**CyberSEA Research Lab**
Carleton University
https://carleton.ca/cybersea/
@carleton-cybersea

**Systems and Computer Engineering**
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6

**Posting#:** 2027-PHD-CDE-01

November 13, 2026

# Position Available: Ph.D. Candidate

*Model-Driven Analysis of Cyberattack Consequences in Critical Systems*

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively seeking a doctoral student to work on a funded research project on the topic of model-driven analysis of cyberattack consequences in critical systems, starting in September 2027 or sooner.

## Project Description and Objectives

Critical cyber-physical systems support essential services in areas such as healthcare, manufacturing, water treatment, energy, and transportation. A successful cyberattack on one part of these systems can disrupt digital functions, interfere with physical processes, and ultimately cause serious operational, safety, environmental, or economic consequences. These consequences may also spread through connections and dependencies that are difficult to recognize before an incident occurs. Understanding how this harm can propagate is essential for designing systems that remain safe and reliable, even when some security defences are ineffective or fail.

Many cybersecurity methods focus primarily on finding vulnerabilities, preventing attacks, or estimating how likely an attack is to occur. Although these activities are important, they provide limited support for answering a different and increasingly important question: *What harmful consequences could occur if an attack succeeds, and how could those consequences spread through the system?*

The objective of this Ph.D. project is to develop a formal, model-driven framework for identifying and analyzing *cyberattack consequence pathways*. A consequence pathway describes how an adversarial action can affect system components and functions, propagate through cyber and physical dependencies, and eventually produce mission-critical harm. By analyzing these pathways during system design, the proposed research will help engineers identify where serious consequences may concentrate and make informed decisions about system architecture and security mitigations before deployment.

**Project Keywords:**

- cybersecurity
- cyber-physical systems
- consequence pathways
- model-driven engineering
- software architecture
- formal methods
- graph algorithms
- modeling and simulation
- critical infrastructure

## Duties and Responsibilities

The successful candidate will conduct original doctoral research leading to a dissertation and peer-reviewed publications. The anticipated research activities include:

1. Investigating and extending architecture modeling languages to represent cyberattack consequences, propagation mechanisms, affected system functions, and mitigation measures.

2. Developing formal models and automated analysis techniques for reasoning about cyberattack consequence pathways in complex system architectures.
3. Developing methods for analyzing consequence pathways, accounting for factors such as impact severity, uncertainty, cascading effects, and mitigation effectiveness.
4. Developing and evaluating prototype tools and applying the proposed modeling and analysis approaches through simulation experiments and critical cyber-physical system case studies.
5. Collaborating with other members of the research team and communicating research results through scholarly publications, conference presentations, and technical demonstrations.

## Expected Research Contributions

The specific direction of the research will be refined with the successful candidate. Anticipated contributions include:

- A formal modeling framework for representing cyberattack consequences and their propagation through complex system architectures.
- New methods and algorithms for identifying, analyzing, and evaluating cyberattack consequence pathways and critical system dependencies.
- Computational tools and techniques for integrating consequence-driven analysis into system modeling and design activities.
- Empirical evidence and case studies demonstrating the effectiveness and practical applicability of the proposed framework and methods.

## Desired Skills/Qualifications

Suitable candidates will have a Master's degree in Software Engineering, Computer Science, Systems Engineering, Cybersecurity, or a closely related field.

Ideal candidates will be self-motivated, intellectually curious, and able to work both independently and collaboratively. Candidates should have strong analytical and problem-solving abilities, effective written and oral communication skills, and an interest in conducting rigorous research with practical relevance.

Applicants should demonstrate preparation or experience in several of the following areas:

- software or systems modeling and architecture;
- model-driven engineering or formal methods;
- cybersecurity or security engineering;
- algorithms, graph theory, or network analysis;
- modeling, simulation, or automated analysis; and
- cyber-physical systems, critical infrastructure, or research software development.

Candidates should also demonstrate an ability to read and synthesize technical literature, formulate research questions, design and conduct rigorous evaluations, and communicate research results clearly. Evidence of previous research experience, scholarly writing, software development, or peer-reviewed publication will be considered an asset.

All candidates must satisfy the Minimum Admission Requirements for Doctoral Programs at Carleton University. International candidates must also ensure that they satisfy the English as a Second Language Requirements. In all cases, these requirements will be strictly enforced when evaluating an application for admission.

## Funding

Successful candidates for this position will be *eligible for funding* in the form of a research assistantship. Specific funding details are determined at the time of offer and consider numerous factors such as academic standing, research potential, availability of funds, eligibility for teaching assistantship and/or scholarships, etc.

## Research Training Environment

The successful candidate will join a collaborative research environment within the CyberSEA Research Lab, focused on identifying, measuring, and mitigating the consequences of cyberattacks on critical cyber-physical systems. The candidate will have opportunities to collaborate with other Master's and doctoral researchers working on related research projects and interdisciplinary problems.

The candidate will receive regular individual research supervision and participate in group meetings, research seminars, skills-development activities, and peer mentoring. Training and professional development will include research methodologies, technical skills relevant to the project, scientific writing, and the effective communication of research results.

The candidate will be encouraged and supported in publishing research at international conferences and in peer-reviewed journals, presenting at research and professional events, and developing the skills needed to conduct independent research and collaborate effectively within a research team.

## Host Research Institute Information

Carleton University is a public comprehensive university, founded in 1942, in Ottawa, Ontario, Canada. The research-intensive Faculty of Engineering and Design at Carleton University is recognized as one of Canada's leading institutions in the study and research of engineering, architecture, industrial design and information technology. Since the inception of engineering at Carleton in 1945, our experts have pushed the bounds of innovation and discovery. Carleton focuses on anticipating the needs of industry and society, and offers forward-thinking programs with real world application and produces research that is helping to shape our present and future. The Department of Systems and Computer Engineering is a recognized world-class institution in software engineering, computer systems engineering, communications engineering, and biomedical engineering. Together with the Department of Electronics, the Department of Systems and Computer Engineering constitutes one of the largest and most research-intensive centres for Electrical and Computer Engineering and Software Engineering education and research in Canada. The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab conducts advanced academic research to develop systematic and rigorous approaches for evaluating and assuring the cyber security of software-dependent systems.

## Further Information

For more information about Graduate Studies at Carleton University and the Department of Systems and Computer Engineering, please visit: https://carleton.ca/sce/graduate-studies/. For more information about applying for Graduate Studies at Carleton University, please visit: https://graduate.carleton.ca/apply-online/. For more information about funding for Graduate Studies, please visit: https://graduate.carleton.ca/financial-assistance/admissions-funding/.

## Application Enquiries

Due to the high volume of generic and automated enquiries, only messages that explicitly identify an open position currently posted by the CyberSEA Research Lab and clearly explain how the applicant's background, experience, and research interests align with that position will be considered. Generic enquiries or messages that do not demonstrate a specific connection to the advertised project will not receive a response.

## How to Apply

Interested applicants are to send a **CV** and **Statement of Interest** detailing your research interests, background, and experience by email to the CyberSEA Lab Director using the contact information below. Please include the specific **position posting number** in the subject line of your email.

**Jason Jaskolka, Ph.D., P.Eng.**
Systems and Computer Engineering | Carleton University
Canal Building 6206 | 1125 Colonel By Drive | Ottawa, ON K1S 5B6
jason.jaskolka@carleton.ca
https://carleton.ca/jaskolka/
@jason-jaskolka

For more information about how to apply, please visit: https://carleton.ca/cybersea/positions-available/

## Application Deadline

Applications will be reviewed as they arrive until a suitable candidate is found.