liberal arts & professional studies | YORK U

Managing Risks to Critical Infrastructure

AP/DEMS4707 A
FALL 2024

Course Information

Course Instructor: David Baumken
E-mail:Dbaumken@yorku.ca
Phone:
Office Hours & Location:TDB

Course Time & Days: 2:30pm – 5:00pm Tuesdays
Class Location: Winters College 118
Course eClass site: TBD

Tutorials, Labs and TA Contact Information
N/A

Land Acknowledgment

York University recognizes that many Indigenous Nations have longstanding relationships with the territories upon which York University campuses are located that precede the establishment of York University. York University acknowledges its presence on the traditional territory of many Indigenous Nations. The area known as Tkaronto has been care taken by the Anishinabek Nation, the Haudenosaunee Confederacy, and the Huron-Wendat. It is now home to many First Nation, Inuit, and Métis communities. We acknowledge the current treaty holders, the Mississaugas of the Credit First Nation. This territory is subject of the Dish with One Spoon Wampum Belt Covenant, an agreement to peaceably share and care for the Great Lakes region (LA&PS Land Acknowledgement).

Course Overview

Critical infrastructure (CI) are the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security and economic wellbeing of nations. Critical infrastructure can be stand-alone or interconnected and interdependent. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic and societal effects, and significant harm to public confidence. The course focuses on Canada but also examines how other countries define and manage their critical infrastructure.

Course Description

Students of the Managing Risks to Critical Infrastructure course will research threats, vulnerabilities and risks (all hazards) to critical infrastructure from the perspective of managing risks to ensure for reliability through appropriate protection and resiliency measures, regulations/laws strategies and practices as well as the importance, ways and means, of conducting periodic risk and resiliency assessments. Examine and assess regulatory requirements, legislation and due diligence for optimal reliability through the effective management of risks by critical infrastructure owners and operators. Events (incidents) and threats to critical infrastructures stemming from accidents, physical and cyber attacks by criminals, terrorists and nation states are undertaken.

Pre-Requisites: 3rd year AP/DEMS or permission of the Course Director
Course Credit Exclusions (CCE):

Course Learning Objectives

By the end of this course, students will be able to:

- Demonstrate though research and assignments an understanding of effective risk management strategies and plans, application of risk assessment methodologies, vulnerabilities and risks reduction and strategies and practices for enhancing and measuring resiliency
- Demonstrate through research and assignments the understanding of the complexity, challenges and importance of enhancing resiliency of critical infrastructure with respect to the societal and economic consequences arising from human-made events including malicious physical and cyber attacks
- Demonstrate through research an understanding of the complexities of CI, the inter-connectedness of dependencies and the cascading effects and complicating factors of failing critical infrastructure.
- Develop an understanding of the potential consequences of the changing climate on vulnerable critical infrastructure and approaches to managing the risks.
- Develop through various means of learning an understanding of the critical importance of access to credible actionable information from credible sources and the potential consequences of dis-information.
- Develop an understanding of the common and not so common (high impact low frequency), and unpredictable (Black Swan) type threats, vulnerabilities and associated risks to critical infrastructures that have resulted in or pose a significant threat of inflicting catastrophic damage and interruption of CI operations with societal and economic consequences.
- Develop an understanding of the various ‘actors’ that pose a threat to critical infrastructure owners and operators. This includes nation states perpetrating cyber and conventional warfare, terrorists, domestic extremists, criminals, special interest groups

such as environmental and animal right activists and the threat and associated challenges posed by ‘Insiders’ and the ‘lone wolf’.

- Develop an understanding of regulatory and due diligence/ethical challenges for effective reliability and protection measures, government, society and stakeholder reliability expectations and associated challenges, including costs of managing risks.
- Develop an understanding of government regulations and associated legislation for the protection of critical infrastructure.
- Develop critical thinking skills,and communication skills.
- Develop an understanding of the legislation and associated weaknesses and gaps for the protection and privacy of personal information.
- Develop an understanding for the use of Artificial Intelligence (AI) both effectively and responsibly for written and visual assignments and evaluate the outputs of AI (ChatGPT3) in the context of accuracy, reliability, and potential biases and differentiate where ChatGPT3 provides value versus human effort.

Course Organization

The course eclass site will reflect weekly class subject matter for each class. Professor Baumken will assign required readings and or research each week that will require 1 to 2 hours to complete in preparation for the next class.

The first 60 minutes or less will cover the learning objectives for the class and the coming weeks reading assignment posted to the eclass site. A ‘round table’ discussion will follow where students are given the opportunity to share course relevant ‘in the news’ events that they have learned and they feel should be of interest to the class.

10 minute break

The next 30 to 40 minutes students will either view a video provided by the professor
Or read a short article/paper provided by the professor
Or conduct research at the direction of the professor
Or undertake research project work.

10 minute break

The next 30 minutes will be spent on reviewing and otherwise discussing the video or article/paper.

The next 30 minutes will be spent on new material (Professor lecture)

Instructor Office Hours and Communication Guidelines

Time can be schedule before class commences

Required Course Materials

Required weekly reading material will be provided by the professor and posted to the eclass site no later than every Wednesday in advance of the following Tuesday class for which it is due.

Optional Course Materials

Recommended reading (not required however the following books are excellent cyber threat resources)

- Sandworm by Andy Greenburg (A new era of cyber war and the hunt for the Kremlin's most dangerous hackers)

Or

- The Perfect Weapon by David E. Sanger (War, Sabotage and Fear in the Cyber Age

Technical Requirements

Several platforms will be used in this course (e.g., eClass, Zoom, etc.) where students will interact with the course materials, the course director/TA, as well as with each other.

Here are some useful links for computing information, resources, and help:

- Student Guide to eClass
- Zoom@YorkU Best Practices
- Zoom@YorkU User Reference Guide
- eLearning Getting Started (LA&PS eServices)
- Student Guide to Remote and Online Learning

To determine Internet connection and speed, there are online tests, such as Speedtest, that can be run. If you need technical assistance, please consult the University Information Technology (UIT) Student Services web page or write to askit@yorku.ca.

Course Evaluations

- **Class Participation in lectures, debates as well as class attendance 40%**
- **In class written assignment 20% October 29, 2024**
- **Final assignment 40% In class written assignment on December 3, 2024**

Course Evaluation Chart

Assessment	Due Date	Weight %	Course Learning Outcome
Class Participation in lectures, debates and attendance	End of classes December 3, 2024	40%	Oral demonstration of learning objejectives
In class written assignment	October 29, 2024	20%	Mid term assessment of learing objectives to date
Final in class written assignment	December 3, 2024	40%	Written demonstration of course learning objectives
		100%	

Assessment Descriptions

[Text]

How to Submit Assessments

[Text]

Late Work Policy

[Text]

Missed Tests and Exams

[Text]

How to Use Citations in this Course

[Text]

Resources to help with citations:

- I need to cite and reference, Learning Commons
- Drop-in Research Support, YorkU Libraries

- Writing Centre
- SPARK Student Papers & Academic Research Kit

Grading

The grading scheme for this course conforms to the 9-point system used in undergraduate programs at York University. For a full description of the York grading system, visit the York University Academic Calendar.

Grade	Grade Point	Percent Range	Description
A+	9	90-100	Exceptional
A	8	80-89	Excellent
B+	7	75-79	Very Good
B	6	70-74	Good
C+	5	65-69	Competent
C	4	60-64	Fairly Competent
D+	3	55-59	Passing
D	2	50-54	Marginally Passing
E	1	(marginally below 50%)	Marginally Failing
F	0	(below 50%)	Failing

Course Schedule

Important Dates

Explore the York University Academic Calendar to find a list of important dates, such as class start/end dates, drop deadlines, holidays and more.

Weekly Course Schedule

**Following sequence of course subject matter may change.*

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 1 Sept 10, 24	**Roles and responsibilities of government (federal, provincial, municipal)** • Examination of the 10 Canadian critical infrastructure sectors and the relationships with Provincial CI Programs, other nations including but not limited to the United States sectors and their inter-relationships. • Overarching objective of the National Strategy (mandate of Canadian Federal Government's Sector Networks). • Ministerial responsibilities for CI and oversight on private sector CI owners and operators • Regulations – enforceable standards and guidelines (not enforceable) for the protection and reliability of critical infrastructure goods and services. Private sector CI owners and operators (practices) due diligence for protecting assets, ensuring for reliability and resiliency.		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 2 Sept 17, 24	**Critical thinking** • Theoretical principals in relation to managing risks to critical infrastructure **Trust, its importance to nations critical infrastructure protection programs** • Utilizing the theories related and inferred in Canada's National CI Strategy and as the cornerstone of information sharing, identify strengths, weaknesses of relationships including value propositions of government private sector partnership for the protection of critical infrastructure. **Risk and vulnerability reduction, theories and effective (best) practices** • Reducing vulnerabilities (reducing inter-dependencies, enhancing resiliency), mitigating and even eliminating risks. Importance of redundancy • Hardening assets (cross reference high impact low frequency type events in terms of associated costs utilizing examples including severe solar storm effects on vulnerable CI assets of the electrical GRID and satellites) • Supply chain • Inter-dependencies • Outsourcing		

Class 3 Sept 24, 24	**Dependencies and inter-dependencies.** • CI Interconnectedness, complexities and cascading consequences when CI catastrophically fails. • Challenges and importance of identifying and documenting inter-dependencies. • Strategies for managing tolerance for loss, complicating factors that compound situations (cascading effect of another CI's contingency/failure). **Risk types (applicable to CI's)** • Regulatory (including cost burdens), hidden, reputational, operational • Acceptance of risk, asset replacement strategies for aging infrastructure • Climate Risks (wind, precipitation, ice, wild fires, extreme temperatures, drought, flooding) • Cyber **Sources of risk management information** • All hazards approach, examination of credible sources of expert information. • Information types including but not limited to - Situational Awareness, Information Sharing and Analysis, Incident Analysis and Warnings (centers), CERTS, Government Operations Centers, threats, risks, vulnerability, expert best practices information sources. • Credible sources (who, what, when)		

Class 4 Oct 1, 24	**Critical infrastructure protection (including reliability, security and risk management) regulations, legislation/laws** • In-depth examination of (select) CI regulations, analysis of effectiveness, measurement methods (including theories), associated compliance obligations, sanctions/penalties **Reliability** • Examine regulatory agencies and CI's commitment (strengths and weaknesses), challenges and strategies to achieve reliability targets. • Examine CI best practices, Standards and Guidelines (comparison of Canadian versus US and also examine accountability including but not limited to US GAO) • Normal Accident Theory in relation to CI Failures due to complexity, interconnectedness, Highly Reliable Organizations (High Reliability Theory) **Resiliency** • Properties of resilience (robustness, redundancy, resourcefulness, rapidity and organizational learning). Dimensions of resilience (technical, organizational, social and economic). • Resiliency of critical infrastructure can be evidenced by but is not limited to: • Reduced failure probabilities –The reduced likelihood of damage and failures to critical		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
	infrastructure, systems, assets, and nodes; • Reduced consequences from failures – Minimal injuries, deaths, infrastructure and property damage, negative economic and societal impact or consequences; • Reduced recovery time – The time required to restore to normal levels of service or functionality. • Information sharing (all levels of government, law enforcement/intelligence agencies and private sector CI owners and operators). Need to know, right to know and importance of needing to share.		
Class 5 Oct 8, 24	**Risk management and risk assessment.** • Examination of risk assessment methodologies and theoretical protection measures. • Risk management effective practices (including examination of notable standards and guidelines). • Should social media be regulated? This will be discussed in conjunction with critical thinking and dis-information learning that will be reoccurring throughout the course as there are a number of aspects that touch on multiple course concepts		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 6 Oct 22, 24	**Environment** • Role in relation to critical infrastructure (State of the Urban Forest in the Greater Toronto Area – is the environment critical infrastructure?) Research Ontario's climate change plan/policy in relation to CI's and impact on consumers. **Criminal, terrorist and domestic extremists and insider threats to critical infrastructure** • Terrorist/extremists. Examination of tactics CI's can use to deter terrorists, insiders and manage the risks.		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 7 Oct 29, 24	**In class Assignment 1** **Cyber threats, vulnerabilities and risks to critical infrastructures** • Examination of the vulnerabilities and risks of supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS). • Cyber warfare, cyber espionage, cyber vandalism (war fare, criminal acts) state and non-sate actors, societal and economic consequences, publics perception of risk • CI's as targets of cyber warfare. Examination of Humanitarian Laws applicability to cyber warfare by nation states on critical infrastructure (examination of the Tallinn Manual, the International Committee of the Red Cross and the Geneva Convention).		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 8 Nov 5, 24	**Threats, vulnerabilities and risks to critical infrastructures** • Examination of catastrophic loss of CI's due to severe weather events. • Severe solar storms, geomagnetic disturbances, geomagnetic inducted current impact on vulnerable CI's, risk management practices including but not limited to asset hardening, monitoring. **Highly Reliable Organizations** • Principals and characteristics of 'highly reliable' critical infrastructures.		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 9 Nov 15, 24	**Managing Climate Change Risks to Critical Infrastructure** • Focus is on 'forward looking' climate change adaption measures, vulnerability assessments and resiliency planning, to the effects of the changing climate on Canadian and US transmission and distribution electricity systems. • The various climate hazards and expected time horizons are assessed in identifying vulnerabilities and risks of assets, components, equipment and system operations that can lead to damage, destruction, failure, and the exacerbation of the aging process. • Existing asset design and construction criteria, methods and associated standards when coupled with projections of increased severity of climate hazards could exacerbate the aging of assets and potentially exceed failure thresholds.		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes

Class 10
Nov 22, 24
	Legislation/regulations for the protection and access of information as it relates to CI's and individuals.
	• Access to, protection of, ownership of Information and Data (as per Emergency Management Act, National CI Strategy, PEPIDA, PIPPA amongst others).
	  ○ Examination of the vulnerabilities and risks and the strength/weakness/gaps in regulations.
	  ○ Cyber data breaches, Examination of the rights and expectations for privacy of personal information from the perspective of citizens/customers.		

Week	Readings and Activities	Assessment Due Dates	Learning Outcomes
Class 11 Nov 29, 24	**High impact low frequency incidents (HILF)** • Planning/predicting HILF incidents. Risk/costs of protecting vulnerable CI's. (Examination of the threat of pandemics, geomagnetic disturbances, coordinated terrorist attacks on vulnerable CI's and risk reduction measures and practices). **Managing the unpredictable.** Predicting the unpredictable, Black Swans, positive, negative, grey and True Black Swans • Prediction, uncertainty and randomness of significant incidents (Black Swans) impacting or threatening CI's. (Known versus the unknown and the influence of experience) • Whistle Blowing (protection for whistle blowers, importance for managing risks), supported by a case study. **Effects based targeting of critical infrastructure** • CI as a target of nation state military attacks (Russia's war on Ukraine) • Can this risk be mitigated or even managed?		
Class 12 Dec 3, 24	Course subject matter review and Final in class assignment		

Course Policies

Please review the course policies in this section. All students are expected to familiarize themselves with the following information:

- Student Rights & Responsibilities
- Academic Accommodation for Students with Disabilities

Academic Integrity

Academic integrity is a fundamental and important value of York University. As a York student, you are responsible for understanding and upholding academic integrity by completing your own work. Connect with reliable on-campus resources that can support your work in ways that uphold academic honesty values of honesty, trust, fairness, responsibility, and courage. To better understand the serious consequences of breaching academic honesty policies, familiarize yourself with the *Senate Policy on Academic Honesty*. You can learn more about upholding academic integrity in your courses by exploring the Guiding Principles for LA&PS webpage.

Generative Artificial Intelligence (GenAI)

Students are not permitted to use generative artificial intelligence (AI) in this course. Submitting any work created (in whole or part) through the use of generative AI tools will be considered a violation of York University's *Senate Policy on Academic Honesty*. Using AI apps such as ChatGPT, GPT-3, DALL-E, translation software among others to complete academic work **without your instructor's knowledge or permission**, is considered to be a breach of academic honesty. For more information, please review AI Technology & Academic Integrity: Information for Students.

If you're not sure whether using an AI app for your academic work is acceptable, it is recommended that you:

- Carefully review the guidelines for your assessments
- Check for any messages from your instructor on eClass
- Ask your instructor or TA if they are permitting the use of these tools

Turnitin

To promote academic integrity in this course, students will normally be required to submit their written assignments to Turnitin (via the course's eClass site) for a review of textual similarities and the detection of possible plagiarism. In so doing, students will allow their material to be included as source documents in the Turnitin.com reference database, where they will be used only for the purpose of detecting plagiarism. The terms that apply to the University's use of the Turnitin service are

described on the Turnitin.com website. York students may opt out of using Turnitin. If you wish to opt out, you should contact your instructor as soon as possible.

Accessibility

York University is committed to creating a learning environment which provides equal opportunity to all members of its community. If you anticipate or experience any barriers to learning in this course, please discuss your concerns with your instructor as early as possible. For students with disabilities, contact Student Accessibility Services to coordinate academic accommodations and services. Accommodations will be communicated to Course Directors through a Letter of Accommodation (LOA). Accommodations for tests/exams normally require three (3) weeks (or 21 days) before the scheduled test/exam to arrange.

Religious Observance Accommodation

York University is committed to respecting the religious beliefs and practices of all members of the community and making reasonable and appropriate accommodations to adherents for observances of special significance. Should any of the dates specified in this syllabus for course examinations, tests, or deadlines conflict with a date of religious significance, please contact the instructor within the first three (3) weeks of class. If the date falls within the formal examination periods, you must complete and submit a Religious Accommodation for Examination Form at least three (3) weeks before the start of the exam period.

Intellectual Property

Course materials are designed for use as part of this particular course at York University and are the intellectual property of the instructor unless otherwise stated. Third-party copyrighted materials (such as book chapters, journal articles, music, videos, etc.) have either been licensed for use in this course or fall under an exception or limitation in Canadian copyright law. Students may not publish, post on an Internet site, sell, or otherwise distribute any course materials or work without the instructor's express permission. Course materials should only be used by students enrolled in this course.

Copying this material for distribution (e.g., uploading material to a commercial third-party website) may lead to a charge of misconduct according to York's *Code of Student Rights and Responsibilities*, the *Senate Policy on Academic Honesty*, and/or legal consequences for copyright violations.

Student Support and Resources

York University offers a wide range of student supports resources and services, including everything from writing workshops and peer mentorship to wellness support and career guidance. Explore the links below to access these on-campus resources:

- Academic Advising is available to provide students support and guidance in making academic decisions and goals.
- Student Accessibility Services are available for support and accessibility accommodation when required.
- Student Counselling, Health & Wellbeing offers workshops, resources, and counselling to support your academic success.
- Peer-Assisted Study Sessions (PASS) Program provides student study sessions for students to collaborate and enhance their understanding of course content in certain courses.
- Student Numeracy Assistance Centre at Keele (SNACK) supports students in courses involving math, stats, and Excel.
- The Writing Centre provides multiple avenues of writing-based support including drop-in sessions, one-to-one appointments, a Multilingual Studio, and an Accessibility Specialist.
- Centre for Indigenous Student Services offers a community space with academic, spiritual, cultural, and physical support, including writing and learning skills programs.
- ESL Open Learning Centre (OLC) supports students with building proficiency in reading, writing, and speaking English.
- Learning Skills Services provides tips for time management, effective study and learning habits, keeping up with coursework, and other learning-related supports.
- Learning Commons provides links to supports for time management, writing, study skills, preparing for exams, and other learning-related resources.
- Roadmap to Student Success provides students with timely and targeted resources to help them achieve academic, personal, and professional success.
- Office of Student Community Relations (OSCR) is responsible for administering the *Code of Student Rights & Responsibilities* and provides critical incident support.
- Peer Mentorship helps students transition through their first year by connecting them with upper-year students. The mentors can help find supports and resources. They also lead a community hub on campus.
- goSAFE is staffed by York students and can accompany York community members to and from any on-campus location, such as the Village Shuttle pick-up hub, parking lots, bus stops, or residences.

For a full list of academic, wellness, and campus resources visit Student Support & Resources.