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-02

November 13, 2026

Position Available: M.A.Sc. Candidate

Metrics for Measuring Cyberattack Impacts on Critical Systems

The Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University is actively seeking a Master's student to work on a funded research project on the topic of metrics for measuring cyberattack impacts on 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 operations, damage equipment, interrupt essential services, create safety or environmental hazards, and produce significant economic losses.

Cybersecurity assessments often describe the expected impact of an attack using broad categories such as "low," "medium," or "high." Although these categories can support preliminary assessments, they may not provide enough evidence for engineers and decision-makers to compare attack scenarios, prioritize security investments, or determine whether a proposed mitigation meaningfully reduces the consequences of an attack.

More precise assessments require credible metrics. For example, the impact of an attack might be measured in terms of service downtime, recovery time, financial loss, physical damage, loss of system functionality, environmental harm, or effects on human safety. However, existing impact metrics are distributed across cybersecurity, safety, resilience, dependability, and critical-infrastructure research. Their definitions, assumptions, units, evidence requirements, and intended uses can differ significantly.

Some metrics directly measure the severity of a consequence, while others provide only indirect indicators or proxies. A measure of system downtime, for example, may provide useful evidence of operational disruption but may not fully describe the resulting economic, safety, or societal consequences. Similarly, a financial estimate may combine several different forms of harm while obscuring important assumptions or uncertainties.

The objective of this M.A.Sc. project is to identify, organize, and evaluate quantitative metrics for measuring the consequences of cyberattacks on critical cyber-physical systems. The research will develop a structured and extensible catalog that explains what each metric measures, what evidence it requires, what assumptions it makes, and the situations in which it can support a credible impact assessment.

Project Keywords:

- cybersecurity
- cyber-physical systems
- security metrics
- impact measurement
- quantitative analysis
- systematic literature review
- consequence assessment
- cyber resilience
- risk assessment
- 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. Conducting a systematic review of existing approaches and metrics for measuring the physical, operational, economic, safety, environmental, and other consequences of cyberattacks on critical systems.
2. Developing a structured and extensible catalog of impact metrics, including their definitions, measurement units, evidence requirements, assumptions, limitations, and application contexts.
3. Classifying and analyzing metrics based on the consequence dimensions they measure, their relationships to other metrics, and their suitability for different systems and decision contexts.
4. Developing criteria and guidance for evaluating and selecting appropriate impact metrics, considering factors such as validity, interpretability, evidence requirements, and practical usefulness.
5. Applying and evaluating selected metrics through critical cyber-physical system case studies, 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 and extensible catalog of quantitative metrics for measuring the consequences of cyberattacks on critical cyber-physical systems.
- A classification and analysis of impact metrics that identifies their measurement characteristics, application contexts, relationships, and limitations.
- Evaluation criteria and practical guidance for selecting appropriate metrics based on consequence types, system characteristics, available evidence, and intended decisions.
- A structured representation and case-study evaluation demonstrating the applicability and practical value of the proposed measurement catalog.

Desired Skills/Qualifications

Suitable candidates will have a Bachelor's degree in Software Engineering, Computer Science, Computer Engineering, Cybersecurity, Systems Engineering, Data Science, Applied Mathematics, 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 demonstrate preparation or interest in several of the following areas:

- cybersecurity, security engineering, or cyber risk assessment;
- cyber-physical systems or critical infrastructure;
- security, safety, dependability, or resilience assessment;
- quantitative analysis, applied statistics, or measurement methods;
- empirical research, systematic literature reviews, or data analysis; and
- modeling, simulation, or research software development.

Candidates should be comfortable reading and synthesizing technical literature, working with quantitative information, examining the assumptions behind numerical measures, and documenting analytical decisions clearly. Previous experience

with cybersecurity projects, systematic or structured literature reviews, quantitative research, experimental design, data analytics, scientific software development, or scholarly writing 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.