DEMS4707– Managing Risks to Critical Infrastructure – Fall Term 2022-2023
Course Director, Adjunct Professor – David Baumken
david.baumken@gmail.com or dbaumken@yorku.ca
Tuesdays 2:30am to 5:30pm

Students of the Managing Risks to Critical Infrastructure course will research threats, vulnerabilities and risks 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 natural disasters, accidents, physical and cyber attacks by criminals, terrorists and nation states are undertaken.

Critical infrastructure (CI) refers to 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.

The first 60 minutes or less will cover the learning objectives for the class and the coming weeks reading assignment posted to the Moodle site. A round table discussion will follow where students are given the opportunity to share something course relevant 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 group 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).

Learning Objectives
Students will;

- Develop an understanding of effective risk management strategies and plans including but not limited to the conduct and application of numerous risk assessment methodologies.
- Develop an understanding of complexity, challenges and importance of enhancing resiliency of critical infrastructure with respect to the societal and economic consequences arising from natural disasters, man made events including malicious physical and cyber attacks and accidents.
- 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 complexities of CI, the inter-connectedness of dependencies and the cascading effects of failing critical infrastructure.
- 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, written and verbal communication skills and group work.

**Following course subject matter is in no particular order. Moodle site will reflect weekly class subject matter for each class. Professor will assign required readings each week that will require 1 to 2 hours to complete*

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.

- Should social media be regulated? This will be in the form of a case study, a reoccurring theme throughout the course as there are a number of aspects that touch on multiple course concepts

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.
- 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.

Critical thinking

- Theoretical principals in relation to managing risks to critical infrastructure (a case study will be used to reinforce critical thinking capability which will be important in completing assignment and the quiz).

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 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.

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
- Aging CI, acceptance of risk, asset replacement strategies for aging infrastructure

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).
- Whistle Blowing (protection for whistle blowers, importance for managing risks), supported by a case study (737 Max aircraft problems with MCAS).
- Prediction, uncertainty and randomness of significant incidents (Black Swans) impacting or threatening CI's. (Known versus the unknown and the influence of experience)

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)

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

Natural disasters, 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.

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).

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.

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.

High impact low frequency incidents (HILF)

- Planning/predicting HIFL 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.

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?

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 (impending) climate change plan/policy in relation to CI's and impact on consumers.
- Climate change and its impact on CI (exasperating the aging of certain vulnerable CI assets)

Assignments and Grading Student (demonstration of achieving learning objectives)

- **First assignment 25%** (research paper, approximately 2500 words excluding references. Topic of your choosing incorporating the applicable to your topic course concepts and theories taught thus far in the course. Due October 18, 2022. Students are encouraged to discuss their intended topic and research papers content with the professor.

- **Group Research Project 15%** Students will work in two groups on a research assignment assigned by the professor during class 2 September 20. Time will be allocated most weeks during class for the groups to collaborate however additional time outside of normal class time will be needed. During a class yet to be decided upon each group will present their findings. Highly recommended that each group prepare a visual presentation such as Powerpoint or similar type, include a bibliography and list each of the group members. It is up to each group to determine member responsibilities in achieving scope and objectives of the research project.
- **Final assignment 60%** (formal academic research paper, 4000-5000 words excluding references. Topic of your choosing incorporating the applicable to your topic course concepts and theories from the perspective of managing risks, reliability and resiliency (societal and or economic consequences). Due December 13, 2022. Students are encouraged to discuss their intended topic and research papers content with the professor.

- The first and final assignment submission shall be the student's original works, not previously submitted in other courses.

- Late final assignment unless previously approved (has to be a very good reason to request professor approval for late submission) penalized 5% per day

First and Final Assignment Formatting

- Academic research paper formatting, citations – one of the common styles such as MLA (Modern Language Association), which is commonly used for papers in the Liberal Art and Humanities. Or APA (American Psychological Association) commonly used in the social sciences.
  - 250 words/page double-spaced.
  - Supporting diagrams, tables, charts, pictures should be included where appropriate/available

Grading

http://gradstudies.yorku.ca/current-students/regulations/courses-grading/

Review the course learning objectives and my Marking Rubric posted to the Moodle site and please contact me should you need any clarification

Course Reading Material

- Required weekly reading material will be provided by the professor and posted to the Moodle site no later than every Wednesday in advance of the following Tuesday class for which it is due.
- Recommended reading (not required however the following books are excellent 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

University & School Policies

https://www.yorku.ca/laps/sas/academic-resources/common-course-policies/