School of Cybersecurity

Daniel Takabi, Director

The School of Cybersecurity administers two degrees (a BS in Cybersecurity with majors in cybersecurity and cyber operations and an MS in Cybersecurity) and an interdisciplinary minor in cybersecurity. The School's strategic priority is to deliver exceptional academic programs for both resident and distance students to cultivate the cybersecurity workforce and enhance the nation's cybersecurity talent. The School supports undergraduate and graduate students and faculty to achieve healthy and sustainable growth of the cybersecurity program. The mission of the School also includes developing high-impact, cross-disciplinary research initiatives that center on cybersecurity and conducting outreach and community engagement, being a source of cybersecurity expertise to the community, the Hampton Roads region, the Commonwealth of Virginia, and the nation.

Programs

Master of Science Programs

- Cybersecurity (MS) (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-ms/)
- Cybersecurity with a Concentration in AI Security (MS) (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-ai-security-ms/)
- Cybersecurity with a Concentration in Cyber Conflict and Cyber Crime (MS) (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-cyber-conflict-crime-ms/)
- Cybersecurity with a Concentration in Cybersecurity Risk Management (MS) (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-risk-management-ms/)

Certificate Program

- Cybersecurity Risk Management Certificate (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-risk-management-certificate/)

CYPD 630 Cybersecurity Compliance Methodologies I (3 Credit Hours)
Students review and analyze the concepts and interrelationships underlying cybersecurity compliance methodologies, including the NIST Risk Management Framework (RMF); Federal Risk and Authorization Management Program (FedRAMP); NIST 800-171; CMMC; NIST Cyber Security Framework (CSF); and NIST 800-53. Students develop competencies to utilize NIST RMF Steps 1-3/FedRAMP Steps 1-2.

CYPD 631 Cybersecurity Compliance Methodologies Lab I (3 Credit Hours)
In a virtual lab system, students execute the NIST RMF Steps 1-3: Categorization, Security Control Selection and Security Control Assessment, and complete the associated analysis and documentation as required by NIST/FedRAMP/CMMC.

CYPD 632 Cybersecurity Compliance Methodologies II (3 Credit Hours)
Students develop the competencies to utilize the NIST RMF, Steps 4-6: Implementation, Authorization and Monitoring /FedRAMP, Steps 3-4. Students analyze how these steps relate to the CMMC accreditation process.

CYPD 633 Cybersecurity Compliance Methodologies Lab II (3 Credit Hours)
In a virtual lab system, students execute NIST RMF Steps 4-6: Implementation, Authorization and Monitoring, and complete the associated analysis and documentation, as required by the NIST/FedRAMP/CMMC frameworks.

CYPD 634 Audit and Risk Assessment Methods (3 Credit Hours)
Students review and analyze selected CISA, CISM, and CRISC audit and assessment function domains. Utilizing their domain knowledge, students complete case study audit and assessment tasks.

CYPD 635 Compliance Frameworks for the Enterprise (3 Credit Hours)
Students compare and contrast multiple compliance frameworks including ISO 27001, California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and Service Organization Control 2 (SOC2). They will examine selected intersections and redundancies in these frameworks and how to address them in a global context. Their analysis will include examining crosswalks between the NIST RMF and selected frameworks.

CYSE 516 Cyber Defense Fundamentals (3 Credit Hours)
This course focuses on cybersecurity theory, information protection and assurance, and computer systems and networks security. The objectives are to understand the basic security models and concepts, learn fundamental knowledge and tools for building, analyzing, and attacking modern security systems, and gain hands-on experience in cryptographic algorithms, security fundamental principles, and Internet security protocol and standards. (Offered fall)
Prerequisites: permission of the instructor
Pre- or corequisite: ECE 355 or equivalent or permission of the instructor

CYSE 519 Cyber Physical System Security (3 Credit Hours)
Cyber Physical Systems (CPS) integrate computing, networking, and physical processes. The objectives of this course are to learn the basic concepts, technologies and applications of CPS, understand the fundamental CPS security challenges and national security impact, and gain hands-on experience in CPS infrastructures, critical vulnerabilities, and practical countermeasures.
Prerequisites: ECE 355 or permission of the instructor

CYSE 520 Applied Machine Learning in Cybersecurity (3 Credit Hours)
This course introduces the concepts and technologies of machine learning with a focus on applications related to cybersecurity. The objectives are to learn fundamental knowledge and practical experience and identify the use case of machine learning techniques in cybersecurity. The course will discuss traditional and advanced machine learning techniques, e.g., neural network, deep convolutional neural network, generative adversarial network, and transfer learning algorithms. Students will engage in oral and written communication by reporting and presenting the materials of the course project.

CYSE 525 Cybersecurity Strategy and Policy (3 Credit Hours)
This course explores cybersecurity policy and strategy and introduces students to the essentials of strategy development and policy making in cybersecurity. Topics considered include planning principles in cyber strategy; risk management and cybersecurity policy; the connections between cybersecurity policies, businesses, and governmental institutions; the knowledge, skills, and abilities needed to develop and implement cybersecurity policy; the social, political and ethical implications that arise in cybersecurity policies and strategies; strategies to assess cybersecurity policy; and the ties between national security and cybersecurity policy.

CYSE 526 Cyber War (3 Credit Hours)
This course explores the national security dimensions of cybersecurity and examines cyber war in international relations. Exploration of cyber war begins with an examination of cybersecurity as a component of national security and investigates the topics of U.S National Cybersecurity and other national approaches to cyber war. The topics of cyber deterrence, cyber as a military domain, the roles of international organizations in cyber war, cyber terrorism, the role of social media, and information warfare will be discussed. The international dimension of cybersecurity is also discussed.

CYSE 595 Topics in Cybersecurity (1-3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described in information distributed to academic advisors.
Prerequisites: permission of the instructor

CYSE 596 Topics in Cybersecurity (1-3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described in information distributed to academic advisors.
Prerequisites: permission of the instructor

CYSE 597 Tutorial Work in Special Topics in Cybersecurity (1-3 Credit Hours)
Independent reading and study on a topic to be selected under the direction of an instructor. Conferences and papers as appropriate.
Prerequisites: approval of the Director of the Center for Cybersecurity Education and Research

CYSE 598 Tutorial Work in Special Topics in Cybersecurity (1-3 Credit Hours)
Independent reading and study on a topic to be selected under the direction of an instructor. Conferences and papers as appropriate.
Prerequisites: approval of the Director of the Center for Cybersecurity Education and Research

CYSE 600 Cybersecurity Principles (3 Credit Hours)
This course provides an overview of the field of cybersecurity. It covers core cybersecurity topics including computer system architectures, critical infrastructures, cyber threats and vulnerabilities, cryptography, cryptographic protocol design, information assurance, network security, and risk assessment and management. Students are expected to become familiar with fundamental security concepts, technologies and practices, and develop a foundation for further study in cybersecurity.

CYSE 601 Advanced Cybersecurity Techniques and Operations (3 Credit Hours)
This course introduces tools and techniques used to secure and analyze large computer networks and systems. It will include significant hands-on lab work. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform malware detection, forensic investigation, and practice techniques for penetration testing.

CYSE 603 Advanced Cybersecurity Law and Policy (3 Credit Hours)
This course addresses two major cyber law subject matters. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from civil and criminal perspectives. The second part, which builds upon the first, will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace are in compliance with U.S. law, regulations, directives and policies.

CYSE 605 Leadership and Management in Cybersecurity (3 Credit Hours)
This course introduces skills to manage technical professionals and lead strategic change in their organization. Based on the basic operations and functionality of cybersecurity systems, students will learn the management of cybersecurity technical professionals, including how to effectively lead and manage teams, how to launch and assess organizational change initiatives, and how to work effectively within an interdependent group to achieve common goals.

CYSE 607 Advanced Digital Forensics (3 Credit Hours)
This course introduces the concepts and technologies of digital forensics. Students will learn the advanced techniques and tools utilized for collecting, processing, and preserving digital evidence on computers, mobile devices, networks, and cloud computing environments. Students will also engage in oral and written communication to report digital forensic findings and prepare court presentation materials.

CYSE 610 Advanced Cryptography (3 Credit Hours)
This course studies advanced topics in cryptography. It begins with an overview of necessary background in algebra and number theory, private- and public-key cryptosystems, and basic signature schemes. It then upgrades the design and analysis of modern cryptography, including how the security model is defined, how practical cryptographic algorithms work, and how to exploit flaws in the current models of cryptography.

CYSE 615 Mobile and Wireless Security (3 Credit Hours)
An overview of wireless and mobile security providing students with practical and theoretical experiences. Topics include smartphone security, mobile Internet security, mobile location privacy, and wireless ad hoc, mesh, and sensor network security.

CYSE 625 Advanced Ethical Hacking and Penetration Testing (3 Credit Hours)
This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. Students will discover how system vulnerabilities can be exploited and learns to avoid such problems.

CYSE 635 AI Security and Privacy (3 Credit Hours)
This course focuses on Machine Learning (ML) security and privacy. Students will understand and explore the vulnerabilities of the ML models, learn how to develop and deploy defenses to mitigate possible attacks, and gain hands-on experience to protect private data during model training and testing.

CYSE 695 Advanced Topics in Cybersecurity (1-3 Credit Hours)
The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described by academic advisors.
Prerequisites: Permission of the instructor

CYSE 697 Independent Study in Cybersecurity (3 Credit Hours)
This course allows students to develop specialized expertise by independent study (supervised by a faculty member).

CYSE 698 Master's Project (3 Credit Hours)
This capstone course provides opportunities to synthesize and apply the knowledge and skills to solve real-world cyber security problems.