July 9, 2019

**4707 – Managing Risks to Critical Infrastructure – Fall Term 2019-2020**

**Course Director, Adjunct Professor – David Baumken,**

**david.baumken@gmail.com or** **dbaumken@yorku.ca**

Students of the Managing Critical Infrastructure course will research and otherwise investigate threats, vulnerabilities and risks to critical infrastructure from the perspective of ensuring for reliability through appropriate protection and resiliency measures, regulations/laws strategies, practices and theories. Examine and assess regulatory requirements, legislation and due diligence in terms of ensuring 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 (warriors) is 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.

Course Introduction (first class)

* Course learning objectives, assignments (2), and course grading (review and discussion of the two Marking Rubrics that I use).
* Overview of the 12 lectures, weekly required readings, research and the course Moodle site.
* Core CI Protection elements and concepts – Reliability, Resiliency, Inter-dependencies, Vulnerabilities, Information Sharing, Risk Management
* Definition of critical infrastructure. CI Characteristics – complex processes, tightly coupled (inter-connected) with significant dependency on other CI’s (inter-dependencies)
* Control/ownership of critical infrastructure (private sector versus government controlled)

*\*Following subject matter is in no particular order (see Moodle site for weekly class subject matter content).*

Roles and responsibilities of Government (federal, provincial, municipal)

* Examination of the 10 Canadian 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.

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 strength/weakness/gaps in regulations through the use of case studies
	+ Cyber Data breaches. Examination of the rights and expectations for privacy of personal information from the perspective of citizens/customers. Examination of case hacks/attacks including but not limited to Equifax)
* 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 assignments).

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. Assessment/measurement of metrics through the examination of events including but not limited to Super Storm (Hurricane) Sandy, Ice Storm 2013.
* 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). *CI employee’s* w*illingness to respond can depend on their own perception of risk, dedication etc. Emergency Managers, Business Continuity Planners and Human Resources role and responsibilities in being influencers to WTR.*
* Class/research assignment – strategies and best practices of organizational learning in relation to reducing CI vulnerabilities and risks to natural and technological disasters or in response and recovery to health emergencies (pandemics or other type acute infectious agents).
* Examination of CI resiliency through research of current events, development of resilience measurements, principals and practices, take home assignment/case study on resilience challenges and potential resiliency measurements of your choice of CI’s.
* Measuring Resiliency (principals and theory, review of NATO Resiliency Guidelines)

Redundancy

* Definition and importance of redundancy, CI examples
* Case study - airplanes, Boeing 737 Max 8/9, Lion Air (Oct 2018), Ethiopian Air March 10, 2019), and including regulatory agency/regulations oversight/compliance/reporting

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).
* Integrated critical infrastructures versus competitive support service. (Contracting out and the evolution of certain CI’s business operations).

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)
* Analysis of 1000, 100, 50-year catastrophic events (ie Alberta relocation of 59 homes due to high risk of repeated flooding).

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

* Industrial Control Systems, Examination of the vulnerability of Supervisory Control and Data Acquisition (SCADA) systems
* ICS attack chain (Assantte paper)
* 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 as applicable the Geneva Convention).

Criminal, Terrorist and Domestic Extremists and Insider Threats to Critical Infrastructure

* Terrorist/extremists. Anti terrorism. Examination of tactics CI’s can use to deter terrorists, and manage the risks.

Trust, its importance to a nation’s Critical Infrastructure Protection Programs and their strategies

* Utilizing the theories related and inferred in the 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. Managing the Unpredictable

* Planning/predicting HIFL incidents. Risk/Costs of protecting vulnerable CI’s. (examination of the threat of geomagnetic disturbances on vulnerable CI’s and risk reduction measures and practices)
* 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
* 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., at home assignment/case study for in-class discussion)

**Assignments**

* **Assignment 1, 35% (1500-2500 word research paper)**

Analysis of a relatively current (in the news) incident/event/situation, directly involving or through cascading, affects critical infrastructure from the perspective of consequences (or potential) to societal or economic expectations, or in relation to regulations/laws. Due date October 22, 2019

* **Assignment 2, 65%** (formal research paper, 4000-5000 words excluding references, plus a 5-minute (informal) presentation during the last class (week 12) on your topic). 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). Assignment 2 is due December 13, 2019.
* **All assignment submissions shall be the student’s original works, not previously submitted in other courses, without my express prior consent.**
* **Late assignments unless previously approved (has to be a very good reason to request my approval for late submission) penalized 5% per day.**

**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 the two Marking Rubric’s that I use.

Core course (mandatory) reading material will be posted in advance on the Moodle website. Additional recommended resources include but are not limited to the following:

* Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure

By [Kevin Quigley](http://www.mqup.ca/quigley--kevin-contributor-119333.php), [Ben Bisset](http://www.mqup.ca/bisset--ben-contributor-119334.php) and [Bryan Mills](http://www.mqup.ca/mills--bryan-contributor-119335.php). McGill- Queens University Press (2017)

* “Critical Infrastructure, Homeland Security and Emergency Preparedness” by Radvanovsky, Robert & McDougall, Allan, , Second Edition CRC Press, Taylor & Francis Group (2010)
* Tallinn Manual, Cambridge University Press, April 2013. NATO Cooperative Cyber Defense Centre of Excellence
* “Normal Accidents, Living With High Risk Technologies”, by Charles Perrow, 1984 Basic Books.
* “The Black Swan, The Impact of the Highly Improbable”, by Nassim Nicholas Taleib, 2007 Random House
* “Critical Infrastructure, Understanding its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies”, by Macaulay, Tyson, CRC Press, Taylor & Francis Group (2009)

**Learning Objectives**

Students will:

* Develop an appreciation 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 operations (reliability).
* Develop an understanding of the complexities of CI, the inter-connectedness of dependencies and the cascading effects of a failing critical infrastructure on those mitigation strategies and enhancing resiliency through building in redundancy and rapidity, and also the importance of organizational learning.
* Develop a comprehensive understanding of effective risk management strategies and plans including the application of the numerous risk assessment methodologies and the challenges and importance of enhancing resiliency 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 various ‘actors’ that pose a threat to critical infrastructure owners and operators. This includes nation states perpetrating cyber 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 appreciation 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 a comprehensive understanding of government regulations and associated legislation for the protection of critical infrastructure.

Research and Scholarship

* Research the complexities and inter-connectedness of critical infrastructure from the perspective of critical dependencies and the cascading consequences of a natural or man made disaster identifying and or theorizing on vulnerabilities and unmitigated risks.
* Research cyber attacks differentiating the types of attacks, (cyber warfare, crime, espionage, vandalism), perpetrators (state and non-state actors), CI’s as targets, intended and unintended consequences in relation to CI’s being a target.
* Identify for the purpose of developing resiliency strategies and plans, complicating factors cascading from a disaster on those dependent on the critical services or goods.

Application of Knowledge

* Analysis of risk management practices including but not limited to enhancement of resiliency, identifying strengths, weaknesses and gaps based on actual incidents and theoretical disaster events.
* Analyze catastrophic critical infrastructure failures, interruptions, leading to the identification including quantification, of the social-economic impact /consequence.
* Student assignments should, and as applicable to the topic, reflect the core critical infrastructure protection elements: reliability, resiliency, redundancy, inter-dependencies, vulnerabilities, information sharing, risk management.

**RELEVANT UNIVERSITY REGULATIONS**

**Deferred Exams:** Deferred standing may be granted to students who are unable to write their final examination at the scheduled time or to submit their outstanding course work on the last day of classes. Details can be found at <http://myacademicrecord.students.yorku.ca/deferred-standing>

Any request for deferred standing on medical grounds must include an Attending Physician's Statement form; a “Doctor’s Note” will not be accepted.

DSA Form: <http://www.registrar.yorku.ca/pdf/deferred_standing_agreement.pdf>

Attending Physician's Statement form: <http://registrar.yorku.ca/pdf/attending-physicians-statement.pdf>

In order to apply for deferred standing, students must register at

<http://apps.eso.yorku.ca/apps/adms/deferredexams.nsf>

Followed by handing in a completed DSA form and supporting documentation directly to the main office of the School of Administrative Studies (282 Atkinson) and add your ticket number to the DSA form. The DSA and supporting documentation must be submitted no later than five (5) business days from the date of the exam. These requests will be considered on their merit and decisions will be made available by logging into the above mentioned link. No individualized communication will be sent by the School to the students (no letter or e-mails).

**Students with approved DSA will be able to write their deferred examination during the School's deferred examination period. No further extensions of deferred exams shall be granted. The format and covered content of the deferred examination may be different from that of the originally scheduled examination. The deferred exam may be closed book, cumulative and comprehensive and may include all subjects/topics of the textbook whether they have been covered in class or not. Any request for deferred standing on medical grounds must include an Attending Physician's Statement form; a “Doctor’s Note” will not be accepted.**

**Academic Honesty**: The Faculty of Liberal Arts and Professional Studies considers breaches of the Senate Policy on Academic Honesty to be serious matters. The Senate Policy on Academic Honesty is an affirmation and clarification for members of the University of the general obligation to maintain the highest standards of academic honesty. As a clear sense of academic honesty and responsibility is fundamental to good scholarship, the policy recognizes the general responsibility of all faculty members to foster acceptable standards of academic conduct and of the student to be mindful of and abide by such standards. Suspected breaches of academic honesty will be investigated and charges shall be laid if reasonable and probable grounds exist.

Students should review the York Academic Honesty policy for themselves at:

<http://www.yorku.ca/secretariat/policies/document.php?document=69>

Students might also wish to review the interactive on-line Tutorial for students on academic integrity, at:

<https://spark.library.yorku.ca/academic-integrity-what-is-academic-integrity/>

 **Grading Scheme and Feedback Policy:** The grading scheme (i.e. kinds and weights of assignments, essays, exams, etc.) shall be announced, and be available in writing, within the first two weeks of class, and, under normal circumstances, graded feedback worth at least 15% of the final grade for Fall, Winter or Summer Term, and 30% for ‘full year’ courses offered in the Fall/Winter Term be received by students in all courses prior to the final withdrawal date from a course without receiving a grade, with the following exceptions:

*Note: Under unusual and/or unforeseeable circumstances which disrupt the academic norm, instructors are expected to provide grading schemes and academic feedback in the spirit of these regulations, as soon as possible.* For more information on the Grading Scheme and Feedback Policy, please visit: <http://www.yorku.ca/univsec/policies/document.php?document=86>

 **In-Class Tests and Exams - the 20% Rule**: For all Undergraduate courses, except those which regularly meet on Friday evening or on a weekend, tests or exams worth more than 20% will not be held in the two weeks prior to the beginning of the official examination period. For further information on the 20% Rule, please visit: <http://secretariat-policies.info.yorku.ca/policies/limits-on-the-worth-of-examinations-in-the-final-classes-of-a-term-policy/>

  **Reappraisals**: Students may, with sufficient academic grounds, request that a final grade in a course be reappraised (which may mean the review of specific pieces of tangible work). Non-academic grounds are not relevant for grade reappraisals; in such cases, students are advised to petition to their home Faculty. Students are normally expected to first contact the course director to discuss the grade received and to request that their tangible work be reviewed. Tangible work may include written, graphic, digitized, modeled, video recording or audio recording formats, but not oral work. Students need to be aware that a request for a grade reappraisal may result in the original grade being raised, lowered or confirmed. For reappraisal procedures and information, please visit the Office of the Registrar site at: <http://myacademicrecord.students.yorku.ca/grade-reappraisal-policy>

 **Accommodation Procedures:** LA&PS students who have experienced a misfortune or who are too ill to attend the final examination in an ADMS course should not attempt to do so; they must pursue deferred standing. Other students should contact their home Faculty for information. For further information, please visit: <http://ds.info.yorku.ca/academic-support-accomodations/>

**Religious Accommodation**: York University is committed to respecting the religious beliefs and practices of all members of the community, and making accommodations for observances of special significance to adherents. For more information on religious accommodation, please visit:
<https://w2prod.sis.yorku.ca/Apps/WebObjects/cdm.woa/wa/regobs>

**Academic Accommodation for Students with Disabilities (Senate Policy)**

The nature and extent of accommodations shall be consistent with and supportive of the integrity of the curriculum and of the academic standards of programs or courses. Provided that students have given sufficient notice about their accommodation needs, instructors shall take reasonable steps to accommodate these needs in a manner consistent with the guidelines established hereunder. For more information, please visit the Counselling and Disability Services website at <http://www.yorku.ca/dshub/>

York’s disabilities offices and the Registrar’s Office work in partnership to support alternate exam and test accommodation services for students with disabilities at the Keele campus. For more information on alternate exams and tests please visit <http://www.yorku.ca/altexams/>

Please alert the Course Director as soon as possible should you require special accommodations.