École de criminologie **Été 2023**
Université de Montréal

Plan de cours

CRI 3950 - Criminalité informatique

Lundi 8h30-11h30 / 12h30-15h30

Francis Fortin
Francis.Fortin \at\ umontreal.ca

Disponibilités :
Avant le cours, après le cours et 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

Objectifs généraux

Les changements technologiques au sens large ont amené une transformation dans les façons de commettre des crimes. Les auteurs mais aussi les agences d'application de la loi doivent maintenant tenir compte des éléments virtuels et dématérialisés afin d'évoluer dans ce nouveau contexte. Le présent cours se veut donc une introduction à cette problématique et vise l'atteinte des objectifs généraux suivants :

Objectifs spécifiques

À la fin du cours, l'étudiant sera capable de :

1. Classifier les différents lieux virtuels et technologies criminogènes, en évaluant les risques et les conséquences de ces environnements en ligne à l'aide de ses connaissances théoriques et pratiques acquises.
2. Analyser les différentes formes de la criminalité informatique, en utilisant les outils théoriques et pratiques acquis pour comprendre les motivations des criminels informatiques
3. Évaluer les risques et les conséquences de la criminalité informatique et de justifier ses choix en utilisant ses connaissances théoriques et pratiques pour proposer des solutions efficaces pour prévenir et réprimer ces crimes.

Approches pédagogiques

Afin d'apporter un éclairage varié sur les multiples facettes de la criminalité informatique et assurer l'atteinte de nos objectifs généraux, nous aurons recours à différentes techniques d'enseignement. En plus de cours magistraux, nous réaliserons une séance au laboratoire

informatique et des conférenciers aborderont un thème spécifique. Il est attendu que les étudiants effectuent toutes les activités pédagogiques proposées incluant les textes associés à chaque cours.

Modalités d'évaluation des apprentissages

Outils d'évaluation

Outil d'évaluation	Pondération	Échéance
Examen Intra	25%	2023-05-29
Travail de session (10% court exposé – 30% travail)	40%	2023-06-12
Examen Final	35%	2022-06-19

Présentation des travaux

Des fiches expliquant les détails ainsi que les modalités d'évaluation seront disponibles sur l'espace Studium du cours.

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

Date	**Contenu**
	Bloc introduction et concepts
2023-05-01	**Cours 1.** Lundi 1er mai - AM • Présentation du plan de cours • Histoire d'Internet • Présentation des services Internet et des principes technologiques sous-jacents **Lectures complémentaires :** • Bergeron, A., Pamar, M. et Paquette, S. (2020). "Introduction et définitions de la cybercriminalité." Dans Fortin, F. (Éd.). Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal, Canada: Les Presses Internationales Polytechnique.
2023-05-01	**Cours 2.** Lundi 1 mai – PM • Usages problématiques d'Internet. • Droit et informatique **Lecture(s) obligatoire(s) :** • Lavoie, P. E., Fortin, F., & Ouellet, I. (2013). Usages problématiques d'Internet. In F. Fortin (Ed.), Cybercriminalité: Entre inconduite et crime organisé. Montréal, QC: Les Presses Internationales Polytechnique [en ligne] https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/26677/Cybercriminalite%cc%81_Chapitre4.pdf?sequence=1&isAllowed=y **Lectures complémentaires :** • R. c. Tremblay. • Code criminel en ligne : ○ http://laws-lois.justice.gc.ca/fra/lois/C-46/ • Lapointe, Stéphane (1999). Vers l'organisation d'une cyberpolice au Canada et au Québec, Mémoire de maîtrise, Faculté des Arts et des Sciences, École de criminologie.

Bloc : Intervention policière et environnement virtuel	
2023-05-08	**Cours 3.** AM • Intervention policière sur Internet • L'utilisation des médias sociaux par les agences d'application de la loi • Exploration de lieux virtuels pour travail de session **Lecture obligatoire :** • Delle Donne, J. et Fortin, F. (2020). Pratiques policières et utilisation des médias sociaux. Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 21-36). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Krone, T. (2005). International police operations against online child pornography. Trends & Issues in Crime and Criminal Justice, No. 296. Canberra: Australian Institute of Criminology.
2023-05-08	**Cours 4.** PM • Intervention policière sur Internet (conférencier) • Les nouveaux lieux et plateformes virtuels : Darkweb, Cryptomonnaies • Exploration de lieux virtuels pour travail de session **Lecture obligatoire :** • 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. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 203-226). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Sur Studium.
Bloc : Atteintes à l'intégrité physique	
2023-05-15	**Cours 5.** AM • Activités à caractère sexuel sur Internet partie I – la pornographie juvénile **Lecture obligatoire :** • Paquette, S., Bergeron, A. et Fortin, F. (2020). Matériel d'exploitation sexuelle d'enfants sur Internet : étendue du phénomène, auteurs d'infractions et enjeux légaux. Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 37-58). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Fortin, F., & Roy, J. (2006). Profils des consommateurs de pornographie juvénile arrêtés au Québec: l'explorateur, le pervers et le polymorphe. Criminologie, 107-128. • GOYETTE, M., RENAUD, P., ROULEAU, J. L., & FORTIN, F. (2008). Évaluation et intervention auprès de consommateurs de pornographie juvénile sur internet. Revue québécoise de psychologie, 29(3), 147-160.
2023-05-15	**Cours 6.** PM • Activités à caractère sexuel sur Internet partie II – le leurre informatique **Lecture obligatoire :**

	• Paquette, S., Bergeron, A. et Fortin, F. (2020). Sollicitation à des fins sexuelles : un état de la question sur le leurre d'enfant par voie informatique. Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 59-76). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Briggs, P., Simon, W.T. et Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the Internet enabled a new typology of sex offender? Sexual Abuse: A Journal of Research and Treatment, 23(1), 72–91. http://doi.org/10.1177/1079063210384275 • DeHart, D., Dwyer, G., Seto, M.C., Moran, R., Letourneau, E. et Schwarz-Watts, D. (2016). Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*. Doi: http://dx.doi.org/10.1080/13552600.2016.1241309
2023-05-22	**Férié – Pas de cours**
2023-05-29	**Cours 7.** AM • Examen Intra
2023-05-29	**Cours 8.** PM • Cyberintimidation, cyberharcèlement et menaces **Lectures obligatoires :** • Macilotti G. (2020), Cyberintimidation et cyberharcèlement à l'heure d'Internet Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 81-108). Montréal, Canada : Presses internationales Polytechnique **Lectures complémentaires :** • Desfachelles, M. & Fortin, F. (2019). Le sexting secondaire chez les adolescent·e·s. Origine et enjeux d'une source de cyberintimidation. *Déviance et Société*, vol. 43(3), 329-357. • Ryan, N. (2013). Intimidation à l'heure d'Internet dans F. Fortin (Ed.), *Cybercriminalité: Entre inconduite et crime organisé*. Montréal, QC: Les Presses Internationales Polytechnique [en ligne] https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/26682/Cybercriminalite%CC%81_Chapitre9.pdf?sequence=1
Section sécurité informatique et diffusion d'information	
2023-06-05	**Cours 9.** AM • Pirates et « hackers » • Sociologie des pirates informatiques **Lectures obligatoires :** • Fortin, F. et Desjardins, V. (2020). Piratage informatique : du sous-sol au Web clandestin. Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 153-174). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Jordan, T., & Taylor, P. (1998). A sociology of hackers. The Sociological Review, 46(4), 757-781. • Dupont, B., Côté, A.-M., Savine, C. & Décary-Hétu, D. (2016). The ecology of trust among hackers. Global Crime, 17(2), 129-151. • Décary-Hétu, D., Dupont, B. et Fortin, F. (2014), « Policing the hackers by hacking them: Studying online deviants in IRC chat rooms », in Anthony Masys (sous la direction de), *Networks and network analysis for defence and security*, Springer, New York, pp. 63-82.
2023-06-05	**Cours 10.** PM

	• Tendances, piratage et les nouvelles formes de fraude **Lectures obligatoires :** • Rioux, A. (2020). Rançongiciels d'hier à demain. Dans Fortin, F. (Dir.), Cybercrimes et enjeux technologiques. Contexte et perspectives (pp. 153-174). Montréal, Canada : Presses internationales Polytechnique. **Lectures complémentaires :** • Blanchard, F et Fortin, F. (2013). Nouveaux habits de la vieille fraude : une vision « écosystémique » des fraudeurs, de leurs instruments et de leurs victimes Dans F. Fortin (Ed.), Cybercriminalité: Entre inconduite et crime organisé. Montréal, QC: Les Presses Internationales Polytechnique [en ligne] https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/26685/Cybercriminalite%CC%81_Chapitre12.pdf?sequence=1&isAllowed=y
2023-06-12	**Cours 11.** AM • Propagande haineuse, désinformation et mobilisation • *Hacktivisme (cybermilitantisme)*: l'exemple d'Anonymous et Qanon. **Lectures obligatoires :** • Fortin, F. (2013). Haine et utilisation d'Internet par les propagandistes Dans F. Fortin (Ed.), Cybercriminalité: Entre inconduite et crime organisé. Montréal, QC: Les Presses Internationales Polytechnique [en ligne] https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/26677/Cybercriminalite%cc%81_Chapitre4.pdf?sequence=1&isAllowed=y **Lectures complémentaires :** • Bérubé, M., et Ducol, B. (2020). "La propagande extrémiste à l'ère numérique : évolution, défis et réponses." Dans Fortin, F. (Éd.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal, Canada: Les Presses Internationales Polytechnique. • Crosset. V. (2020). "Botnets sociaux : manipulation de l'information et propagande computationnelle." Dans Fortin, F. (Éd.) Cybercrimes et enjeux technologiques : contexte et perspectives. Montréal, Canada: Les Presses Internationales Polytechnique.
2023-06-12	**Cours 12.** PM • Présentations orales de type « express » des travaux de session
2022-06-19	**Cours 13.** AM **Examen Final**

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.

Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.

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, Steven (2002) *Cybercrime: Vandalizing the information society*. Boston: Addison-Wesley.

Jordan, T. & Taylor P. (2004) *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

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., and Clarke, R.V. (2003) *Superhighway robbery: Preventing e-commerce crime*. Portland, OR: Willan.

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

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

Stambaugh, H., Beaupre, D. S. Icove,D. S. Baker, Cassady, W. & 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. & 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 premier cycle

Nous vous invitons aussi à consulter le règlement pédagogique :
https://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/reglement-des-etudes-de-premier-cycle/#c54619

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. La journée du dépôt, l'étudiant a jusqu'à 23h55 précisément pour remettre son travail via Studium. Dans tous les cas, c'est l'heure de Studium qui prévaudra.

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.