THE GEORGE WASHINGTON UNIVERSITY
School of Engineering and Applied Science (SEAS)
SEAS Online Programs Office

STUDENT GUIDELINES: DOCTOR OF ENGINEERING DEGREE IN CYBERSECURITY ANALYTICS

STUDENT GUIDELINES:
DOCTOR OF ENGINEERING DEGREE IN CYBERSECURITY ANALYTICS

Table of Contents

STUDENT GUIDELINES:
DOCTOR OF ENGINEERING DEGREE IN CYBERSECURITY ANALYTICS

Doctor of Engineering Program Overview

The online Doctor of Engineering program in Cybersecurity Analytics [D.Eng.(CA)] consists of a minimum of 45 credit hours divided into 2 stages. The first stage comprises a classroom experience of 10 graduate-level, 3-credit-hour courses culminating in the student's submission—and the faculty's acceptance—of the praxis proposal. The second stage comprises an independent research effort of at least 15 credit hours of praxis research culminating in the praxis defense. These stages must be completed by specific deadlines in keeping with the accelerated nature of the program. After completing the classroom courses, the student develops and defends an original praxis in the field of Cybersecurity Analytics. Students can expect to complete all requirements within 2 years. If sufficient progress is made, extensions may be permitted.

The objectives of the Doctor of Engineering program in Cybersecurity Analytics are to ensure that graduates are able 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.

1. Registration

The student must maintain continuous enrollment throughout the doctoral program. Semester enrollment information is distributed by the SEAS Online Programs Office by email before the start of each semester, and registration is processed directly by the office on the date listed in that email, on the condition that the student has fulfilled academic and financial obligations to the university.

Registration holds are placed on the accounts of students with outstanding balances. Our office cannot process registration when there is a registration hold on the account. For this reason, students must make payments on time each semester. Late payment of tuition is possible grounds for removal from the doctoral cohort. Find withdrawal and tuition refund policies at https://seasonline.gwu.edu/about-us/policies-procedures-doctoral.

2. The Classroom Stage

2.1 Leaves of Absence/Transfer of credit

Leaves of Absence. Students enter the program as members of a cohort (group), are registered as a cohort, and take their courses in lockstep in successive semesters until completion of the program. The D.Eng.(CA) curriculum is determined by the faculty, and course information is provided to students by email from the SEAS Online office before the start of each semester. A D.Eng. student who finds it necessary to interrupt active pursuit of the degree may petition the office for a leave of absence by emailing a full explanation and attaching a completed LOA form and any supporting documentation to seasdoc@gwu.edu. Petitions are usually answered within two workweeks. Leaves of absence may be granted for family emergency (up to 6 months), physical or mental health treatment (up to 6 months), or deployment to active military duty (up to one year).

Transfer credit: Transfer of credit is not permitted in doctoral programs.

2.2 Grading and Scholarship

To complete the classroom stage of the D.Eng.(CA), students must satisfactorily complete the required curriculum of 30 credit hours, complete each course with a grade of ***B-*** or better, and achieve a minimum final GPA of 3.2.

If a D.Eng. student receives any grade below B-, graduate study is terminated, and further enrollment is prohibited. Any student whose cumulative GPA falls below 3.2 will be automatically placed on probation. While on probation, a student must maintain a GPA of 3.2 or higher for the 2 courses completed in any session or their enrollment will be terminated. Probation will be lifted once the student's cumulative GPA exceeds 3.2.

GW uses the following grading system for graduate students: **A, B, C, F**; other grades that may be assigned are **A−, B+, B−, C+, C-**. Individual course grades are based on a standard curve relative to the class average.

2.3 The Praxis Proposal

In the program's last classroom course, SEAS 8499: Praxis Development for Cybersecurity, students propose and defend the praxis they wish to undertake during the research phase. The praxis synthesizes engineering theory and practice to create value for practical use. For an acceptable praxis, the student must think critically, combining reflection and action to put forward a specific, useful application to solve an authentic problem. The praxis should engage an existing, "real," Cybersecurity Analytics issue and take a new approach to its resolution, applying theory and practice to recommend a worthwhile solution. The praxis must use the latest Cybersecurity Analytics concepts and tools.

With the consent of one or both of SEAS Online Programs Academic Director Professor Shahram Sarkani and Co-Director Professor Thomas A. Mazzuchi, the student may focus the praxis on one of the sample areas of research below, or on an area outside of these:

- 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

The praxis proposal is submitted to one or both Academic Directors and to the SEAS 8499 instructor. It must include: 1) a clear problem description, 2) the goals of the study, 3) identification of data availability, and 4) a detailed explanation of the solution method to be used. The praxis proposal is defended in the 8499 class and must be passed before the student is admitted to candidacy for the D.Eng.(CA) to begin research and work on the praxis.

3. The Research Stage

Following successful completion of the classroom stage, the student is admitted to candidacy for the D.Eng. and is enrolled in SEAS 8199: Praxis Research for Doctor of Engineering, to conduct the research to be developed into the praxis.

The 15 credit hours of SEAS 8199 taken in the research stage are used to develop and write the praxis. Students are registered for a minimum of 6 credit hours in each Fall and Spring semester and 3 credit hours in Summer. Extensions may be granted case by case if the student is making acceptable progress.

Students are required to submit the first two chapters of the praxis (Introduction and Literature Review) by the end of the first semester of research and receive approval from the advisor. Students who fail to do so will meet with the program directors to discuss the path forward.

The average minimum amount of out-of-class or independent learning you should expect to perform each semester in the research course is approximately 20 hours per week.

3.1 Praxis Research Advisors

The program faculty assign doctoral research advisors to the D.Eng. candidates as they enter the research phase. Students work with their assigned advisor for the remainder of the program.

3.2 Research Advising Meetings and Feedback

Each session’s advising meeting dates are communicated to the cohort by the research advisor.

Advisor directly manages the research course SEAS 8199 through Blackboard. Deadlines for submitting slides for the research meetings are set by the advisor and communicated to the students through Blackboard or by email.

Advisees are required to attend the research meetings. Candidates are responsible for submitting slides covering research progress to the advisor by the deadline provided in the meeting announcement. Slides must be submitted for all meetings, even if the student will be absent.

Students receive written feedback from the advisor after each advising meeting. Progress is noted as:

- **Green**–Student is making sufficient progress toward stage 2 completion
- **Yellow**–Student is making some progress, but is in danger of not meeting program timeline
- **Red**–Student is making insufficient progress

If the advisor determine that the student makes insufficient progress in a semester, an NC ('No Credit') grade is assigned for SEAS 8199 on the transcript and the candidate's program and research toward the D.Eng. is terminated. A one-time courtesy option to convert in the current semester to a post-master's professional degree (Engineer or Applied Scientist) is offered.

3.3 Research Submissions

All versions of the praxis paper must be forwarded to the program advisor for review and approval. All final advisor-approved praxes must be sent to seasonline@gwu.edu for academic integrity review prior to submission. *See "3.5 A Note on Academic Integrity"* below.

3.4 The Praxis Defense

Upon successful completion of all prior requirements, the candidate must submit the final praxis, approved by the advisor, to seasonline@gwu.edu with a request for AIR evaluation. An email confirmation is sent once the item has passed and is approved for submission. Below are guidelines and instructions for the praxis defense (final examination):

- See the Appendix to this document, "Researching and Writing the Praxis Paper."
- Refer to https://library.gwu.edu/seas-etds for praxis format guidelines.
- The praxis paper proper (the body of the paper) should be approximately 80 pages. When including all front and back matter -- contents, lists, references, appendixes -- the praxis paper should not exceed 150 pages.
- Once the advisor approves the final version of the praxis, you forward it to seasonline@gwu.edu requesting an Academic Integrity Review (AIR).
- Upon receiving your final praxis from you, the office submits it for AIR. If it

does not pass, we notify you asking that any problems be fixed.

- When the praxis meets AIR requirements, the final examination is scheduled and details are announced by email. At that time, all graduation paperwork and committee information are provided.
- Membership on the committee of examiners consists of at least 3 faculty members. Effective Fall 2018, no outside advisor will be required.
- The student submits the praxis to the committee by email depending on the preference of the committee member.
- The defense presentation should include a restatement of the problem under study, a description of the data used or dataset created, a description of the assumptions used in the analysis, and a discussion of the results and how they will be used.
- When the final examination committee is convinced of the quality and originality of the candidate's contribution to knowledge as well as his or her mastery of the scholarship and research techniques in the field, the committee recommends the candidate for the degree of Doctor of Engineering.
- Praxis submission deadlines (no later than the dates shown) for the final paper to be ready for defense, after AIR approval, in order to defend and graduate in the semester listed are:

Semester	**Deadline**
Spring	April 1
Summer	July 15
Fall	November 15

- After a successful praxis defense, students must submit the advisor-approved final version to GW's ETD system. Before submitting, the praxis must be properly formatted, following the GW ETD Formatting and Submission guidelines.

3.5 A Note on Academic Integrity

All papers are expected to use proper citation and pass the AIR without issue. If a paper fails the AIR, the SEAS Online Programs Office provides a courtesy report to the student so that appropriate updates can be made. Submissions with academic integrity concerns that do not pass the review on the 3rd attempt may be forwarded to the GW Academic Integrity Council for additional evaluation. The GW Code of Academic Integrity may be viewed at http://www.gwu.edu/~ntegrity/.

In researching the praxis, and in any published and public results, the candidate must follow GW policies on research conduct and the use of copyrighted material. See http://my.gwu.edu/files/policies/ResearchMisconductPolicy.pdf and http://library.gwu.edu/etd/copyright.

4. Graduation Clearance and Diplomas

After a successful praxis defense, the SEAS Online Programs Office assembles all necessary documents for graduation clearance.

Degrees are conferred in January, May, and August. To be recommended by the faculty for graduation, a student must have met the admission requirements of the school in which registered; completed satisfactorily the scholarship, curriculum, and other requirements for the degree; filed an application for graduation by the date requested; and be free from all indebtedness to the university. Enrollment is required in the semester at the close of which the degree is to be conferred, and all degree requirements must be completed by the last day of final examinations for that semester.

Diplomas are mailed 12-14 weeks following the date of degree conferral, barring unforeseen circumstances. Diplomas are mailed to the Diploma Address in the record. The candidate is responsible to enter this address in the GWeb information system and make any updates. See the following link for graduation application instructions: https://registrar.gwu.edu/online-graduation-application-instructions. The Diploma Address must be entered before the application for graduation is submitted.

If you do not receive the diploma by 12-14 weeks after your graduation date, check the online transcript to see if the degree was conferred. If it was conferred, the missing diploma must be reported to the Registrar's Graduation Services Office within 6 months. After that time a fee is charged for a replacement diploma. Also check to see if there are any financial holds on the account. A diploma is only sent if the balance owed is less than $500. If the degree was not conferred, check with the SEAS Online Programs office.

5. Commencement

Participation in the annual commencement ceremonies in May is open to students who have applied to graduate in that spring semester or who graduated in the preceding fall or summer semester.

Doctoral candidates who have not successfully defended their praxes and completed their ETD approval form by April 1 may not participate in either the May commencement ceremonies or the SEAS graduation ceremony.

Students who apply to graduate after the published deadlines are not guaranteed commencement materials and may not be listed in the commencement program. Find more information about University Commencement at https://commencement.gwu.edu/.

6. Administration

The SEAS Online Programs staff is responsible for monitoring and tracking student progress. For this reason, all communication related to the D.Eng.(CA) program must involve the Office (seasdoc@gwu.edu). Relevant communications comprise advisor/student interaction, research inquiries, and all other program-related information. Additionally, students are expected to keep the Office informed of their current contact information, such as email address, home address, and telephone numbers including cell phone numbers.

Find university policies and regulations in the George Washington University Bulletin at http://www.gwu.edu/~bulletin/.

The University reserves the right to change courses, programs, fees, and the academic calendar, or to make other changes deemed necessary or desirable, giving advance notice of change when possible.

APPENDIX: RESEARCHING AND WRITING THE PRAXIS PAPER

TABLE OF CONTENTS

1 Introduction

Generally speaking, a praxis is “the practical application of a theory.”[1] In academia, a praxis for the Doctor of Engineering stands between a thesis for a master’s degree and a dissertation for a research doctorate such as the Doctor of Philosophy (Ph.D.).

A master’s thesis usually addresses a subject of limited scope that has been researched by the student by consulting published source material or has been explored by limited experimentation by known techniques; there is normally no expectation of publishing the results in a professional venue. A dissertation for a research doctorate explores uncharted territory in a carefully circumscribed area of knowledge. It may involve invention of new research techniques or technology, and is by definition a contribution of new knowledge to the subject field; such work is normally reported in a technical journal, where it is available to everyone.

In contrast, the applied research for the GW School of Engineering and Applied Science Doctor of Engineering (D.Eng.) degree is written up as a praxis, in which engineering theory and practice are synthesized to create value for practical use. The praxis is a report on a practical problem in the field of study. It could be the description of the application of advanced engineering tools to a complex cybersecurity problem.

The D.Eng. in Cybersecurity Analytics, D.Eng.(CA), degree requires that a candidate write a praxis paper. This document provides guidance for D.Eng.(CA) candidates and advisor on the preparation of the praxis.[2]

2 Doctor of Philosophy Research vs. Doctor of Engineering Research

Ph.D. research leads to foundational, basic findings that are publishable in peer-reviewed journals or books. The Ph.D. holder tends to practice engineering in the academy or in research investigation in a specific area.

The D.Eng. demands that the student’s research be applied to solve an actual problem; thus, research for the D.Eng. is applied, rather than foundational like research for the Doctor of Philosophy (Ph.D.). The aim of D.Eng. research is to develop original solutions to real-world industry problems using the latest engineering concepts and techniques—to apply the knowledge directly to problems encountered in daily life. While focusing on engineering practice, D.Eng. research in the field of Cybersecurity Analytics also develops the practitioner’s leadership potential.

In short, the essential difference between research toward the Ph.D. and toward the D.Eng. is the “basic” nature of the former and the “applied” nature of the latter.

Basic research (Ph.D.) can be defined as “systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts *without specific applications* towards processes or products in mind”[3] (emphasis added). Directed toward increasing fundamental knowledge and understanding in the field of study, basic research is visionary and high-risk–high-reward. As such, it can lead to applied research or to development of advanced technology.

Applied research (D.Eng.) is a "systematic study to understand the means to meet a recognized and specific need. It is a *systematic expansion and application of knowledge* to develop useful materials, devices, and systems or methods."[4] (emphasis added). Applied research transforms findings of basic research to solutions to specific, complex, real-world problems or technological challenges, establishing their feasibility and practicality.

3 The Cybersecurity Analytics Field of Study

Cybersecurity analytics involves the use of algorithms, statistical analysis, behavioral analytics, machine learning, and other approaches to solve cybersecurity problems where rule-based and signature-based approaches fail. In many ways, cybersecurity analytics is all about analyzing data, identifying correlations and looking at risks and threats based on the data that is collected. The data could be network packet captures, or it could be text data like information collected from a risk assessment. Sometimes the data is very quantitative and can be analyzed with statistical tools looking for trends, sometimes the data contains patterns that allow one to derive clues about an attacker's behavior or the behavior of users.

In addition to quantitative measurements, there may be a great deal of textual data and this can be readily analyzed with some of the latest Natural Language Processing tools and techniques. Artificial Intelligence (AI) and Machine Learning methods are very good at analyzing data for hidden patterns and trends, regardless of the type of data. AI can find correlations in large amounts of data that would overwhelm a human analyst and can help the human extract knowledge contained in the data.

3.1 Research Areas and Topics Acceptable for the Praxis

Potential areas of research for a praxis in Cybersecurity Analytics are:

- New approaches to threat intelligence automation
- Defending against side channel attacks
- Botnet detection and defense
- Addressing the cybersecurity malicious insider threat
- Exploring cybersecurity requirements in the defense acquisition process
- Cybersecurity of networked home medical devices
- Cyber threat intelligence
- Advances in security orchestration, automation and response (SOAR)
- Adversarial machine learning and game theory
- Methods for detecting hardware and software trojans
- Analysis of data related to human behavior relative to technology and social engineering
- Cyber-physical system security
- Innovations in intrusion detection (network and/or host based)

- Blockchain applications (e.g., privacy preservation)
- Cybersecurity challenges in healthcare industries
- Data analytics for active network defense
- Network security metrics and applications
- Internet of things device cybersecurity
- Cryptography for cybersecurity
- Analytics for critical infrastructure protection
- Cybersecurity analytics for risk management
- Cybersecurity metrics and assessment techniques

A few sample praxis topics based on these research areas are:

- Analyzing network traffic: Data analytics to identify anomalous traffic
- Cloud Security: Anomaly detection in the context of cloud computing
- Detect Insider Threats: Using analytics to protect against employees with access to privileged information who purposely or accidentally misuse access causing harm
- Ransomware: Defensive analytics to detect and thwart ransomware attacks
- Unapproved Privileged Data Access: Data exfiltration resulting from privilege escalation can be stopped with cybersecurity analytics methods.
- Observe User Behavior to Perceive Threats: User and Entity Behavior Analytics (UEBA) methods can detect nefarious activities

3.2 Research Methods Acceptable for the Praxis

Cybersecurity analytics involves a diverse range of topics, problems, and questions, and D.Eng. research may use a variety of research methodologies, leveraging the following techniques:

- Statistical learning and analysis techniques
- Machine learning
- Behavioral analysis
- Game theory
- Multicriteria decision making

4 The Praxis

Research for the D.Eng.(CA) praxis is independent applied research guided by a faculty advisor. Upon completing the praxis, students will have achieved the program learning goals.

The D.Eng.(CA) program is largely distinguished by the nature of its research phase. The praxis is a report on the practical resolution of an actual, real-world problem. The praxis describes the phases of the research and reports the research findings in chapters that normally include Introduction; Literature review; Methodology; Results; and Conclusions. These are briefly described below.

4.1 Introduction Chapter

The introduction provides a brief background about the problem that justifies the study. It discusses the significance of the problem, and it must include:

- problem statement (purpose and significance of the study),
- thesis statement (claim of the researcher and potential solution to the problem),
- research questions (suggesting the relationship among variables that should be empirically testable),
- the research objective (statement of the research direction and specific actions), and
- hypotheses (declarative statements about expected or predicted outcomes).

4.2 Literature Review Chapter

Whereas a Ph.D. dissertation is expected to include a comprehensive review of related literature and a summary of all the research that has ever been published on that subject, the D.Eng. praxis literature search need only review those writings that support the practical application of the technology or case study. All available resources, such as books, journal papers, and websites, can be used. The literature review critically analyzes the existing technical body of knowledge related to the problem under study. This critique should demonstrate that the author has a grasp of the major ideas and findings pertaining to his or her topic. The literature review includes an overview of the subject; categorization of the work under review based on such factors as opposing theories and methodologies; an explanation of the similarities and differences of the publications cited; and a critical analysis and evaluation of the works reviewed, including discussion of their strengths and weaknesses.

While, as stated above, a D. Eng. literature review focuses on application of theory and is not necessarily comprehensive, nevertheless, D.Eng. candidates must establish that they have a deep understanding of the topic and awareness of the newest methods and approaches for solving the problem. Peer-reviewed articles published in high-impact journals are highly desirable references for this purpose. The most prestigious journals in Cybersecurity Analytics at the time of this writing include:

- Journal of Information Security and Applications
- IEEE Transactions on Information Forensics and Security
- Decision Support Systems
- IEEE Security & Privacy
- Computers and Security
- Expert Systems with Applications
- IEEE Transactions on Big Data
- IEEE Access (Multidisciplinary)

- IEEE Transactions on Industry Applications

4.3 Methodology Chapter

This chapter contains a detailed overview of how the research was conducted and walks readers through the procedures and steps. The research methodology (or method) is the process of starting from raw data and ending up accepting or rejecting the research hypotheses.

4.4 Results, Discussion, and Conclusions Chapters

The results chapter should present the output, in the form of figures and tables, from applying the research methodology to raw input data. The discussion describes the research results as related to the research questions and hypotheses and refers to the literature review for comparison. The conclusions summarize the overall point(s) that the researcher wants the reader to remember.

5 Bibliography

Godfrey, Patrick. "The Engineering Doctorate (EngD): Developing Leaders for Tomorrow with Industry," http://claiu.fabi.be/home/wp-content/uploads/2011/12/The-Engineering-Doctorate-final-Godfrey.pdf.

Kitagawa, Fumi. "Understanding the EngD Impact: A Pilot Study," University of Manchester on behalf of the AEngD and EPSRC, August 2015.

Sargent, Jr., John F. "Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure." Congressional Research Service, 7- 5700, www.crs.gov, R44711, December 13, 2016.

6 Notes

[1] Merriam-Webster, definition 2. https://www.merriam-webster.com/dictionary/praxis, accessed 28 Feb 2018.

[2] The following writing resources provide useful technical writing assistance: Praxis question (see http://writingcenter.gmu.edu/articles/7605); Thesis statement (see http://writingcenter.unc.edu/handouts/thesis-statements/); Research writing (see https://owl.english.purdue.edu/owl/resource/658/01/).

[3] John F. Sargent Jr., "Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure," Congressional Research Service, 7-5700, www.crs.gov, R44711, December 13, 2016.

[4] Sargent, 2016.

[5] ASME Book Committee, *Guide to the Engineering Management Body of Knowledge,* doi: 10.1115/1.802991, 2010 http://ebooks.asmedigitalcollection.asme.org/book.aspx?bookid= 306 accessed 1 Mar 2018.