Doctor of Philosophy

Cybersecurity (PhD)

Program Director: Mohammad GhasemiGol

The PhD in Cybersecurity prepares students to become advanced researchers, faculty members, and technical leaders in the rapidly evolving field of cybersecurity. The program emphasizes rigorous research, interdisciplinary collaboration, ethical and societal implications of emerging technologies, and hands-on experience in advanced cyber operations and defense. Research in the program is led by faculty affiliated with the School of Cybersecurity. Faculty expertise includes artificial intelligence security, applied cryptography, cyber defense, digital forensics, cyber policy and governance, privacy-preserving systems, malware analysis, trustworthy AI, network security, human factors in cybersecurity, cyber risk management, and critical infrastructure protection.

Students entering the PhD program in Cybersecurity must meet the minimum university graduate admission requirements (https://www.odu.edu/admission/graduate (https://www.odu.edu/admission/graduate/)).

Applicants must hold a bachelor's or master's degree from a regionally accredited U.S. institution or international equivalent, with verified official transcripts. Degrees should normally be in cybersecurity, computer science, information technology, engineering, mathematics, or a closely related field. Students without a background in Cybersecurity or a related field may be considered on an individual basis and may be required to complete leveling coursework prior to beginning the program. Prior to applying for admission, students are encouraged to visit the School's website and ensure that their research interests match those of a faculty member. Applicants are expected to demonstrate preparation in cybersecurity fundamentals, programming, computer networks, operating systems, information assurance, and mathematics relevant to cybersecurity research.

Applicants are required to submit:

· Official transcripts from all colleges and universities attended

· Two letters of recommendation from individuals familiar with the applicant's academic and professional background

· Resume or curriculum vitae

· Personal statement of purpose (SOP)

· GRE scores (waivers may be considered)

International applicants must also satisfy the university's English proficiency requirements.

A candidate for the doctoral degree in cybersecurity must satisfy all university doctoral degree requirements in addition to the following departmental requirements:

- Complete a minimum of 78 credit hours beyond the bachelor's degree or 48 credit hours beyond the master's degree.
- Complete all required core coursework and approved electives.
- Complete Responsible Conduct of Research (RCR) training.
- Attend the School seminars and professional development activities.
- Complete a cybersecurity teaching practicum.
- Develop a dissertation topic that is approved by the student's PhD dissertation advisor.
- Pass the PhD candidacy examination.
- Successfully defend the dissertation proposal.
- Complete a minimum of 18 credit hours of CYSE 899 Doctoral Dissertation.
- Successfully defend the doctoral dissertation.
- Complete the Graduate Teaching Assistant Instructors' Institute (GTAI).

The above requirements must ordinarily be completed within eight years after admission to the PhD program.

Course Requirements.

All students must complete 48 credit hours as specified below.

CYSE 800	Research Methods in Cybersecurity (Research Methods in Cybersecurity should be taken during the student's first year in the PhD program.)	3
CYSE 801	Advanced Cybersecurity Techniques and Operations II	3
CYSE 803	Moral Reasoning for Emerging Technologies	3
CYSE 802	Cybersecurity Seminar	3
CYSE 869	Cybersecurity Practicum (• The teaching practicum requirement must be completed before scheduling the dissertation defense)	3
Advance Electives (Additional approved graduate coursework may be applied with advisor approval.)		*15*
CS 764	Blockchains and Cryptocurrencies: Fundamentals, Technologies, and Economics	
CS 865	Internet of Things Security	
CS 872	Advanced Computer and Network Security	
CS 873	Data Mining and Security	
ENGL 830	The Digital Humanities	
ENMA 801	Digital Systems Engineering	
ENMA 824	Risk Analysis	
ENMA 825	System Risk and Failure Analysis	
ENMA 850	System of Systems Engineering	
ENMA 855	Human System Engineering	
ENMA 871	Risk and Vulnerability Management of Complex Interdependent Systems	
ECE 742	Computer Communication Networks	
IDT 830	Principles and Practices of Human Performance Technology	
IS 721/821	New World Order: Chaos and Coherence	
PSYC 870	Human Factors Psychology	
PSYC 876	Human-Computer Interaction	
CYSE 899	Doctoral Dissertation (• Students are encouraged to publish refereed research papers during the program)	18
Total Credit Hours		**48**

Students without a master's degree in cybersecurity or related field must complete an additional 30 credit hours (for a total of 78 credit hours of graduate coursework) as specified below:

CYSE 600	Cybersecurity Principles	3
CYSE 601	Advanced Cybersecurity Techniques and Operations	3
CYSE 603	Advanced Cybersecurity Law and Policy	3
CYSE 605	Leadership and Management in Cybersecurity	3
CYSE 516	Cyber Defense Fundamentals	3
Restricted Foundation Electives		*15*
CYSE 519	Cyber Physical System Security	
CYSE 520	Applied Machine Learning in Cybersecurity	
CYSE 525	Cybersecurity Strategy and Policy	
CYSE 526	Cyber War	
CYSE 595	Topics in Cybersecurity	
CYSE 607	Advanced Digital Forensics	
CYSE 610	Advanced Cryptography	
CYSE 615	Mobile and Wireless Security	

CYSE 625	Advanced Ethical Hacking and Penetration Testing
CYSE 635	AI Security and Privacy
CYSE 695	Advanced Topics in Cybersecurity
CYSE 697	Independent Study in Cybersecurity
CS 522	Introduction to Machine Learning
CS 564	Networked Systems Security
CS 565	Information Assurance for Cybersecurity
CS 566	Principles and Practice of Cyber Defense
CS 567	Introduction to Reverse Software Engineering
CS 569	Data Analytics for Cybersecurity
CS 580	Introduction to Artificial Intelligence
CS 624	Data Analytics and Big Data
CS 722/822	Machine Learning
CS 733/833	Natural Language Processing
CS 761/861	Malware Analysis and Reverse Engineering
ENMA 625	Introduction to Homeland Security Logistics
IT 634	Cloud Computing and Security
MSIM 670	Cyber Systems Engineering
Total Credit Hours	**30**

Restricted foundational electives and advanced electives are selected in consultation with the advisor and must support the student's preparation for doctoral research. Electives may be drawn from cybersecurity and other approved graduate disciplines relevant to the student's dissertation and research interests.

Advisor

Upon admission to the PhD program, a faculty advisor will be assigned to the student for general guidance. The student is expected to work with the assigned advisor to plan coursework, identify research interests, and select electives that support doctoral preparation. The student is expected to identify a dissertation advisor by the time formal coursework is completed. The dissertation advisor must be a member of the ODU Graduate Faculty and a member of, or affiliated with, the School of Cybersecurity. Changes in advisor assignment require approval of the Graduate Program Director.

Candidacy Examination

Students must complete the candidacy examination process after completion of formal coursework and before becoming heavily involved in dissertation research.

- The candidacy examination includes both written and oral components designed to assess the student's:
- Understanding of cybersecurity research literature
- Ability to critically analyze technical and interdisciplinary problems
- Research communication skills
- Readiness to conduct doctoral-level research

The examination committee is appointed by the Graduate Program Director and consists of at least three graduate-certified faculty members.

Students who fail the candidacy examination may retake the examination once. Two unsuccessful attempts will result in dismissal from the PhD program.

Advancement to Candidacy

Advancement to doctoral candidacy is based on successful completion of all required coursework and successful completion of both the written and oral portions of the candidacy examination. Students who advance to candidacy are eligible to enroll in doctoral dissertation credits.

Dissertation Committee

After advancement to candidacy and approval of the dissertation topic, the Dissertation Committee is formed to supervise dissertation research and evaluate the proposal and final dissertation defense.

The Dissertation Committee:

- Must consist of at least three graduate-certified faculty members
- Must include at least two ODU faculty members
- Must include at least one member external to the student's department or an approved external expert
- It is formed by the dissertation advisor in consultation with the students and the Graduate Program Director.

Dissertation Proposal

The oral examination of the written dissertation proposal, is designed to test the student's knowledge of background material related to the dissertation topic and to determine if the student has identified a significant problem, has a plan of attack, and is ready to proceed with the dissertation research. The proposal should include:

- Literature review and related work
- Problem statement and research objectives
- Proposed methodology
- Evaluation plan
- Timeline and expected contributions

The student presents the proposal publicly, followed by questioning from the Dissertation Committee. The student must receive approval from the dissertation committee to continue to the dissertation research. Students who fail will be allowed to schedule a second proposal defense within one academic semester. If a student does not approval the second time, they will be dismissed from the degree program.

Dissertation

Students must complete a minimum of 18 credit hours of CYSE 899 Doctoral Dissertation. The dissertation must represent an original and significant contribution to cybersecurity research. Students are expected to disseminate research findings through refereed publications, conference presentations, and scholarly activities. Students are required to publish (or have in the revision process) at least one paper in a refereed journal or refereed conference proceedings based on their dissertation work.

Dissertation Defense

The dissertation defense is an oral presentation of the dissertation research and findings, open to the University community. The dissertation committee will examine the candidate's presentation, written dissertation, and responses to questions. The examination committee must be provided with the completed dissertation at least two weeks before the examination date.

The committee will approve, approve with condition(s), or disapprove the dissertation. If the student fails to successfully defend the dissertation, the student may request a second defense, following the same procedures as for the initial defense. If the student fails on the second attempt to defend the dissertation, the student will be terminated from the program.

Time Requirement

The proposed PhD degree program in Cybersecurity will be offered on a full-time and part-time bases. Students entering with a bachelor's degree will be required to attend full-time. Per ODU Policy Graded coursework granted outside the eight-year time limit established for graduate degrees or certificates must be re-validated by an examination before the work can be applied toward the requirements of a degree program.

Additional Program Information

The program provides opportunities for:

- Graduate assistantships
- Interdisciplinary collaboration

- Advanced cybersecurity laboratories
- Access to cybersecurity infrastructure
- Industry and government partnerships
- Research publication and conference participation