École de criminologie **Été 2026**
Université de Montréal

Plan de cours

CRI 3950L – Criminalité informatique

Jeudi – 08h30 - 11h30 et 12h30 - 15h30
Campus Laval

Benoit Gagnon
benoit.gagnon@me.com

Sur rendez-vous

Descripteur du cours

Présentation des principales formes de criminalité informatique. Usages problématiques et criminels d'Internet. Législation et intervention policière dans le cyberespace. Impacts des nouvelles technologies sur le milieu criminel.

Objectifs du cours

Ce cours vise à offrir aux étudiants une vue d'ensemble du monde de la criminalité informatique, de ses dynamiques et des défis de gestion qui y sont associés. Les étudiants seront amenés à explorer diverses problématiques liées aux cybercrimes, tant dans une perspective théorique que pratique en matière de cybersécurité et de gestion des incidents. Le cours permettra aux étudiants de mieux comprendre les forces en jeu dans les processus de sécurité, tout en identifiant les vulnérabilités et les limites des approches actuelles. De plus, les étudiants développeront une perspective critique sur les enjeux entourant la prévention, la détection et la réponse aux cybermenaces. Tout au long de la session, les étudiants seront encouragés à affiner leur sens de l'analyse critique, notamment en ce qui concerne les approches académiques et pratiques développées autour de la criminalité informatique.

Approches pédagogiques

Le cours consiste en une série de cours magistraux axés sur différentes problématiques présentes dans le milieu de la criminalité informatique. Le travail demandé aux étudiants sera dans la logique traditionnelle du 3-3-3 par semaine, soit :

- trois heures de cours;
- trois heures de lectures;
- trois heures d'études diverses.

Ces trois variables peuvent bouger d'une semaine à l'autre, mais le total devrait être d'environ neuf heures. Le travail sera soutenu tout au long de la session, ce qui signifie que les étudiants devront déployer des efforts continus chaque semaine.

Les cours plongeront les étudiants dans des réflexions sur les défis en lien avec la cybercriminalité et en lien avec la sécurité de l'information. Ainsi, les étudiants seront non

seulement mis en contact avec la littérature entourant le domaine, mais ils devront également toucher à la littérature entourant les technologies. Les étudiants suivant ce cours sont fortement suggérés d'avoir une connaissance suffisante de l'anglais, car une bonne proportion de la littérature dans le milieu de la sécurité et de la gestion est anglophone.

Modalités d'évaluation des apprentissages

Outils d'évaluation

Outil d'évaluation	Individuelle ou en équipe?	Pondération	Échéance
1. Exercice du Mitre ATT&CK	En équipe	10 %	28 mai PM
2. Examen	Individuelle	50 %	4 juin PM
3. Rapport de simulation	En équipe	30 %	26 juin
4. Cahier de simulation	En équipe	10 %	26 juin

Présentation des travaux

1. *Exercice du Mitre ATT&CK* (En équipe) - 10%.

- L'objectif de cet exercice est d'initier les étudiants à la plateforme et à la méthodologie d'analyse du Mitre ATT&CK en utilisant un cas distribué en classe.
- Une courte présentation sur le cadre d'analyse sera effectué au début de la séance.

2. *Examen* (individuel) - 50%

- L'examen permettra de vérifier si les élèves ont bien compris les concepts enseignés et s'ils sont capables de les appliquer dans une situation réelle.
- L'examen sera constitué d'un cas d'analyse en criminalité informatique. L'étudiant se verra distribuer un cas au début de l'examen. Ce cas contiendra différent éléments de preuves techniques et non techniques. L'étudiant devra les lire, les comprendre, les assembler et faire son rapport d'enquête.
- Le rapport devra comprendre cinq sections (les critères de correction sont sur StudiUM). Le rapport fera appels à des connaissances criminologiques générales, mais également des
- L'examen sera à livre ouvert. Il est permis d'utiliser l'IA, mais les sections ou l'IA a été utilisé devra être mentionné dans le rapport d'enquête.
- L'étudiant bénéficiera de 2h50 pour faire son rapport.

3. *Rapport de simulation* (en équipe - déposé sur StudiUM en format PDF) – 30 %

La simulation est un travail d'équipe qui impliquera la gestion d'une crise et une recherche documentaire. Les étudiants devront produire un rapport expliquant les grandes lignes de l'intérêt national de leur État. Ce document servira de guide pour la conduite de la simulation. Les étudiants devront également produire un rapport chronologique de leurs processus décisionnel durant la simulations. Un gabarit fournira les grandes lignes de ce qui est demandé dans le cours. L'analyse globale devra comporter environ 50 pages, excluant les pages de présentation et les annexes.

4. *Cahier de simulation* (en équipe - déposé sur StudiUM en format .zip) – 10 %

Le cahier de simulation constitue la base de la recherche de l'étudiant pour la simulation. Il devra contenir l'ensemble des lectures qui ont été faites par les étudiants pour gérer leur crise. Les textes devront être déposés dans un fichier qui sera divisé par thématiques - au choix des étudiant. Le fichier complet sera noté selon la qualité des sources utilisées.

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+	Très bon	77
3	B		73
2,7	B-		70
2,3	C+	Bon	65
2	C		60
1,7	C-		57
1,3	D+	Passable	54
1	D		50
0	E	Échec	-de 50

Déroulement du cours

01. jeudi 7 mai AM - Introduction au cours

- Présentation de la classe et du professeur
- Explication du syllabus et des objectifs du cours
- Explication des évaluations, des activités et autres éléments pertinents
- Explication des attentes en lien avec les lectures
- Formulation des attentes pour les cours

02. Jeudi 7 mai AM et PM - Comprendre la technologie

- Comprendre le jargon informatique.
- Comment fonctionne un ordinateur?
- Comment fonctionne un réseau?
- Les bases de la réseautique, et de la compréhension de l'informatique.

• Lecture de logs.

03. Jeudi 14 mai AM - Historique de l'informatique et de l'Internet - Absence du professeur, cours asynchrone versés sur StudiUM

• Compréhension des développements
• Pourquoi la criminalité et les technologies?
• Tendances à prendre en considération

Lecture obligatoire - Chapitre 8 :
Fortin, F., Desjardins, V. (2020). Piratage informatique : du sous-sol au Web Clandestin. Dans Fortin, F. (Eds.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

04. Jeudi 14 mai PM - Cybercriminalité : théorie, notion et usages problématiques - Absence du professeur, cours asynchrone versés sur StudiUM

• La compréhension du cyberespace
• La notion de « cyber » et la relation au crime
• Les problèmes juridiques de l'informatique et de la criminalité informatique
• Typologie de maliciels
• Typologie des types de fraudes
• Sophistication des attaques
• Exemples d'attaques

Lecture obligatoire - Chapitre 9 du livre :
Rioux, A. (2020). Rançongiciels : d'hier à demain. Dans Fortin, F. (Eds.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

05. Jeudi 21 mai AM - Technologies problématiques et acteurs problématiques

• Darkweb
• Chiffrement
• Cryptomnnaie
• Les acteurs problématiques de l'Internet

Lecture obligatoire - Chapitre 14 du livre :
Péloquin, O. et Fortin, F. (2020). Tendances criminelles et technologies. Dans Fortin, F. (Eds.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

06. Jeudi 21 mai PM - Le capitalisme de données et de surveillance

• Les cinq étape du capitalisme de données
• Délinquance et surveillance économique
• Relations avec Foucault et la notion de savoir-pouvoir
• La collecte de données criminelle (databrokers, rainbow tables et autres)

Visionnement documentaire : Shoshana Zuboff on surveillance capitalism

Lecture obligatoire (disponible sur StudiUM) :

Granjon, Fabien (2021). Sur l'âge du capitalisme de surveillance. Le combat pour un avenir humain face aux nouvelles frontières du pouvoir de Shoshana Zuboff. Questions de communication, 41. P. 455-472.

07. Jeudi 28 mai AM - Propagande et désinformation

- Survol de la problématique de la désinformation
- Fermes de trolls et de désinformation
- Espionnage économique
- Guerre informatique
- Risques aux élections

Lecture obligatoire - Chapitre 12 du livre :
Crosset. V. (2020). Botnets sociaux : manipulation de l'information et propagande computationnelle. Dans Fortin, F. (Eds.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

08. Jeudi 28 mai PM - L'analyse Mitre ATT&CK pour comprendre les incidents de sécurité

- Présentation d'analyse Mitre ATT&CK
- Remise du travail d'analyse (en groupe)

Lecture obligatoire - Chapitre 10 du livre :
Décary-Hétu, D., Mousseau, V. et Mulder, X. (2020). Toujours plus haut : étude du réseau social et des promotions sur un forum d'ingénieurs sociaux. Dans Fortin, F. (Eds.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

09. Jeudi 4 juin AM

- Théories du nudging
- Techniques d'ingénierie sociale
- Architecture de choix

Lecture obligatoire - En ligne sur StudiUM :
Stajano, F., & Wilson, P. (2011). Understanding scams: A taxonomy and taxonomy of attack methods. In 2011 IEEE Symposium on Security and Privacy (pp. 318-333).

10. Jeudi 4 juin PM - Examen en classe

- Examen en classe sur StudiUM - Analyse de cas

11. Jeudi 11 juin AM - Nudging et ingénierie sociale

- Simulation

12. Jeudi 11 juin PM - Maliciels et fraudes informatiques

- Simulation

13. Jeudi 18 juin AM - Piratage étatique

- Simulation

14. Jeudi 18 juin PM - Principes de sécurité de l'information

- Simulation et debriefing

Lectures obligatoires et références bibliographiques

Livre obligatoire, disponible à la coop
Fortin, F. (2020). Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal : Les Presses Internationales Polytechnique.

Autres références fournies sur StudiUM.

Références bibliographiques
Brenner, S. W. (2007) Cybercrime: Re-thinking crime control strategies. In Crime online. Edited by Yvonne Jewkes,12–28. Portland, OR:Willan.

Britz, M.T. (2009). Computer forensics and cybercrime: An introduction. 2d ed. Upper Saddle River, NJ:Prentice Hall.

Dolan, K.M. (2004) Internet auction fraud: The silent victims. Journal of Economic Crime Management 2 (1): 1–22.

Finn, J. (2004) A survey of online harassment at a university campus. Journal of Interpersonal Violence 19 (4): 468–483.

Furnell, S. (2002) Cybercrime: Vandalizing the information society. Boston: Addison-Wesley.

Jordan, T. et Taylor P. (2004) Hacktivism and cyberwars: Rebels with a cause? London: Routledge. Levy, S. (1984) Hackers: Heroes of the computer revolution. Garden City, NY: Anchor Doubleday.

McQuade, S. C., III (2006) Understanding and managing cybercrime. Boston: Allyn and Bacon.

Newman, G.R., et Clarke, R.V. (2003) Superhighway robbery: Preventing e-commerce crime. Portland, OR: Willan.

Olson, P. (2013). We Are Anonymous. Random House.

Quayle, E. et Taylor, M. (2002) Child pornography and the Internet: Perpetuating a cycle of abuse. Deviant Behavior 23:331–361.

Quayle, E. et Taylor, M. (2003) Child pornography: An Internet crime. New York: Routledge.

Stambaugh, H., Beaupre, D. S. Icove,D. S. Baker, Cassady, W. et Williams, W.P. (2001) Electronic crime needs assessment for state and local law enforcement. Washington, DC: U.S. Department of Justice. Office of Justice Programs. National Institute of Justice.

Taylor, P.A. (1999) Hackers: Crime in the digital sublime. New York: Routledge.

Taylor, R. W., Caeti,T.J., Loper,D.K., Fritsch, E. J. et Liederbach, J. (2006) Digital crime and digital

terrorism. Upper Saddle River, NJ: Pearson Prentice Hall.

Wall, D. (2001). Crime and the Internet. New York: Routledge.

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

L'enregistrement de ce cours, en tout ou en partie, et par quelque moyen que ce soit, n'est permis qu'à la seule condition d'en avoir obtenu l'autorisation préalable de la part de la chargée de cours ou du chargé de cours. L'autorisation d'enregistrement n'entraîne 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,

Règlement des études de cycle supérieur

Nous vous invitons aussi à consulter le règlement pédagogique : https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/enseignement/ens30_2-reglement-pedagogique-etudes-superieures-postdoctorales.pdf

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.

À noter que l'étudiant doit remplir le formulaire et le remettre au responsable ou au TGDE de son programme :
https://safire.umontreal.ca/fileadmin/Documents/FAS/SAFIRE/Documents/3-Ressources-services/Ressources-formulaires/Protocole_et_formulaire_de_demande_de_r%C3%A9vision_de_notes_%C3%80_ENVOYER.pdf

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 date de 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/fileadmin/Documents/FAS/SAFIRE/Documents/Avis_absence_examen_form.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.