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-02

November 13, 2026

Position Available: Ph.D. Candidate

Quantifying Cyberattack Impacts in Critical Cyber-Physical 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 focused on quantifying the impacts of cyberattacks on critical cyber-physical 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 operations, damage equipment, interrupt essential services, create safety or environmental hazards, and produce significant economic losses. These consequences may emerge immediately, develop gradually, or cascade across interconnected components and systems.

Understanding that an attack could cause harm is only the first step. Engineers and decision-makers must also determine how severe the consequences could become, how different forms of harm should be compared, and how confident they can be in the available estimates. Without credible answers to these questions, it is difficult to prioritize security investments, compare mitigation options, or determine whether a system adequately limits its most serious cyber risks.

Many cybersecurity assessments use qualitative ratings such as "low," "medium," or "high," or combine likelihood and impact into simplified risk scores. Although these approaches can support preliminary analysis, they may obscure important differences among physical, operational, functional, economic, safety, environmental, and societal impacts. They may also provide limited support for representing consequences that change over time, interact with one another, or remain uncertain because of incomplete knowledge.

The objective of this Ph.D. project is to develop an integrated and uncertainty-aware framework for quantifying the impacts of cyberattacks on critical cyber-physical systems. The research will investigate how multiple consequence measures can be combined into rigorous, transparent, and interpretable assessments without concealing the assumptions, limitations, or uncertainty associated with the underlying evidence.

Project Keywords:

- cybersecurity
- cyber-physical systems
- impact measurement
- security metrics
- uncertainty quantification
- quantitative risk assessment
- Bayesian networks
- sensitivity analysis
- cascading impacts
- modeling and simulation
- data analytics
- 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 evaluating existing approaches for measuring the physical, operational, economic, safety, environmental, and societal consequences of cyberattacks on critical systems.
2. Developing methods for integrating multiple impact measures and accounting for uncertainty in cyberattack scenarios, system behaviour, and consequence assessments.
3. Investigating and applying appropriate analytical and computational techniques for modeling uncertainty, propagating its effects through impact assessments, and communicating assessment results.
4. Developing and evaluating computational tools and methods for analyzing cyberattack impacts, including temporal and cascading consequences, and comparing attack scenarios and potential security mitigations.
5. Conducting empirical evaluations using critical cyber-physical system case studies, simulations, and documented cyber incidents, and communicating research findings through scholarly publications and presentations.

Expected Research Contributions

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

- New approaches and methods for measuring and assessing the consequences of cyberattacks on critical cyber-physical systems.
- Techniques for integrating multiple consequence measures and accounting for uncertainty in impact assessments.
- Computational tools and supporting case studies to demonstrate the application of consequence-driven assessment in critical-system domains.
- New knowledge and empirical evidence to support more informed cybersecurity and engineering decisions based on the potential consequences of cyberattacks.

Desired Skills/Qualifications

Suitable candidates will have a Master's degree in Software Engineering, Computer Science, Computer Engineering, Systems Engineering, Cybersecurity, Applied Mathematics, Data Science, 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 quantitative research with practical relevance.

Applicants should have a background or demonstrated interest in several of the following areas:

- cybersecurity, security engineering, or cyber risk assessment;
- probability, statistics, quantitative modeling, or uncertainty analysis;
- data analysis, simulation, or modeling of complex systems;
- security, safety, dependability, or resilience assessment; and
- cyber-physical systems, industrial control systems, or critical infrastructure.

Candidates should be comfortable working with incomplete and heterogeneous evidence, clearly documenting analytical assumptions, and critically evaluating the validity and limitations of quantitative results. Experience with empirical research, experimental design, scientific software development, data visualization, or peer-reviewed publication will be considered an asset. Effective written and oral communication skills are also essential.

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.