UNIVERSITY OF TORONTO

FACULTY OF APPLIED SCIENCE AND ENGINEERING

ELITE Master's Program

APS1025H1F2018 Infrastructure Protection Planning

Course Outline

Introduction

Our world is changing. The trends in technology have fundamentally changed the way we live work and play. This causes a steady concentration of value, such that an extreme event can result in far greater impact to operations and businesses than previously. Infrastructure defines the world we live in and encompasses the natural, built and virtual domains. We need to think of infrastructure as systems that fulfil a service to our operations, whether municipal, corporate, national or even international. Some infrastructure enables the essential functions that define our ability to operate, live and thrive. These are known as Critical Infrastructure and it is vital to protect the purpose that they exist to fulfil. Critical Infrastructure Protection (CIP) is not about protecting assets, though this is part of it. It is about protecting capability – life, property and economy. Yet, in this rapidly changing world, so many of the familiar protection processes and procedures are based on assumptions that are less and less valid. We need to be able to work from first principles if we are to effectively protect our infrastructure now and into an uncertain future.

Extreme events come in many forms, from natural to human-caused. However, they do not happen in isolation. Flooding can cause an extended power failure. Under the right conditions, this can make looting more likely. In fact, we can't really separate threats and hazards into convenient single risk events. Instead, we must consider a broad spectrum of hazards, identifying the changing likelihood and severity of coincident and correlated hazards to the threat that we are particularly interested in. This is known as a hazard profile and one of the key products of all-hazards analysis that we must investigate when considering how to protect infrastructure.

Join us as we explore the first principles of CIP, the risk management processes that provide the structure and auditable processes that we use, and how we determine how to identify the right tools for a given operation and situation. This course builds on many of the same principles and concepts taught in APS1024 Infrastructure Resilience Planning, but that course is by no means a pre-requisite. We will build our understanding, drawing upon the existing experiences and perspectives of the class body, apply these protection principles and concepts, and discuss how we might use them in practice. The course is practice-biased, with a walk-through/talk-through followed by real protection consulting projects for real clients in real time. Students can add these projects to their experience portfolio. As is common in practice, so in class and after the first day you will form into project teams for the remainder of the course.

When you complete this course you will be able to direct CIP planning in engineering projects, conduct the analysis and develop and present strategy proposals. This course is recognized internationally by the Register of Security Engineers and Specialists.

Course Designation

APS1025 Infrastructure Protection Planning, starting Saturday, 27 October 2018. The course will be full days, from 09:00 to 17:00 with 30mins for lunch. It will run over four Saturdays in MY350, a TEAL classroom. A foundation course of the CRCI that is recognised by the international Register of Security Engineers and Specialists; http://www.crci.utoronto.ca/education/academic/infrastructure-courses.

Calendar:

27 Oct 18 Course introductions and administration
We begin with a brief exploration of strategy, the role of infrastructure and the purpose of protection, focussing on the need for protection and resilience to be in balance in order to deliver effective protection of the operation that the infrastructure facilitates. We will then explore the evolution of protection through a review of poliorcetics to modern day CIP, leading to a series of principles and 'rules of thumb'. We then analyse the physical environment and broader risk context. We finish the day exploring the concept and practice of security integration, drawing together the different aspects discussed through the day.
Three references will be posted on Quercus for familiarisation before the next lecture. These references will provide the means to analyse site protection and security integration.
Project Each syndicate will then be assigned a real client with a real-time security integration issue. The syndicates are to contact their client to conduct interviews and surveys and develop a concept solution based upon the sound application of first principles.

3 Nov 18 Picking up from the previous day's discussion and the assigned reading, we will investigate the site survey and the performance criteria we require of the different security systems.
Site Survey The class will break into syndicates for a tutored walk-through / talk-through of a site with particular security integration issues. The problems will be analysed as syndicates and solutions discussed in open forum.

10 Nov 18 **Tutorials** Each syndicate will have the opportunity to arrange a tutorial with the professor to discuss their client's security issues and the developing concept for addressing the specific identified security requirement.

17 Nov 18 **Group submissions of projects and presentations** Each syndicate will present its project concept solution to the clients' representatives in class.
Examination.

Evaluation

One project, representing 60% of the total course marks. This is a practical survey and research project that requires a first principles approach and critical assessment of the available information. Marks will be awarded separately for the project report (60%), decision brief (20%) and presentation (20%).

There is also a two-hour oral examination comprising 3 assigned questions to each project team. Each project syndicate will be given a question that they will have 20 minutes to prepare an answer, which will be presented and justified before the whole class. Each will be critiqued by the instructing staff. This is repeated until each syndicate has answered all three questions. This form of examination reflects the actual concept development in practice and assess the ability of each syndicate member to grasp the core principles and concepts and apply them to a given challenge. With the benefit of immediate feedback and learning from other syndicate presentations, this examination process is also very much part of the learning process. The final exam represents 40% of the total course marks. The examination will be closed book.

Materials

You are expected to read "After the Flood: Exploring Operational Resilience" by Hay. Written for the APS1024 Infrastructure Resilience Planning course, it explains and references all the core principles and concepts used for a systems level understanding. You should also review Nadel's "Building Security," which you may wish to rent from the UofT Bookstore. A useful book to also read is "The Edge of Disaster" by Flynn, also at the UofT Bookstore.

The three further references will be distributed in PDF on Quercus on the first day of the course. "After the Flood" is also available from Ben McNally books on Bay Street.

Address course questions and (correspondence) course work submissions to me at alec.hay@utoronto.ca