School of Cybersecurity

School of Cybersecurity

Saltuk Karahan, Interim 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.

Master of Science in Cybersecurity

Chunsheng Xin, Graduate Program Director

The Master of Science in Cybersecurity is a 30-credit hour non-thesis degree program. It is designed to prepare cyber security technology leaders. Graduates will develop skills and competencies in technical aspects of cyber security and will be prepared to assume responsibility for the management of cybersecurity projects and coordination of cyber operation teams. It also provides preparation for students desiring to pursue doctoral studies or teach cybersecurity courses in 2- and 4-year colleges and universities.

The program is offered in online format and with the option for local students to attend classes on campus. The required core courses focus on the fundamental knowledge of cybersecurity, covering advanced cybersecurity principles, techniques, and operations, as well as advanced topics in law, policy, management and leadership in cybersecurity. Students will have opportunities to choose five restricted electives to learn about different aspects of cybersecurity. The capstone course provides opportunities to synthesize and apply the knowledge and skills to solve real-world cybersecurity problems.

Application Procedures

The completed application for the Master of Science Cybersecurity program will include the following items:

1. Official copies of transcripts from all colleges/universities attended.
2. Two letters of recommendation from individuals familiar with applicant’s professional and/or academic background.
3. A current resume.
4. A statement of professional goals and academic objectives.
5. A completed application form.
6. Receipt of the application fee. Checks should be made payable to Old Dominion University.
7. TOEFL test scores, sent directly from the ETS to ODU International Graduate Admission Office must accompany international applications for applicants with a degree issued outside of the United States.

Applications to Old Dominion University can be completed on-line at http://www.odu.edu/admission/graduate (http://www.odu.edu/admission/graduate/).

The applicant is responsible to ensure that all application materials are received and the application is complete in all respects.

Curriculum and Requirements

This program consists of four core courses (12 credit hours), five electives (15 credit hours), and one capstone course (3 credit hours). The four core courses focus on the fundamental knowledge of cybersecurity, covering advanced cybersecurity principles, techniques, and operations, as well as advanced topics in law, policy, management and leadership in cybersecurity.

The five electives provide students with opportunities to learn about different aspects of cybersecurity, e.g., in information systems, network systems, mobile and wireless systems, operating systems, and cyber-physical systems. Courses are also offered to address such important cybersecurity topics as reverse software engineering, digital forensics, threat modeling, and ethical hacking and penetration testing.

The capstone course brings together students in their final semester of study to synthesize knowledge from their previous coursework and apply it to solve real-world cybersecurity problems. The faculty member who teaches the capstone course will work with industrial and academic partners who will serve as external mentors of the capstone course. Each student in the capstone course will discuss—with both faculty member and mentor—development of her/his master’s project that aims to solve a cybersecurity problem in a real-world business setting.

Core Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 600</td>
<td>Cybersecurity Principles</td>
</tr>
<tr>
<td>CYSE 601</td>
<td>Advanced Cybersecurity Techniques and Operations</td>
</tr>
<tr>
<td>CYSE 603</td>
<td>Advanced Cybersecurity Law and Policy</td>
</tr>
<tr>
<td>CYSE 605</td>
<td>Leadership and Management in Cybersecurity</td>
</tr>
</tbody>
</table>

Restricted Elective Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 564</td>
<td>Networked Systems Security</td>
</tr>
<tr>
<td>CS 565</td>
<td>Information Assurance for Cybersecurity</td>
</tr>
<tr>
<td>CS 566</td>
<td>Principles and Practice of Cyber Defense</td>
</tr>
<tr>
<td>CS 567</td>
<td>Introduction to Reverse Software Engineering</td>
</tr>
<tr>
<td>CS 569</td>
<td>Data Analytics for Cybersecurity</td>
</tr>
<tr>
<td>CYSE 516</td>
<td>Cyber Defense Fundamentals</td>
</tr>
<tr>
<td>CYSE 519</td>
<td>Cyber Physical System Security</td>
</tr>
<tr>
<td>CYSE 520</td>
<td>Applied Machine Learning in Cybersecurity</td>
</tr>
<tr>
<td>CYSE 525</td>
<td>Cybersecurity Strategy and Policy</td>
</tr>
<tr>
<td>CYSE 526</td>
<td>Cyber War</td>
</tr>
<tr>
<td>CYSE 595</td>
<td>Topics in Cybersecurity *</td>
</tr>
<tr>
<td>CYSE 596</td>
<td>Topics in Cybersecurity *</td>
</tr>
<tr>
<td>CYSE 597</td>
<td>Tutorial Work in Special Topics in Cybersecurity</td>
</tr>
<tr>
<td>CYSE 598</td>
<td>Tutorial Work in Special Topics in Cybersecurity</td>
</tr>
<tr>
<td>CYSE 607</td>
<td>Advanced Digital Forensics</td>
</tr>
<tr>
<td>CYSE 610</td>
<td>Advanced Cryptography</td>
</tr>
<tr>
<td>CYSE 615</td>
<td>Mobile and Wireless Security</td>
</tr>
<tr>
<td>CYSE 625</td>
<td>Advanced Ethical Hacking and Penetration Testing</td>
</tr>
<tr>
<td>CYSE 635</td>
<td>AI Security and Privacy</td>
</tr>
<tr>
<td>CYSE 697</td>
<td>Independent Study in Cybersecurity *</td>
</tr>
<tr>
<td>IT 624</td>
<td>Information Technology Assurance Services</td>
</tr>
<tr>
<td>IT 685</td>
<td>Introduction to Information Security</td>
</tr>
<tr>
<td>MSIM 670</td>
<td>Cyber Systems Engineering</td>
</tr>
</tbody>
</table>

Capstone Course

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 698</td>
<td>Master's Project</td>
</tr>
</tbody>
</table>

Total Hours

<table>
<thead>
<tr>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Courses</td>
<td>15</td>
</tr>
<tr>
<td>Electives</td>
<td>15</td>
</tr>
<tr>
<td>Capstone</td>
<td>15</td>
</tr>
</tbody>
</table>

Note on CYSE 595, CYSE 596, and CYSE 697: CYSE 595 can be taken multiple times by a student as long as the CYSE 595 courses have different titles. However, if a student has already taken a CYSE 595 course, which is converted to a regularly numbered course (generally the same title) in a future semester, the student cannot take the converted course any more. The rules of CYSE 595 are also applicable to CYSE 596. CYSE 697 can also be taken multiple times by a student, but the research topics on different CYSE 697 courses need to be different.
Recommended Plan of Study for Full-Time Students

**First Year**

<table>
<thead>
<tr>
<th>First Term</th>
<th>Hours</th>
<th>Second Term</th>
<th>Hours</th>
<th>Summer Term</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 600</td>
<td>3</td>
<td>CYSE 601</td>
<td>3</td>
<td>CYSE 698</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 605</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Elective</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Elective</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total credit hours: 30

**Recommended Plan of Study for Part-Time Students**

**First Year**

<table>
<thead>
<tr>
<th>First Term</th>
<th>Hours</th>
<th>Second Term</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 600</td>
<td>3</td>
<td>CYSE 601</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 605</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
</tr>
</tbody>
</table>

Second Year

<table>
<thead>
<tr>
<th>First Term</th>
<th>Hours</th>
<th>Second Term</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 603</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
</tr>
<tr>
<td>Restricted Elective</td>
<td>3</td>
<td>Restricted Elective</td>
<td>3</td>
</tr>
</tbody>
</table>

Total credit hours: 30

**MS in Cybersecurity Concentration Areas**

The MS in Cybersecurity concentrations are designed for the students who are interested to focus on a specific area in cybersecurity. An admitted student can be accepted to a concentration upon the approval of the Graduate Program Director. The concentration will be posted on the transcript.

**Artificial Intelligence (AI) Security Concentration**

Artificial Intelligence (AI) security is an integral part of cybersecurity. This concentration will expose students to sophisticated AI security principles and tools.

**Required Core Courses**

- 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

**Required Electives for Concentration**

- CS 522 Introduction to Machine Learning 3
- CS 580 Introduction to Artificial Intelligence 3
- CS 569 Data Analytics for Cybersecurity 3
- CYSE 652 Applied Machine Learning in Cybersecurity 3
- CYSE 635 AI Security and Privacy 3

**Capstone**

CYSE 698 Master's Project 3

**Total Hours** 30

**Cyber Conflict and Cyber Crime Concentration**

**Required Core Courses**

- 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

**Required Electives for Concentration**

- CYSE 525 Cybersecurity Strategy and Policy 3
- CYSE 526 Cyber War 3
- CYSE 607 Advanced Digital Forensics 3
- CYSE 595 Topics in Cybersecurity (International Aspects of Cybersecurity) 3
- CYSE 595 Topics in Cybersecurity (Human Factors and Policy Management in Cybersecurity) 3

**Capstone**

CYSE 698 Master's Project 3

**Total Hours** 30

**Cybersecurity Risk Management Concentration**

This concentration is a linked concentration for the students in Cybersecurity Risk Management Certificate program. After the students complete the certificate program, if they seek to further enhance knowledge and skills in cybersecurity, they can be accepted to this concentration. When students complete the program, they will have a comprehensive understanding of cybersecurity as well as project experience in applying the NIST Risk Management Framework (RMF) to practical problems of information security and security auditing.

**Required Core Courses**

- 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

**Required Electives for Concentration**

- Select five of the following:
  - CYPD 630 Cybersecurity Compliance Methodologies I 3
  - CYPD 631 Cybersecurity Compliance Methodologies Lab I 3
  - CYPD 632 Cybersecurity Compliance Methodologies II 3
  - CYPD 633 Cybersecurity Compliance Methodologies Lab II 3
  - CYPD 634 Audit and Risk Assessment Methods 3
  - CYPD 635 Compliance Frameworks for the Enterprise 3

**Capstone**

CYSE 698 Master's Project 3

**Total Hours** 15

**Financial Aid**

Sources of financial aid available to students include:

1. Research and teaching assistantships and
2. Loans.
Cybersecurity Risk Management Graduate Certificate

A key tool for addressing the mounting cyber threats is the NIST Risk Management Framework required by the Federal Information Security Act (FISMA). When students complete the certificate program, they will have a comprehensive understanding of it as well as project experience in applying the NIST Risk Management Framework (RMF)—the foundational framework which guides information security and information security auditing.

Certificate Program Admission Information

The following admission requirements will apply to all applicants. All students must:

- Submit a completed online application and the application fee.
- Submit transcripts of all undergraduate and graduate work from regionally accredited institutions.

Applicants who have not earned a degree in the United States must also submit:

- Current scores on the Test of English as a Foreign Language (TOEFL),
- A sample of scholarly writing, and three recommendations, at least one of which evaluates proficiency in English.

Certificate Program Requirements

Students are required to complete the following six graduate courses. The curriculum is based on standards established by the National Institute of Standards and Technology. Students are required to maintain a minimum GPA of 3.0/4.0.

Required Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYPD 630</td>
<td>Cybersecurity Compliance Methodologies I</td>
<td>3</td>
</tr>
<tr>
<td>CYPD 631</td>
<td>Cybersecurity Compliance Methodologies Lab I</td>
<td>1</td>
</tr>
<tr>
<td>CYPD 632</td>
<td>Cybersecurity Compliance Methodologies Lab II</td>
<td>2</td>
</tr>
<tr>
<td>CYPD 633</td>
<td>Cybersecurity Compliance Methodologies Lab II</td>
<td>2</td>
</tr>
<tr>
<td>CYPD 634</td>
<td>Audit and Risk Assessment Methods</td>
<td>1</td>
</tr>
<tr>
<td>CYPD 635</td>
<td>Compliance Frameworks for the Enterprise</td>
<td>1</td>
</tr>
</tbody>
</table>

CYBERSECURITY Courses

**CYSE 516. Cyber Defense Fundamentals, 3 Credits.**
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 Credits.**
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 Credits.**
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 Credits.**
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 Credits.**
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 Credits.**
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. Prerequisite: permission of the instructor.

**CYSE 596. Topics in Cybersecurity, 1-3 Credits.**
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. Prerequisite: permission of the instructor.

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

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

**CYSE 600. Cybersecurity Principles, 3 Credits.**
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 Credits.**
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 Credits.**
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 Credits.
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 Credits.
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 Credits.
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 Credits.
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 Credits.
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 Credits.
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 Credits.
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 Credits.
This course allows students to develop specialized expertise by independent study (supervised by a faculty member).

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