École de criminologie **Automne 2021**
Université de Montréal

Plan de cours **modifié**

CRI 6721 – Protections d'infrastructures complexes

Jeudi – 16h-19h
Salle C-4141 – Pavillon Lionel-Groulx

Arnaud Palisson
arnaud.palisson@umontreal.ca

Descripteur du cours

Menaces et vulnérabilités particulières des installations de grande envergure. Difficultés liées aux grands espaces, aux organisations complexes et aux populations importantes.

Objectifs du cours

Le cours s'adresse aux étudiants à la maitrise[1] en criminologie (option Sécurité intérieure) et au DESS en sécurité intérieure.

Les infrastructures complexes (IC) peuvent prendre diverses formes. Il peut s'agir d'installations sur un territoire étendu hébergeant nombre d'organismes variés, de locaux accueillant du public en grand nombre, ou encore d'infrastructures essentielles au fonctionnement d'un État et au bien-être de sa population.

Mais elles ont toutes un point commun : elles sont indissociables de nos sociétés modernes. À ce titre, elles constituent des cibles d'intérêt pour des organisations et des individus malintentionnés désireux de troubler la paix publique et de menacer la sécurité intérieure. Protéger les infrastructures complexes constitue par conséquent un défi que doivent relever conjointement les entreprises chargées de les administrer et les institutions garantes de la sécurité publique.

Objectifs généraux

À la fin de la session, l'étudiant aura intégré les idées fondamentales propres à la stratégie de protection des infrastructures complexes, dans une optique de gestion des risques de sureté.

Objectifs spécifiques

Par ailleurs, l'étudiant sera capable de poser un diagnostic préliminaire de sureté et de proposer des mesures de sécurisation d'une infrastructure complexe. Il sera à même d'évaluer l'efficacité des pratiques traditionnelles de protection et de déterminer si elles peuvent être améliorées, complétées, voire remplacées par de nouvelles méthodes de sureté.

1 Ce document est rédigé conformément aux règles de la nouvelle orthographe.

Approches pédagogiques

Compte tenu de l'ampleur du sujet abordé, ce cours ne prétend nullement à l'exhaustivité. Il choisit de se concentrer sur les éléments essentiels de la matière et de susciter une réflexion sur les meilleures façons de protéger les infrastructures complexes – plutôt que de simplement énoncer les façons de faire actuellement en place. Les étudiants seront encouragés à développer une approche critique, notamment en ce qui concerne les standards et bonnes pratiques en usage dans ce secteur d'activités.

La majorité des séances prendront la forme de séminaires basés notamment sur les exposés de l'enseignant, ainsi que sur les lectures et visionnements indiqués aux étudiants. Ceux-ci devront être familiarisés avec la langue anglaise, en raison de l'abondance et de la pertinence de la littérature anglo-saxonne dans notre champ d'étude.

Certaines séances intégreront des travaux en sous-groupes et des études de cas. D'autres enfin comprendront des jeux pédagogiques, développés ou adaptés par l'enseignant dans le but d'illustrer des concepts fondamentaux, de poser clairement certains enjeux essentiels et de nourrir la réflexion quant à une protection adéquate des infrastructures complexes.

Modalités d'évaluation des apprentissages

Outils d'évaluation

Outils d'évaluation	Pondération	Échéance
1. Dissertation intratrimestrielle - Analyse de risque *Travail individuel* Identification et estimation des différents éléments de risque posés par le scénario de 2 films de fiction se déroulant en contexte d'IC. Critères de correction : cohérence dans l'application des méthodes d'estimation, degré d'analyse, qualité de l'expression écrite.	30 %	21 oct.
2. Présentation orale - Jeu pédagogique *Travail collectif* (2 étudiants) – *Évaluation en collectif* Présentation orale d'une fiche de menace préparée à l'avance, dans le cadre d'un jeu pédagogique consacré à la gestion des risques d'une IC fictive, et opposant deux équipes. Critères de correction : pertinence et niveau d'analyse de la menace fictive, fluidité de la présentation orale.	20 %	28 oct.
3. Dissertation finale *Travail collectif – Évaluation en collectif + individuel* Sujet librement choisi en lien avec une problématique propre à la protection d'infrastructures complexes (telles que transport de passagers, d'énergie ou de fret (routier, aérien, maritime), infrastructures pétrolières, barrages hydroélectriques, sites nucléaires, hôpitaux, centres commerciaux, enceintes sportives,... Critères de correction : degré d'analyse, pertinence des sources bibliographiques, originalité dans l'approche du sujet, qualité de l'expression écrite.	50 %	9 déc.

Présentation des évaluations

Les travaux rédigés (évaluations 2 et 3) doivent être remis en version électronique, au format **PDF** ; dimensions 8 ½ x 11; marges à 2,5 cm. **max.** ; police *Times New Roman*, *Calibri* ou similaire, à 11 points ; texte à 1 ½ interligne.

Barème de notation

Grille de conversion des pourcentages			
Points	Note littérale	Valeur	Pourcentage
4,3	A+	Excellent	90
4	A		85
3,7	A–		80
3,3	B+	Bon	77
3	B		73
2,7	B–		70
2,3	C+	Passable	65
2	C		60
1,7	C–	Échec	57
1,3	D+		54
1	D		50
0	E		– de 50

Déroulement du cours

Date	Cours	Éléments de contenu	Lectures / exercices préparatoires
2 sept.	**1**	**Présentation du plan, de l'orientation et des objectifs** • Définitions et délimitation du contenu du cours • Présentation de l'approche pédagogique et des évaluations • Pourquoi une approche de gestion des risques ?	Graham, 2011 Roche, 2010 Schneier, 2003, 2008
9 sept.	**2**	**Introduction à la gestion des risques de sureté** • Concept de gestion des risques de sureté • Modèles de gestion des risques	Tanquintic-Misa, 2014 Torbey, 2017 Tran, 2014 Frankenheimer 1964
16 sept.	**3**	**Présentation d'une méthode d'appréciation des risques** • Présentation globale • Présentation des éléments de risque sous le contrôle de l'IC : actif, vulnérabilité, impact	Frankenheimer, 1964
23 sept.	**4**	**Actifs critiques et vulnérabilités inhérentes aux IC** • Criticité des actifs : typologie et évaluation • Deux exemples : périmètres de protection et infrastructures ouvertes au public	Association canadienne de l'électricité, 2015

30 sept.	**5**	**Les éléments du risque de sureté hors du contrôle de l'IC : la "Menace" au sens large** • Spécificité de la menace dans les risques de sureté • Typologie des menaces • Sources et modes d'évaluation	Civil Aviation Authority Israel, 2014 De Cillis et al., 2013
7 oct.	**6**	**La menace terroriste en contexte d'IC** • Concept, définitions et typologies du terrorisme • Leur utilité pour évaluer la menace terroriste sur les IC	Aboudjaffar, 2016 Stewart et Mueller, 2014
14 oct.	**7**	**Les partenaires de sureté** • Typologie des partenaires • Leur intégration dans la sureté des IC	Brandes, 2011, 2013 Eychenne, 2016 Merchet, 2016
21 oct.	**Pas de cours (semaine de relâche)**		
28 oct.	**8**	**Évaluation – Jeu pédagogique** *Synthèse de la première partie du cours* Appréciation (et traitement sommaire) des risques de sureté, dans le cadre du parc de la série télé *Westworld*. Le jeu opposera deux équipes : l'une chargée d'assurer la sureté des lieux, l'autre de la mettre à l'épreuve.	Nolan et Joy, 2016 Palisson, 2018
4 nov.	**9**	**Les techniques traditionnelles de sureté** • Sureté aléatoire • Vidéosurveillance • Enquêtes pré-embauche • Palpations et fouilles • Adéquation de la technologie	Bergman, 2011 Schneier, 2005b Stewart, 2013
11 nov.	**10**	**Évaluation comportementale de la menace** • Évaluation comportementale et profilage racial • Origines et principes de l'évaluation comportementale • Illustrations	Brandes, 2013 Kelly, 2009 Ormerod et Dando, 2015 Schneier, 2012 Weinberger, 2010
18 nov.	**11**	**Tactiques défensives** • Spécificités quant à la protection des IC • Adéquation des matériels et techniques • Illustrations	Danaher, 2001 ÉNPQ, 2013
25 nov.	**12**	**Cyber-risque opérationnel** • Enjeux • Niveaux de risque • Modes opératoires spécifiques	Brito et Watkins, 2011 Grant, 2017 Odlyzko, 2019 Schneier, 2003, 2005a
2 déc.	**13**	**Cyber-risque informationnel** • Les trois domaines de la sécurité de l'information • Enjeux spécifiques aux IC • Protection tout au long du processus de l'information	Ensey, 2017 Spitzner, 2016

Lectures obligatoires et références bibliographiques

Une bibliographie plus complète est disponible sur le site StudiUM du cours.

Articles de revue et monographies

Association canadienne de l'électricité (2015). Les répercussions du vol de cuivre commis dans les infrastructures électriques canadiennes : danger, coût élevé et menace pour la fiabilité. Repéré à https://electricity.ca/wp-content/uploads/2017/05/Voldecuivre.pdf

Brito, J. et Watkins, T. (2011). Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy, dans *Harvard Law School National Security Journal*, 3(39). Repéré à http://mercatus.org/sites/default/files/publication/Loving-Cyber-Bomb-Brito-Watkins.pdf

Danaher, J. (2001). dans Gracie, R., Gracie, R. (2014). *Jiu-jitsu brésilien – Théorie et technique*. 2e éd., Noisy-sur-École, France : Budo éditions, 22-28. Repéré à http://bit.ly/2yPXlko

De Cillis, F., De Maggio, M. C., Pragliola, C. et Setola, R. (2013). Analysis of Criminal and Terrorist Related Episodes in Railway Infrastructure Scenarios. *Journal of Homeland Security & Emergency Management*, 10(2), 1-30, Repéré à : https://bit.ly/3alh1Pa

École nationale de police du Québec. Centre de savoirs disciplinaires (2013). *Modèle national de l'emploi de la force: document explicatif*. Nicolet, École nationale de police du Québec. Repéré à https://bit.ly/3izEw9N

Graham, A. (2011). Canada's Critical Infrastructure: When is Safe Enough Safe Enough?. MacDonald-Laurier Institute. Repéré à http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

Odlyzko, A. (2019). Cybersecurity is not very important. *Ubiquity*, juin 2019, 1-23. doi: 10.1145/3333611. Repéré à http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf

Ormerod, T. C. et Dando, C. (2015). Finding a Needle in a Haystack: Toward a Psychologically Informed Method for Aviation Security Screening. *Journal of Experimental Psychology: General*, 144(1), 76-84. Repéré à http://www.apa.org/pubs/journals/releases/xge-0000030.pdf

Roche, J.-J. (2010). Prospective sécuritaire et anticipation romanesque ; Romanciers 3 – Experts 0. *Les Cahiers de la Sécurité*, n°13. Repéré à https://www.geostrategia.fr/prospective-securitaire-et-anticipation-romanesque-romanciers-3-experts-0/

Stewart, M. G. et Mueller, J. (2014). Cost-benefit analysis of airport security: Are airports too safe?. *Journal of Air Transport Management*, 35, 19–28. Repéré à http://politicalscience.osu.edu/faculty/jmueller/JATMfin.pdf

Weinberger, S. (2010, mai). Intent to deceive?. *Nature*, 465(27), 412-415. doi:10.1038/465412a. Repéré à http://www.nature.com/news/2010/100526/full/465412a.html

Webographie

Aboudjaffar (2016, 22 septembre). « When I'm in the shower/I'm afraid to wash my hair (…) » [Billet de blogue]. Repéré à http://aboudjaffar.blog.lemonde.fr/2016/09/22/mook/

Bergman, R. (2011, janvier). *The Dubai Job*. GQ. Repéré à https://www.gq.com/story/the-dubai-job-mossad-assassination-hamas

Brandes, A. (2011, 26 juillet), Good security without intel? [Billet de blogue]. Repéré à https://chameleonassociates.com/good-security-system/

Brandes, A. (2012, 29 mai), Peach pie [Billet de blogue]. Repéré à https://chameleonassociates.com/gun-threat/

Brandes, A. (2013, 6 aout), The prime directive [Billet de blogue]. Repéré à https://chameleonassociates.com/security-services/

Civil Aviation Authority Israel (2014, 23 juillet). Declaration regarding the safe operation of Ben-Gurion Airport during Operation "Protective Edge" in Gaza. Repéré à : http://bit.ly/2ThHhRV

Ensey, C. (2017, 4 janvier). Ransomware Has Evolved, And Its Name Is Doxware. Repéré à https://www.darkreading.com/attacks-breaches/ransomware-has-evolved-and-its-name-is-doxware/a/d-id/1327767

Eychenne, A. (2016, 7 septembre). *Agents de sécurité : ces forçats sous-payés et déconsidérés des dispositifs anti-terroristes*. Basta!. Repéré à https://www.bastamag.net/Agents-de-securite-les-forcats-sous-payes-et-deconsideres-de-la-dissuasion-anti

Grant, R. (2017, 5 octobre). *The Disturbing Rise of Cyberattacks Against Abortion Clinics*. Wired. Repéré à https://www.wired.com/story/cyberattacks-against-abortion-clinics/

Kelly, C. (2009, 30 décembre). *The 'Israelification' of airports: High security, little bother*. The Toronto Star. Repéré à https://www.thestar.com/news/world/2009/12/30/the_israelification_of_airports_high_security_little_bother.html

Marietta Police Department (2021, février). *BJJ Training Program – Data Summary*, Repéré à https://bit.ly/3lVOlE8

Merchet, J.-D. (2016, 17 juin). *Terrorisme : Israël, ce pays où l'armée n'est pas déployée dans les rues.* L'Opinion. Repéré à https://www.lopinion.fr/blog/secret-defense/terrorisme-israel-pays-l-armee-n-est-pas-deployee-dans-rues-104979

Palisson, A. (2013a, 27 février). Protection du périmètre extérieur des aéroports – Un paradoxe [Billet de blogue]. Repéré à https://rapports-minoritaires.net/2013/protection-du-perimetre-des-aeroports/

Richardson, B. (2010, 30 octobre). The Danger of Airport Pat-Downs. Repéré à https://www.thedailybeast.com/articles/2010/10/30/airport-pat-downs-the-new-tsa-rules-are-a-mistake.html

Schneier, B. (2003, 15 juin). The Risks of Cyberterrorism. Repéré à https://www.schneier.com/crypto-gram/archives/2003/0615.html#1

Schneier, B. (2004, 15 avril). National Security Consumers. Repéré à https://www.schneier.com/crypto-gram/archives/2004/0515.html#9

Schneier, B. (2005a, janvier). Cyberwar. Repéré à https://www.schneier.com/crypto-gram/archives/2005/0115.html#10

Schneier, B. (2005b, juillet). Searching Bags in Subways. [Billet de blogue]. Repéré à https://www.schneier.com/blog/archives/2005/07/searching_bags.html

Schneier, B. (2008, 3 avril). *The difference between feeling and reality in security*. Wired. Repéré à https://www.wired.com/2008/04/securitymatters-0403/

Schneier, B. (2012, 9 mai). *The Trouble with Airport Profiling*. Forbes. Repéré à https://www.forbes.com/sites/bruceschneier/2012/05/09/the-trouble-with-airport-profiling/

Spitzner, L. (2016, 13 juillet). Why The Spectacular Growth in Ransomware?. [Billet de blogue]. Repéré à https://www.sans.org/security-awareness-training/blog/why-spectacular-growth-ransomware

Stewart, S. (2013, 4 juillet). The Problem with Background Investigations. [Billet de blogue]. Repéré à https://eliteeservices.blogspot.com/2013/07/stratfor-problems-with-background.html

Tanquintic-Misa, E. (2014, 25 mars). *Security at Brisbane International Airport Breached by a Pair of Scissors, 2,000 Passengers Affected*. International Business Times. Repéré à http://www.ibtimes.com.au/security-brisbane-international-airport-breached-pair-scissors-2000-passengers-affected-1335790

Tran, C. (2014, 27 septembre). *Hundreds of passengers evacuated at Sydney Airport after man forgot to go through security screening because he was concentrating on his iPad*. The Daily Mail. Repéré à http://www.dailymail.co.uk/news/article-2771629/Security-looking-man-Sydney-Airport-walked-terminal-without-passing-security-screening.html

Filmographie

Frankenheimer, J. (réalisateur). (1964). *The Train* [Film cinématographique]. Beverly Hills, Californie : United Artists.

Frankenheimer, J. (réalisateur). (1977). *Black Sunday* [Film cinématographique].Hollywood, Californie : Paramount.

Nolan, J. et Joy, L. (auteurs). (2016-2018). *Westworld* [Série télévisée]. New-York, NY : Home Box Office.

Ludographie

Palisson, A. (2013b). *Démasquez le Joker* [Jeu pédagogique]. Montréal, Québec.

Palisson, A. (2013c). *Terrori5^{3}me* [Jeu pédagogique]. Montréal, Québec.

Palisson, A. (2016). *Gare centrale* [Jeu pédagogique]. Montréal, Québec.

Palisson, A. (2018). *Westworld, 2048 – Livret des règles* [Jeu pédagogique]. Montréal, Québec.

Torbey, S. (2010-2017). *Onirim* [Jeu de cartes]. Mahopac, New York : Z-Man Games – [Jeu vidéo]. Roseville, Minnesota : Asmodée Digital. Disponible en ligne : https://www.asmodee-digital.com/fr/onirim/ (Android/iOS/Windows/Mac/Linux)

Renseignements utiles

Site web de l'École de criminologie : www.crim.umontreal.ca

Nous vous invitons à consulter le guide étudiant de votre programme :
https://crim.umontreal.ca/ressources-services/ressources-et-formulaires/

Captation visuelle ou sonore des cours

Il est interdit de faire une captation audio ou vidéo du cours, en tout ou en partie, et par quelque moyen que ce soit, sans le consentement écrit du chargé de cours. L'autorisation d'enregistrement n'entraine d'aucune façon la permission de reproduction ou de diffusion sur les médias sociaux ou ailleurs des contenus captés. Ces dernières sont interdites sous toutes formes et en tout temps.

L'usage de tout document déposé sur *StudiUM* pour chaque cours est assujetti à l'engagement de chaque étudiant à respecter la propriété intellectuelle et le droit à l'image.

Règlement pédagogique des études supérieures et postdoctorales

Nous vous invitons aussi à consulter le règlement pédagogique :
https://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/reglement-pedagogique-des-etudes-superieures-et-postdoctorales/#chapitre-i-definitions

Révision de l'évaluation (article 9.5)

Au plus tard 21 jours après l'émission du relevé de notes, l'étudiant qui, après vérification d'une modalité d'évaluation a des raisons sérieuses de croire qu'une erreur a été commise à son endroit peut demander la révision de cette modalité en adressant à cette fin une demande écrite et motivée au doyen ou à l'autorité compétente de la faculté responsable du programme auquel il est inscrit. Si le cours relève d'une autre faculté, la demande est acheminée au doyen ou à l'autorité compétente de la faculté responsable du cours.

a) Demande recevable

Si la demande est recevable, le doyen ou l'autorité compétente en informe l'étudiant par écrit et invite immédiatement le professeur à réviser l'évaluation dans un délai qu'il détermine, mais ne dépassant pas 21 jours. La note peut être maintenue, diminuée ou majorée. Le relevé de notes est ajusté en conséquence.

b) Demande non recevable

Si la demande n'est pas recevable, le doyen ou l'autorité compétente en informe l'étudiant par écrit avec motif à l'appui dans les 28 jours suivant la réception de la demande.

Si la décision à cette demande demeure insatisfaisante il existe un processus de demande de révision exceptionnelle (consulter le règlement pédagogique pour plus d'informations).

Retard dans la remise des travaux (article 9.7b)

Les pénalités de retard sont applicables à toutes les évaluations prévues dans ce cours. Toute demande pour reporter la remise d'un travail doit être présentée à la responsable du programme. Les travaux remis en retard sans motif valable seront pénalisés de 10 % le premier jour et de 5 % chacun des quatre jours suivants. Le délai ne peut dépasser cinq jours.

Justification d'une absence (article 9.9)

L'étudiant doit motiver, par écrit, toute absence à une évaluation ou à un cours faisant l'objet d'une évaluation continue dès qu'il est en mesure de constater qu'il ne pourra être présent à une évaluation et fournir les pièces justificatives. Dans les cas de force majeure, il doit le faire le plus rapidement possible par téléphone ou courriel et fournir les pièces justificatives dans les cinq jours ouvrés suivant l'absence.

Le doyen ou l'autorité compétente détermine si le motif est acceptable en conformité des règles, politiques et normes applicables à l'Université.

Les pièces justificatives doivent être dûment datées et signées. De plus, le certificat médical doit préciser les activités auxquelles l'état de santé interdit de participer, la date et la durée de l'absence, il doit également permettre l'identification du médecin.

À noter que l'étudiant doit remplir le formulaire et le remettre au responsable ou au TGDE de son programme :
https://safire.umontreal.ca/public/FAS/safire/Documents/Avis_absence_examen_form-19-28mai-2020.pdf

Plagiat et fraude (article 9.10)

La politique sur le plagiat et la fraude sont applicables à toutes les évaluations prévues dans ce cours. Tous les étudiants sont invités à consulter le site web http://www.integrite.umontreal.ca/ et à prendre connaissance du Règlement disciplinaire sur le plagiat ou la fraude concernant les étudiants. Plagier peut entrainer un échec, la suspension ou le renvoi de l'Université.

StudiUM

Un site Internet du cours sera mis à disposition à partir du réseau interne de l'Université, *StudiUM*. Les étudiants auront accès illimité au site durant toute la session, et ce depuis le réseau interne de l'Université comme depuis leurs propres connexions Internet.

Le chargé de cours assurera un suivi constant du contenu du site, ce qui permettra notamment aux étudiants de recevoir régulièrement des informations diverses concernant le cours, recevoir des documents en ligne, être tenus au courant des conférences, se renseigner sur les consignes du travail de session, etc.

Pour avoir accès au site, l'étudiant doit être dûment inscrit à l'Université et être détenteur d'un UNIP, ce qui lui donnera accès à son portail *UdeM*.