A research-based, interdisciplinary Doctor of Philosophy (PhD) in Cybersecurity combines a strong security technical foundation with a security policy and social sciences perspective. It seeks to prepare graduates to advance the state of the art in systems, networks, and the Internet in industry, academia, and government. The interdisciplinary nature of the program distinguishes it from traditional doctoral degree programs in computer science, engineering, or social sciences and makes it unique in the Boston area.

Students who choose the PhD in Cybersecurity program have a strong desire to pursue academic research solving critical cybersecurity challenges facing today's society. The PhD program is a natural path for students in the college's Master of Science in Cybersecurity (http://www.ccs.neu.edu/graduate/degree-programs/m-s-in-information-assurance/) program who want to pursue research and students with bachelor's degrees and an interest in research-focused careers. Students who pursue careers in advancing the state of the art of cybersecurity have an opportunity to gain:

- A strong technical foundation in cybersecurity and an interdisciplinary perspective based on policy and social science
- A path to a research-focused career coupled with depth in information assurance research at a leading institution, one of the earliest designees by NSA/DHS as a National Center of Academic Excellence in Information Assurance Research, Information Assurance/Cyber Defense, and Cyber Operations
- The opportunity to work with and learn from faculty who are recognized internationally for their expertise and contributions in information assurance from Northeastern's Khoury College of Computer Sciences, the Department of Electrical and Computer Engineering, and the College of Social Sciences and Humanities
- Access to research projects at Northeastern’s research centers focused on security:
  - The Cybersecurity and Privacy Institute (https://cyber.csis.northeastern.edu/about/): The mission of Northeastern's Cybersecurity and Privacy Institute (the Institute) is to safeguard critical technology. Forging partnerships with experts in industry, government, and academia worldwide, the Institute's faculty and students develop, protect, and enhance technologies on which the world relies—from mobile devices and "smart" IoT applications to tomorrow's self-driving cars and delivery drones. Their expertise spans algorithm auditing; cloud security; cryptography; differential privacy; embedded device security; internet-scale security measurements; machine learning; big data; security, malware, and advanced threats; network protocols and security; web and mobile security; and wireless network security.
  - The International Secure Systems Lab (http://www.isеclab.org/), affiliated with Northeastern, a collaborative effort of European and U.S. researchers focused on web security, malware, and vulnerability analysis; intrusion detection; and other computer security issues.
  - The ALERT Center (http://www.northeastern.edu/alert/), where Northeastern is the lead institution, a multiuniversity Department of Homeland Security Center of Excellence involved in research, education, and technology related to threats from explosives.

The benefits of the Boston area:

- World-renowned for academic and research excellence, the Boston area is also home to some of the nation's largest Department of Defense contractors and government and independent labs such as MIT Lincoln Lab, MITRE, and Draper Lab.

Degree Requirements

The PhD in Cybersecurity degree requires completion of at least 48 semester credit hours beyond a bachelor's degree. Students who enter with an undergraduate degree will typically need four to five years to complete the program, and they will be awarded a master's degree en route to the PhD.

Doctoral Degree Candidacy

A student is considered a PhD degree candidate after completing the core courses with at least a 3.500 grade-point average (GPA), with no grades lower than a B in the core courses, and either publishing a paper in a strong conference or journal or passing an oral exam that is conducted by a committee of three cybersecurity faculty members and based on paper(s) written by the student.

Residency

One year of continuous full-time study is required after admission to the PhD candidacy. During this period, the student will be expected to make substantial progress in preparing for the comprehensive examination.

Teaching Requirement

All cybersecurity PhD students must satisfy the teaching requirement in order to graduate. This requirement is fulfilled when the student works as a teaching assistant (TA) or instructor of record (IoR) for one semester and during this semester:

- Teaches at least three hours of classes
- Prepares at least one assignment or quiz or equivalent

PhD students are expected to satisfy the teaching requirement some time after completing their first year and at least one semester prior to scheduling their PhD defense.

Dissertation Advising

The doctoral dissertation advising team for each student consists of two cybersecurity faculty members, one in a technical area. When appropriate, the second faculty advisor will be from the policy/social sciences area.

Dissertation Committee

A PhD student's dissertation committee consists of the two members of the dissertation advising team plus two others: One is a member of the cybersecurity faculty, and the other is an external examiner who is knowledgeable about the student's research topic.

Comprehensive Examination

A PhD student must submit a written dissertation proposal and present it to the dissertation committee. The proposal should identify the research problem, the research plan, and the potential impact of the research on the field. The presentation of the proposal will be made in an open forum,
and the student must successfully defend it before the dissertation committee after the public presentation.

**DISSERTATION DEFENSE**
A PhD student must complete and defend a dissertation that involves original research in cybersecurity.

**AWARDING OF MASTER’S DEGREES**
Students who enter the PhD in Cybersecurity program with a bachelor’s degree have the option of obtaining a master’s degree from one of the departments participating in the program. To do so, they must meet all of the department’s degree requirements.

**Program Requirements**

**Bachelor’s Degree Entrance**
Complete all courses and requirements listed below unless otherwise indicated.

**Milestones**
Qualifying exam and area exam
Annual review
Dissertation proposal
Dissertation committee
Dissertation defense

**Core Requirements**
A grade of B or higher is required in each core course. A cumulative 3.500 GPA is required for the core requirement.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Foundations</strong></td>
<td></td>
</tr>
<tr>
<td>CY 5770</td>
<td>Software Vulnerabilities and Security</td>
<td>4</td>
</tr>
<tr>
<td>or EECE 5641</td>
<td>Introduction to Software Security</td>
<td></td>
</tr>
<tr>
<td>CY 6740</td>
<td>Network Security</td>
<td>4</td>
</tr>
<tr>
<td>or EECE 5699</td>
<td>Computer Hardware and System Security</td>
<td></td>
</tr>
<tr>
<td>CY 5240</td>
<td>Cyberlaw: Privacy, Ethics, and Digital Rights</td>
<td>4</td>
</tr>
</tbody>
</table>

**Electives and Tracks**
Select at least two courses from one track: 8

### Hardware Security
- CS 6410: Compilers
- CS 6710: Wireless Network
- EECE 5666: Digital Signal Processing
- EECE 7352: Computer Architecture
- EECE 7364: Mobile and Wireless Networking
- EECE 7390: Computer Hardware Security

### Machine Learning
- CS 6140: Machine Learning
- CS 7150: Deep Learning
- CY 6720: Machine Learning in Cybersecurity and Privacy
- EECE 5644: Introduction to Machine Learning and Pattern Recognition
- EECE 7397: Advanced Machine Learning

### Network Security
- CS 5700: Fundamentals of Computer Networking

### Systems Security
- CS 6410: Compilers
- CS 7600: Intensive Computer Systems
- CS 7610: Foundations of Distributed Systems
- CY 5130: Computer System Security
- EECE 7352: Computer Architecture

### Theory
- CS 7800: Advanced Algorithms
- CS 7805: Complexity Theory
- EECE 7337: Information Theory

### Usable Security and Privacy
- CS 6350: Empirical Research Methods
- CS 6760: Privacy, Security, and Usability
- CS 7260: Visualization for Network Science
- CS 7340: Theory and Methods in Human Computer Interaction
- INSH 6300: Research Methods in the Social Sciences
- INSH 6302: Qualitative Methods
- INSH 6500: Statistical Analysis
- INSH 7400: Quantitative Analysis

### Cybersecurity Policy
- CRIM 6200: Criminology
- CRIM 6262: Evidence-Based Crime Policy
- CY 5200: Security Risk Management and Assessment
- CY 5210: Information System Forensics
- CY 5250: Decision Making for Critical Infrastructure
- POLS 7341: Security and Resilience Policy
- POLS 7441: Cyberconflict

**Electives**
Selected in consultation with advisor from the graduate-level CS, ECE, and CSSH courses.

### Dissertation
Complete the following (repeatable) course until graduation:
- CY 9996: Dissertation Continuation
Program Credit/GPA Requirements
48 total semester hours required
Minimum 3.000 GPA required

Advanced Entry Program Requirements
Degree Requirements
Incoming PhD in cybersecurity students who have already completed a Master of Science in an adjacent field may petition to the graduate program administration for advanced entry. Advanced entry petitions are reviewed by the program administration on a case-by-case basis. Please note that advanced entry does not waive by itself any part of the PhD coursework requirements. As a degree conferral requirement, a minimum of 16 semester hours of coursework beyond the 32 semester hours of the master’s degree is required of advanced entry PhD students (48 semester hours is required of standard entry PhD students). A grade of B or higher is required in each course. A cumulative 3.500 GPA is required for the core requirement.

Doctoral Degree Candidacy
Refer to the PhD Cybersecurity overview (p. 1) for admission to candidacy requirements.

Residency
Refer to the PhD Cybersecurity overview (p. 1) for residency requirements.

Teaching Requirement
Refer to the PhD Cybersecurity overview (p. 1) for teaching requirements.

Dissertation Advising
Refer to the PhD Cybersecurity overview (p. 1) for dissertation advising requirements.

Dissertation Committee
Refer to the PhD Cybersecurity overview (p. 1) for dissertation committee requirements.

Comprehensive Examination
Refer to the PhD Cybersecurity overview (p. 1) for comprehensive examination requirements.

Dissertation Defense
Refer to the PhD Cybersecurity overview (p. 1) for dissertation defense and completion requirements.

Complete all courses and requirements listed below unless otherwise indicated.

Milestones
Qualifying exam and area exam
Annual review
Dissertation proposal
Dissertation committee
Dissertation defense

Core Requirement
Students are required to take all core courses unless otherwise determined by the program. Students must maintain a minimum GPA of 3.500 as well as earn a grade of B or better in each core course.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY 5770 or EECE 5641</td>
<td>Software Vulnerabilities and Security or Introduction to Software Security</td>
<td>4</td>
</tr>
<tr>
<td>CY 6740 or EECE 5699</td>
<td>Network Security or Computer Hardware and System Security</td>
<td>4</td>
</tr>
<tr>
<td>CY 5240</td>
<td>Cyberlaw: Privacy, Ethics, and Digital Rights</td>
<td>4</td>
</tr>
</tbody>
</table>

Electives and Tracks
Students are required to take all courses unless otherwise determined by the program.

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 6410</td>
<td>Compilers</td>
<td></td>
</tr>
<tr>
<td>CS 6710</td>
<td>Wireless Network</td>
<td></td>
</tr>
<tr>
<td>EECE 5666</td>
<td>Digital Signal Processing</td>
<td></td>
</tr>
<tr>
<td>EECE 7352</td>
<td>Computer Architecture</td>
<td></td>
</tr>
<tr>
<td>EECE 7364</td>
<td>Mobile and Wireless Networking</td>
<td></td>
</tr>
<tr>
<td>EECE 7390</td>
<td>Computer Hardware Security</td>
<td></td>
</tr>
<tr>
<td>CS 6140</td>
<td>Machine Learning</td>
<td></td>
</tr>
<tr>
<td>CS 7150</td>
<td>Deep Learning</td>
<td></td>
</tr>
<tr>
<td>CY 6720</td>
<td>Machine Learning in Cybersecurity and Privacy</td>
<td></td>
</tr>
<tr>
<td>EECE 5644</td>
<td>Introduction to Machine Learning and Pattern Recognition</td>
<td></td>
</tr>
<tr>
<td>EECE 7397</td>
<td>Advanced Machine Learning</td>
<td></td>
</tr>
<tr>
<td>CS 5700</td>
<td>Fundamentals of Computer Networking</td>
<td></td>
</tr>
<tr>
<td>CS 6710</td>
<td>Wireless Network</td>
<td></td>
</tr>
<tr>
<td>CS 7610</td>
<td>Foundations of Distributed Systems</td>
<td></td>
</tr>
<tr>
<td>CY 5130</td>
<td>Computer System Security</td>
<td></td>
</tr>
<tr>
<td>CY 6750</td>
<td>Cryptography and Communications Security</td>
<td></td>
</tr>
<tr>
<td>EECE 5155</td>
<td>Wireless Sensor Networks and the Internet of Things</td>
<td></td>
</tr>
<tr>
<td>EECE 5576</td>
<td>Wireless Communication Systems</td>
<td></td>
</tr>
<tr>
<td>EECE 7336</td>
<td>Digital Communications</td>
<td></td>
</tr>
<tr>
<td>EECE 7364</td>
<td>Mobile and Wireless Networking</td>
<td></td>
</tr>
<tr>
<td>EECE 7374</td>
<td>Fundamentals of Computer Networks</td>
<td></td>
</tr>
<tr>
<td>EECE 7393</td>
<td>Analysis and Design of Data Networks</td>
<td></td>
</tr>
<tr>
<td>CS 6410</td>
<td>Compilers</td>
<td></td>
</tr>
<tr>
<td>CS 7600</td>
<td>Intensive Computer Systems</td>
<td></td>
</tr>
<tr>
<td>CS 7610</td>
<td>Foundations of Distributed Systems</td>
<td></td>
</tr>
<tr>
<td>CY 5130</td>
<td>Computer System Security</td>
<td></td>
</tr>
<tr>
<td>EECE 7352</td>
<td>Computer Architecture</td>
<td></td>
</tr>
<tr>
<td>CS 7800</td>
<td>Advanced Algorithms</td>
<td></td>
</tr>
<tr>
<td>CS 7805</td>
<td>Complexity Theory</td>
<td></td>
</tr>
<tr>
<td>EECE 7337</td>
<td>Information Theory</td>
<td></td>
</tr>
</tbody>
</table>
Cybersecurity, PhD

**Usable Security and Privacy**
- CS 6350 Empirical Research Methods
- CS 6760 Privacy, Security, and Usability
- CS 7260 Visualization for Network Science
- CS 7340 Theory and Methods in Human Computer Interaction
- INSH 6300 Research Methods in the Social Sciences
- INSH 6302 Qualitative Methods
- INSH 6500 Statistical Analysis
- INSH 7400 Quantitative Analysis

**Cybersecurity Policy**
- CRIM 6200 Criminology
- CRIM 6262 Evidence-Based Crime Policy
- CY 5200 Security Risk Management and Assessment
- CY 5210 Information System Forensics
- CY 5250 Decision Making for Critical Infrastructure
- POLS 7341 Security and Resilience Policy
- POLS 7441 Cyberconflict

**Electives**
Selected in consultation with advisor from the graduate-level CS, ECE, and CSSH courses. 20

**Dissertation**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY 9990</td>
<td>Dissertation Term 1</td>
<td></td>
</tr>
<tr>
<td>CY 9991</td>
<td>Dissertation Term 2</td>
<td></td>
</tr>
</tbody>
</table>

Complete the following (repeatable) course until graduation:
- CY 9996 Dissertation Continuation

**Program Credit/GPA Requirements**
Minimum 16 semester hours required
Minimum 3.000 GPA required