Bachelor of Science in Cybersecurity

Bachelor of Science - Cyber Operations Major

Hongyi Wu, Program Coordinator and Faculty Advisor (h1wu@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.

Lower-Division General Education

Written Communication* 6
Oral Communication 3
Mathematics (MATH 211 and MATH 212 required) 8
Language and Culture 0-6
Information Literacy and Research 3
Human Creativity 3
Interpreting the Past 3
Literature 3
Philosophy and Ethics (met in the major by PHIL 355E) 3
Impact of Technology (met in the major by CYSE 200T) 8
Human Behavior (CRJS 215S or SOC 201S required) 3

Prerequisites 22
CS 150 Problem Solving and Programming I
CS 170 Introduction to Computer Architecture I
CS 250 Problem Solving and Programming II
CS 252 Introduction to Unix for Programmers
CS 270 Introduction to Computer Architecture II
ECE 241 Fundamentals of Computer Engineering
ECE 304 Probability, Statistics, and Reliability

Core Courses 12
CYSE 200T Cybersecurity, Technology, and Society
CYSE 301 Cybersecurity Techniques and Operations
CYSE 425W Cybersecurity Strategy and Policy
CYSE/CRJS 406 Cyber Law

Elective Credit as Needed for the Required 120 Credit Hours 1

Approved Program Electives (Choose two) 6
CS 476 Systems Programming
CYSE 407 Digital Forensics
ECE 483 Embedded Systems
IT 417 Management of Information Security

Bachelor of Science - Cybersecurity Major

Saltuk Karahan, Program Coordinator and Advisor ccsger@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 a variety of credit options including portfolio review, CLEP, DANTES, and departmental exams. For more information about the cybersecurity interdisciplinary program, email ccsger@odu.edu or Professor Hongyi Wu (h1wu@odu.edu).

No more than two classes, or six credits, may be counted for both the major and a minor.

Lower-Division General Education

Written Communication* 6
Oral Communication 3
Mathematics (MATH 162M required) 3

Total Hours 120-126

* 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.
Interdisciplinary Writing Course

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS 300W</td>
<td>Interdisciplinary Theory and Concepts</td>
</tr>
</tbody>
</table>

Core Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYSE 200T</td>
<td>Cybersecurity, Technology, and Society</td>
</tr>
<tr>
<td>CYSE 250</td>
<td>Basic Cybersecurity Programming and Networking</td>
</tr>
<tr>
<td>CYSE 300</td>
<td>Introduction to Cybersecurity</td>
</tr>
<tr>
<td>CYSE 301</td>
<td>Cybersecurity Techniques and Operations</td>
</tr>
<tr>
<td>CYSE/CRJS/CS 406</td>
<td>Cyber Law</td>
</tr>
<tr>
<td>CYSE 425W</td>
<td>Cybersecurity Strategy and Policy (C or better required)</td>
</tr>
<tr>
<td>CS 462</td>
<td>Cybersecurity Fundamentals</td>
</tr>
</tbody>
</table>

Principles Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRJS 405</td>
<td>Cybercrime and Cybersecurity</td>
</tr>
<tr>
<td>CS 463</td>
<td>Cryptography for Cybersecurity</td>
</tr>
<tr>
<td>CS 464</td>
<td>Networked Systems Security</td>
</tr>
<tr>
<td>or ECE/MSIM 411</td>
<td>Networked System Security</td>
</tr>
<tr>
<td>CS 465</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>or IT 418</td>
<td>Information Assurance</td>
</tr>
<tr>
<td>CYSE 495</td>
<td>Topics in Cybersecurity (Cybersecurity and Policy)</td>
</tr>
<tr>
<td>or POLS 495</td>
<td>Topics in Political Science</td>
</tr>
<tr>
<td>ECE/MSIM 416</td>
<td>Cyber Defense Fundamentals</td>
</tr>
<tr>
<td>ECE/MSIM 419</td>
<td>Cyber Physical System Security</td>
</tr>
<tr>
<td>ECE/MSIM 470</td>
<td>Foundations of Cyber Security</td>
</tr>
<tr>
<td>IT 315</td>
<td>Introduction to Networking and Security</td>
</tr>
<tr>
<td>IT 417</td>
<td>Management of Information Security</td>
</tr>
<tr>
<td>PHIL 355E</td>
<td>Cybersecurity Ethics</td>
</tr>
</tbody>
</table>

Application Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 467</td>
<td>Introduction to Reverse Software Engineering</td>
</tr>
<tr>
<td>CS 471</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>CYSE 407/CRJS 395</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>CYSE/POLS 495</td>
<td>Topics in Cybersecurity (Cyberwar)</td>
</tr>
<tr>
<td>ECE/MSIM 417</td>
<td>Secure and Trusted Operating Systems</td>
</tr>
<tr>
<td>ECE 452</td>
<td>Introduction to Wireless Communication Networks</td>
</tr>
<tr>
<td>ECE 455</td>
<td>Network Engineering and Design</td>
</tr>
<tr>
<td>IT 410</td>
<td>Business Intelligence</td>
</tr>
</tbody>
</table>

Capstone Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT 416</td>
<td>Network Server Configuration and Administration</td>
</tr>
<tr>
<td>IT 419</td>
<td>Enterprise Cyber Defense</td>
</tr>
<tr>
<td>IT 461</td>
<td>Implementing Internet Applications</td>
</tr>
</tbody>
</table>

Electives (minimum of 22 credit hours)

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.

Electives

Elective courses may be taken for the remainder of the minimum 120 credits required for the degree.

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 the writing intensive (W) course in the major with a grade of C or better, and completion of Senior Assessment.

Four-Year Plan - Cybersecurity - BS

http://catalog.odu.edu/undergraduate/collegeofartsletters/interdisciplinarystudies/bs-ids-cybersecurity/cybersecurity-bs-fouryearplan

This is a suggested curriculum plan to complete this degree program in four years. Please consult information in this Catalog, Degree Works, and your academic advisor for more specific information on course requirements for this degree.

Interdisciplinary Minor - Cybersecurity

Saltuk Karahan, Department of Political Science and Geography, 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 cyber crime 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:
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 required 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 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 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 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 405 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. Prerequisite: 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.

3 Bachelor of Science in Cybersecurity
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 425W. 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 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 entrepreneurialships 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.

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.

INTERDISCIPLINARY STUDIES Courses

IDS 307T. Digital Writing. 3 Credits.
This course introduces students to issues of writing in various digital environments like web pages, email, blogs, wikis, and discussion boards. It also introduces fundamentals of hypertext authoring, digital and visual rhetoric, and image manipulation. Prerequisites: ENGL 110C and ENGL 211C or ENGL 221C or ENGL 231C.

IDS 368. Internship in Interdisciplinary Studies. 1-6 Credits.
An opportunity to integrate service and applied learning experience with interdisciplinary perspectives. Prerequisite: junior standing and permission of individualized interdisciplinary studies program coordinator.

IDS 369. Internship in Conservation Leadership. 3-6 Credits.
As part of the Conservation Leadership minor, this graded internship will provide an opportunity to integrate service and applied learning experience with interdisciplinary perspectives. 200 hours are required for the 3-credit option, and 400 hours are required for the 6-credit option. Prerequisites: BIOL 466W/OEAS 466W/IDS 466W and BIOL 467/OEAS 467/IDS 467.

IDS 397. Independent Study. 1-6 Credits.

IDS 398. Independent Study. 1-6 Credits.

IDS 400/500. Study Abroad. 0 Credits.

IDS 466W. Introduction to Mitigation and Adaptation Studies. 3 Credits.
Students will be introduced to the science underpinning mitigation of human-induced changes in the Earth system, including but not limited to climate change and sea level rise, and adaptation to the impacts of these changes. The course will cover the environmental hazards and the opportunities and limitations for conservation, mitigation and adaptation. This is a writing intensive course. Cross listed with BIOL 466W and OEAS 466W. Prerequisites: BIOL 291 or permission of instructor.

IDS 467. Sustainability Leadership. 3 Credits.
In this class, students will discover what makes a leader for sustainability. They will consider a range of global and local crises from a leadership point of view in the context of sustainability science, which addresses the development of communities in a rapidly changing social, economic, and environmental system-of-systems environment. The course will be based on taking a problem-motivated and solution-focused approach to the challenges considered. The course includes a service learning project focusing on a leadership experience in solving a real-world environmental problem. Prerequisite: BIOL 466W or OEAS 466W or IDS 466W.

IDS 493. IDS Electronic Portfolio Project. 3 Credits.
The preparation of an electronic portfolio integrating the student's academic study, work experiences, skill identification and work products. Alternative formats are used for varying uses of the portfolio. Prerequisites: IDS 300W or permission of the instructor and senior standing.

IDS 494. Entrepreneurship in Interdisciplinary Studies. 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 entrepreneurialships provide will help students understand how academic knowledge leads to transformations, innovations, and solutions to different types of problems. Prerequisite: IDS 300W and approval of the program coordinator.

IDS 495. Topics in Integrative Studies. 3 Credits.
Focused study of selected topics linking perspectives, research and applications from a variety of disciplines. Emphasis is on disciplinary synthesis. Prerequisite: IDS 300W.

IDS 497. IDS Individualized Senior Project. 3 Credits.
This course is a vehicle for the execution of the senior project requirement of the Interdisciplinary Studies Program. The project will be negotiated between the student, faculty sponsors, and the program. Open only to individualized integrative studies majors. Prerequisites: IDS 300W, permission of the instructor and an approved individualized integrative studies curriculum plan.