Bachelor of Science Degree in Interdisciplinary Studies - Cybercrime Major

Bachelor of Science Degree in Interdisciplinary Studies - Cybercrime Major

Roderick Graham, Program Coordinator and Faculty Advisor (rgraham@odu.edu)

This program explores cybercrime from an interdisciplinary perspective that merges the disciplines of criminal justice, computer science, philosophy, and information technology. Students will receive a foundational understanding of crime and criminal justice and more in-depth understanding about cybersecurity, cyber law, and digital forensics. In addition, students will receive a basic introduction to information technology.

While many crimes have decreased over the past 25 years, the one group of crimes that has increased dramatically is cybercrimes. Careers responding to cybercrime have grown tremendously over the past decade. While many of these careers require in-depth understanding about computer engineering and computer science, many careers also require a broader orientation grounded in the social sciences. Across the country there are 350,000 current vacancies in cybersecurity-related careers. Roughly ten percent of those vacancies are in Virginia.

Cybersecurity experts across the world agree that academic programming should be interdisciplinary in nature. While many universities have difficulty developing interdisciplinary majors, the IDS degree at ODU provides a national model that can be used to develop a cybercrime major grounded in the social sciences. ODU’s current cybersecurity and cyber operations majors fill the employment gap for technologically-driven careers. The cybercrime major will fill the employment gap in the area of policy- and legal-driven careers.

Lower-Division General Education

<table>
<thead>
<tr>
<th>Category</th>
<th>Credit Hours</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 102M or Math 103M required)</td>
<td>3</td>
</tr>
<tr>
<td>Language and Culture</td>
<td>0-6</td>
</tr>
<tr>
<td>Information Literacy and Research (can be met by PHIL 290G)</td>
<td>0-3</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 (can be met in the major by CYSE 200T/IT 200T or IT 360T)</td>
<td>0-3</td>
</tr>
<tr>
<td>Human Behavior (met in the major by CRJS 215S)</td>
<td></td>
</tr>
</tbody>
</table>

Interdisciplinary Studies Core

<table>
<thead>
<tr>
<th>Course</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS 300W Interdisciplinary Theory and Concepts (grade of C or higher required)</td>
<td>3</td>
</tr>
<tr>
<td>CYSE 368 Cybersecurity Internship</td>
<td>3</td>
</tr>
<tr>
<td>or CYSE 494 Entrepreneurship in Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>IDS 493 IDS Electronic Portfolio Project</td>
<td>3</td>
</tr>
<tr>
<td>Cybercrime Core *</td>
<td>12</td>
</tr>
<tr>
<td>CRJS 405 Cybercrime and Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>CYSE/CRJS 406 Cyber Law</td>
<td></td>
</tr>
<tr>
<td>CYSE 407 Digital Forensics</td>
<td></td>
</tr>
</tbody>
</table>

Select one of the following:

- PHIL 290G Philosophy of Digital Culture
- PHIL 355E Cybersecurity Ethics

Criminology Core * 15

- CRJS 215S Introduction to Criminology
- CRJS 222 The Criminal Justice System
- SOC 337 Introduction to Social Research

Select two from the following:

- CRJS 320 Law and Social Control
- CRJS 323 Police in American Society
- CRJS 340 White-Collar Crime
- CRJS 344 Social Science and Crime Mapping
- CRJS 415 Courtroom As a Social System
- CRJS 421 Deviant Behavior
- CRJS 462 Substantive Criminal Law

CYSE Electives at the 300/400 level

Technical Base ** 15-17

Select three from the following:

- IT/CYSE 200T Cybersecurity, Technology, and Society
- IT 205 Introduction to Object-Oriented Programming
- IT 360T Principles of Information Technology
- CS 150 Problem Solving and Programming I
- CYSE 250 Basic Cybersecurity Programming and Networking
- CYSE 300 Introduction to Cybersecurity

Select two from the following:

- CS 170 Introduction to Computer Architecture I
- CS 250 Problem Solving and Programming II
- CYSE 301 Cybersecurity Techniques and Operations
- IT 315 Introduction to Networking and Security
- IT 325 Web Site and Web Page Design
- IT 450 Database Concepts
- ECE 355 Introduction to Networks and Data Communications

Total Hours 80-97

* 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.

** Further math may be necessary for upper-level electives (for example, CYSE 300 requires MATH 162M).

*** Offered online only.

+ Other courses may be substituted with approval of the program coordinator.

++ Prerequisites may be required; review course description or consult advisor. Other courses may be substituted with approval of the program coordinator.

Electives

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

Upper-Division General Education

- Option A. Approved Minor, 12-24 hours; also second degree or second major
- Option B. Interdisciplinary Minor, 12 hours specified by the department, 3 of which may be in the major area of study
- Option C. International business and regional courses or an approved certification program, such as teaching licensure
• Option D. Two Upper-Division Courses from outside the College of Arts and Letters or from the Social Science Component within the College of Arts and Letters that are not required by the major (6 hours).

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 - IDS - Cybercrime Major - BS (http://catalog.odu.edu/undergraduate/collegeofartsletters/interdisciplinarystudies/cybercrime/ids-cybercrime-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.

Cybercrime Interdisciplinary Minor

Roderick Graham, Program Coordinator and Faculty Advisor (rgraham@odu.edu)

The interdisciplinary minor in cybercrime provides students with an understanding of crime and deviance in the digital environment. Students will be required to take two introductory courses in the cybercrime and cybersecurity majors, respectively. In these core courses, students will learn the fundamental issues involved in cybersecurity (computer system architectures, critical infrastructures, cyber threats and vulnerabilities) and cybercrime (defining and describing the different types of computer-related crimes, the techniques used by law enforcement, and the legal issues inherent in combating cybercrime). They can then expand their knowledge by taking electives in psychology, political science, criminal justice, information technology, or cybersecurity. The minor aspires to develop graduates who can think critically about how human behavior impacts and is impacted by computer technologies.

Three credit hours in the interdisciplinary minor 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. Interdisciplinary minors require 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. Course substitutions may be approved by the interdisciplinary minor coordinator.

Prerequisite

| CRJS 215S | Introduction to Criminology * |
| Core ** | 6 |
| CRJS 405 | Cybercrime and Cybersecurity |
| CYSE 300 | Introduction to Cybersecurity |
| Electives | 6 |
| CRJS 340 | White-Collar Crime |
| CRJS 344 | Social Science and Crime Mapping |
| IT 315 | Introduction to Networking and Security |
| IT 360T | Principles of Information Technology |
| CRJS/CYSE 406 | Cyber Law |
| CRJS 395/396/495/496 | Topics in Criminal Justice *** |
| CYSE 407 | Digital Forensics |
| PHIL 355E | Cybersecurity Ethics |
| PSYC 307 | Institutionalization of Human-Centered Computing |

| PSYC 344 | Human Factors |
| POLS 350T | Technology and War |
| Total Hours | 12 |

* Not included in the calculation of the grade point average for the minor.
** The two courses from the core and the two electives must be selected from at least two different disciplines with no more than six credits from any one discipline.
*** Must be approved by the program coordinator.

Digital Forensics Certificate

A certificate in Digital Forensics is available. Please refer to the School of Continuing Education (https://www.odu.edu/cepd) for specific information.

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.

Bachelor of Science Degree in Interdisciplinary Studies - Cybercrime Major

2
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. 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 cryptographical 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.

CYSE 419. 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 entrepreneurship 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 495/496. 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 496/497. 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 498/499. 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 300W. Interdisciplinary Theory and Concepts. 3 Credits.
An examination of the history, concepts and application of interdisciplinary study. This course includes an analysis of similarities and differences in academic disciplines and the application of interdisciplinary approaches to a specific topic of study. This is a writing intensive course. Prerequisite: a grade of C or better in ENGL 211C, ENGL 221C or ENGL 231C.

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 entrepreneurship provides 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.