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 of security 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.ccis.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.iseclab.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 adviser will be from the policy/social science 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>CS 5700</td>
<td>Fundamentals of Computer Networking</td>
<td>4</td>
</tr>
<tr>
<td>or EECE 7336</td>
<td>Digital Communications</td>
<td></td>
</tr>
<tr>
<td>CY 5770</td>
<td>Software Vulnerabilities and Security</td>
<td>4</td>
</tr>
<tr>
<td>CY 6740</td>
<td>Network Security</td>
<td>4</td>
</tr>
<tr>
<td>or CY 6750</td>
<td>Cryptography and Communications Security</td>
<td></td>
</tr>
<tr>
<td>CY 5200</td>
<td>Security Risk Management and Assessment</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 Specializations**
Note: Consult faculty adviser for other acceptable courses.
Complete 28 semester hours from the following:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<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>CS 5600</td>
<td>Computer Systems</td>
<td></td>
</tr>
<tr>
<td>or EECE 7352</td>
<td>Computer Architecture</td>
<td></td>
</tr>
<tr>
<td>CY 6120</td>
<td>Software Security Practices</td>
<td></td>
</tr>
<tr>
<td>POLS 7341</td>
<td>Security and Resilience Policy</td>
<td></td>
</tr>
<tr>
<td>CS 5500</td>
<td>Foundations of Software Engineering</td>
<td></td>
</tr>
<tr>
<td>CS 6140</td>
<td>Machine Learning</td>
<td></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY 9996</td>
<td>Dissertation Continuation</td>
<td></td>
</tr>
</tbody>
</table>

**Program Credit/GPA Requirements**
48 total semester hours required
Minimum 3.000 GPA required

**Advanced Entry PhD Program Requirements**

**Degree Requirements**
Advanced entry for the PhD Cybersecurity requires completion of at least 16 semester credit hours beyond a bachelor’s degree. Students also must complete the required core courses. 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.

**Degree Requirements**
Advanced entry for the PhD Cybersecurity requires completion of at least 16 semester credit hours beyond a bachelor’s degree. Students also must
complete the required core courses. 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 must complete all core courses, unless a waiver has been approved by a faculty adviser. 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><strong>Fundamentals</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 5700</td>
<td>Fundamentals of Computer Networking</td>
<td></td>
</tr>
<tr>
<td>or EECE 7336</td>
<td>Digital Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CY 5770</td>
<td>Software Vulnerabilities and Security</td>
<td></td>
</tr>
<tr>
<td><strong>Security and Cyberlaw</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CY 6740</td>
<td>Network Security</td>
<td></td>
</tr>
<tr>
<td>or CY 6750</td>
<td>Cryptography and Communications Security</td>
<td></td>
</tr>
<tr>
<td>CY 5200</td>
<td>Security Risk Management and Assessment</td>
<td></td>
</tr>
<tr>
<td>CY 5240</td>
<td>Cyberlaw: Privacy, Ethics, and Digital Rights</td>
<td></td>
</tr>
</tbody>
</table>

**Electives**
Code Title Hours

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

**Track 1: Network/Communication Security**
- CS 6710 Wireless Network
- EECE 5666 Digital Signal Processing

**Track 2: System Security**
- CS 5600 Computer Systems
- or EECE 7352 Computer Architecture
- CY 6120 Software Security Practices

**Track 3: Policy/Society**
- POLS 7341 Security and Resilience Policy

**General Electives**
- CS 5500 Foundations of Software Engineering
- CS 6140 Machine Learning
- CS 6200 Information Retrieval
- CS 6350 Empirical Research Methods
- CS 7610 Foundations of Distributed Systems
- CS 7800 Advanced Algorithms
- CS 7810 Foundations of Cryptography
- CY 6720 Machine Learning in Cybersecurity and Privacy
- CY 7790 Special Topics in Security and Privacy
- EECE 7204 Applied Probability and Stochastic Processes
- EECE 7205 Fundamentals of Computer Engineering
- EECE 7337 Information Theory

**Dissertation**
Code Title Hours
- CY 9990 Dissertation Term 1
- CY 9991 Dissertation Term 2
Complete the following (repeatable) course until graduation:
- CY 9996 Dissertation Continuation

Note: Consult faculty adviser for other acceptable courses.