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.

Bachelor of Science - Cybersecurity Major

Saltuk Karahan, Program Coordinator and Advisor skarahan@odu.edu (http://catalog.odu.edu/(skarahan@odu.edu)

The Bachelor of Science degree with a major in cybersecurity provides opportunities for students to integrate education and training with the application of problem-solving skills in the lab environment. Courses are drawn from the disciplines of philosophy, computer science, computer engineering, information technology, and criminal justice to examine the multi-faceted nature of cybersecurity. Students admitted to the program have the opportunity to study the principles and application courses depending on which Principles and Application courses they select.

Cybersecurity - BS (http://catalog.odu.edu/undergraduate/schoolofcybersecurity/cybersecurity-bs-fouryearplan/)

- The four-year plan is a suggested curriculum to complete this degree program in four years. It is just one of several plans that will work and is presented only as broad guidance to students. Each student is strongly encouraged to develop a customized plan in consultation with their academic advisor. Additional information can also be found in Degree Works.

No more than two classes, or six credits, may be counted for both the major and a minor. Some minors may allow fewer credits to share.

Lower-Division General Education

<table>
<thead>
<tr>
<th>Course</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written Communication</td>
<td>6</td>
</tr>
<tr>
<td>Oral Communication</td>
<td>3</td>
</tr>
<tr>
<td>Mathematics (MATH 162M required)**</td>
<td>3</td>
</tr>
<tr>
<td>Language and Culture</td>
<td>0-6</td>
</tr>
<tr>
<td>Information Literacy and Research</td>
<td>3</td>
</tr>
<tr>
<td>Human Creativity</td>
<td>3</td>
</tr>
<tr>
<td>Interpreting the Past</td>
<td>3</td>
</tr>
<tr>
<td>Literature</td>
<td>3</td>
</tr>
<tr>
<td>Philosophy and Ethics (can be met by PHIL 355E)</td>
<td>0-3</td>
</tr>
<tr>
<td>The Nature of Science</td>
<td>8</td>
</tr>
<tr>
<td>Impact of Technology (met with CYSE 200T/IT 200T in the major)</td>
<td>3</td>
</tr>
<tr>
<td>Human Behavior (CRJS 215S or SOC 201S)</td>
<td>3</td>
</tr>
</tbody>
</table>

Prerequisite Courses 15-36

Students may be required to complete an additional 15-36 hours of prerequisite courses depending on which Principles and Application courses they select.

Interdisciplinary Writing Course

- IDS 300W Interdisciplinary Theory and Concepts 3

Core Courses 24

- CYSE/IT 200T Cybersecurity, Technology, and Society
- CYSE 201S Cybersecurity and the Social Sciences
- CYSE 250 Basic Cybersecurity Programming and Networking
- CYSE 300 Introduction to Cybersecurity
- CYSE 301 Cybersecurity Techniques and Operations
- CYSE/CRJS/CPD 406 Cyber Law
- CYSE 425W Cybersecurity Strategy and Policy (C or better required)
- or POLS 425W Cybersecurity Strategy and Policy
- CS 462 Cybersecurity Fundamentals

Principles Courses 9

Select three courses from the following. The coursework allows students to apply fundamental cybersecurity theories and techniques in their selected application domains.

- CRJS 310 Cybercriminology: Foundations
- CS 463 Cryptography for Cybersecurity
- CS 464 Networked Systems Security
- CYSE 495 Topics in Cybersecurity (Human Factors and Policy Management in Cybersecurity)
- ECE/MSIM 416 Cyber Defense Fundamentals
- ECE/MSIM 419 Cyber Physical System Security
- ECE/MSIM 470 Foundations of Cyber Security
- IT 315 Introduction to Networking and Security
- IT 417 Management of Information Security
- IT 418 Enterprise Information Assurance
- or CS 465 Information Assurance for Cybersecurity
- PHIL 355E Cybersecurity Ethics

Application Courses 9

Select three courses from the following. The coursework allows students to apply fundamental cybersecurity theories and techniques in their selected application domains.

- CYSE 270 Linux System for Cybersecurity
- CYSE 280 Windows System Management and Security
- CYSE 407/ CRJS 395 Applied Forensics
- CYSE 420 Applied Machine Learning in Cybersecurity
- CYSE 426 Cyber War
- or POLS 426 Cyber War
- CYSE 450 Ethical Hacking and Penetration Testing
- CS 467 Introduction to Reverse Software Engineering
- CS 471 Operating Systems
- ECE 452 Introduction to Wireless Communication Networks
- ECE 455 Network Engineering and Design
- IT 410 Business Intelligence
- IT 416 Network Server Configuration and Administration
- IT 419 Enterprise Cyber Defense
- IT 461 Implementing Internet Applications
- RMI 412 Property & Liability Insurance Company Operations
- or RMI 443 Enterprise Risk Management

Capstone Courses 6

- CYSE 368 Cybersecurity Internship
- or CYSE 494 Entrepreneurship in Cybersecurity
- IDS 493 IDS Electronic Portfolio Project

Electives (minimum of 19 credit hours) 19

1 School of Cybersecurity
Students can take the electives from any discipline at ODU and/or complete prerequisites for Principles and Application courses, as needed, to complete the required 120 credit hours. However, no more than 29 credits from courses in the Strome College of Business may be applied to the degree requirements, including named elective courses and general electives (ACCT, BNAL, ECON, FIN, IT, OPMT, MSCM, MGMT, ENTR, MKTG).

<table>
<thead>
<tr>
<th>Total Hours</th>
<th>120-150</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Grade of C or better required in both written communication courses and in ENGL 110C before declaring major. ENGL 231C is recommended as the second written communication course.</td>
</tr>
<tr>
<td>**</td>
<td>MATH 211 and MATH 212 are required as prerequisites for selected upper-division ECE and MSIM courses.</td>
</tr>
<tr>
<td>***</td>
<td>No more than 29 credits from courses in the Strome College of Business may be applied to the degree requirements, including named elective courses and general electives (ACCT, BNAL, ECON, FIN, IT, OPMT, MSCM, MGMT, ENTR, MKTG).</td>
</tr>
<tr>
<td>+</td>
<td>Other courses may be substituted with the approval of the program coordinator.</td>
</tr>
</tbody>
</table>

**Electives**

Elective courses may be taken for the remainder of the minimum 120 credits required for the degree. No more than 29 credits from courses in the Strome College of Business may be applied to the degree requirements, including named elective courses and general electives (ACCT, BNAL, ECON, FIN, IT, OPMT, MSCM, MGMT, ENTR, MKTG).

**Upper-Division General Education**

Met in the major.

**Requirements for Graduation**

Requirements for graduation include a minimum cumulative grade point average of 2.00 overall and in the major, 120 credit hours, which must include both a minimum of 30 credit hours overall and 12 credit hours of upper-level courses in the major program from Old Dominion University, completion of ENGL 110C, ENGL 211C or ENGL 221C or ENGL 231C, and one of the writing intensive (W) courses in the major with a grade of C or better, and completion of Senior Assessment.

**Bachelor of Science - Cyber Operations Major**

Peng Jiang, Program Coordinator and Faculty Advisor (pjiang@odu.edu)

Cyber Operations is an interdisciplinary major encompassing the entire scope of cyberspace and related operations that are both technical and non-technical (i.e., ethical, legal, human-centered, etc.) in nature. Cyber Operations is a complementary discipline to Cybersecurity. Cyber Operations places a particular emphasis on technologies and techniques applicable to all operational and system levels. Coursework in Cyber Operations balances theory, practice and hands-on labs inspired by real-life scenarios. Skills and competencies emphasized are in system attack, infiltration, exploitation, defense, mitigation, and recovery.

Graduates of the Bachelor of Science degree with the Cyber Operations major will have the skills and proficiencies that are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations. Therefore, they will play a role in the enhancement of the national security posture of the nation.

**Four-Year Plan - Cyber Operations Major - BS** (http://catalog.odu.edu/undergraduate/schoolofcybersecurity/cyberoperations-bs-fouryearplan/)

- The four-year plan is a suggested curriculum to complete this degree program in four years. It is just one of several plans that will work and...
Upper-Division General Education

Met through 300/400-level prerequisite courses.

Requirements for Graduation

Requirements for graduation include a minimum cumulative grade point average of 2.00 overall and in the major, 120 credit hours, which must include both a minimum of 30 credit hours overall and 12 credit hours of upper-level courses in the major program from Old Dominion University, completion of ENGL 110C, ENGL 211C or ENGL 221C or ENGL 231C, and the writing intensive (W) course in the major with a grade of C or better, and completion of Senior Assessment.

Cybersecurity Interdisciplinary Minor

Saltuk Karahan, School of Cybersecurity, Coordinator (skarahan@odu.edu)

This interdisciplinary minor in cybersecurity is focused on the technological, structural, social, and legal frameworks used to secure computer networks and software. The study of cybersecurity combines multiple fields including computer science, engineering, information technology, criminal justice, and philosophy, to name a few. In an effort to promote the security of computer networks, software, and cyber information, an interdisciplinary understanding about technological, legal, philosophical, and structural aspects of cybersecurity is needed. This minor will provide students from different majors the knowledge they need to prevent or respond to cyber incidents they are likely to encounter in their careers.

Course options are as follows:

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRJS 310</td>
<td>Cybercriminology: Foundations</td>
<td>3</td>
</tr>
<tr>
<td>CS 462</td>
<td>Cybersecurity Fundamentals</td>
<td>3</td>
</tr>
<tr>
<td>or ECE/MSIM 470</td>
<td>Foundations of Cyber Security</td>
<td></td>
</tr>
<tr>
<td>CS 463</td>
<td>Cryptography for Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CS 464</td>
<td>Networked Systems Security</td>
<td>3</td>
</tr>
<tr>
<td>CS 465</td>
<td>Information Assurance for Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CS 466</td>
<td>Principles and Practice of Cyber Defense</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 300</td>
<td>Introduction to Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 301</td>
<td>Cybersecurity Techniques and Operations</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 406</td>
<td>Cyber Law</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 407</td>
<td>Digital Forensics</td>
<td>3</td>
</tr>
<tr>
<td>ECE 416</td>
<td>Cyber Defense Fundamentals</td>
<td>3</td>
</tr>
<tr>
<td>or MSIM 416</td>
<td>Cyber Defense Fundamentals</td>
<td></td>
</tr>
<tr>
<td>ECE 419</td>
<td>Cyber Physical System Security</td>
<td>3</td>
</tr>
<tr>
<td>or MSIM 419</td>
<td>Cyber Physical Systems Security</td>
<td></td>
</tr>
<tr>
<td>EET 405</td>
<td>Data Communications and Computer Networks</td>
<td>3</td>
</tr>
<tr>
<td>or EET 412</td>
<td>Wireless Communication Systems</td>
<td></td>
</tr>
<tr>
<td>IT 416</td>
<td>Network Server Configuration and Administration</td>
<td>3</td>
</tr>
<tr>
<td>IT 417</td>
<td>Management of Information Security</td>
<td>3</td>
</tr>
<tr>
<td>IT 418</td>
<td>Enterprise Information Assurance</td>
<td>3</td>
</tr>
<tr>
<td>IT 419</td>
<td>Enterprise Cyber Defense</td>
<td>3</td>
</tr>
<tr>
<td>IT 461</td>
<td>Implementing Internet Applications</td>
<td>3</td>
</tr>
<tr>
<td>PHIL 355E</td>
<td>Cybersecurity Ethics</td>
<td>3</td>
</tr>
<tr>
<td>RMI 443</td>
<td>Enterprise Risk Management</td>
<td>3</td>
</tr>
<tr>
<td>or RMI 412</td>
<td>Property &amp; Liability Insurance Company Operations</td>
<td></td>
</tr>
</tbody>
</table>

The interdisciplinary minor in cybersecurity requires 12 credit hours of 300/400-level courses selected from at least two different disciplines with a maximum of six credits from any one discipline. For completion of the interdisciplinary minor, students must have a minimum overall cumulative grade point average of 2.00 in all courses specified as a requirement for the minor exclusive of lower-level courses and prerequisite courses. At least six hours of upper-level courses must be taken through courses offered by Old Dominion University. Three credit hours may be in the major, if a major course is listed as an option for the interdisciplinary minor. As such, it will be credited toward both the major and the interdisciplinary minor.

CYBERSECURITY Courses

**CYSE 001. Cybersecurity SFS LeADERS. 0 Credits.**
This course outlines the curricular and co-curricular requirements for Scholarship for Service Students in the Cyber LeADERS program.

**CYSE 100. Cyber Explorers and University Orientation. 1 Credit.**
This course provides an introduction to cyber hygiene and orientation to university life.

**CYSE 200T. Cybersecurity, Technology, and Society. 3 Credits.**
Students will explore how technology is related to cybersecurity from an interdisciplinary orientation. Attention is given to the way that technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

**CYSE 201S. Cybersecurity and the Social Sciences. 3 Credits.**
This course addresses the social, political, legal, and ethical, and economic dimensions of cybersecurity through a social science framework. Students are introduced to a human-factors approach to understanding cybersecurity threats. Attention is given to the social factors that contribute to cyber incidents and the political and legal mechanisms that are developed to control the behaviors of those who create risks and cybersecurity incidents. The class also explores how cybersecurity is studied by social scientists in various social science disciplines.

**CYSE 202G. Information Literacy for Cybersecurity. 3 Credits.**
This course provides an in-depth introduction to information literacy from library and information science, information ethics, and computer science perspectives along with applications to cybersecurity research and professional activity. This course is aligned with Old Dominion University’s general education learning outcomes for information literacy. Prerequisites: ENGL 110C.

**CYSE 250. Basic Cybersecurity Programming and Networking. 3 Credits.**
This course introduces the cybersecurity-centric programming and networking concepts. Students will develop problem solving skills by using low-level programming languages (including C and assembly) and learn fundamentals of network protocols. This course is the technical base for students to take cybersecurity major courses. No prior knowledge of programming and networking is assumed. Prerequisite: MATH 162M or higher.

**CYSE 270. Linux System for Cybersecurity. 3 Credits.**
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 is the technical base for students to take cybersecurity major courses.

**CYSE 280. Windows System Management and Security. 3 Credits.**
This course introduces tools and techniques used to configure, manage and implement Windows and its security-related features. Students will install, configure, manage and secure Windows client & server operating systems and related networking environment using a variety of software tools. This course also details how to mitigate malware threats, identify security issues by using auditing and the Advanced Threat Analysis feature in Windows Server, secure virtualization platform, and use new deployment options for enhancing the security.
CYSE 300. Introduction to Cybersecurity, 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, 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. Prerequisite: MATH 162M or permission of the instructor.

CYSE 301. Cybersecurity Techniques and Operations, 3 Credits.
This course introduces tools and techniques used to secure and analyze large computer networks and systems. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform forensic investigation, and practice techniques for penetration testing. Prerequisite: MATH 162M or permission of the instructor.

CYSE 368. Cybersecurity Internship, 1-6 Credits.
This course allows students to volunteer to work in an agency related to cybersecurity. Students must volunteer for 50 hours per course credit and complete course assignments. Prerequisite: approval by the Director of the Center for Cybersecurity Education and Research.

CYSE 395. Topics in Cybersecurity, 1-3 Credits.
Study of selected topics in cybersecurity. Prerequisites: junior standing.

CYSE 404. Law and Digital Forensics, 3 Credits.
This course will focus on the intersection of digital forensics and the criminal justice system, namely how digital forensics is understood and applied to key criminal justice, constitutional and statutory considerations within the criminal justice system. Students will explore such topics as the nature and types of cybercrime; search and seizure principles in the digital world; finding, handling and maintaining chain of custody of digital evidence; interviewing individuals relating to digital evidence and related activities; and testifying in court about digital evidence matters. Prerequisites: Junior standing or permission of instructor.

CYSE 406. Cyber Law, 3 Credits.
This course tackles two major cyber law subjects. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from traditional civil, and to a lesser extent, traditional criminal perspectives. The second part 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. The course will also introduce students to miscellaneous cybersecurity topics such as the Federal Acquisition Requirements. Prerequisite: junior standing.

CYSE 407. Digital Forensics, 3 Credits.
This course introduces the basic concepts and technologies of digital forensics. Students will learn the fundamental 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. Prerequisites: declared major and junior standing.

CYSE 409. Crime and Computer Applications, 3 Credits.
The purpose of this interdisciplinary course is to introduce students to the ways in which computers are involved in the commission and the investigation of crime. Students will learn the fundamentals of cryptography and steganography and the tools used to perform these activities Students will also use forensic software to identify, gather, and verify relevant digital evidence. Cross-listed with CRJS 409. Prerequisite: CRJS 310 or permission of instructor.

CYSE 416/516. 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) Prerequisite: permission of the instructor. Pre- or corequisite: ECE 355 or equivalent or permission of the instructor.

CYSE 417. Digital Leadership, 3 Credits.
This course explores technology as it relates to leadership experiences. Theories, case studies and real world examples are analyzed to show both successful and unsuccessful uses of online and digital approaches that inform leaders’ communication strategies. Students will explore how their own digital identities may impact their futures as leaders. They will also learn how to create digital identities that will shape their professional identities throughout their careers. Prerequisites: Junior standing or permission of instructor.

CYSE 419/519. 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. Prerequisite: ECE 355 or permission of the instructor.

CYSE 420/520. 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. Prerequisites: CYSE 250 or permission of the instructor.

CYSE 425W/525. Cybersecurity Strategy and Policy, 3 Credits.
This writing intensive 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. Prerequisites: ENGL 110C and ENGL 211C or ENGL 221C or ENGL 231C with a grade of C or better and CYSE 200T or POLS 101S.

CYSE 426/526. 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. Prerequisites: CYSE 200T or POLS 101S or permission of the instructor.

CYSE 450. Ethical Hacking and Penetration Testing, 3 Credits.
This course introduces the basic terminologies used in ethical hacking and useful tools in relation to penetration testing on Kali Linux. Students will learn to explore the vulnerabilities in various systems and operate the industry-leading tools and framework to perform the penetration testing on different target systems. Prerequisites: CYSE 270 and CYSE 301 or permission of the instructor.

CYSE 494. Entrepreneurship in Cybersecurity, 3 Credits.
This course is designed to help students enhance their personal and professional development through innovation guided by faculty members and professionals. It offers students an opportunity to integrate disciplinary theory and knowledge through developing a nonprofit program, product, business, or other initiative. The real-world experiences that entrepreneurs provide will help students understand how academic knowledge leads to transformations, innovations, and solutions to different types of problems. The course can be delivered either as an independent project for individual students or as group projects similar to those sometimes offered in topics courses. Prerequisite: Approval by the Director of the Center for Cybersecurity Education and Research.

School of Cybersecurity
CYSE 495/595. 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 496/596. 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 497/597. 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. Prerequisites:
senior standing and approval of the Director of the Center for Cybersecurity
Education and Research.

CYSE 498/598. 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. Prerequisites:
senior standing and approval of the Director of the Center for Cybersecurity
Education and Research.