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-GD-01

November 13, 2026

Position Available: M.A.Sc. Candidate

Developing Agentic AI Prototypes for Automated Network Security Analysis and Cyber Defence

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 focused on developing agentic artificial intelligence (AI) prototypes for automated network security analysis and cyber defence, starting in September 2027 or sooner. The project will be conducted in collaboration with General Dynamics Mission Systems–Canada (GDMS-C).

Project Description and Objectives

Modern computer networks are increasingly complex, dynamic, and difficult to defend. Organizations rely on interconnected systems, devices, applications, and communication services to support their operations. As these environments grow, security analysts must continuously interpret network configurations, monitor system activity, investigate alerts, assess vulnerabilities, and determine how to respond to emerging threats. The volume and diversity of available network and security information can make these tasks increasingly difficult to perform efficiently and consistently.

Artificial intelligence has the potential to help analysts manage this complexity. In particular, agentic artificial intelligence (AI) systems combine the reasoning capabilities of large language models (LLMs) with access to specialized cybersecurity tools, network data, and external knowledge. Rather than simply generating textual responses, AI agents can plan sequences of actions, select and invoke appropriate tools, interpret the results, and adapt their approach as new information becomes available. These capabilities create opportunities to automate or augment cybersecurity activities such as network discovery, configuration analysis, vulnerability investigation, and defensive decision-making.

However, applying agentic AI to operational cybersecurity environments presents several challenges. AI agents must be able to access and interpret information from diverse network data sources, interact reliably with existing security tools and application programming interfaces, and reason about potentially incomplete or changing information. Their actions and recommendations must also be relevant, reliable, and consistent with the security objectives of the environment. Developing practical agentic AI solutions therefore requires investigating suitable architectures, tools, information models, and workflows, as well as evaluating their effectiveness in representative network environments.

The objective of this M.A.Sc. project is to develop and evaluate a lightweight agentic AI prototype for automated network security analysis and cyber defence. The research will investigate how LLM-based AI agents can interact with network environments and cybersecurity tools to collect and interpret network information, identify potential threats and vulnerabilities, and recommend or support defensive actions. The work will involve defining network information models, identifying relevant data sources, establishing data collection and monitoring environments, and developing and evaluating agentic workflows for automated network analysis.

Project Keywords:

- cybersecurity
- artificial intelligence
- agentic AI
- large language models
- network security analysis
- cyber defence
- network monitoring
- vulnerability assessment
- threat detection
- security automation
- cybersecurity tools
- AI agent workflows

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 existing research on agentic artificial intelligence, large language models, AI-driven cybersecurity, network security analysis, and the use of AI agents for security automation, and identifying relevant architectures, tools, and techniques.
2. Defining network information models and identifying relevant data sources, cybersecurity tools, and application programming interfaces (APIs) to support AI agent interactions with network environments and security infrastructure.
3. Establishing data collection and monitoring environments to support experimental deployments, including identifying and integrating sources of network configuration, asset, vulnerability, and security event information.
4. Evaluating LLM-based agentic architectures, tools, and workflows for cybersecurity automation and reasoning, including their ability to interpret network information, invoke appropriate tools, investigate potential threats and vulnerabilities, and adapt their actions based on observed results.
5. Designing, developing, and evaluating a lightweight agentic AI prototype for automated network security analysis and cyber defence, including contributing to related research and development activities within the General Dynamics Mission Systems–Canada (GDMS-C) projects.
6. Collaborating with other members of the research team, meeting with project stakeholders and industry partners, including GDMS-C representatives, to discuss project requirements, research progress, technical developments, and evaluation results, and communicating research outcomes through technical reports, 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 network information model and identification of relevant data sources to support agentic AI-driven network security analysis.
- An evaluation of LLM-based agentic architectures, cybersecurity tools, and integration approaches for automated network analysis and vulnerability investigation.
- Agentic workflows that enable AI agents to collect and interpret network information, interact with cybersecurity tools, and support automated security analysis and defensive decision-making.
- A lightweight prototype demonstrating the application of agentic AI to network security analysis and cyber defence, together with experimental results evaluating its capabilities, effectiveness, and limitations.

Desired Skills/Qualifications

SuSuitable candidates will have a Bachelor's degree in Software Engineering, Computer Systems Engineering, Commmunications Engineering, Information Technology, Computer Science, or a 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:

- artificial intelligence, machine learning, or large language models;
- agentic AI systems, autonomous agents, or AI-driven workflow automation;
- cybersecurity, network security analysis, or vulnerability assessment;
- computer networks, network monitoring, or network and system administration;
- software development, programming, or integration of tools and APIs; and
- data modeling, experimental design, or research software development.

Candidates should be comfortable reading and synthesizing technical literature, working with network and security information, evaluating technical tools and software architectures, developing and testing software prototypes, and documenting experimental methods and results clearly. Previous experience with cybersecurity projects, AI or LLM-based applications, agent frameworks, graph algorithms, network analysis, data analytics, API integration, scientific software development, or scholarly writing will be considered an asset.

Because this research involves collaboration with an industry partner and may involve access to controlled systems, software, data, or facilities, the successful candidate may be required to comply with applicable confidentiality, information-security, access-control, or research-agreement requirements.

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 Environment

The successful candidate will join a collaborative, interdisciplinary research environment within the General Dynamics Mission Systems–Canada/Carleton University Cyber Operations Reference Lab (GCOR Lab), hosted by the CyberSEA Research Lab at Carleton University. The GCOR Lab supports applied research in cybersecurity and cyber operations, bringing together projects in cyber training and simulation, network modelling, artificial intelligence, and resilient network services. The candidate will have opportunities to collaborate with undergraduate researchers, graduate students, and postdoctoral fellows working on complementary projects, engage with the broader research activities of the CyberSEA Research Lab, and interact with industry partners and other project stakeholders.

The candidate will receive regular research supervision and participate in research group meetings, technical discussions, collaborative development activities, and peer mentoring. Training and professional development will include research methodologies, technical skills relevant to the project, practical experience with cybersecurity tools and technologies, scientific writing, and the effective communication of research results. The collaborative environment will provide opportunities to learn from researchers with different levels of experience and contribute to multidisciplinary research activities.

The candidate will be encouraged and supported in presenting their work at research and professional events, contributing to technical reports and scholarly publications, and developing the skills needed to conduct independent research and collaborate effectively within a research team. Opportunities to engage directly with project partners, including General Dynamics Mission Systems–Canada, will provide exposure to industry perspectives, applied research challenges, and the practical considerations involved in translating research outcomes into operational contexts.

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 (Jason Jaskolka: jason.jaskolka@carleton.ca) and Project Lead Researcher (Ali Sadeghi Jahromi: AliSadeghijahromi@cmail.carleton.ca). Please include the specific **position posting number** in the subject line of your email.

Contact

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.