INFORMATION AND SECURITY TECHNOLOGIES

National Geospatial Technology (GeoTech) Center of Excellence
PI: *Vincent DiNoto* • ***Institution:*** *Jefferson Community and Technical College, Louisville, KY*
Website: *https://www.geotechcenter.org*

GeoTech Center is a National Center of Excellence from NSF's Advanced Technological Education initiative. Its goals are to: "Create a national clearinghouse of exemplary geospatial curriculum materials, resources and national services; Increase the capacity to educate geospatial technicians through new partnerships and collaborations; Increase the quantity, quality and diversity of geospatial technicians to meet U.S. workforce needs; Provide a unifying voice for geospatial technology education interests in organizations, industry and government; and Increase the number of community and technical college geospatial faculty and secondary school teachers participating in geospatial professional development."

National Convergence Technology Center (CTC)
PI: *Ann Beheler* • ***Institution:*** *Collin County Community College, Frisco, TX*
Website: *https://connectedtech.org*

The mission of the National Convergence Technology Center is "to meet the growing need for skilled specialists in the area of Convergence Technology and Home Technology Integration." The CTC focuses on leading national efforts to ensure that students are prepared with up-to-date IT skills to be highly employable upon completion of a two-year degree. CTC addresses curricular needs required by extensive changes expected in the industry, creates new business-led regional hubs (r-hubs) of influence to broaden dissemination and sustainability, creates and disseminates IT skill standards authored by the BILT, and provides products and services required to implement and support programmatic changes in community and technical college IT programs to promote graduates' success.

National CyberWatch Resource Center (NCC)
PI: *David Tobey* • ***Institution:*** *Prince George's Community College, Largo, MD*
Website: *https://www.nationalcyberwatch.org*

In 2012, following a successful tenure as an Advanced Technological Education (ATE) regional center, the National CyberWatch Center (NCC) was funded to serve as the ATE program's national center for cybersecurity education. Having fulfilled that role, NCC has transitioned to an ATE resource center, with a narrower scope, and continues to host some of the key resources and activities that it previously developed to support cybersecurity education and workforce development in community colleges.

National Cybersecurity Training and Education (NCyTE) Center
PI: *Corrinne Sande* • ***Institution:*** *Whatcom Community College, Bellingham, WA*
Website: *https://www.ncyte.net*

The National Cybersecurity Training & Education (NCyTE) Center leverages previous NSF grants, projects funded by the National Security Agency (NSA), and the expertise of partners to provide leadership for cybersecurity education in community and technical colleges and related secondary school programs that build America's skilled technical workforce in cybersecurity. The center pursues four strategic goals: expanding educational pathways and the diversity of cybersecurity programs to meet the nation's workforce needs, developing and deploying leading-edge cybersecurity curricula, cultivating engagement with employers (business, industry, government) and career opportunities for students, and disseminating resources to improve current and future directions of cybersecurity education.

INFORMATION
ATE Centers

MICRO AND NANOTECHNOLOGIES

Nanotechnology Applications and Career Knowledge Resource Center (NACK Center)
PI: *Osama Awadelkarim* • ***Institution:*** *Pennsylvania State University-University Park, State College, PA*
Website: *http://nano4me.org*

The Nanotechnology Applications and Career Knowledge (NACK) Resource Center offers a nation-wide nanotechnology education approach that includes providing resources and assistance to the nanotechnology education infrastructure. These resources can strengthen and streamline efforts to ensure that students develop industry-relevant knowledge, skills, and abilities. In addition, the project maintains web courses and remote equipment access, as well as provides faculty professional development to ensure that faculty remain at the cutting-edge of nanotechnology advances.

Northeast Advanced Technological Education Center (NEATEC)
PI: *Robert Geer* • ***Institution:*** *SUNY Polytechnic Institute, Albany, NY*

NEATEC (Northeast Advanced Technological Education Center) is an ATE Regional Center funded by the National Science Foundation (NSF). The long-term goal of this center is to “deliver cutting-edge educational and training programs, coordinate student recruitment and cooperative employment opportunities, research emerging workforce trends and training needs, and disseminate findings and best practices for the benefit of its partners, the regional economy as a whole, and other communities seeking answers for similar challenges.” On the NEATEC site, visitors will find information about the center, its partners, and a growing list of digital resources for educators and students.

Support Center for Microsystems Education (SCME)
PI: *Matthias Pleil* • ***Institution:*** *University of New Mexico, Albuquerque, NM*
Website: *http://scme-support.org*

The Support Center for Microsystems Education (SCME) offers workforce development models, materials, and opportunities for communities creating Microsystems technology clusters. The website, provided by Central New Mexico Community College, provides clear definitions and resources for this important field. It includes video presentations, workshop information, curricula, and in-class projects aligned with Central New Mexico Community College classes. Teachers can use these classes as models for designing or improving their own courses, while students can learn about microsystems education through examples, projects, articles, and additional helpful websites.

The Micro Nano Technology Education Center (MNT-EC)
PI: *Jared Ashcroft* • ***Institution:*** *Pasadena City College, Pasadena, CA*
Website: *https://micronanoeducation.org*

Micro- and nanotechnology enhances the performance of common devices like computers, cell phones, and medical sensors. It also improves products such as tennis balls, cloth, and bandages. With the growing use of these technologies, the micro- and nanotechnology industries are expected to experience significant growth. To support the workforce needed for these industries, this project establishes the NSF Advanced Technological Education Program’s Micro Nano Technology Education Center (MNT-EC). The MNT-EC increases the number of community college faculty in micro- and nanotechnology education, leading to more students receiving degrees and certificates in these fields. This project contributes to the preparation of a skilled technical workforce, crucial for the nation’s economy, security, and health.

WELCOME TO THE CyAD Conference

Welcome to the two-day **Cybersecurity Across Disciplines (CyAD)** Conference hosted by the National Cybersecurity Training & Education Center (NCyTE)! We are thrilled to have you join us for this exciting event.

This conference is tailored for community/technical college faculty across various fields, including Cybersecurity, Aerospace, Automotive, Marine and Geospatial Technologies, Business, Healthcare, and disciplines associated with Autonomous Technologies such as Automation and Manufacturing. Regardless of your background, this conference provides valuable insights and opportunities for all attendees.

Participate in breakout workshops that explore critical aspects of cybersecurity within your discipline. Topics include ***manufacturing and automation, critical infrastructure, business, healthcare and life sciences, automotive and autonomous systems,*** among others. Gain customized training, case studies, and scenarios relevant to your field. Witness demonstrations of cutting-edge resources and tools that enhance cybersecurity practices. Network with faculty members from diverse disciplines and learn from field experts.

We warmly welcome you to the CyAD Conference to expand your cybersecurity knowledge and discover its application in your specific field. This event promises valuable insights, connections, and resources for all attendees. Thank you for being a part of this exciting conference, and we eagerly anticipate your active participation!

CyAD is organized by the National Cybersecurity Training & Education Center (NCyTE) in partnership with Moraine Valley Community College.

2023 CyAD CONFERENCE
Mission

In an increasingly digitized society, the significance of cybersecurity extends beyond traditional boundaries. It has become essential for professionals across various disciplines, including Cybersecurity, Aerospace, Automotive, Marine and Geospatial Technologies, Business, Healthcare, and Autonomous Technologies such as Automation and Manufacturing.

The CyAD Conference aims to shed light on the critical role cybersecurity plays in these diverse fields. It recognizes that every discipline faces unique challenges and risks concerning cybersecurity and addressing them requires collaborative efforts and interdisciplinary approaches.

By bringing together community/technical college faculty from different disciplines, this conference fosters an environment of knowledge-sharing, learning, and collaboration. It provides an opportunity to explore the intersections between cybersecurity and these various fields, identify common challenges, and develop strategies to teach cybersecurity in these fields.

Understanding cybersecurity from a multidisciplinary perspective is vital because threats and vulnerabilities can arise from unexpected sources. By examining cybersecurity across disciplines, we can uncover innovative solutions, learn from best practices, and apply them in our respective fields.

At the CyAD Conference, you will have the chance to engage in interactive workshops, informative sessions, and engaging discussions that bridge the gap between cybersecurity and your specific discipline. Gain insights into emerging threats, explore effective strategies, and discover practical tools and resources to strengthen cybersecurity practices in your field.

We invite you to be a part of this dynamic conference, where cybersecurity and interdisciplinary collaboration converge. Together, let's explore the interconnectedness of our disciplines and work towards a more secure and resilient future.

THANK YOU TO THE
NSA and Microsoft Philanthropies

We would like to express our sincere gratitude for the support and involvement of the National Security Agency (NSA) and Microsoft Philanthropies in the first Cybersecurity Across Disciplines (CyAD) Conference. Your participation and financial assistance have played a pivotal role in ensuring the success of the conference!

Thanks to your generous support, the conference will have a significant impact on enhancing the attendee's collective ability to defend against cybersecurity attacks by increasing awareness and fostering defense across disciplines. Faculty members from diverse academic backgrounds across the United States will engage in discussions about the current cybersecurity threats prevalent in various disciplines. They will also gain invaluable insights from cutting-edge research, innovative ideas, and industry perspectives, allowing them to develop strategies for establishing a more robust and comprehensive education platform.

Your support means attendees will be better equipped to address existing gaps in cybersecurity education, both today and in the future. We are grateful for your support and look forward to future collaborations!

THANK YOU TO OUR 2023
CyAD Committees

ADVISORY AND PLANNING

Corrinne Sande
NCyTE Center Senior Advisor, National Cybersecurity Training and Education Center (NCyTE)

John Sands
Professor and Department Chair, Computer Integrated Technologies, Moraine Valley Community College

Jared Ashcroft
Principal Investigator, Micro Nano Technology Education Center (MNT-EC)

Marilyn Barger
Senior Educational Advisor Florida Advanced Technological Education Center (FLATE)

Jonathan Beck
Executive Director and PI, National Center for Autonomous Technologies (NCAT)

Nick Rotindo
Director, National Electric Vehicle Consortium (NEVC)

Vincent DiNoto
Director and Principal Investigator, National Geospatial Technology Center of Excellence (GeoTech)

James Hewlett
InnovATEBIO Co-PI, Professor of Biology, National Biotechnology Education Center (InnovATEBIO)

Chris Rondeau
Program Director of Network Security, Bossier Parish Community College

Anna Carlin
CIS Department Coordinator and Instructor, Executive Director, Hornet Security Education Center, Fullerton College

Virginia Swyndroski
Office Manager, Moraine Valley Community College

Michael Gonzalez
Program Coordinator and Graphic Design, Moraine Valley Community College

Anna Ritchey
Project Manager, National Cybersecurity Training and Education Center (NCyTE)

Trina Bol
Operations, Travel, and Events Manager, National Cybersecurity Training and Education Center (NCyTE)

2023 CyAD CONFERENCE
Keynote Speakers

Sanjay Goel

Professor and Chair, School of Business,
Information Security and Digital Forensics, University of Albany

"The Promise and Challenge of Artificial Intelligence"

Sanjay Goel is a Professor and Chair of the Information Security and Digital Forensics Department in the School of Business. He is also the Director of the Forensics Analytics Complexity for Energy and Transportation Systems (FACETS) and the Digital Forensics BS and MS programs at the university. With a Ph.D. in Mechanical Engineering from RPI and an undergraduate degree from the Indian Institute of Technology, Delhi, he previously worked at the GE Global Research Center, focusing on AI and optimization techniques for turbine design. His research interests include information security, cyber warfare, self-organizing systems, optimization, and cyber-physical systems, particularly in the context of traffic coordination, smart grids, and social networks.

Dr. Goel actively contributes to international cyber policy development and is committed to improving cybersecurity education. He has received numerous awards for teaching, research, and academic service, including the Promising Inventor's Award and the Excellence in Research Award. Additionally, he has secured substantial grant funding and has published extensively in top journals. As a recognized international expert, he has delivered plenary talks and presentations at various conferences, including the Annual Symposium on Information Assurance and the International Conference on Digital Forensics and Cyber Crime (ICDF2C), which he established.

Justin Valentino

Technical Education Content Developer,
Cisco Meraki

"Network Visibility: The Key to Preventing Tomorrow's Breaches"

Justin Valentino is a highly experienced Cisco Meraki Technical Education Content Developer, currently working with Meraki Product Enablement. With over 14 years of experience in the field, Justin has established himself as a seasoned professional in the IT industry.

Upon graduating from Moraine Valley Community College in 2008, Justin joined the IT workforce in the city of Chicago. He continued his education as an online student and earned a B.S. degree in Computer Networking & Telecommunications from FHSU in Hays, KS, while studying in their Cisco Networking Academy. Justin later received two separate master's degrees, one in Computer Systems Networking & Telecommunications and the other in Instructional Technology from FHSU.

Over the course of his professional journey, Justin has had the opportunity to collaborate with multiple Cisco teams and held diverse roles, allowing him to develop a wealth of experience in the field. His current role at Cisco Meraki within the Product Enablement team, where he is focused on driving the adoption of the Cisco Meraki wireless platform, is a testament to his extensive knowledge and expertise in this area.

Justin holds multiple certifications, including CCNP Enterprise, CWDP, CySA+, CMSS, and several specializations. He remains dedicated to expanding his knowledge and skills in the industry, as he is currently pursuing his CCIE exam study track and expecting to obtain his CCIE by 2024.

2023 CyAD CONFERENCE

Speaker Information

Irfan Ahmed
Associate Professor,
Virginia Commonwealth University

Ann-Claire Anderson
Senior Vice President, Center for Occupational Research and Development (CORD)

James Ashley
Director of Research and Development,
NICE Challenge Project at CSUSB

Marilyn Barger
Senior Educational Advisor,
Florida Advanced Technological Ed (FLATE)

Jonathan Beck
Executive Director and PI,
National Center for Autonomous Technologies (NCAT)

Ann Beheler
Consultant/NITIC, Center for Occupational Research and Development (CORD)

Andrew Bruce
Adjunct Instructor,
Clark College

Hongmei Chi
Professor,
Florida A&M University

Kristine Christensen
Professor, Computer Information Systems,
Moraine Valley Community College

Ulka Clark
Professor and Director,
University of North Carolina Wilmington

Kevin Cooper
Principal Investigator,
National Electric Vehicle Consortium

Deanne Cranford-Wesley
Director of Cybersecurity,
North Carolina Central University

Rafat Elsharef
Faculty,
Milwaukee Area Technical College

Ervin Frenzel
Director of Cybersecurity,
University of North Texas

Nathaniel Fuller
Adjunct Professor,
Purdue University

Jeff Greer
Professor,
University of North Carolina Wilmington

Alex Hillock
Cybersecurity Content Lead,
NICE Challenge Project at CSUSB

Tony Hills
STEM Faculty,
Northwestern State Community College

Mun-Wai Hon
Assistant Professor,
Northern Virginia Community College

2023 CyAD CONFERENCE

Speaker Information

Jiri Jirik

Director of Educational Pathways National Center, Moraine Valley Community College

Kyle Jones

Professor and Chair, Sinclair College

Mike Kwiatkowski

STEM Faculty, Northwestern State Community College

Huijun Li

Professor, Florida A&M University

Sanjay Madria

Professor, Missouri University of Science and Technology

Michael Masino

Information Technology Instructor, Madison Area Technical College

Scot McLemore

Executive in Residence, Advanced Technologies, Columbus State Community College

Lawrence McWherter

Assistant Professor, Cybersecurity, Columbus State Community College

George Meghabghab

Professor of Computer Science, Roane State Community College

Stephen Miller

Co-PI, NCyTE and Director, Eastern New Mexico University-Ruidoso Branch Community College

Michael Qaissaunee

Chair of Engineering and Technology, Brookdale Community College

Costis Toregas

Director, Cyber Security and Privacy Research Institute, The George Washington University

Jesse Varsalone

Associate Professor, University of Maryland Global Campus

Rick Vaughn

Chair, Micro Nano Technology - Education Center (MNT-EC), Rio Salado College

Nate Walters

Security Architect, Tacoma Public Utilities

Stephanie Wascher

Professor, Computer and Information Systems, Rock Valley College

Tobi West

Department Chair, Coastline College

Doug Witten

Assistant Professor, Wayne State University

PROGRAM PARTICIPATION
Track Types

AUTOMOTIVE AND AUTONOMOUS SYSTEMS

The Automotive and Autonomous Systems track focuses on addressing the cybersecurity challenges unique to the automotive industry and autonomous technologies. Participants will engage in interactive sessions, gaining insights into securing connected vehicles, protecting vehicle-to-vehicle and vehicle-to-infrastructure communications, and ensuring the safety of autonomous driving algorithms. Through customized training, case studies, and practical scenarios, participants will enhance their understanding of automotive cybersecurity and learn to integrate real-world examples into their teaching. This track provides valuable knowledge and resources for preparing students to tackle cybersecurity issues in automotive and autonomous systems.

BUSINESS

The Business track focuses on the critical cybersecurity aspects that organizations face in today's digital landscape. Participants will gain insights into the protection of sensitive data, safeguarding customer information, securing financial transactions, and ensuring the resilience of business operations. This track may cover topics such as risk management, data privacy and compliance, secure software development practices, threat intelligence, and incident response planning. Attendees will learn about the latest cybersecurity trends and strategies for mitigating risks and building a strong security posture within their organizations.

CRITICAL INFRASTRUCTURE

The Critical Infrastructure track delves into the unique cybersecurity considerations associated with protecting critical infrastructure systems such as power grids, transportation networks, and communication systems. Participants will explore the vulnerabilities and potential impacts of cyber attacks on these essential services, as well as strategies for detecting, preventing, and responding to such threats. This track may cover topics such as secure network architectures for critical infrastructure, threat modeling, incident response planning, and resilience of critical systems against cyber threats.

HEALTHCARE AND LIFE SCIENCES

The Healthcare & Life Sciences track explores the unique challenges and vulnerabilities in securing sensitive patient data, medical devices, and healthcare systems. Participants will delve into topics such as protecting electronic health records, securing telehealth platforms, ensuring the privacy of patient information, and addressing the growing threat of ransomware attacks targeting healthcare facilities. This track may also cover the intersection of cybersecurity and medical device safety, regulatory compliance, and incident response planning specific to the healthcare industry.

MANUFACTURING AND AUTOMATION

This workshop track focuses on the critical aspects of cybersecurity within the manufacturing and automation industries. It explores the challenges and vulnerabilities that arise in securing interconnected systems, industrial control systems, and the Internet of Things (IoT) devices. Participants will examine best practices and innovative approaches to safeguarding manufacturing processes, supply chains, and intellectual property from cyber threats. Topics covered may include secure design and operation of smart factories, risk management in industrial environments, and securing industrial automation systems against attacks.

2023 CyAD SCHEDULE
At a Glance

TUESDAY • AUGUST 1, 2023		
Breakfast on your own		
7:15am - 4:00pm	Registration Open	M-Building
8:00am - 9:15am	**Welcome and Opening Keynote**	Moraine Rooms
9:30am - 11:45am	**Cybersecurity Workshops for All Disciplines**	Moraine Rooms
12:00pm - 1:00pm	Working Lunch (Boxed Lunch)	Moraine Rooms
1:15pm - 4:30pm	**Multidisciplinary Workshops** (Concurrent)	Moraine Rooms
3:45pm - 4:30pm	**NICE Challenge**	Moraine Rooms
4:45pm - 5:15pm	Day 1 Closing Remarks	Moraine Rooms
5:15pm	Dinner On Your Own	

WEDNESDAY • AUGUST 2, 2023		
Breakfast on your own		
7:15am - 11:00am	Registration Open	M-Building
8:00am - 9:00am	**Session Series 1** (9 concurrent sessions)	T-Building
9:15am - 10:15am	**Session Series 2** (8 concurrent sessions)	T-Building
10:15am - 10:45am	Break	
10:45pm - 11:45am	**Session Series 3** (9 concurrent sessions)	T-Building
12:00pm - 1:00pm	Working Lunch (Boxed Lunch)	Moraine Rooms
1:15pm - 4:00pm	**Working Activity**	Moraine Rooms
4:00pm - 4:30pm	Conference Closing	Moraine Rooms
4:30pm	Dinner On Your Own	

2023 CyAD SCHEDULE

Tuesday Agenda • Aug. 1

TIME	DESCRIPTION	LOCATION
7:15am - 4:00pm	Registration Open & Badge Pick-Up	M-Building
8:00am - 9:15am	**Conference Opening and Keynote** **Featured Speakers:** Corby Hovis, NSF, Michele Robinson, NCyTE; Pamela Haney, MVCC; John Sands, MVCC **Keynote Speakers:** Sanjay Goel, University of Albany Justin Valentino, Cisco Meraki	Moraine Rooms
9:30am - 11:45am	**Cybersecurity Workshops for All Disciplines**	
	Cybersecurity 101: Protecting Our Digital World *Mike Qaissaunee, Brookdale Community College*	Moraine Rooms
	OT/IT Compliance and Monitoring Techniques Using Security Onion *Mike Masino, Madison Area Technical College*	T101 & T102
12:00pm - 1:00pm	**Working Lunch** (Boxed Lunch) **Featured Speakers:** Kevin Cooper, NEVC; Marilyn Barger, FLATE; Jonathan Beck, NCAT; Ann-Claire Anderson, CORD	Moraine Rooms
1:15pm - 4:30pm	**Multidisciplinary Workshops** (5 Concurrent)	
	Manufacturing Cybersecurity *Marilyn Barger, FLATE and Kyle Jones, Sinclair College*	Moraine Room 1
	Critical Infrastructure Security *TBA and Rafet Elsharef, Milwaukee Area Technical College*	Moraine Room 2
	Cybersecurity for Business *Larry McWherter, Columbus State Community College and Jiri Jirik, Moraine Valley Community College* ***-AND-*** **Cybersecurity for Life Sciences, Biotechnology, and Bio Sciences**	Moraine Room 3
	Security for Automotive / Autonomous Systems / Electric Vehicles *Jonathan Beck, NCAT, Kevin Cooper, National Electric Vehicle Consortium, and Jesse Varsalone, University of Maryland Global Campus*	T600
3:30pm - 3:45pm	Break	
3:45pm - 4:30pm	**NICE Challenge - Hands-On ICS/OT Cyber Challenges for Higher Ed.** *James Ashley and Alex Hillock, NICE Challenge Project at CSUSB* ***(This challenge takes place during the last 45min of the Manufacturing Cybersecurity and Critical Infrastructure Security Workshops.)***	Moraine Rooms 1 & 2
4:45pm - 5:15pm	**Day 1 Closing Remarks**	Moraine Rooms
4:30pm	Dinner on your own	

2023 CyAD SCHEDULE

Wednesday Agenda • Aug. 2

TIME	DESCRIPTION	LOCATION
7:15am - 11:00am	Registration Open & Badge Pick-Up	M-Building
8:00am - 9:00am	**Session Series 1** (9 Concurrent)	
	Digital Forensic Analysis of Software Code and Mobile Devices *Mun-Wai Hon, Northern Virginia Community College* **Track:** Critical Infrastructure	T101
	How Are Industrial Control Systems Insecure by Design? A Deeper Insight into Real-World PLCs *Irfan Ahmed, Virginia Commonwealth University* **Track:** Critical Infrastructure	T102
	SCADA System & Security: An Overview for Non-Technical Audiences *Andrew Bruce, Clark College and Nate Walters, Tacoma Public Utilities* **Track:** Critical Infrastructure	T701
	Unraveling the Gordian Knot: Interweaving AI, Business, and Cybersecurity for Robust Digital Ecosystems *Michael Qaissaunee, Brookdale Community College* **Track:** Business	T703
	Unlocking the Potential of GPT in Business Education: Addressing Challenges and Promoting Effective Implementation *Deanne Cranford-Wesley, North Carolina Central University* **Track:** Business	T704
	Holistically Building the Cybersecurity Workforce: Where Are We 12 Years Later? *Costis Toregas, The George Washington University* **Track:** Business	T709
	Cross Disciplinary Externships *Kyle Jones, Sinclair College* **Track:** Manufacturing	T710
	Intersections between Cybersecurity, Semiconductor Manufacturing, Precision Optics, and Nanotechnology *Rick Vaughn, Rio Salado College* **Track:** Manufacturing	T953
	Comparison Analysis on Performance of mHealth Apps Among Culturally Sensitive Communities *Hongmei Chi and Huijun Li, Florida A&M University* **Track:** Healthcare and Life Sciences	T-Building - Fogelson Theater

2023 CyAD SCHEDULE

Wednesday Agenda • Aug. 2

TIME	DESCRIPTION	LOCATION
9:15am - 10:15am	**Session Series 2** (8 Concurrent)	
	Pentesting Critical Infrastructure IoT Devices *Jesse Varsalone, University of Maryland Global Campus* **Track:** Critical Infrastructure	T101
	Designing for the Designer: Security Architect Development and Support *Jeff Greer, Geoff Stoker, and Ulka Clark, University of North Carolina Wilmington* **Track:** Critical Infrastructure	T102
	Weaving the Extensible Bills of Materials (xBOM) Fabric *Nathaniel Fuller, Purdue University* **Track:** Critical Infrastructure	T701
	National Information Technology Innovation Center Approach to Tapping Employer Expertise to Lead Innovation *Ann Beheler, Consultant for CORD* **Track:** Business	T703
	Identifying and Engaging Adjoining Career Fields to Increase Cybersecurity Training Efficacy *Ervin Frenzel, University of North Texas, James Freddle, Collin College, and James Phelps, Nova Southeastern University* **Track:** Business	T704
	Cybersecurity in Engineering and Manufacturing Applications Using Blockchain *Sanjay Madria, Missouri University of Science and Technology* **Track:** Manufacturing	T710
	ICS Incident Response and Tabletops: Lessons Learned From Oldsmar 2021 Water Treatment Breach *George Meghabghab, Roane State Community College* **Track:** Manufacturing	T953
	The Convergence and Importance of Cyber in Renewable Energy and Electric Vehicle Sectors *Kevin Cooper, National Electric Vehicle Consortium* **Track:** Automotive and Autonomous Systems	T-Building - Fogelson Theater
10:15am - 10:45am	Break	

2023 CyAD SCHEDULE

Wednesday Agenda • Aug. 2

TIME	DESCRIPTION	LOCATION
10:45am - 11:45am	**Session Series 3** (9 Concurrent)	
	Web Server Security - Patterns and Practice *Doug Witten, Wayne State University* **Track:** Critical Infrastructure	T101
	Intersection of Semiconductor Manufacturing and IT Education and the Opportunity for Community Colleges *Scot McLemore, Columbus State Community College* **Track:** Manufacturing	T102
	AI in Cybersecurity *Stephanie Wascher, Rock Valley College* **Track:** Critical Infrastructure	T701
	Cybersecurity--Conversations on Training For Business Professionals *Andrew Bruce, Clark College and Nate Walters, Tacoma Public Utilities* **Track:** Business	T703
	How to Use the CISA CSET Tool for Risk Assessments Across Multidisciplinary Business Sectors *Stephen Miller, Eastern New Mexico University-Ruidoso Branch Community College* **Track:** Business	T704
	Alumni Perceptions of Cybersecurity Employment Preparation Using the NICE Framework *Tobi West, Coastline College* **Track:** Business	T709
	Cybersecurity for Advanced Manufacturing Organizations *Tony Hills and Mike Kwiatkowski, Northwestern State Community College* **Track:** Manufacturing	T710
	Cybersecurity of Additive Manufacturing: G-Code and Firmware-Level Attacks and Side-Channel Monitoring Detection *Irfan Ahmed, Virginia Commonwealth University* **Track:** Manufacturing	T953
	CMMC Across Industries *Kristine Christensen and Jiri Jirik, Moraine Valley Community College* **Track:** Business	T-Building - Fogelson Theater
12:00pm - 1:00pm	**Working Lunch** (Boxed Lunch) **Table Discussion:** Introduction to CLARK, NCyTE Center	Moraine Rooms
1:15pm - 4:00pm	**Working Activity** *John Sands, Moraine Valley Community College*	Moraine Rooms
4:00pm - 4:30pm	**Conference Closing**	Moraine Rooms

2023 CyAD CONFERENCE
Workshop Descriptions

CYBERSECURITY WORKSHOPS FOR ALL DISCIPLINES

TUESDAY • 9:30AM - 11:45AM

Cybersecurity 101: Protecting Our Digital World

Room: Moraine Rooms

Mike Qaissaunee, Brookdale Community College

This presentation aims to simplify the complexities of cybersecurity and provide attendees with the knowledge, understanding, and tools needed to implement and adapt to the digital world. We will begin by defining cybersecurity and emphasizing its importance, particularly in light of increasing cyber crime and data breaches. Exploring various types of cybersecurity like network, application, cloud, information, and endpoint security, we will also discuss common threats such as phishing, malware, ransomware, and social engineering, along with their potential impacts. By examining real-world examples in sectors like healthcare, finance, education, government, and technology, we will demonstrate the relevance of cybersecurity. We will highlight best practices including regular updates, strong passwords, two-factor authentication, backups, and employee training. Lastly, we will explore the future of cybersecurity, including AI and machine learning, while emphasizing the need for continuous learning, adaptation, and implementation of best practices. Attendees will leave with a comprehensive understanding of cybersecurity and actionable steps to enhance their own cybersecurity measures.

OT/IT Compliance and Monitoring Techniques Using Security Onion

Room: T101 & T102

Michael Masino, Madison Area Technical College

Security Onion is a free and open Linux distribution that offers various functionalities such as threat hunting, enterprise security monitoring, and log management. Within Security Onion, there is a native web interface that includes built-in tools used by analysts for responding to alerts, conducting investigations, organizing evidence, monitoring system performance, and ensuring regulatory compliance. The focus of this session will be on the application of Security Onion for regulatory compliance.

One of the built-in tools available in Security Onion is Wazuh, which is a free and open-source security platform. Wazuh combines Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) capabilities. Its primary purpose is to assist with implementing compliance requirements and offering visibility for regulatory compliance support. Wazuh achieves this through automation, enhanced security controls, log analysis, and incident response. The default Wazuh ruleset includes support for frameworks and standards such as PCI DSS, HIPAA, NIST 800-53, TSC, and GDPR. Furthermore, it is possible to monitor for custom compliance standards. Wazuh can be deployed across various environments, including on-premises, virtualized, containerized, and cloud-based environments, providing host-based intrusion detection and log forwarding capabilities.

In addition to Wazuh, Security Onion also offers several third-party tools that complement its functionalities. These tools include Elasticsearch, Logstash, Kibana, Suricata, Zeek (formerly known as Bro), Stenographer, CyberChef, and NetworkMiner. These tools further enhance the capabilities of Security Onion, allowing for comprehensive security monitoring, log analysis, and network traffic analysis.

2023 CyAD CONFERENCE
Workshop Descriptions

MULTIDISCIPLINARY WORKSHOPS

TUESDAY • 1:15PM - 4:30PM

Manufacturing Cybersecurity

Room: Moraine Room 1

Marilyn Barger, FLATE and Kyle Jones, Sinclair College

The Manufacturing Cybersecurity workshop will cover essential aspects of cybersecurity in manufacturing and automation operations. Participants will have the opportunity to delve into major topics such as cyber threats and attack vectors, as well as strategies for securing communication protocols including Industrial Ethernet Applications, Modbus, and Ethernet POWERLINK. Protocol analysis will be emphasized to enhance participants' understanding of potential vulnerabilities. Moreover, the workshop will explore the importance of safeguarding PLCs, smart sensors, smart actuators, IoT devices, and other end devices. Wireless technologies will also be examined in relation to cybersecurity considerations. Additionally, the workshop will address the challenge of scaling cybersecurity measures across the entire digital terrain, ensuring comprehensive protection. Lastly, the workshop will focus on aligning cybersecurity frameworks and implementing industry best practices to foster a robust security posture in manufacturing and automation operations.

Critical Infrastructure Security

Room: Moraine Room 2

TBA and Rafet Elsharef, Milwaukee Area Technical College

The Critical Infrastructure Security workshop will focus on the examination of critical aspects of cybersecurity in relation to various critical infrastructure sectors. Participants will gain insights into major topics such as cyber threats and attack vectors specific to critical infrastructure systems. Strategies for securing video and audio systems, including Voice over Internet Protocol (VoIP), will be discussed to mitigate potential vulnerabilities. The workshop will also cover securing HVAC systems, transportation and logistics networks, energy systems and production facilities, roads and traffic control systems, and water systems including sewage treatment. Moreover, participants will learn about the importance of cybersecurity measures for police and first responders in order to ensure the resilience and effectiveness of emergency services. Through this workshop, attendees will acquire valuable knowledge and practical approaches to enhance cybersecurity in critical infrastructure sectors.

Cybersecurity for Business

Room: Moraine Room 3 (Combined with Cybersecurity for Life Sciences, Biotechnology, and Bio Sciences)

Larry McWherter, Columbus State Community College and Jiri Jirik, Moraine Valley Community College

The Cybersecurity for Business workshop introduces risk management in business operations, covering topics such as threat vectors, cybersecurity legislation, and legal liability. It emphasizes business information systems management and security, including enterprise security measures, secure communications, cloud security, and risk management strategies. Participants will also learn about auditing, compliance, and organizational governance for maintaining a strong cybersecurity posture. This workshop offers valuable knowledge and practical approaches to manage cybersecurity risks in business operations.

2023 CyAD CONFERENCE
Workshop Descriptions

MULTIDISCIPLINARY WORKSHOPS (cont.)

TUESDAY • 1:15PM - 4:30PM

Cybersecurity for Life Sciences, Biotechnology, and Bio Sciences

Room: Moraine Room 3 (Combined with Cybersecurity for Business)

The Cybersecurity for Life Sciences, Biotechnology, Bio Sciences workshop focuses on information and information systems management within a healthcare environment. Participants will explore various topics related to law and legal requirements, industry compliance, and best practices when handling health patient records and treatment information. Major topics covered in the workshop include security considerations specific to healthcare providers and life sciences, conducting HIPAA security risk analysis and ensuring compliance, implementing effective risk management strategies, designing and developing secure systems, testing and operating secure systems, enterprise cybersecurity risk management in healthcare, wireless and mobile security measures, and securing communications, devices, and protocols. By attending this workshop, participants will gain valuable knowledge and insights to enhance information security and management practices in healthcare settings.

Security for Automotive / Autonomous Systems / Electric Vehicles

Room: T600

Jonathan Beck, NCAT

The Security for Automotive / Autonomous Systems / Electric Vehicles workshop focuses on exploring the contemporary automation and security risks associated with semi-autonomous vehicles, as well as the inherent vulnerabilities present in various technologies integrated into modern vehicles. It covers several major topics, including automobile security and vulnerabilities, wireless communication methods such as Bluetooth and mobile communication, secure communications, devices, and protocols. Additionally, it delves into the aspects of dual-band Wi-Fi/GPS/Global Navigation Satellite System, 4G/5G cellular connectivity, cameras, onboard diagnostics, remote keyless entry and ignition, subscription-based communications, vehicle-to-everything (V2X) communication, and autonomous navigation utilizing light detection and radar technologies.

NICE CHALLENGE

TUESDAY • 3:45PM - 4:30PM

NICE Challenge - Hands-On ICS/OT Cyber Challenges for Higher Ed.

Room: Moraine Rooms 1 & 2

James Ashley and Alex Hillock, NICE Challenge Project at CSUSB

(This challenge takes place during the last 45min of the Manufacturing Cybersecurity and Critical Infrastructure Security Workshops.)

This workshop is designed in a train-the-trainer style, featuring new hands-on ICS/OT-focused cyber challenges from the NICE Challenge Project. Participants will have the opportunity to learn about and engage with the latest ICS/OT NICE Challenges, gaining practical experience. Additionally, they will discover how to effectively incorporate these free and easily accessible web-based experiences into their classes and clubs.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 1

WEDNESDAY • 8:00AM - 9:00AM

Digital Forensic Analysis of Software Code and Mobile Devices

Room: T101 **Track: Critical Infrastructure**

Mun-Wai Hon, Northern Virginia Community College

With the increasing amount of mobile devices and embedded software, checking for issues and vulnerabilities in the software used would provide more visibility into any flaws or design attributes that could pose a risk to information theft or misuse. This presentation would provide a brief summary scope of the area given the surge or Internet of Things (IoT) devices, software supply chain concerns, and the relative lack of embedded security for operational technology components. Attendees would see examples of problematic software code and forensic images of cellular phones along with the open source tools to do their own evaluations. The presentation would also feature some point of common software weaknesses and ways to address them.

How Are Industrial Control Systems Insecure by Design? A Deeper Insight into Real-World PLCs

Room: T102 **Track: Critical Infrastructure**

Irfan Ahmed, Virginia Commonwealth University

Programmable logic controllers (PLCs) in industrial control systems have design features to enable engineering operations, such as real-time control of a physical process. These features have weaknesses that make the PLCs vulnerable to different attacks (network/firmware-based). This presentation discusses these features and attacks exploiting them, including direct firmware object manipulation (DFOM), return-oriented programming (ROP) on PLCs, control logic infection, data execution attacks, denial of engineering operations (DEO) attacks, and fragmentation and noise padding attacks. The presentation further covers security requirements to consider while designing a PLC.

SCADA System & Security: An Overview for Non-Technical Audiences

Room: T701 **Track: Critical Infrastructure**

Andrew Bruce, Clark College and Nate Walters, Security Architect for Tacoma Public Utilities

In an increasingly interconnected world run by SCADA systems, understanding their use and how to secure them is becoming crucial to an expanding range of industry sectors. This presentation seeks to unravel the intricacies of SCADA systems and security, bridging the gap between specialized knowledge and a broad understanding of their critical role in enabling modern society. The presentation will open with an accessible introduction to SCADA systems, their application across various industries, and their critical importance to modern infrastructure. We'll illuminate the purpose and functionality of these systems by using real-world examples. Next, we'll delve into the world of SCADA security. By discussing the inherent vulnerabilities of these systems, we aim to shed light on the potential risks and their implications on industries and society as a whole The presentation will conclude with an exploration of emerging trends in SCADA security and discuss future threats and advancements.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 1 (cont.)

WEDNESDAY • 8:00AM - 9:00AM

Unraveling the Gordian Knot: Interweaving AI, Business, and Cybersecurity for Robust Digital Ecosystems

Room: T703 **Track: Business**

Michael Qaissaunee, Brookdale Community College

The Gordian Knot is a metaphor that comes from a legendary chapter in the life of Alexander the Great. According to the story, an oracle had prophesied that anyone who could untie a particularly complex knot tied by Gordius, the king of Phrygia, would become the ruler of all Asia. Many tried and failed to untie the knot until Alexander the Great simply sliced it in half with his sword in an unconventional solution, hence "cutting the Gordian knot." In the context of modern problems, the Gordian Knot metaphor often represents a problem that seems insurmountably complex and almost impossible to solve in a traditional, straightforward way. Our talk examines how AI, business, and cybersecurity work together in today's digital world. We'll discuss how new AI technology helps spot cybersecurity threats and respond to them quickly. Also, we'll show how businesses can use AI to understand and manage their digital risks better, reducing downtime and helping them to keep running smoothly.

Unlocking the Potential of GPT in Business Education: Addressing Challenges and Promoting Effective Implementation

Room: T704 **Track: Business**

Deanne Cranford-Wesley, North Carolina Central University

In this presentation, I'll explore how GPT (Generative Pre-trained Transformer) can revolutionize business education. GPT offers exciting opportunities for interactive learning, problem-solving, and simulated business scenarios. However, implementing GPT in education faces challenges such as ethics, data quality, curriculum integration, and educator training. We'll discuss strategies to overcome these challenges, including ethical guidelines, data curation, and fostering critical thinking with GPT-generated content. Real-world success stories and best practices will be shared, showcasing GPT's transformative impact on business education. We'll also explore future perspectives and emerging trends in GPT for business education.

Holistically Building the Cybersecurity Workforce: Where Are We 12 years Later?

Room: T709 **Track: Business**

Costis Toregas, The George Washington University

In 2012, IEEE S&P published a paper "Holistically building the Cybersecurity Workforce" by Hoffman, Burley and Toregas (Vol 10, Issue 2, March 2012). The focus of this paper was "... to propose a holistic approach to developing the cybersecurity workforce based on careful integration of workforce development strategies into a plan that involves educators, career professionals, employers, and policymakers....". Twelve years later, one of the authors will review the basic tenets of this early paper, and comment on barriers that have not enabled this vision to be fully implemented. Looking at faculty priorities and the dramatic expansion of cybersecurity topics will be contrasted against student and employer interests. The August 2023 CyAD event is proof that the topic of cross-disciplinary education is still important, so bridges to earlier thinking and consideration of practical experiences can help the CYAD participants construct a vision more likely to succeed.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 1 (cont.)

WEDNESDAY • 8:00AM - 9:00AM

Cross Disciplinary Externships

Room: T710 **Track: Manufacturing**

Kyle Jones, Sinclair College

Over the summer of 2023, 30 faculty members were selected to work on Cross-disciplinary externships. These Cross-disciplinary externships were targeted at manufacturing and helping faculty better understand gaps in current educational programs. By bringing together experts from various disciplines, providing hands-on experiences, and teaching manufacturing techniques to design and implement secure systems, faculty can gain a more comprehensive understanding of the field and the skills needed to succeed in the industry.

Intersections Between Cybersecurity, Semiconductor Manufacturing, Precision Optics, and Nanotechnology

Room: T953 **Track: Manufacturing**

Rick Vaughn, Rio Salado College

The STEM department at Rio Salado College develops innovative training programs to serve non-traditional populations in a variety of modalities. The Micro Nano Technology - Education Center brings together Community Colleges, Universities, and industry partners to enhance the quality of education for students who then become higher quality technicians for our industry. In this session, Dr. Rick Vaughn will examine several key questions about the intersections between Cybersecurity, Semiconductor Manufacturing, Precision Optics, and Nanotechnology. Topics include security concerns and internships/apprenticeships, distance education, artificial intelligence, data management and security, IT vs OT, and the role of national ATE centers in supporting collaboration.

Comparison Analysis on Performance of mHealth Apps Among Culturally Sensitive Communities

Room: T-Building - Fogelson Theater **Track: Manufacturing**

Hongmei Chi and Huijun Li, Florida A&M University

Recent advances in mobile devices, such as smartphones, have fundamentally changed how people work and communicate with each other. It enables the rapid spread of smartphone applications (apps) that provide services in many aspects of life such as education, lifestyle, social media, productivity, entertainment, and game apps. Moreover, the pandemic accelerates the spread of mobile apps, especially in the domain of healthcare because of cultural and privacy sensitivity, being portable, and being easily accessible. In the field of healthcare, mHealth apps can provide tools and assistance for physical health management and mental health intervention. The research focuses on the effect of the mHealth app in the domain of mental health intervention. The research aims to compare and analyze the performance and effect of mHealth apps among different cognitive games cultural communities to improve the effectiveness of games and improve memory and concentration in the domain of the mental.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 2

WEDNESDAY • 9:15AM - 10:15AM

Pentesting Critical Infrastructure IoT Devices

Room: T101 **Track: Critical Infrastructure**

Jesse Varsalone, University of Maryland Global Campus

In the presentation, we would first demonstrate how to add modules and services to an IoT device. We may include insecure services, default passwords, or misconfigurations in our setup. In the second part of the presentation, we will walk through scanning and exploitation of the IoT device.

Designing for the Designer: Security Architect Development and Support

Room: T102 **Track: Critical Infrastructure**

Jeff Greer, Geoff Stoker, and Ulka Clark, University of North Carolina Wilmington

For two years, a small team of faculty members at UNCW have been working on an applied research project to improve the practice of security by design as a means for reducing or eliminating enterprise cyber risk. This initiative is aligned with the DOE's new Cyber-Informed Engineering strategy which is being promoted as a model for all critical infrastructure sectors. As a means for improving security by design, the researchers looked at the three elements of work which are people, process, and technology. They were evaluated both jointly and severally. Improvement opportunities were identified for all three work elements. Topics to be covered during the presentation include 1) NIST SP800-39, 2) security architect education, 3) best practice design concepts for managing enterprise cyber risk, 4) the use of model-based system engineering for developing and documenting a cyber risk management strategy, and 5) enhanced classroom methods for teaching enterprise cybersecurity.

Weaving the Extensible Bills of Materials (xBOM) Fabric

Room: T701 **Track: Critical Infrastructure**

Nathaniel Fuller, Purdue University

Today's systems are composed of a hybrid of proprietary and open-source elements with supply chains extending geographically, temporally, technically, and organizationally. Consumers struggle to evaluate compliance with security standards, licensing regulations, and vulnerability analysis. Recent motivating examples with material impacts include (1) malicious code infiltration into SolarWinds' Orion, (2) remote code execution vulnerabilities in Apache Log4j, and (3) the discovery that a component in the F-35 fighter jet originated from China caused the Pentagon to temporarily halt delivery. Legacy Bills of Materials (BOMs) remain relevant for modern supply chain illumination for all asset types. The authors are designing an eXtensible Bill of Material ([x]BOM) pattern with accompanying reference architecture to digitize BOMs. Importantly, the 'x' represents a variable, or type of BOM, versus the extensibility of the BOM's content.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 2 (cont.)

WEDNESDAY • 9:15AM - 10:15AM

National Information Technology Innovation Center Approach to Tapping Employer Expertise to Lead Innovation

Room: T703 **Track: Business**

Ann Beheler, Consultant for CORD

The Business & Industry Leadership Team Model (BILT) is widely accepted across the country as an effective high engagement model for putting employers in a co-leadership role for academic programs. The BILT approach provides means to deepen employer relationships and garner granular curricular guidance using minimal time from both employers and faculty members. The model is in use by more than 100 colleges and projects nationally, often in multiple disciplines. The basic model relies on industry subject matter experts addressing the knowledge and skills they predict they will want to hire 12-36 months into the future for one program at a time. The process uses an efficient, structured, repeatable, online voting process followed by a facilitated active discussion to prioritize the knowledge and skills for the faculty to use in making curricular modifications. This session covers a variation of the BILT approach to efficiently and effectively address a variety of related programs.

Identifying and Engaging Adjoining Career Fields to Increase Cybersecurity Training Efficacy

Room: T704 **Track: Business**

Ervin Frenzel, University of North Texas, James Freddle, Collin College and James Phelps, Nova Southeastern University

This seminar provides recommendations for connecting existing career fields to various cybersecurity countermeasures to correct an oversight that has long haunted the people, processes, and technology model. The belief cybersecurity only deals with securing technology prevents incorporation of needed skill sets to counter the lack of people and process skills associated with technology and technologists. An analysis of ACM, IEEE, and other existing cybersecurity documentation clearly indicates a need to increase training in the people and processes countermeasures to effectively train cybersecurity technicians. ACM and IEEE technologists recognize a lack of non-technical skills within the technical fields, technologists need to further embrace nontechnical specialists who can broaden the base knowledge within cybersecurity. Incorporation of people skill experts, such as sociologists and psychologists, can greatly enhance the effectiveness of techniques to counter cyberattacks.

Cybersecurity in Engineering and Manufacturing Applications Using Blockchain

Room: T710 **Track: Manufacturing**

Sanjay Madria, Missouri University of Science and Technology

In manufacturing, collaborative product development faces security challenges that require proper access control measures and robust provenance tracking. Access control ensures authentication and authorization, while provenance tracking stores a comprehensive activity history to detect malicious behavior. To achieve these security goals without relying on a single trusted entity, we propose using blockchain's distributed immutable ledger. By recording all activities on the blockchain, malicious entities cannot alter or remove traces. With an immutable record, we can detect and reverse malicious activities if needed.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 2 (cont.)

WEDNESDAY • 9:15AM - 10:15AM

ICS Incident Response and Tabletops: Lessons Learned from Oldsmar 2021 Water Treatment Breach

Room: T953 **Track: Manufacturing**

George Meghabghab, Roane State Community College

Industrial Control Systems incident response adapts traditional incident response phases to suit engineering environments, prioritizes safety in every phase, and includes different multi-team stakeholders. ICS incident response stakeholders include engineering operators, external control system support vendors, government agencies, physical safety teams, physical security teams, IT security, ICS security, etc., with direction from the owner/ operators of the ICS facilities. The talk will focus on the different phases of Incident Response in Industrial Control Systems(ICS) compared to traditional incident responses. Also the notion of tabletops is introduced to help look at the different scenarios that could impact any ICS. The purpose of the tabletop is to facilitate actionable security discussions among teams. The objective of the exercise is to improve existing industrial incident response preparedness. Tabletop scenarios improve on the Incident Response as mentioned above.

The Convergence and Importance of Cyber in Renewable Energy and Electric Vehicle Sectors

Room: T-Building - Fogelson Theater **Track: Automotive/Autonomous Systems**

Kevin Cooper, National Electric Vehicle Consortium

The global shift towards electric vehicles (EVs) promises a cleaner and more sustainable future for transportation. However, as the EV ecosystem expands, it also introduces new cybersecurity challenges. This presentation aims to explore the critical need for robust cybersecurity measures in the implementation of electric vehicles and supporting infrastructure. By examining the potential risks, vulnerabilities, and consequences of cyberattacks, we will delve into effective strategies and best practices to secure the EV ecosystem. Join us as we unravel the world of EV cybersecurity and discover how we can ensure a safe and resilient future for electric mobility.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 3

WEDNESDAY • 10:45AM - 11:45AM

Web Server Security - Patterns and Practice

Room: T101 **Track: Critical Infrastructure**

Doug Witten, Wayne State University

Malicious actors are always searching for websites that don't adhere to the strictest standards. Web Servers that utilize out-of-box software such as Apache Server are typically easy prey to those seeking to exploit some vulnerability causing damage that costs real money to the business. We will show techniques to strengthen Apache deploys using easy-to-configure settings that thwart most known attacks.

Intersection of Semiconductor Manufacturing and IT Education and the Opportunity for Community Colleges

Room: T102 **Track: Manufacturing**

Scot McLemore, Columbus State Community College

The resurgence of US semiconductor manufacturing is a national call to action; that will require recruiting, educating, and supporting a workforce that is anticipating to add tens of thousands of new jobs within the next few years. The Micro Nano Technology Education Center (MNT-EC), a nationwide consortium of thirty-eight community colleges that believes authentic partnerships with industry and four-year universities are key to addressing semiconductor workforce needs in both technician training and in educating graduate level engineers. Newly announced semiconductor fabrication facilities in Ohio, Arizona, Indiana, New York, and Kansas have led to a need to increase the number of semiconductor workers, including technicians and engineers. The recently signed CHIPS and Science Act provides $52 billion of funding to support the semiconductor industries, with over $5 billion allocated for workforce development. This presentation focuses on how community colleges and the can support both technician education and preparing a diverse student population for transfer into semiconductor disciplines for continued learning. Also, learn more about the employer-led programs at Maricopa including the AzAMI Intel® Quick Start Program and the MITI Artificial Intelligence (AI) Program.

AI in Cybersecurity

Room: T701 **Track: Critical Infrastructure**

Stephanie Wascher, Rock Valley College

The workshop aims to provide participants with a comprehensive understanding of how artificial intelligence (AI) can be effectively utilized in the field of cybersecurity. Participants will look at different AI methods and resources that can improve threat detection, remediation, and prevention measures as well as discuss ethical issues and biases in AI such as cybersecurity constraints and concerns, and ensuring accountability and transparency in AI-powered systems.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 3 (cont.)

WEDNESDAY • 10:45AM - 11:45AM

Cybersecurity Conversations on Training For Business Professionals

Room: T703 **Track: Business**

Andrew Bruce, Clark College and Nate Walters, Tacoma Public Utilities

Cybersecurity is a business conversation, and it always has been. Our best and first line of defense is our end users, and they are also our biggest vulnerabilities. This presentation aims to help business educators and professionals train the next generation of end users to be cybersecurity aware business professionals. The presentation will focus on key talking points, using Andrew's almost two decades of experience across multiple industries to illustrate how the right training makes the company more secure, all while placing the topics in easy to understand and relatable business examples, and avoiding the stigma of "Tech Speak" Training is our best line of defense, and helping to build key understanding makes the conversation at the business level easier for both the Cybersecurity professional and the business, with the end goal to invest in trainings that increase security and profitability, while decreasing risk and compliance concerns.

How to Use the CISA CSET Tool for Risk Assessments Across Multidisciplinary Business Sectors

Room: T704 **Track: Business**

Stephen Miller, Eastern New Mexico University-Ruidoso Branch Community College

This workshop will provide a hands-on CSET Tool risk assessment learning experience across multidisciplinary business sectors that can be used in academia, business, and government. The workshop will allow participants to perform a risk assessment of their business sectors using the CSET Tool. The workshop will include an example of how to integrate the CSET Tool into curriculum in multiple disciplines. Attendees should bring their own laptops.

Alumni Perceptions of Cybersecurity Employment Preparation Using the NICE Framework

Room: T709 **Track: Business**

Tobi West, Coastline College

The cybersecurity workforce suffers from an ongoing talent shortage and a lack of information correlating cybersecurity education programs to alumni employment outcomes. This study evaluated the post-graduation employment outcomes of alumni that attended two-year colleges designated by the National Security Agency as Centers of Academic Excellence in Cyber Defense (CAE-CD). Stakeholders of this project are faculty, employers, students, government agencies, the NSA, and organizations that rely on cybersecurity talent to keep their systems secure from cyberattacks. The resulting knowledge can be used by two-year colleges to focus on the most relevant work roles, evaluate significant gaps to identify additional specialized programs for curriculum development, integrate content for industry certifications that students have prepared for, consider extracurricular activities that alumni have identified as important. Others can leverage the results to inform workforce development efforts.

2023 CyAD CONFERENCE
Session Descriptions

SESSION SERIES 3 (cont.)

WEDNESDAY • 10:45AM - 11:45AM

Cybersecurity for Advanced Manufacturing Organizations

Room: T710 **Track: Manufacturing**

Tony Hills and Mike Kwiatkowski, Northwestern State Community College

This presentation will introduce the audience to a set of freely available virtual training scenarios covering cybersecurity as encountered in advanced manufacturing environments. The presentation will demonstrate how common cybersecurity issues such as unencrypted data can negatively impact manufacturing devices such as networked sensors or PLCs. The presentation will show how these vulnerabilities can be mitigated. The audience will be encouraged to practice the concepts being demonstrated by working through one of the scenario labs.

Cybersecurity of Additive Manufacturing: G-Code and Fimware-Level Attacks and Side-Channel Monitoring Detection

Room: T953 **Track: Manufacturing**

Ifran Ahmed, Virginia Commonwealth University

This presentation will provide an understanding of the attack surface of additive manufacturing, including g-code and firmware-level attacks. It will cover sabotage attacks on both a printing environment and a printed object. Further, it will discuss side channel monitoring for an additive manufacturing process to detect cyberattacks. This presentation will provide real-world examples of attacks on the Ultimaker 3 printer, such as dynamic-thermal and localized filament-kinetic attacks and low-magnitude infill structure manipulation attacks, and further discuss a spatiotemporal G-code modeling approach to detect these attacks.

CMMC Across Industries

Room: T-Building - Fogelson Theater **Track: Business**

Kristine Christensen and Jiri Jirik, Moraine Valley Community College

Learn how the CMMC certification can provide a competitive edge for businesses across industries. This framework demonstrates robust cybersecurity controls, which builds trust with customers, reduces reputational damage, and protects the bottom line. We'll discuss potential challenges, including cost, employee training, and navigating the certification process. As the threat landscape evolves, the CMMC may be updated and applied to other federal agencies, creating new opportunities for businesses to differentiate themselves through their cybersecurity posture.

2023 CyAD CONFERENCE
Working Activity

WORKING ACTIVITY

WEDNESDAY • 1:15PM - 4:00PM

Interdisciplinary Focused Group Session

Room: Moraine Rooms

John Sands, Moraine Valley Community College

In this activity, participants from various disciplines will come together to collaborate and contribute information for Clark, a comprehensive knowledge resource. The primary objective is to create nanomodules, which are one-hour-long learning objects, for each discipline represented.

The activity will commence with focused group sessions, where participants will share their expertise, insights, and research findings related to their respective disciplines. Through collaborative discussions, the participants will work towards generating valuable information that can be incorporated into Clark, thereby enriching the knowledge base.

To ensure effective learning outcomes, the participants will apply Bloom's taxonomy, which provides a framework for developing a range of cognitive skills. For example, they might aim to create nanomodules that demonstrate higher-order thinking skills such as analysis, evaluation, and synthesis. This will facilitate the creation of engaging and intellectually stimulating learning materials.

Before starting the module creation process, the participants will prepare an outline to structure the content and ensure a logical flow of information within each discipline's nanomodule. The outline will serve as a guide, enabling participants to organize their thoughts, determine the sequence of topics, and identify any gaps in the material.

To facilitate the teaching process, the participants will have access to a provided template. This template will offer a standardized format that ensures consistency across all the nanomodules. By adhering to the template, participants can present information in a clear and concise manner, enabling effective knowledge transfer.

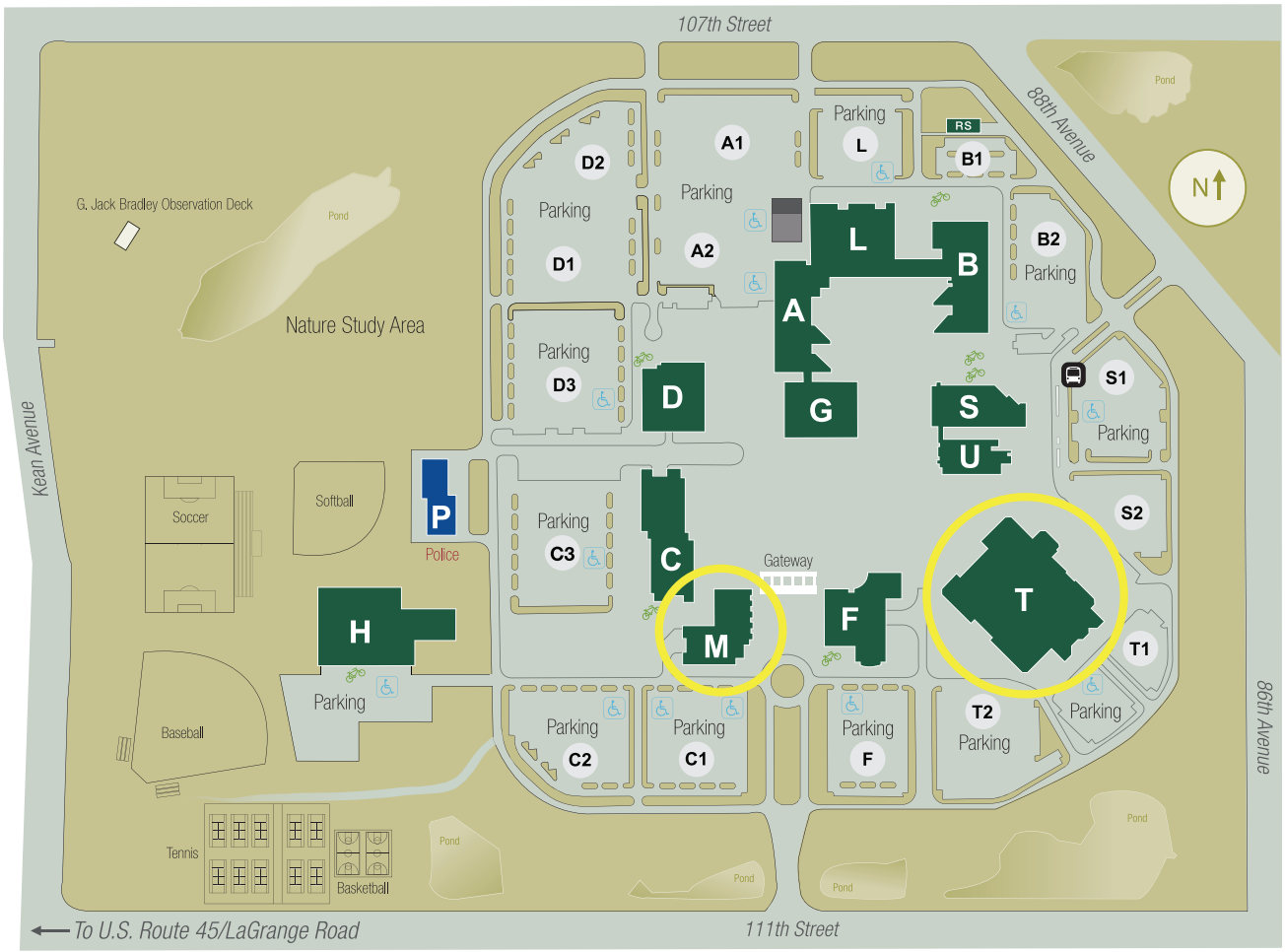
Throughout the activity, participants will have access to necessary materials for teaching purposes. These materials may include textbooks, research papers, online resources, multimedia assets, and any other relevant sources of information. By utilizing these materials, participants can enhance the depth and breadth of the knowledge presented in the nanomodules.

By engaging in this collaborative interdisciplinary activity, participants will contribute to Clark's knowledge repository, fostering interdisciplinary learning and knowledge exchange. The resulting nanomodules will serve as valuable resources, enabling learners to delve into various disciplines and acquire essential knowledge in a concise and engaging manner.

2023 CyAD CONFERENCE

Venue Maps

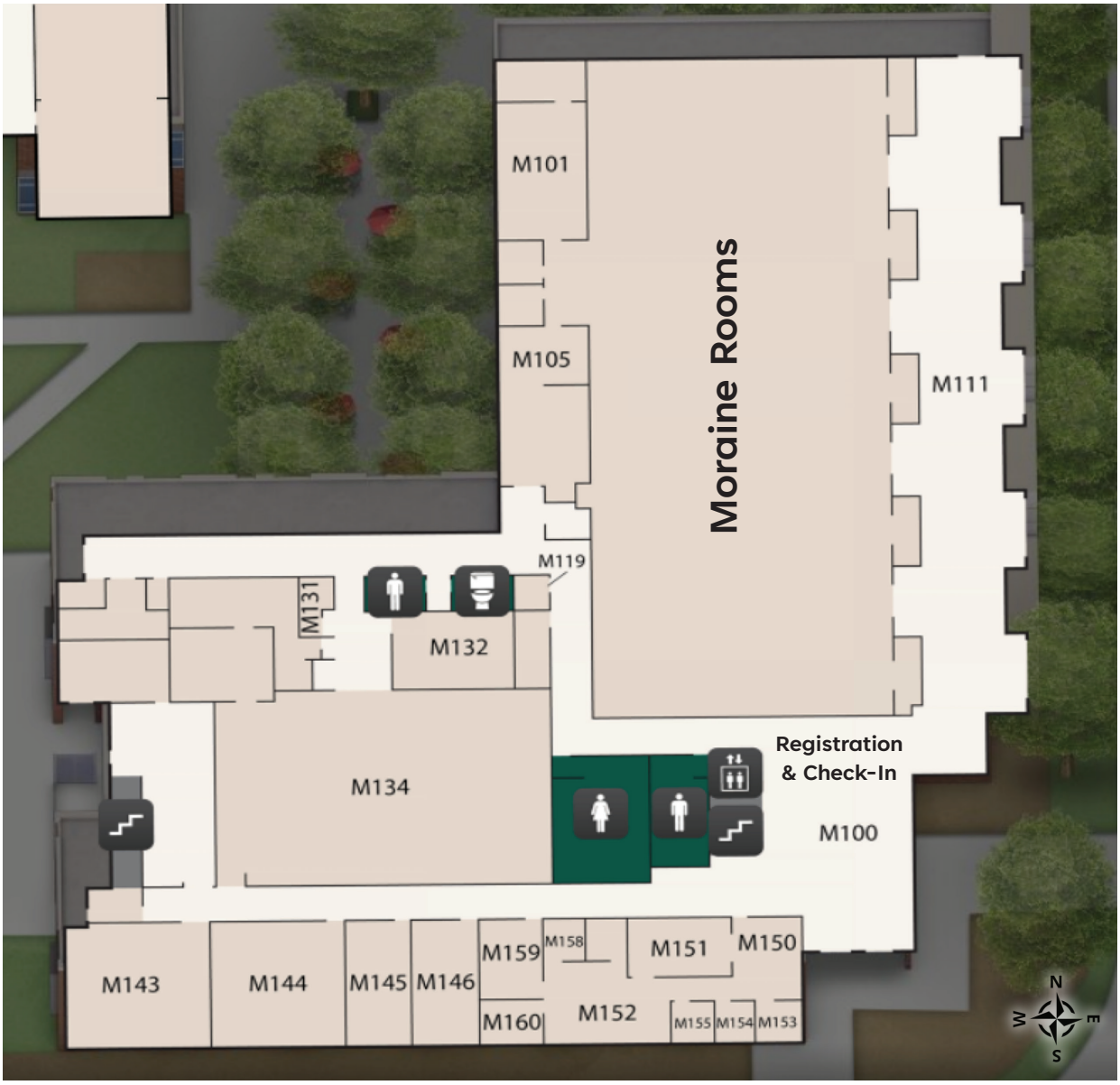
MVCC CAMPUS



2023 CyAD CONFERENCE

Venue Maps

MVCC BUILDING M



2023 CyAD CONFERENCE
Venue Maps

MVCC BUILDING T