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-MASC-CDE-01

November 13, 2026

Position Available: M.A.Sc. Candidate

Developing a Cyberattack Consequence Taxonomy for Critical Systems

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively looking for a Master's student to work on a funded research project on the topic of developing a cyberattack consequence taxonomy for 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 of these systems can disrupt digital functions, interfere with physical processes, interrupt essential services, and ultimately produce serious operational, safety, environmental, or economic consequences.

Understanding how these consequences arise is challenging. Relevant information is distributed across academic research, cybersecurity standards, vulnerability databases, security advisories, and reports of real-world incidents. These sources often describe attacks and their consequences using different terminology, levels of detail, and assumptions. As a result, it can be difficult for engineers to compare incidents, reuse existing knowledge, or determine which consequences may be relevant to a system under development.

The objective of this M.A.Sc. project is to develop a structured taxonomy and machine-readable knowledge model for describing how cyberattacks can lead to harmful consequences in critical cyber-physical systems. The taxonomy will provide a common language for describing important concepts such as initial cyber events, affected system components and functions, cyber-to-physical interactions, propagation mechanisms, operational disruptions, and resulting consequences.

Project Keywords:

- cybersecurity
- cyber-physical systems
- consequence taxonomy
- consequence pathways
- knowledge representation
- ontology engineering
- incident analysis
- model-driven engineering
- critical infrastructure

Duties and Responsibilities

The successful candidate will conduct research leading to an M.A.Sc. thesis and peer-reviewed publications. The anticipated research activities include:

1. Reviewing academic research, cybersecurity standards, vulnerability information, security advisories, and documented cyber incidents to identify concepts and relationships relevant to cyberattack consequences in critical cyber-physical systems.

2. Developing a structured taxonomy of cyberattack consequence pathways and outcomes, including clear definitions, classification criteria, relationships, and examples covering cyber events, affected system assets and functions, propagation mechanisms, system dependencies, and resulting harms.
3. Representing the taxonomy as a machine-readable ontology and developing methods for connecting consequence knowledge to system models, incident evidence, cybersecurity standards, and other relevant knowledge sources.
4. Applying the proposed taxonomy and ontology to critical-system case studies, including exploring their use in annotating system models and identifying plausible consequence pathways.
5. Evaluating the completeness, consistency, usability, extensibility, and practical value of the proposed taxonomy and ontology, collaborating with other members of the research team, and communicating research results through scholarly publications and presentations.

Expected Research Contributions

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

- A structured taxonomy of cyberattack consequence pathways and outcomes, with definitions and relationships connecting cyber events, affected system functions, propagation mechanisms, dependencies, and resulting consequences.
- A machine-readable ontology that formalizes the taxonomy and supports the representation, retrieval, reuse, and extension of consequence knowledge.
- Methods and supporting tool capabilities for connecting the taxonomy and ontology to system models, incident evidence, and relevant cybersecurity knowledge sources to identify plausible consequence pathways.
- Case-study evidence demonstrating the completeness, consistency, usability, and practical value of the proposed taxonomy and ontology as a foundation for model-driven analysis of cyberattack consequences.

Desired Skills/Qualifications

Suitable candidates will have a Bachelor's degree in Software Engineering, Computer Science, Computer Engineering, Information Technology, Cybersecurity, Systems Engineering, 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 interest in several of the following areas:

- cybersecurity, security engineering, or cyber incident analysis;
- cyber-physical systems or critical infrastructure;
- requirements engineering, software or systems modeling, or conceptual modeling;
- knowledge representation, ontology engineering, or semantic technologies;
- systematic literature reviews, qualitative analysis, or research synthesis; and
- research software development, prototyping, or tool development.

Candidates should be comfortable reading and synthesizing technical literature, organizing complex information, defining concepts precisely, and documenting research decisions clearly. Previous experience with cybersecurity projects, literature reviews, conceptual modeling, data analysis, or software development 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.