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 on-campus and online 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 for Cybersecurity (MS) (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-ai-for-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

- Artificial Intelligence (AI) in Cyber Defense Certificate (http://catalog.odu.edu/graduate/cybersecurity/artificial-intelligence-in-cyber-defense-certificate/)
- Cybersecurity Risk Management Certificate (http://catalog.odu.edu/graduate/cybersecurity/cybersecurity-risk-management-certificate/)
- Trustworthy Artificial Intelligence Certificate (http://catalog.odu.edu/graduate/cybersecurity/trustworthy-artificial-intelligence-certificate/)

CYSE 510 Artificial Intelligence (AI) Methods and Models (3 Credit Hours)
This course offers an introduction to Artificial Intelligence (AI). Students will explore the field's fundamental concepts, techniques, and applications. Methods, such as Generative AI (GenAI) that enable machines to learn and process information, and models, such as machine learning (ML) that uses data sets to recognize patterns and make decisions without human intervention will be covered. The course is designed for non-specialists and does not require prior computer science or programming knowledge.

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 521 Generative AI in Cybersecurity (3 Credit Hours)
This course provides an in-depth examination of the intersection between Generative AI (Gen AI) and Cybersecurity. It focuses on the dual nature of advanced AI systems as both enhancers and potential threats to security infrastructure. Students will acquire a comprehensive understanding of the underlying principles, algorithms, and practical applications of Gen AI models in the discovery of attack vectors, identification of cyber threats, and automation of security tasks. Additionally, the course will address defensive strategies aimed at mitigating the risks stemming from AI-driven cyberattacks.

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 530 Introduction to Cybersecurity Risk Management (3 Credit Hours)
This course addresses the broad topic of risk management and how risk, threats, and vulnerabilities impact information systems. Areas of instruction include how to assess and manage risk based on defining an acceptable level of risk for information systems. Elements of a business impact analysis (BIA), business continuity plan (BCP), disaster recovery plan (DRP), and computer incident response team (CIRT) plan will also be discussed.

CYSE 531 Advanced Techniques Cybersecurity Risk Management (3 Credit Hours)
Expert-level approach on the Risk Management Framework (RMF) system Authorization to Operation (ATO), including Continuous cATO. Curriculum that is aligned to the NIST SP 800-53, Revision 5. Advanced topics include Assess and Authorize, System Categorization, Security Control Assessment, System Test Results, Plan of Action and Milestones (POA&M), and Continuous Monitoring (CONMON).

CYSE 532 Cyber Risk CSF/CMMC (3 Credit Hours)
This course introduces cybersecurity, the NIST Cybersecurity Framework (CSF), and the Cybersecurity Maturity Model Certification (CMMC) program. Topics to be addressed include the risk management fundamentals, IT risk management, and cyber risk controls; cyber threats and vulnerabilities; data security and sanitization; the NIST CSF, including its core functions, categories, and subcategories; and the CMMC comprising its levels, domains, and implementation guidelines.

CYSE 533 Cyber Risk FedRAMP/Audit (3 Credit Hours)
This course explores the Federal Risk and Authorization Management Program (FedRAMP) and Auditing. Topics to be addressed include an overview of the FedRAMP framework, including its objectives, components, and stages; the needed documents and guidelines to develop system security plans and security assessment reports; the NIST Risk Management Framework (RMF) comprising its different stages and the adoption mechanism; FISMA compliance and auditing assessment; and real-world case studies and future challenges.

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 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 instructor

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 602 Advanced Techniques for Cyber Defense (3 Credit Hours)
This course offers a deep dive into advanced cybersecurity techniques and operations, aiming to bolster cyber defense strategies. Participants will explore state-of-the-art methodologies encompassing threat analysis, incident response, ethical hacking, secure network architecture, and proactive mitigation strategies. Through immersive, hands-on experiences and real-world simulations, learners will develop the expertise required to adeptly secure digital environments against ever-evolving cyber threats. This course may be used as a leveling course.

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 608 Windows System for Cybersecurity (3 Credit Hours)
This course teaches the basic fundamentals of using and creating Windows Server domains using PowerShell. It also covers topics like active directory, server administration, and technologies such as Group Policy, Network Policy Server (NPS), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). Additionally, it includes lessons on disk management, firewall administration, and Windows Server Networking Services like IPv4, IPv6, and more. This course may be used as a leveling course.

CYSE 609 Fundamentals of Linux System for Cybersecurity (3 Credit Hours)
This course introduces the basic operations in major Linux distros for cybersecurity using both graphical interface and command-line interface. Students will learn about the basic installation and configuration, file systems management, shell scripts, and user authentication in Linux systems. This course may be used as a leveling course.

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 626 Web Archiving Theory, Practice, and Implications (3 Credit Hours)
An interdisciplinary introduction to web archiving fundamentals including web crawling, collection development and summarization including planning, analyzing, and sharing collections. Includes a review of ethical and legal issues, trustworthiness, preservation, security, and cultural impact of web archiving.
Prerequisites: This course is intended for Cybersecurity students

CYSE 630 Introduction to Cybersecurity Risk Management (3 Credit Hours)
This course addresses the broad topic of risk management and how risk, threats, and vulnerabilities impact information systems. Areas of instruction include how to assess and manage risk based on defining an acceptable level of risk for information systems. Elements of a business impact analysis (BIA), business continuity plan (BCP), disaster recovery plan (DRP), and computer incident response team (CIRT) plan will also be discussed.

CYSE 631 Advanced Techniques Cybersecurity Risk Management (3 Credit Hours)
Expert-level approach on the Risk Management Framework (RMF) system Authorization to Operation (ATO), including Continuous cATO. Curriculum that is aligned to the NIST SP 800-53, Revision 5. Advanced topics include Assess and Authorize, System Categorization, Security Control Assessment, System Test Results, Plan of Action and Milestones (POA&M), and Continuous Monitoring (CONMON).

CYSE 632 Cyber Risk CSF/CMMC (3 Credit Hours)
This course introduces cybersecurity, the NIST Cybersecurity Framework (CSF), and the Cybersecurity Maturity Model Certification (CMMC) program. Topics to be addressed include the risk management fundamentals, IT risk management, and cyber risk controls; cyber threats and vulnerabilities; data security and sanitization; the NIST CSF, including its core functions, categories, and subcategories; and the CMMC comprising its levels, domains, and implementation guidelines.

CYSE 633 Cyber Risk FedRAMP/Audit (3 Credit Hours)
This course explores the Federal Risk and Authorization Management Program (FedRAMP) and Auditing. Topics to be addressed include an overview of the FedRAMP framework, including its objectives, components, and stages; the needed documents and guidelines to develop system security plans and security assessment reports; the NIST Risk Management Framework (RMF) comprising its different stages and the adoption mechanism; FISMA compliance and auditing assessment; and real-world case studies and future challenges.

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 640 Trustworthy and Responsible AI (3 Credit Hours)
This course introduces the concepts and the characteristics of trustworthy AI and the essential building blocks of AI trustworthiness with a focus on safety, reliability, resiliency, accountability and transparency, explainability and interpretability, fairness, and ethics. Students will gain an understanding of Trustworthy and Responsible AI concepts and gain hands-on experience in developing AI systems in a responsible and trustworthy manner.

CYSE 645 Advanced Cybersecurity Risk Management Practices (3 Credit Hours)
Expert-level approach on the Risk Management Framework (RMF) system Authorization to Operation (ATO), including Continuous cATO. Curriculum that is aligned to the NIST SP 800-53, Revision 5. Advanced topics include Assess and Authorize, System Categorization, Security Control Assessment, System Test Results, Plan of Action and Milestones (POA&M), and Continuous Monitoring (CONMON).

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.

CYSE 800 Research Methods in Cybersecurity (3 Credit Hours)
Students learn how to use multiple research methods to conduct cybersecurity research. Students will conduct a multi-method research project in interdisciplinary groups.
Prerequisites: CYSE 600

CYSE 801 Advanced Cybersecurity Techniques and Operations II (3 Credit Hours)
Students apply the tools and techniques learned in Advanced Cybersecurity Techniques and Operations. Virtual laboratory work is conducted, and students produce scientific reports describing the results of their analyses, investigations, and diagnoses.
Prerequisites: CYSE 601

CYSE 802 Cybersecurity Seminar (3 Credit Hours)
Introduces new PhD students to the study of cybersecurity through an interdisciplinary lens through different fields of study offered as doctoral programs at ODU. Students will read studies published by ODU scholars and discuss how interdisciplinary research informs society. Students will identify possible research agendas for their doctoral studies. Professional development will be included.

CYSE 803 Moral Reasoning for Emerging Technologies (3 Credit Hours)
This course provides training in how to think critically and inclusively about moral and ethical concerns in the context of new, emerging, and developing technologies. In these contexts where ethical guidelines and practices have not been fully developed, it is necessary to have experience with flexible and adaptive training in identifying and thinking through moral concerns. Students will develop these skills through a study of philosophy of technology, history of technology, and Science and Technology Studies combined with active and creative forms of speculative application of these theories and methods.

CYSE 869 Cybersecurity Practicum (3 Credit Hours)
This course satisfies the cybersecurity PhD teaching requirement. During the semester enrolled, the student must be assigned as a teaching assistant or instructor of record and teach at least three hours of class and prepare at least one assignment, quiz or equivalent. PhD students are expected to satisfy the teaching requirement after completing their first year of study and at least one semester prior to scheduling their PhD defense.

CYSE 899 Doctoral Dissertation (1-9 Credit Hours)
Research for the doctoral dissertation.