THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

DOCTOR OF ENGINEERING IN Cybersecurity Analytics ONLINE

Introduction

The School of Engineering and Applied Science Online Programs awards the Doctor of Engineering (D.Eng.) degree in Cybersecurity Analytics. Offered on weekends, this D.Eng. cohort will begin in August 2021 with a target graduation date of August 2023. Applicants should normally hold a master's degree in engineering, applied science, mathematics, computer science, information technology or related field from an accredited institution.

The Doctor of Engineering in Cybersecurity Analytics

The D.Eng. in Cybersecurity Analytics addresses the widespread need for practitioners who can apply advanced knowledge from the program of study to address real-world cybersecurity challenges, whereas a PhD in cybersecurity contributes to fundamental research.

The D.Eng. in Cybersecurity Analytics empowers the student to plan and implement security measures to protect an organization's network and systems, implement strategies to track threats and monitor networks for security breaches, build secure and resilient computer systems with subject matter expertise in cybersecurity analytics, advanced tools and techniques for ensuring confidentiality, integrity, and availability of an organization's data and systems.

Curriculum

The curriculum comprises 45 credit hours divided into a classroom phase of 10 graduate-level, 3 credit hour courses, and a research phase during which the student writes and defends a praxis paper. The research phase requires a minimum of 15 credit hours.

Proposed Courses

CSCI 6015 Cyber Forensics
CSCI 6016 Applied Network Defense
EMSE 6547 Cyber Resilience
EMSE 6769 Applied Machine Learning for Engineers
ECE 6005 Computer Architecture and Design
ECE 6160 Secure Computer Architecture (Prereq: ECE 6005)
SEAS 6410 Security Data Visualization (Prereq: SEAS 6414 or permission of the instructor)
SEAS 6414 Analytical Tools for Cyber Analytics
SEAS 6415 Applied Cryptography and Data Protection (Prereq: SEAS 6414)
SEAS 6499 Praxis Development for Cybersecurity

Course work culminates in the praxis proposal, a research report that proposes a practice-based solution – to a problem in cybersecurity of the student's own choosing – that could be used by cybersecurity practitioners.

Classroom Phase Schedule

Course sessions last 10 weeks. Classes meet Saturday mornings from 9:00 am-12:00 pm and afternoons from 1:00-4:00 pm (all times Eastern). This program is taught in an accelerated, cohort format in which students take all courses in lock step. Classes cannot be taken out of sequence, attendance at all class meetings is expected, and students must remain continuously enrolled; i.e., leaves of absence are permitted only in medical or family emergency, or in case of deployment to active military duty.

Session	#Courses	#Credit Hours	Tentative Dates
Fall-1 2021	2	6	August 14 – October 16, 2021
Fall- 2 2021	2	6	October 23 - January 15, 2022
Spring-1 2022	2	6	January 22 – March 26, 2022
Spring-2 2022	2	6	April 2 – June 4, 2022
Summer 2022	2	6	June 11 – August 13, 2022

** No classes on Thanksgiving, Christmas, and New Year Weekends*

Research Phase (Min. 15 Credit Hours)

In order to be successfully awarded the D.Eng. degree, students must earn a grade point average of at least 3.2 in the 10 classroom courses, and no grade below B-. Upon completion of the classroom phase, students are registered for a minimum of 15 credit hours (ch) of SEAS 8199 Praxis Research: 6 ch in Fall 2022, 6 ch in Spring 2023 and 3 ch in Summer 2023. A single semester extension through Fall 2023 (6 ch) may be granted. Students who do not successfully complete the requirements will have their work transferred to a professional degree program. Throughout the research phase, the student develops the praxis on an advisor-approved topic related to cybersecurity. Faculty research directors meet with students at least once per month, who are expected to attend each meeting.

Research Areas for Praxis

With the advisors' consent, the student may elect to focus on an area within the Cybersecurity field. Below, find sample areas of research:

- Addressing the Cybersecurity Malicious Insider threat
- Exploring Cybersecurity Requirements in the Defense Acquisition Process
- Internet of Things Device Cybersecurity
- Cybersecurity of Networked Home Medical Devices
- Cybersecurity Challenges in Healthcare Industries

Cost

All classes meet live online through synchronous distance learning technologies. Classes are recorded for future viewing. Tuition is billed at $1570 per credit hour for the 2021-2022 year. Required digital textbooks and software are provided at no additional cost. A non-refundable tuition deposit of $495, which is applied to tuition in the first semester, is required when the student accepts admission.

Course Descriptions

See also http://bulletin.gwu.edu/courses

CSCI 6015 Cyber Forensics. Acquiring, preserving and analyzing digitally stored information while ensuring that this information is admissible as evidence in a court of law. Principles and techniques for cyber forensics investigations using industry-standard forensic process.

CSCI 6016 Applied Network Defense. Computer security: protection aspects of the Internet. Cryptographic tools to provide security, such as shared key encryption (DES, 3DES, RC and more), public key encryption, key exchange, and digital signature. Internet protocols and applications.

EMSE 6547 Cyber Resilience. Resilience planning for cybersecurity; assessment and modeling approaches to limit system failure toward creating a cyber-resilient organization; recognition, resistance, recovery, reinstatement from the perspectives of information technologists and engineering managers; existing cybersecurity reliance frameworks; potential policies to sustain a healthy and robust security posture.

EMSE 6769 Applied Machine Learning for Engineers. A broad introduction to fundamental concepts and techniques in machine learning from the perspective of the systems engineer. The field of machine learning explores algorithms that can learn from examples (e.g. experience) without pre-programmed rules or that can make predictions based automated analysis of prior data. This course provides students with knowledge of the theory and practice of machine learning leveraging an open source framework to explore the ideas, algorithms and techniques, without a prior background in programming. Topics covered in the course include the relationship between Data Mining and Machine Learning, Machine Learning and Statistics, Fundamental concepts (preparing/cleansing input data, attribute selection, sampling), linear models, clustering, training/testing/cross-validation, decision trees, probabilistic methods, deep learning, auto-encoders, convolutional neural networks and ensemble learning methods.

ECE 6005 Computer Architecture and Design. Advanced topics in computer architecture and design; instruction-level parallelism, thread-level parallelism, memory, multithreading, and storage systems.

ECE 6160 Secure Computer Architecture. Building blocks of secure hardware and systems: trusted execution environment, security engines; side and covert channels in computing systems; hardware trojans; physically unclonable functions and challenges; obfuscation strategies.

SEAS 6410. Security Data Visualization. Visualization aspect of security data, including study of data analytics and scaling up information security, security metrics and security monitoring techniques focusing on industry applications. Tools for security data visualization and analytics.

SEAS 6415 Applied Cryptography and Data Protection: Introduction to cryptographic techniques, case studies for real-life applications of modern cryptographic solutions, classical cryptographical algorithms (AES, RSA, RC4) and techniques (symmetric, asymmetric-public key cryptography, hash functions), digital signatures, key management and distribution. Advanced topics such as zero-knowledge proofs and zero-trust architectures.

SEAS 6414 Analytical Tools for Cyber Analytics. This course is designed to provide students with the basic foundations for application of deterministic, probabilistic, and statistical models to address problems in cyber analytics.

SEAS 6499 Praxis Development for Cybersecurity. Overview of research methods. Aims and purpose of the praxis. Development of praxis research strategies, formulation and defense of a praxis proposal. Praxis proposal defense must be passed before the student is admitted to degree candidacy to undertake praxis work. Restricted to students who have completed all required coursework for the D.Eng. in the field of Cybersecurity Analytics.

SEAS 8199 Praxis Research. Independent applied research in cybersecurity culminating in the final praxis report and final examination for the degree of Doctor of Engineering. May be repeated for credit. Restricted to students in the D.Eng. in the field of Cybersecurity Analytics.

The University reserves the right to adjust course offerings, schedules, and tuition rates.