# IEEE CARS

## CYBER AWARENESS & RESEARCH SYMPOSIUM

OCTOBER 28-29, 2024
UNIVERSITY OF NORTH DAKOTA
PROGRAM BOOKLET

UND has been designated as a National Center of Academic Excellence in Cyber Research (CAE-R) institution through 2029.

UNIVERSITY OF NORTH DAKOTA
LEADERS IN ACTION

IEEE CARS
CYBER AWARENESS & RESEARCH SYMPOSIUM

# THANK YOU TO OUR SPONSORS

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

UND UNIVERSITY OF NORTH DAKOTA
UNIVERSITY INFORMATION TECHNOLOGY

Microsoft

waterfall

TOWSON UNIVERSITY

High Point NETWORKS

DAKOTA DIGITAL ACADEMY
NORTH DAKOTA UNIVERSITY SYSTEM

NETWORKCENTER INCORPORATED

DAKOTA STATE UNIVERSITY

IEEE ComSoc Chicago Chapter
IEEE Communications Society

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

ALZHEIMER'S ASSOCIATION®

The Cyber Awareness & Research Symposium (CARS) is jointly hosted by the University of North Dakota Center for Cyber Security Research (C2SR) and the University of North Dakota Information Technology.



IEEE CARS
CYBER AWARENESS & RESEARCH SYMPOSIUM

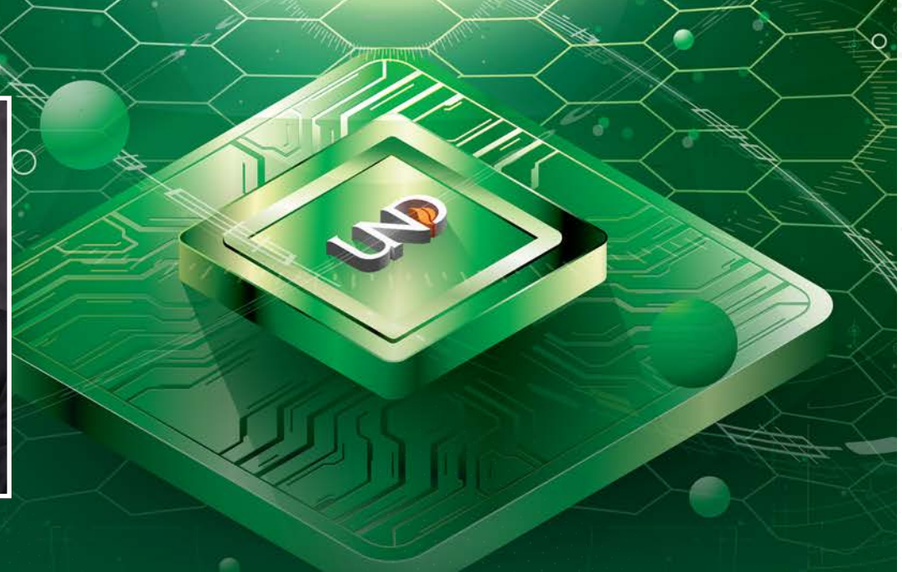


The IEEE Cyber Awareness & Research Symposium (CARS) is jointly hosted by the University of North Dakota Center for Cyber Security Research (C2SR) and University Information Technology (UIT).

# TABLE OF CONTENTS



UND UNIVERSITY OF NORTH DAKOTA
LEADERS IN ACTION



Greetings Everyone,

It is my pleasure to welcome you to theIEEE Cyber Awareness & Research Symposium (CARS), a dynamic gathering of professionals, academics, and students dedicated to advancing the frontiers of cybersecurity. As threats continue to grow in complexity and scope, there is a pressing need for innovative solutions and collaborative efforts. This year's symposium aims to disseminate knowledge that safeguards our digital world, and we are honored to host some of the brightest minds and leading organizations in the field.

Over the next two days, we are privileged to feature speakers from renowned organizations such as Waterfall Security, Microsoft, High Point Networks, Salesforce, Visa, and Arizona State University. These distinguished experts will provide invaluable insights through keynote talks, technical workshops, and hands-on sessions. Their expertise spans a range of critical topics within the cybersecurity landscape, including fraud detection, machine learning, and specialized security domains. Our goal is to create a platform where industry leaders and academic researchers can converge, fostering meaningful discussions and generating actionable insights.

In line with this year's theme of innovation and collaboration, we have designed two paper session tracks focusing on key areas of cybersecurity research: (1) The AI and Machine Learning in Cyber Security track explores cutting-edge applications of artificial intelligence, showcasing how these technologies are reshaping our approach to cyber threat detection and prevention. (2) The Specialized Security Domains track delves into emerging areas of cybersecurity, offering insights into sectors facing unique and evolving security challenges. These sessions will be presented by both in-person and online participants, reflecting the symposium's commitment to inclusivity and a global exchange of ideas.

We are particularly excited to host a Capture the Flag (CTF) tournament, where high school and university students will test their knowledge and problem-solving skills in categories such as web security, binary exploitation, and more. This competition not only promotes the practical application of cybersecurity concepts but also nurtures the next generation of cybersecurity professionals. The energy and enthusiasm from the participants are sure to be among the highlights of the event.

This symposium would not have been possible without the dedication of our sponsors, partners, and organizing committee. I extend my heartfelt thanks to everyone who contributed their time, resources, and expertise to make this event a success.

Thank you for being part of this important conversation. I look forward to the ideas and collaborations that will emerge from this year's symposium.

**Dr. Prakash Ranganathan**

Director, Center for Cyber Security Research (C2SR)
Associate Professor
IEEE Senior Member of Electrical Engineering

College of Engineering & Mines
University of North Dakota
prakash.ranganathan@UND.edu | 701.777.4431



## October 28, 2024

| Time | Topic | Speaker | Parallel Sessions |
|---|---|---|---|
| 7:00-8:00 a.m. | Breakfast (MU Ballroom) | | |
| 8:00-8:05 a.m. | Opening Remarks (MU Ballroom) | Chancellor Mark R. Hagerott | |
| 8:05-8:15 a.m. | Welcome Note (MU Ballroom) | Dr. Prakash Ranganathan | |
| 8:15-9:00 a.m. | **Keynote Talk 1:** Attack Trends in Critical Infrastructure and Industrial Control Systems (MU Ballroom) | Rees Machtemes, Waterfall Security | |
| 9:00-10:30 a.m. | **Workshop A:** Cyber Security for Everyone (MU Ballroom) | Jamie Maguire, Sr. Security Engineer, High Point Networks, Fargo | |
| 10:30-10:45 a.m. | Coffee Break (MU Ballroom) | | |
| 10:45-11:30 a.m. | **Keynote Talk 2:** Security and Safety of Internet-Connected Cyber-Physical Systems (MU Ballroom) | Dr. Hokeun Kim, Assistant Professor, School of Computing and Augmented Intelligence, Arizona State University | |
| 11:30-12:00 p.m. | Lunch (MU Ballroom) | | |
| 12:00-12:45 p.m. | **Keynote Talk 3:** Security, then, now, and future (MU Ballroom) | Shaun Gimberline (Microsoft) | |
| 12:45-1:45 p.m. | Paper Sessions #1 (Room 245), #2 (Room 340) | | 12:45-4:45 p.m.<br>**Cyber Capture the Flag (CTF)**<br>(Event in Room 318 -B)<br>(Viewing in Ball Room) |
| 1:45-2:45 p.m. | Paper Sessions #3 (Room 245), #4 (Room 340) | | |
| 2:45-3:45 p.m. | Paper Sessions #5 (Room 245), #6 (Room 340) | | |
| 3:45-4:45 p.m. | Paper Sessions #7 (Room 245), #8 (Room 340) | | |
| 4:45-6:00 p.m. | Dinner & Awards (MU Ballroom) | | |

## October 29, 2024

| Time | Topic | Speaker | Parallel Sessions |
|---|---|---|---|
| 8:00-8:30 a.m. | Breakfast | | |
| 8:30-10:00 a.m. | **Workshop B:** Machine Learning for Cyber Security using ScikitLearn | Sanjaikanth E Vadakkethil Somanathan Pillai ,Senior Systems Analyst, Visa Inc. | |
| 10:00-10:15 a.m. | Coffee Break | | |
| 10:15-12:15 p.m. | **Workshop C:** Fraud detection using AI-ML | Prasenjit Banerjee, Director of Technical architecture at Salesforce | |
| 12:15-12:45 p.m. | Lunch | | 12:00-4:00 p.m.<br>**Cyber Infrastructure for Smart Electric Grids: Enhancing Security and Resilience Workshop**<br>Workshop Leaders:<br>Anurag K. Srivastava<br>Venkatesh Venkataramanan<br>Barry Jones<br>Andrew Ginter |
| 12:45-1:45 p.m. | Paper Sessions #9, 10 | | |
| 1:45-2:45 p.m. | Paper Sessions #11, 12 | | |
| 2:45-3:45 p.m. | Paper Sessions #13, 14 | | |
| 3:45-4:45 p.m. | Paper Sessions #15, 16 | | |
| 4:45-5:00 p.m. | Closing Remarks | Dr. Prakash Ranganathan | |

IEEE CARS

CYBER AWARENESS & RESEARCH SYMPOSIUM

## ABOUT THE ANNUAL IEEE CYBER AWARENESS & RESEARCH SYMPOSIUM (CARS)

CARS is jointly hosted by the UND Center for Cyber Security Research (C2SR) and UIT to promote state-of-the-art cyber security activities and raise awareness.

The symposium will provide networking opportunities for industry professionals, academia, students, and the community. Conference attendees will gain an understanding of emerging concepts in artificial intelligence (AI)-driven threat intelligence, data science for cybersecurity, advanced persistent threats (APTs), open-source intelligence (OSINT).

CARS is a great way to stay informed about the current cyber threat landscape. It caters to a broad audience of academics, students, and industry professionals through its featured line of talks based on the awareness and research themes.

Learn more about UND's Center for Cyber Security Research on page 22.

## POPULAR TOPICS DISCUSSED:

- AI and Machine Learning in Cyber Security
- Human-Centric Cyber Security
- Critical Infrastructure Security
- Specialized Security Domains
- Network and IoT Security
- Cyber Security Awareness/Industry

**Want to learn more? Visit IEEE-CARS.org.**



# SPEAKER BIOGRAPHIES

## Mark R. Hagerott

Dr. Mark R. Hagerott is Chancellor for the North Dakota University System.

Prior to his move back home to North Dakota, Dr. Hagerott served on the faculty and held numerous academic leadership roles at the United States Naval Academy. He also served as a planning and strategy director in one of the largest U.S. Army educational organizations, NATO Training Mission, which included the Afghanistan army, police, air force, and medical school programs. Hagerott served as distinguished professor and deputy director of the Center for Cyber Security Studies at the Naval Academy and served on the Defense Science Board summer study of unmanned systems 2014-2015. He is a commissioner on the Midwestern Higher Education Compact, and Western Interstate Commission for Higher Education. Hagerott chaired the Secretary of the Navy's Education Reform Task Force in 2022.

Chancellor Hagerott's research and writing are focused on the evolution of technology, education, and changes in technical career paths, and he is the author of multiple articles and book chapters, with a recent emphasis on unmanned systems. He served as a non-resident cyber Fellow of the New America Foundation, 2015-2017.

Prior to his transition to an academic career path, Hagerott held numerous leadership positions in the U.S. Navy, both aboard ships and in administrative positions in the Department of Defense. A certified naval nuclear engineer in power generation and distribution, he served as chief engineer for a major environmental project defueling of two atomic reactors. Hagerott also ran tactical data networks for the Navy and rose to ship command prior to his career in higher education. He also served in both Bush administrations, as a White House Fellow in the first Bush administration; and in the office of the Deputy Secretary of Defense in the second Bush administration.

Hagerott holds a B.S. from the U.S. Naval Academy, an M.A. in political science and economics from Oxford University where he attended as a Rhodes Scholar, and a Ph.D. in history from University of Maryland.

The chancellor hails from a multi-generation North Dakota family of farmers and energy producers. The Hagerott-Brandenburg family homesteaded in Center and Mandan before statehood, where his father continues work on the fourth-generation farm, and his mother's family came with the first Bakken oil boom.

## Rees Machtemes, P.Eng.

Rees is the lead threat researcher for the annual Waterfall / ICSStrive OT Threat Report and writes frequently on the topic of OT / ICS cybersecurity. Being solutions-focused, he champions INL's Cyber-Informed Engineering program and regularly provides advice and commentary to government agencies and standards bodies issuing OT security guidance. Rees is a professional engineer with 15 years of industry experience in power generation and transmission substation automation, food and beverage plant automation, public and government telecom, data centres and IT support. He holds a B.Sc. in Electrical Engineering from the University of Alberta.

Rees is the lead threat researcher for the annual Waterfall / ICSStrive OT Threat Report and writes frequently on the topic of OT / ICS cybersecurity. Being solutions-focused, he champions INL's Cyber-Informed Engineering program and regularly provides advice and commentary to government agencies and standards bodies issuing OT security guidance. Rees is a professional engineer with 15 years of industry experience in power generation and transmission substation automation, food and beverage plant automation, public and government telecom, data centres and IT support. He holds a B.Sc. in Electrical Engineering from the University of Alberta.

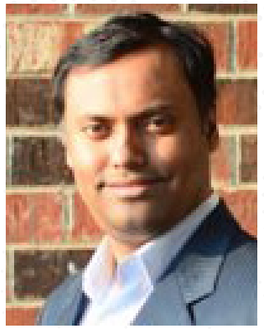
## Hokeun Kim

Hokeun Kim is an assistant professor in the School of Computing and Augmented Intelligence at Arizona State University. He received his Ph.D. degree in EECS from UC Berkeley in 2017 with a focus on Internet of Things security. His research focuses on cyber-physical systems, computing systems interacting with humans and the physical world, especially safety and security aspects. His research interests include software and hardware support for time-sensitive, Internet-connected, and intelligent cyber-physical systems. He won the ACM/IEEE Best Paper Award and received an IEEE Micro Top Picks Honorable Mention for his research contributions to the Internet of Things and computer architecture research.

## Sanjaikanth E. Vadakkethil Somanathan Pillai

Sanjaikanth E. Vadakkethil Somanathan Pillai is a Senior Systems Analyst for Visa Inc. with 16 years of industry experience. Sanjaikanth completed his bachelor's degree from The University of Calicut, India, and his Master's in Electrical and Computer Engineering (Software Engineering) from The University of Texas at Austin. He is currently studying toward a Ph.D. in Computer Science at The University of North Dakota. His expertises include application programming, automation, performance optimization, and data research.





## Prasenjit Banerjee

Prasenjit Banerjee is a Director of Technical architecture at Salesforce. He is a Fellow of the British Computer Society and an Industry expert in API Security , Management and Governance. He has been working on API Security and best practices for the last 8 years . Prasenjit has overall 16 years of experience in Integration architecture , Event Driven Architecture, SOA and Middleware. Prasenjit holds a Bachelor of Technology from West Bengal University of Technology, India and a MBA from University of Chicago Booth School of Business. Prasenjit is actively involved with professional organizations and is the Chapter Chair for IEEE COMSOC Chicago society and active contributor of IEEE Computer Society. He is also the Co-Chair of the IEEE Real-Time Communications Conference. Prasenjit lives in Chicago with his wife Tamalika and 2 daughters.

## Shaun Gimberline

Shaun Gimberline is a Digital Solutions Specialist at Microsoft with over 20 years of IT experience with a diverse background working in manufacturing, public sector, financial, healthcare and information technology companies. His work has largely been focused on email administration and security. To maintain systems over the years this focus grew into overall compliance and security in organization environments. Shaun holds a bachelor's degree from Fort Hays State University in Information Technology and is currently working towards a master's degree in Information Security and Compliance.

## Jamie Maguire

Jamie Maguire currently works as a Senior Security Engineer at High Point Networks. Jamie has over 10 years of cyber security experience and has previously held roles as a penetration tester, vulnerability manager, network administrator and help desk support. At High Point Networks Jamie is primarily responsible for delivering penetration tests. In addition, Jamie has served as an adjunct faculty member for the University of North Dakota. Jamie currently holds the following certifications: GIAC Penetration Tester (GPEN), GIAC Advanced Penetration Tester and Exploit Researcher (GXPN), Certified CMMC Professional (CCP)

**Register for workshops, see the symposium agenda, and learn more at IEEE-CARS.org.**

# KEYNOTES & WORKSHOPS

## Keynote Talk 1: Attack Trends in Critical Infrastructure and Industrial Control Systems

**OCTOBER 28 // 8:15-9:00 A.M. // BALLROOM**

Presented by Rees Machtemes, Waterfall Security

Waterfall and ICSStrive's 2024 Threat Report documents 68 cyber attacks last year with real-world physical consequences, in manufacturing, energy, and critical industrial infrastructure. Those 68 attacks hit over 500 sites, resulting in shut-downs, production delays or other physical consequences. Insights from the report include a sharp change in impact numbers and attacker practices at the turn of the decade and hacktivist attacks increasing faster than any other kind of attack in the data set. Over 3/4 of the outages were ransomware. Only 1/4 hit the OT network directly, the rest hit only IT networks yet still managed to shut down physical operations. There are only five ways these indirect / IT attacks managed to shut down operations. Join us to dig into the numbers and explore what lessons we should take from the data set.

Also covered: Critical infrastructures were recently taken down. Predatory Sparrow has yet again shutdown Iranian downstream gas ops. "Volt Typhoon" was unmasked lurking in global critical infrastructure. Ukraine credibly reported a supply chain attack on a water and gas telemetry equipment manufacturer, and that they thwarted another attack on an energy facility last September.

In this presentation, you will learn:

- Why are there OT consequences from attacks that target only IT targets, and what does this mean for ICS cybersecurity?
- Why have ransomware attacks with OT impacts apparently slowed down, while overall attack counts continue to increase?
- What important new kinds of attacks and consequences are showing up in the data?

Understanding threats is essential to designing effective defenses. We invite you to join Rees Machtemes to look at how the threat environment is changing.

## Workshop A: Cyber Security for Everyone

**OCTOBER 28 // 9-10:30 A.M. // BALLROOM**

Presented by Jamie Maguire, Sr. Security Engineer, High Point Networks, Fargo

In today's digital age, cyber security is no longer just a concern for IT professionals—it's a critical issue that affects everyone. This presentation aims to demystify the world of cyber security and provide practical tips and strategies that anyone can use to protect themselves online. Whether you're a tech-savvy individual or someone who is just starting to navigate the digital landscape, this session will equip you with the knowledge and tools you need to stay safe. Topics will include understanding common cyber threats, best practices for creating strong passwords, recognizing phishing attempts, and safeguarding personal information. Join us to learn how to make cyber security a part of your everyday life and ensure that you and your loved ones are protected in the digital world.

## Keynote Talk 2: Security and Safety of Internet-Connected Cyber-Physical Systems

**OCTOBER 28 // 10:45-11:30 A.M. // BALLROOM**

Presented by Dr. Hokeun Kim, Assistant Professor, School of Computing and Augmented Intelligence, Arizona State University

Cyber-physical systems (CPS) interacting with humans and the physical world have been increasingly connected to the Internet, forming the Internet of Things (IoT), especially since the recent pandemic. CPS, when connected to the networks, allows remote control, data processing on the cloud, and collaboration with other systems. However, CPS's network connectivity raises serious challenges. Recent cyberattacks on critical infrastructure, including US water systems and energy pipelines, demonstrated the risk of such network-connected CPS. Network latencies involved in the time-sensitive CPS render the timely handling of critical tasks problematic. Moreover, it worsens when combined with IoT and embedded systems challenges, including resource constraints, heterogeneity, scalability, and operation in an open environment. This talk will introduce my multi-disciplinary research approaches to building safe, effective, and connected CPS deployed at scale. I will present an open-source platform for providing essential security processes for connected CPS and the IoT, along with its network architectures resilient against availability threats such as distributed denial of service (DDoS) attacks. I will discuss my full-stack methodology for real-time and efficient CPS, from computer architecture to programming models. I will also introduce my ongoing and future research work for dealing with challenges in network communication of distributed CPS.

## Keynote Talk3 : Security, then, now, and future

**OCTOBER 28 // 12:00-12:45 P.M. // BALLROOM**

Shaun Gimberline, Microsoft

Quick history of security and compliance with a look at the current state and a future of security and the industry, including AI and disrupters in security

## Workshop B: Machine Learning for Cyber Security Using SKLearn

**OCTOBER 29 // 8:30-10:00 A.M.**

Presented by Sanjaikanth E Vadakkethil Somanathan Pillai, Senior Systems Analyst, Visa Inc.

The "Machine Learning for Cyber Security Using SKLearn" workshop is designed to provide a comprehensive introduction to the powerful SKLearn library in Python, covering everything from installation and prerequisites to advanced model building and evaluation techniques. Participants will learn about predefined datasets, data visualization, preprocessing, and feature extraction, followed by hands-on experience in building supervised and unsupervised models. The workshop also delves into model training, evaluation metrics, and performance improvement through hyperparameter tuning and ensemble methods. The session culminates with practical applications in cyber security, demonstrating how machine learning can be effectively used to detect and prevent cyber threats, equipping attendees with the skills to enhance their cyber security measures using SKLearn.

## Workshop: Fraud detection using AI-ML

**OCTOBER 29 // 10:15-12:15 P.M.**

Presented by Prasenjit Banerjee is a Director of Technical architecture at Salesforce

In today's world, every organization, whether large or small, leverages multiple applications to achieve its business outcomes. These applications may be cloud-based or hybrid, and their true potential is unlocked through meaningful integration. APIs serve as the building blocks that connect these systems both internally and externally. However, if these APIs are not properly secured and governed, they can put the entire organization and its business at risk. How can we ensure that APIs are secure by design, regardless of the technology stack used to build them? How can we make API security policy-driven and manageable on demand? In this 2 part workshop we will explore a novel approach to securing and governing enterprise APIs, focusing on the three pillars of people, process, and technology, ensuring robust API security irrespective of the tools and technology stack employed. The first part will look into the layers of API security at On-prem, Edge and Cloud, , clarify conflicting terminologies and look at the different security measures and policies that can be administered to protect APIs against security vulnerabilities and Denial of service attacks The Second part will a hands on component to build and deploy a microservice or API and administer policies on top of it to secure and govern it from incoming requests.

## Cyber Infrastructure for Smart Electric Grids: Enhancing Security and Resilience

**OCTOBER 29 // 12:00-4:00 P.M.**

Presented by Anurag K. Srivastava, Venkatesh Venkataramanan, Barry Jones, and Andrew Ginter.

As the electric grid evolves into a highly interconnected smart system, ensuring its cybersecurity becomes paramount. The Cyber Infrastructure for Smart Electric Grids: Enhancing Security and Resilience Workshop on October 29, 2024, brings together utility professionals, academic researchers, and national lab experts to address the emerging challenges in protecting modern electric infrastructure.

This workshop will cover key topics such as the integration of advanced sensing and communication technologies, effective data management strategies, and robust control mechanisms essential for maintaining grid stability amidst increasing complexity. Participants will also explore the critical differences between Operational Technology (OT) and Information Technology (IT) security, and learn best practices for fostering a resilient and secure smart grid. Join us to gain valuable insights and collaborate on strategies that safeguard the reliability and efficiency of the future electric grid.

**OCTOBER 28 // 12:45-4:45 P.M.**
**MEMORIAL UNION BALLROOM**

## UND CYBERHAWKS

# NATIONAL CAPTURE THE FLAG COMPETITION

The UND CyberHawks National Capture the Flag (CTF) Competition invites U.S. middle school, high school, and college students to demonstrate their cybersecurity skills. Hosted by the University of North Dakota's Center for Cyber Security Research and partnered with MetaCTF, the competition covers areas such as forensics, cryptography, web exploitation, and Modbus communication protocols.

Previously, teams participated in a virtual qualifier from September 16-20, 2024, where they competed in a six-hour CTF challenge. The top 20 teams advanced to the final competition at the UND Memorial Union during the IEEE Cyber Security & Research Symposium (CARS).

Prizes include raffle tickets and awards for the top three teams in each category, totaling over $2,000.

This event is proudly partnered with MetaCTF



# QUALIFYING TEAMS

## HIGH SCHOOL CATEGORY

**Team 1: RRHS Bull Moose Party**
Red River High School
Grand Forks, ND

**Team 2: RRHS Roughriders**
Red River High School
Grand Forks, ND

**Team 3: RRHS Square Deal**
Red River High School
Grand Forks, ND

**Team 4: RRHS Youngest Presidents**
Red River High School
Grand Forks, ND

**Team 5: Seetaram and Miles**
Byron High School
Byron, MN

## UNIVERSITY CATEGORY

**Team 1: Joannatron**
Carnegie Mellon University
Pittsburgh, PA

**Team 2: BYU Cyberia**
Brigham Young University
Provo, UT

**Team 3: Delogrander**
United States Air Force Academy
Air Force Academy, CO

**Team 4: Delograndest**
United States Air Force Academy
Air Force Academy, CO

**Team 5: Cyberlions**
Penn State University
Centre County, PA

**Team 6: UMGC-1-Grad**
University of Maryland Global Campus
Adelphi, MD

**Team 7: breadcrumb**
New York University
New York, NY

**Team 8: root@UNG**
University of North Georgia
Dahlonega, GA

**Team 9: BASH**
Sam Houston State University
Huntsville, TX

**Team 10: Delograndest**
United States Air Force Academy
Air Force Academy, CO

**Team 11: SegfaultRPI**
Rensselaer Polytechnic Institute
Hartford, CT

**Team 12: cmvasquez**
Loyola University Chicago
Chicago, IL

**Team 13: Delogranderest**
United States Air Force Academy
Air Force Academy, CO

**Team 14: Loyola CyberCorps**
Loyola University Chicago
Chicago, IL

**Team 15: nathteam**
Loyola University Chicago
Chicago, IL

**Team 16: NULLIfy**
University of Nebraska Omaha
Omaha, NE

**Team 17: Hackers Rule**
SAG
India

**Team 18: CyberSycamores**
Indiana State University
Terre Haute, IN

**Team 19: Layer Zero**
University of Nevada Las Vegas
Las Vegas, NV

**Team 20: Password123**
University of North Dakota
Grand Forks, ND

**Team 21: Mofongo Malware Busters**
Universidad de Puerto Rico
Rio Pedras, Puerto Rico

# PAPER SESSIONS

**DAY 1 // OCTOBER 28 // 12:45-1:45 P.M. // ROOM 245**

## Session 1, Track 1: AI and Machine Learning in Cyber Security

**Session Chair: Dr. Hassan Reza, University of North Dakota**

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571030227 | In-person | Bi-Directional Transformers vs. word2vec: Discovering Vulnerabilities in Lifted Compiled Code | Gary A. McCully, et.al., Dakota State University, University of Arizona, Georgia Institute of Technology | 12:45-1:00 p.m. |
| 1571057420 | In-person | Automated Detection of Masquerade Attacks with AI and Decoy Documents | Matt Berdychowski and Sergio A. Salinas Monroy, Wichita State University | 1:00-1:15 p.m. |
| 1571063101 | In-person | An EEG-Based User Authentication System Using Event-Related Potentials and Ensemble Learning | Soudabeh Bolouri and Diksha Shukla, University of Wyoming | 1:15-1:30 p.m. |
| 1571063196 | In-person | Federated Learning for Fake News Detection and Data Privacy Preservation | Sanjaikanth E Vadakkethil Somanathan Pillai et.al., University of North Dakota | 1:30-1:45 p.m. |

**DAY 1 // OCTOBER 28 // 12:45-1:45 P.M. // ROOM 340**

## Session 2, Track 2: Specialized Security Domains

**Session Chair: Dr. Craig Rieger, TRECS Consulting**

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571056295 | In-person | Cybersecurity threats in Virtual Reality Environments: A Literature Review | Ananth N. Ramaseri-Chandra and Prasad Pothana, Turtle Mountain College, University of North Dakota | 12:45-1:00 p.m. |
| 1571063986 | In-person | Bridging the Protection Gap: Innovative Approaches to Shield Older Adults From AI-Enhanced Scams | LD Herrera et.al., Dakota State University | 1:00-1:15 p.m. |
| 1571028471 | In-person | A Survey of Unikernel Security: Insights and Trends from a Quantitative Analysis | Alex Wollman and John Hastings, Dakota State University | 1:15-1:30 p.m. |
| 1571056228 | In-person | Cybersecurity in the Oil and Gas Sector: Vulnerabilities, Solutions, and Future Directions | Prasad Pothana, et.al., University of North Dakota, Turtle Mountain College | 1:30-1:45 p.m. |



**DAY 1 // OCTOBER 28 // 1:45-2:45 P.M. // ROOM 245**

## Session 3, Track 1: AI and Machine Learning in Cyber Security

**Session Chair: Dr. Rajesh Godasu, University of North Dakota**

**Location:** Memorial Union Room, 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571063892 | In-person | Anomaly Transformer-based System Log Anomaly Detection | Qinxuan Shi, et.al., University of North Dakota | 1:45-2:00 p.m. |
| 1571063971 | In-person | When XAI Meets CAPTCHA: A Case Study | Ifiok Udoidiok and Jielun Zhang, University of North Dakota | 2:00-2:15 p.m. |
| 1571064002 | In-person | Website Fingerprinting Attacks with Advanced Features on Tor Networks | Donghoon Kim, et.al., Arkansas State University, USA, University of Alberta, Canada, Dankook University, South Korea | 2:15-2:30 p.m. |
| 1571066746 | In-person | Masked Autoencoder for Data Recovery in Polymer Research: Mitigating Data Integrity Threats | Sanjaikanth E Vadakkethil Somanathan Pillai et.al., University of North Dakota | 2:30-2:45 p.m. |

**DAY 1 // OCTOBER 28 // 1:45-2:45 P.M. // ROOM 340**

## Session 4, Track 2: Specialized Security Domains

**Session Chair: Mr. Rees Machtemes, Waterfall Security**

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571060344 | In-person | Virtual Power Plants Security Challenges, Solutions, and Emerging Trends: A Review | Sriram Prabhakara Rao, et.al., University of North Dakota | 1:45-2:00 p.m. |
| 1571063192 | In-person | Medical Advisories as Deterrents in Healthcare Cybercrime | Hadipour and Murimi, University of Dallas | 2:00-2:15 p.m. |
| 1571063987 | In-person | Optimal Dynamic Load Altering Attack on Power Grids via Electrical Vehicle Charging Stations | Nishad Tasnim, et.al., University of Wyoming | 2:15-2:30 p.m. |
| 1571030271 | In-person | SETC: A Vulnerability Telemetry Collection Framework | Ryan Holeman, et.al., Dakota State University | 2:30-2:45 p.m. |

**DAY 1 // OCTOBER 28 // 2:45-3:45 P.M. // ROOM 245**

## Session 5, Track 1: AI and Machine Learning in Cyber Security

**Session Chair: Dr. Sicong Shao, University of North Dakota**

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571066744 | In-person | Exploring the Effectiveness of Synthetic Data in Network Intrusion Detection through XAI | Mohammad Ali and Jielun Zhang, University of North Dakota | 2:45-3:00 p.m. |
| 1571071939 | In-person | Graph Neural Networks Approach for Cyberattack Detection in Smart Grids | Xiao Yue and Guangzhi Qu, Oakland University | 3:00-3:15 p.m. |
| 1571063361 | In-person | Towards Quality Controllable Data Synthesis: A Case Study on Synthesizing Network Intrusions | Fuhao L, et.al., University of North Dakota | 3:15-3:30 p.m. |
| 1571063610 | In-person | Evaluating the Suitability of LSTM Models for Edge Computing | Leslie A. Viviani and Prakash Ranganathan, University of North Dakota | 3:30-3:45 p.m. |

DAY 1 // OCTOBER 28 // 2:45-3:45 P.M. // ROOM 340

## Session 6, Track 2: Specialized Security Domains

### Session Chair: Dr. Tingjun Lei, University of North Dakota

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571062221 | In-person | Navigational Errors in Small Unmanned Aerial Systems (sUAS) - A Short Review | Niroop Sugunaraj, et.al., University of North Dakota | 2:45-3:00 p.m. |
| 1571062226 | In-person | Navigational Dropouts in Small Unmanned Aerial Systems (sUAS) - A Short Review | Niroop Sugunaraj, et.al., University of North Dakota | 3:00-3:15 p.m. |
| 1571063898 | In-person | Security and Privacy Challenges and Opportunities in FinTech | Sanjaikanth E Vadakkethil Somanathan Pillai et.al., University of North Dakota | 3:15-3:30 p.m. |
| 1571028585 | In-person | Transforming Information Systems Management: A Reference Model for Digital Engineering Integration | John Bonar and John Hastings, Dakota State University | 3:30-3:45 p.m. |

DAY 1 // OCTOBER 28 // 3:45-4:45 P.M. // ROOM 245

## Session 7, Track 1: AI and Machine Learning in Cyber Security

### Session Chair: Dr. Jielun Zhang, University of North Dakota

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571062631* | In-person | Confronting the Reproducibility Crisis: A Case Study of Challenges in Cybersecurity AI | Richard H. Moulton et al., Dakota State University | 3:45-4:00 p.m. |
| 1571064303 | In-person | Feature Selection Framework for Optimizing ML-based Malicious URL Detection | Sajjad H. Shah, et.al., University of Wyoming | 4:00-4:15 p.m. |
| 1571063233* | In-person | A Review on Generative Intelligence in Deep Learning based Network Intrusion Detection | Mohammad Ali, et.al, University of North Dakota | 4:15-4:30 p.m. |
| 1571012979 | Online | Feasibility of Machine Learning-Enhanced Detection for QR Code Images in Email-based Threats | Jason Ford and Hala Strohmier Berry, University of South Carolina | 4:30-4:45 p.m. |

DAY 1 // OCTOBER 28 // 3:45-4:45 P.M. // ROOM 340

## Session 8, Track 2: Specialized Security Domains

### Session Chair: Dr. Jun Liu, University of North Dakota

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571039857 | In-person | Enhancing Cybersecurity Awareness in Medical IoT through Gamification with a Card Game Approach | Collins Poku Obeng, et.al., University of North Dakota | 3:45-4:00 p.m. |
| 1571075553 | In-person | Digital Twin Models for Cybersecurity Use Cases in Water Utilities and SCADA Systems: A Review | Sriram Prabhakara Rao, et.al, University of North Dakota | 4:00-4:15 p.m. |
| 1571077955 | In-person | Implementing Lightweight Intrusion Detection System on Resource Constrained Devices | Charles Stolz et.al, University of North Dakota | 4:15-4:30 p.m. |
| 1571080476 | In-person | Incident and Impact Analysis of the CrowdStrike Outage: Lessons Learned and Future Implications | Harish Kolla et.al, University of North Dakota | 4:30-4:45 p.m. |



DAY 2 // OCTOBER 29 // 12:45-1:45 P.M.

## Session 9, Track 1: AI and Machine Learning in Cyber Security

### Session Chair: Dr. Wen-Chen Hu, University of North Dakota

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571062619 | Online | Analysis of Network Intrusion Detection via Explainable Artificial Intelligence: Applications with SHAP and LIME | Ilhan Uysal and Utku Kose, Ersoy University, Turkey | 12:45-1:00 p.m. |
| 1571063188 | Online | Evading VBA Malware Classification using Model Extraction Attacks and Stochastic Search Methods | Brian Fehrman, et.al., South Dakota Mines | 1:00-1:15 p.m. |
| 1571063217 | Online | DynaDetect2.0: Improving Detection Accuracy of Data Poisoning Attacks | Sabrina Perry, et.al., University of Mississipi | 1:15-1:30 p.m. |
| 1571063946 | Online | Exploring AI for Vulnerability Detection and Repair | Onyeka Ezenwoye, et.al., Augusta University | 1:30-1:45 p.m. |

DAY 2 // OCTOBER 29 // 12:45-1:45 P.M.

## Session 10, Track 2: Specialized Security Domains

### Session Chair: Dr. Sicong Shao, University of North Dakota

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571068982* | In-Person | Cost-Benefit Framework for Secure Smart Installations | Gonzales et al., University of Tulsa | 12:45-1:00 p.m. |
| 1571058105 | Online | Decentering the Human: A Posthuman Approach to Cybersecurity Education | Ryan Straight, University of Arizona | 1:00-1:15 p.m. |
| 1571038196 | Online | Blockchain-based Access Control for Personal Data Sharing on Embedded Devices | Farha Masroor and Neena Goveas, BITS Pilani Goa Campus, India | 1:15-1:30 p.m. |
| 1571066679 | Online | An Overview of User Psychological Manipulation Techniques in UI/UX Web Design | Rimsha Riaz, et.al., Instituto Polit´ecnico de Viana do Castelo, Portugal | 1:30-1:45 p.m. |

DAY 2 // OCTOBER 29 // 1:45-2:45 P.M.

## Session 11, Track 1: AI and Machine Learning in Cyber Security

### Session Chair: Dr. Wen-Chen Hu, University of North Dakota

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571066493 | Online | Generating an Instruction Dataset to Build Cyber-Intelligent Large Language Models | Paige Zaleppa, et.al., Towson University | 1:45-2:00 p.m. |
| 1571030095 | Online | Anomaly Detection in Air-Gapped Industrial Control Systems of Nuclear Power Plants | Karthik Thiyagarajan and Issam Hammad, Dalhousie University | 2:00-2:15 p.m. |
| 1571062617 | Online | Cyber Security Training with Generative Artificial Intelligence Supported Web Platform Using IoT Cyber Threat Scenarios | Zehra Hatipoglu, et.al., Suleyman Demirel University, Turkey | 2:15-2:30 p.m. |
| 1571020891 | Online | Extending Q-Learning Agents in SQLi Environments | Marinelli et al., University of Oslo, Norway | 2:30-2:45 p.m. |

DAY 2 // OCTOBER 29 // 1:45-2:45 P.M.

## Session 12, Track 2: Specialized Security Domains

**Session Chair: Dr. Neena Goveas, BITS Pilani Goa Campus, India**

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571066297 | Online | Web Services Analysis and Threat Detection Through Score-Based Anomaly Detection System and Data Visualizations | Jesus A. Rodrıguez Rivera and Dr. Jose Ortiz-Ubarri, University of Puerto Rico | 1:45-2:00 p.m. |
| 1571047930 | Online | The Effectiveness of Education and Fear Appeal to Prevent Spear Phishing Attacks | Faham and Dupuis, University of Washington | 2:00-2:15 p.m. |
| 1571062637 | Online | Cyber Deceptive Countermeasures' Effects on Human-Simulated Attacks | Dakota State University | 2:15-2:30 p.m. |
| 1571017601 | Online | Empowering Shared Mobility Vehicle Riders, Stopping Scams: A Cyber Kill Chain and Awareness Approach to QRishing on College Campuses | Frank Offei Gyimah, et.al., Purdue University | 2:30-2:45 p.m. |

DAY 2 // OCTOBER 29 // 2:45-3:45 P.M.

## Session 13, Track 1: AI and Machine Learning in Cyber Security

**Session Chair: Dr. Thomas Stokke, University of North Dakota**

**Location:** Memorial Union, Room 318 A-B | **Zoom:** https://und.zoom.us/j/93405439114

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571051468 | Online | Friend or Foe? AI and the Evolving Landscape of Ransomware-as-a-Service (RaaS) | Frank Offei Gyimah, et.al., Purdue University | 2:45-3:00 p.m. |
| 1571019318 | Online | Exploring Machine Learning with FNNs for Identifying Modified DGAs through Noise and Linear Recursive Sequences (LRS) | Anthony Rizi, et.al., Dakota State University | 3:00-3:15 p.m. |
| 1571064915 | Online | Generative AI in Phishing Detection: Insights and Research Opportunities | Olga Perera, et.al, Dakota State University | 3:15-3:30 p.m. |
| 1571056626 | Online | Extracting Spatiotemporal Features For Detecting the Beginning of a Network Layer Attack with a Graph Neural Autoencoder and Deep Metric Learning | Mukesh Yadav and Peter Hawrylak, The University of Tulsa | 3:30-3:45 p.m. |



DAY 2 // OCTOBER 29 // 2:45-3:45 P.M.

## Session 14, Track 2: Specialized Security Domains

**Session Chair: Jamison Jangula, University of North Dakota**

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571066704 | Online | Systematic Literature Review of Cybersecurity and User Experience | Rajarathnam and Singh, University of Tennessee | 2:45-3:00 p.m. |
| 1571060815 | Online | PaciPhish: Intelligent and Interpretable Phishing URL Detection Framework | Rahul Choutapally and Tapadhir Das, University of Pacific | 3:00-3:15 p.m. |
| 1571063954 | Online | Anomaly Detection in ICS Networks with Fuzzy Hashing | William Tatum, et.al, Texas A & M University | 3:15-3:30 p.m. |
| 1571028957 | Online | Understanding the Human Factor: Enhancing Cybersecurity Resilience Through Behavioral Insight | Dr. Larry Snyder, Commonwealth University Bloomsbury, PA | 3:30-3:45 p.m. |

DAY 2 // OCTOBER 29 // 2:45-3:15 P.M.

## Session 15, Track 2: Specialized Security Domains

**Session Chair: Dr. Prakash Ranganathan, University of North Dakota**

**Location:** Memorial Union, Room 340 | **Zoom:** https://und.zoom.us/j/98287912006

| Paper ID | Status | Paper | Authors & Affiliation | Time |
|---|---|---|---|---|
| 1571063262 | Online | Password Usage Behavior of Online Users | Jin and Dupuis, University of Washington | 2:45-3:00 p.m. |
| 1571063288 | Online | Identification and Operationalization of Key Risks and Mitigations for the Cybersecurity Risk Management of Home Users | Tsai and Dupuis, University of Washington | 3:00-3:15 p.m |

### UND MEMORIAL UNION GUEST WI-FI

**SSID:** UNION Guest **PSK:** W31Guest

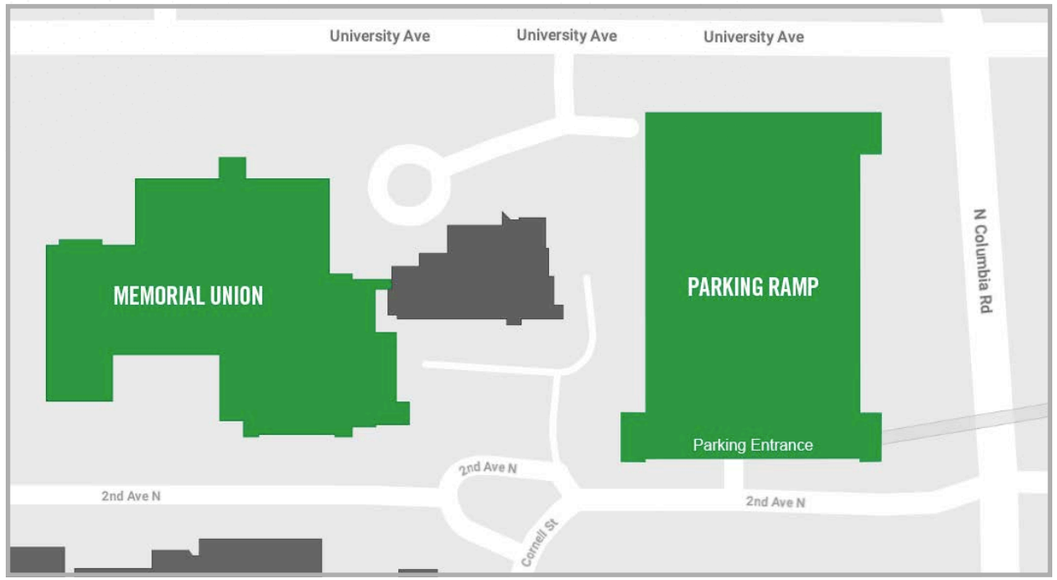
# VENUE MAP



# PARKING & DIRECTIONS

Free event parking for CARS 2024 is located in the UND Parking Ramp, located on the corner of 2nd Avenue N and Columbia Road. There will be a sign posted outside of the ramp.

For all other campus parking locations, payment is required. Paid parking is available using a smart phone by downloading the Passport Parking App. See **UND.edu/transportation/parking/event-parking** for more details.




# HOTELS, DINING, & MORE

Located in Grand Forks, North Dakota, the University of North Dakota is right at home in this vibrant college town of 59,000 people on the border of North Dakota and Minnesota. Ranked one of the most livable cities in the country, Grand Forks is a lively epicenter of events in the region—attendance at UND's men's hockey games is equivalent to 21% of the town's population!

Visit **VisitGrandForks.com** to find hotels, dining, entertainment, and more during your stay in Grand Forks!

LEADERS IN

# CYBER SECURITY

**A national and global leader in cyber security research, we develop cutting edge security solutions to solve next generation cyber security problems.**

engineering.UND.edu/research/cyber-security

## Programs in the UND School of Electrical Engineering & Computer Science:

### Electrical Engineering

Minor
Bachelors of Science (B.S.)
Masters of Science (M.S.)
Masters of Engineering (M.Eng.)
Doctorate (Ph.D. )

### Computer Science

Minor
Bachelors of Science (B.S.)
Masters of Science (M.S.)
Doctorate (Ph.D.)

### Cyber Engineering

Bachelors of Science (B.S.)
*(Pending approval in Fall 2025)

### Cyber Security

Certificate
Minor
Bachelors of Science (B.S.)
Masters of Science (M.S.)

### Data Science

Bachelors of Science (B.S.)
Masters of Science (M.S.)

### Graduate Certificates

Artificial Intelligence & Machine Learning
Ethical Hacking
Computer Forensics
Secure Networks
Cyber Security Analyst



# CENTER FOR CYBER SECURITY RESEARCH

The Center for Cyber Security (C2SR) is a research entity based within College of Engineering & Mines at the University of North Dakota.

The center brings together faculty, researchers, and students working in the field of cybersecurity across departments within the College of Engineering & Mines across campus.

## Primary Objectives:

- Conduct basic and applied research to enhance the security of critical infrastructures, assets, or information resources.
- Increase extra-mural dollars in research funding to thrusts within cyber security by enabling pathways from lab or in-house discoveries to commercialization by working with federal, state, and national labs, communities, and industries.
- Provide information and guidance to government, industry, non-profit organizations, and individuals attempting to solve information cyber security problems.
- Provide training in research activities fostering creative intellect for discoveries in areas within cyber security to develop well-rounded next-generation cyber scholars.
- Act as a resource and liaison for research activities related to cyber security areas for the UND campus, state, and throughout the U.S.
- Coordinate the campus-wide educational, research, outreach, and policy activities related to cyber defense/security or operations.

**Center for Cyber Security Research**
College of Engineering & Mines
University of North Dakota

## Recent Grants

**“Enhancing Substation Physical Security: A Federated Learning Approach for Radar, Acoustic, and Camera Data Fusion”**

ESPS-FL
Amount: $1,308,434 ($983,399 federal) // 01/2025-12/2026)

**“Adaptive Cybersecurity for Distributed Energy Resources: A Game-Theoretic and Machine Learning Approach for Real-Time Threat Detection and Mitigation”**

Department of Energy (DoE)
$525,000 // 10/2023-09/2026

**“Command and Control Technologies Assessment”**

NASA
$412,213 // September 2021-October 2024

**“A56-Evaluating Electro Magnetic Compatibility for UAS Environment”**

Federal Aviation Authority (FAA) ASSURE
$325,000 // 8/2021-8/2023

UND has been designated as a National Center of Academic Excellence in Cyber Research (CAE-R) institution through 2029.

IEEE CARS
CYBER AWARENESS & RESEARCH SYMPOSIUM

# THANK YOU TO OUR SPONSORS

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

UND UNIVERSITY OF NORTH DAKOTA
UNIVERSITY INFORMATION TECHNOLOGY

Microsoft

waterfall

TU TOWSON UNIVERSITY

High Point NETWORKS

DAKOTA DIGITAL ACADEMY
NORTH DAKOTA UNIVERSITY SYSTEM

NETWORKCENTER INCORPORATED

DAKOTA STATE UNIVERSITY

IEEE ComSoc Chicago Chapter
IEEE Communications Society

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

ALZHEIMER'S ASSOCIATION

The Cyber Awareness & Research Symposium (CARS) is jointly hosted by the University of North Dakota Center for Cyber Security Research (C2SR) and the University of North Dakota Information Technology.

UND UNIVERSITY OF NORTH DAKOTA
LEADERS IN ACTION