April 30, 2017

5710 – Critical Infrastructure Protection – Fall Term 2017-18

Course Director, Adjunct Professor – David Baumken, dbaumken@yorku.ca

Students of the Critical Infrastructure Protection Course will explore threats, vulnerabilities and risks to critical infrastructure from the perspective of ensuring for reliability through appropriate protection and resiliency measures, 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 refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security and economic well being 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 Rubric's that I use).
- Overview of the 12 lectures, weekly required readings, research and the course Moodle site.
- Core CIP elements and concepts – Reliability, Resiliency, Inter-dependencies, Vulnerabilities, Information Sharing, Risk Management
- Definition of critical infrastructure. CI Characteristics – complex processes, tightly coupled with significant dependency on other CI's (inter-dependencies)
- Control/ownership of critical infrastructure (private sector versus government controlled)

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

- Examination of the 10 Canadian sectors and the relationships with Provincial CI Programs (Ontario 9), other Nations including the United States Sectors and their inter-relationship.
- Mandate of Canadian Federal Government's Sector Networks.
- Ministerial responsibilities for CI and oversight on private sector CI owners and operators
- Regulatory standards and guidelines for the protection (reliability) of critical infrastructure. Private sector CI owners and operators (practices) due diligence protecting assets, ensuring for reliability and resiliency.
- Newly designated Critical Infrastructure - US elections
  https://www.theatlantic.com/technology/archive/2017/01/why-the-government-classified-elections-as-critical-infrastructure/513122/?utm_source=atltw

Legislation for the Protection and Access of Information as it relates to CI's.

- Access to Information, Emergency Management Act, National CI Strategy and Action Plan, Cyber Security Strategy, Canada – United States Action Plan for Critical Infrastructure
- 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 Infrastructure Protection (including reliability, security and risk management)
Regulations, legislation/laws

- In-depth examination of certain 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 recent events (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)
- Highly Reliable Organizations (HRO), definition, attributes and examples

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

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).
- 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,

Credible 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.

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.

- Case Study, 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
- 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.

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).

Trust, its importance to Nations 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

- Planning/predicting HIFL incidents. Risk/Costs of protecting vulnerable CI's.
- Risks, Cost and the Challenges of Protecting CI's from all Hazards.
- 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 - İs 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% (2000-2500 word research paper)**
  Critical analysis of a relatively current (in the news) incident/event/situation, directly involving or through cascading effect a critical infrastructure from the perspective of consequences (or potential) to societal or economic expectations (trust), or in relation to regulations/laws. Due date October 24, 2017

- **Assignment 2, 65%** (formal academic research paper, 5000-6000 words excluding references, plus a 5-10 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 28, 2017.

- **All assignment submissions shall be the students 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) this style 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 on the Moodle web site. Additional recommended resources include but are not limited to the following;

- "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
- "Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland", Anthony H. Cordesman (Author) , (Author), Justin G. Cordesman (Author)
- "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation", Ted G. Lewis, Wiley Press
- "Critical Infrastructure Protection III: Third IFIP WG 11.10 International Conference", Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers, by Charles Palmer (Editor), Sujeet Shenoi (Editor)
- "21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention", by Randall I. Atlas (Author)
- "Critical Infrastructure Protection in Homeland Security", Published Online: 30 Mar 2006, Editor(s): Lewis, Author(s): Professor Ted G. Lewis, Print ISBN: 9780471786283 Online ISBN: 9780471789543
- "Critical Infrastructure, Understanding its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies", by Macaulay, Tyson, CRC Press, Taylor & Francis Group (2009)
- "Securing 'the Homeland': Critical Infrastructure, Risk and (in)Security", Edited by Myriam Dunn Cavelty & Kristian Søby Kristensen, Routledge, 2007
- "The Art of Deception" by Kevin D. Mitnick. (William L Simon and Steven Woznick 2003)

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 organization 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 war fare, 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