Mapping the Gap: Analysis of Nuclear Cybersecurity Education in U.S. Universities

Myles Nelson, University of Texas at Dallas
Amorita A. Christian, University of Tulsa
Tiffany Haney, Idaho National Laboratory
Charles Nickerson, Idaho National Laboratory

November 12-14, 2025

Cyber Fellows

THE UNIVERSITY of TULSA

Partners


THE UNIVERSITY of
TULSA


Cyber
Fellows


OCII
Oklahoma Cyber
Innovation Institute


INL
Idaho National Laboratory

The New World of Nuclear

Rapid expansion and transformation

- Executive orders and investments to increase nuclear energy capacity from 100 Gigawatts (GW) to 400 GW by 2050
- Increased momentum behind Advanced/Small Modular Reactors (A/SMRs)
- Increased digitalization of nuclear power plants
- AI-fueled energy demand, with corporate investment from leaders like Microsoft and Amazon

Why Nuclear Cybersecurity is Needed

- Transformation has outpaced the development of a cybersecurity workforce equipped to secure modern nuclear systems
- Nuclear operational technology (OT) and industrial control systems (ICS) were not designed with cybersecurity in mind
    - New vulnerabilites raise **urgent** concerns about safety, reliability, and regulatory compliance
    - Consequences of failure are uniquely severe
- Cybersecurity graduates require extensive retraining to become efficient in the nuclear environment
- Convergence of digital transformation and national energy priorities move nuclear cybersecurity from a niche concern to a stragetic imperative

State of Cybersecurity Education

- Proliferation of degree programs, Centers of Academic Excellence, and workforce development initiatives
- Question remains, How well does existing cybersecurity education address the needs of critical infrastructure sectors with unique technical and regulatory constraints?
    - Nuclear energy presents compelling case for further examination
- Study motivated by need to understand current nuclear cybersecurity workforce development within the broader landscape of cybersecurity and nuclear engineering education
    - Explored structural, institutional, and perceptual factors that shape student exposure

Background and Literature Review

- Cybersecurity workforce shortage well documented across critical infrastructure sectors; however, limited information for high-consequence domains such as nuclear energy
- Consistent report of difficulty in finding entry-level professionals with the technical skills and contextual awareness needed to secure OT
    - Challenge compounded in the nuclear sector because of an aging workforce and declining replacement rate
- Workforce development depends on the existence of educational pathways that increase visibility and accessibility for students
- Recent studies highlight the importance of experiential learning in preparing students for workforce demands

Methodology

- Multi-faceted, mixed methods approach to provide a holistic view of the educational landscape in cybsecurity and nuclear engineering programs
- Quantitative analysis of program structures and qualitative insights from expert interviews
- Research questions designed to assess the visibility, integration, and practical relevance of nuclear cybersecurity content. Questions focused on:
    - Curricular integration
    - Hands-on learning and technical skills
    - Faculty expertise and research activity
    - Industry alignment

Methodology

- **Two hypotheses**
  - **H1**: Limited collaboration between cybersecurity and nuclear engineering programs contributes to a shortage of nuclear cybersecurity specialists.
  - **H2**: Universities currently lack structured programs to support nuclear cybersecurity education
- **Data Collection and Analysis**
  - Comparative analysis of 16 cybersecurity programs and 12 nuclear engineering programs
    - 20 universities in the US
    - Various size, type (public/private), and geographic location
  - Detailed review of program structures, curricula, and key focus areas
  - Special attention given to identifying courses related to OT and ICS and the role of experiential learning

Universities and Colleges Reviewed

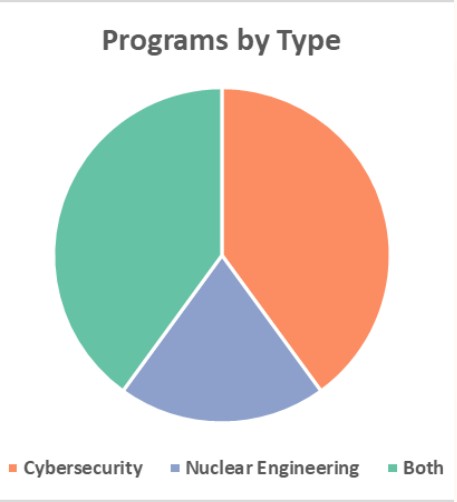
University Name	Program(s)	Location	Public/Private	Student Population
Carnegie Mellon University	Cybersecurity	Pittsburgh, Pennsylvania	Private	15,818
Case Western Reserve University	Cybersecurity	Cleveland, Ohio	Private	12,475
Fisk University	Cybersecurity	Nashville, Tennessee	Private	1,055
Georgia Institute of Technology	Cybersecurity & Nuclear Engineering	Atlanta, Georgia	Public	47,961
Idaho State University	Cybersecurity & Nuclear Engineering	Pocatello, Idaho	Public	12,614
Massachusetts Institute of Technology	Cybersecurity & Nuclear Engineering	Cambridge, Massachusetts	Private	11,886
Meharry Medical College	Cybersecurity & Nuclear Engineering	Nashville, Tennessee	Private	956
Mississippi State University	Cybersecurity	Starkville, Mississippi	Public	22,986
North Carolina State University	Nuclear Engineering	Raleigh, North Carolina	Public	37,873
The Pennsylvania State University	Cybersecurity & Nuclear Engineering	University Park, Pennsylvania	Public	87,995
Purdue University	Cybersecurity & Nuclear Engineering	West Lafayette, Indiana	Public	52,211
Texas A&M University	Nuclear Engineering	College Station, Texas	Public	74,829
University of California, Berkeley	Cybersecurity & Nuclear Engineering	Berkeley, California	Public	45,307
University of Illinois Urbana-Champaign	Cybersecurity & Nuclear Engineering	Urbana-Champaign, Illinois	Public	56,299
University of Michigan	Nuclear Engineering	Ann Arbor, Michigan	Public	52,855
University of South Carolina	Cybersecurity	Columbia, South Carolina	Public	35,364
University of Tennessee	Nuclear Engineering	Knoxville, Tennessee	Public	31,701
University of Texas at San Antonio	Cybersecurity	San Antonio, Texas	Public	34,742
University of Tulsa	Cybersecurity	Tulsa, Oklahoma	Private	3,769
Vanderbilt University	Cybersecurity	Nashville, Tennessee	Private	13,537

Selected Highlights from University Programs

University	Program Highlights
Carnegie Mellon University	Hosts the Software Engineering Institute (SEI); ICS/SCADA security research at CERT division; strong ties to DOE and DHS.
Georgia Institute of Technology	SCADA security research via GTISC and the Cyber-Physical Systems group.
Idaho State University	Offers a Nuclear Operations Technology pathway to BAS in Cyber-Physical Systems; includes industrial cybersecurity certification.
Massachusetts Institute of Technology	While more theoretical, its Lincoln Lab conducts substantial ICS cybersecurity research.
Mississippi State University	One of the earliest ICS security testbeds; DHS/DOE partnership experience.
Purdue University	Center for Education and Research in Information Assurance and Security (CERIAS); OT-focused labs.
University of California, Berkeley	Strong ICS security and critical infrastructure protection work in EECS.
University of Illinois Urbana-Champaign	Cyber Resilient Energy Delivery Consortium (CREDC); extensive work on securing energy systems.
University of South Carolina	Home of the Critical Infrastructure and Industrial Control Systems Cybersecurity Lab.
University of Texas at San Antonio	Top-tier NSA-designated Center of Academic Excellence.

Findings

University Name	Location
Carnegie Mellon University	Pittsburgh, Pennsylvania
Case Western Reserve University	Cleveland, Ohio
Fisk University	Nashville, Tennessee
Mississippi State University	Starkville, Mississippi
University of South Carolina	Columbia, South Carolina
University of Texas at San Antonio	San Antonio, Texas
University of Tulsa	Tulsa, Oklahoma
Vanderbilt University	Nashville, Tennessee
North Carolina State University	Raleigh, North Carolina
Texas A&M University	College Station, Texas
University of Michigan	Ann Arbor, Michigan
University of Tennessee	Knoxville, Tennessee
Georgia Institute of Technology	Atlanta, Georgia
Idaho State University	Pocatello, Idaho
Massachusetts Institute of Technology	Cambridge, Massachusetts
Meharry Medical College	Nashville, Tennessee
The Pennsylvania State University	University Park, Pennsylvania
Purdue University	West Lafayette, Indiana
University of California, Berkeley	Berkeley, California
University of Illinois Urbana-Champaign	Urbana-Champaign, Illinois



Findings

- No formal joint coursework or interdisciplinary projects connecting nuclear engineering and cybersecurity programs
  - Cybersecurity curricula lacked nuclear-specific context
  - Nuclear engineering curricula seldomly addressed cybersecurity
- OT courses usually focused on other sectors, such as oil, gas, or water
- When nuclear-specific cybersecurity content was present, it was typically confined to the graduate-level research or isolated electives
- Hands-on training opportunities that simulate real-world OT environments were limited

Discussion

- Disconnect between cybersecurity and nuclear engineering educational programs
  - Curricular and institutional fragmentation
  - Limited hands-on training
  - Lack of specialized talent
- Proposed solutions
  - Scalable, tiered approach that reflects institutional differences
  - Focus on undergraduate level for early exposure
  - Three-tiered strategy interventions
    - Short-term: low-cost, high-impact activities that introduce nuclear cybersecurity concepts
    - Mid-term: formal integration
    - Long-term: institutionalized nuclear cybersecurity programs and partnerships with industry and national laboratories that provide real-world experience

Conclusion

- Persistent gap in the development of nuclear cybersecurity talent
- Without structured undergraduate engagement, students remain unaware of nuclear cybersecurity as a possible specialization
- Current practices in the nuclear sector are expensive, time-consuming, and inefficient; not scalable or sustainable
- Urgent need to integrate nuclear cybersecurity concepts into existing curricula at the undergraduate level
- Addressing the existing gap is a strategic opportunity for academic institutions

Thank You

Amorita A. Christian
MS, MBA, PMP

amorita-christian@utulsa.edu

www.utulsa.edu

Cyber Fellows