CRI 6234
Nouvelles technologies et crimes

En collaboration avec :

2 septembre 2021 – 2 décembre 2021 / 13h-16h
Salle C-4141, Pavillon Lionel Groulx

Professeur

Benoît Dupont
Bureau C-4114
Téléphone : 514-343-6111 poste 2586
Courriel : benoit.dupont@umontreal.ca
Site : www.benoitdupont.net

Présentation

Les nouvelles technologies sont omniprésentes dans notre vie quotidienne. Elles redéfinissent notre rapport au temps et à l'espace et transforment profondément les relations économiques et sociales. Malgré le sentiment de liberté que beaucoup d'entre elles nous procurent, leur rapport à la sécurité est beaucoup plus ambigu. En effet, tout nouveau cycle d'innovation technologique favorise la productivité des organisations et des individus, qui sont des sources de prospérité économique, mais il génère aussi de nouvelles opportunités criminelles et modifie profondément l'écologie des risques auxquels est confrontée la société. Par ailleurs, les technologies offrent également de nouveaux moyens de surveillance et de contrôle qui inquiètent les défenseurs des libertés individuelles, qui y voient là une menace à la vie privée des citoyens. Ce séminaire tentera donc de jeter un regard criminologique sur le rôle que jouent les nouvelles technologies de l'information dans le cycle criminel, à l'aide des outils conceptuels et méthodologiques que mettent à notre disposition les sciences sociales. Afin de comprendre de manière concrète et appliquée comment les risques numériques affectent les organisations et quelle contribution la criminologie peut apporter aux réponses mises en œuvre par ces dernières, ce séminaire sera dispensé en étroite collaboration avec les équipes de sécurité et de prévention de la fraude du Mouvement des caisses Desjardins. Les modalités d'apprentissage feront appel à la rédaction d'une étude de cas et à la conception d'un programme ou d'un produit de cybersécurité par des équipes d'étudiants qui recevront le soutien d'employés de Desjardins.

Objectifs

- Se familiariser avec les principales approches criminologiques, sociologiques et économiques associées à l'analyse des risques numériques;
- Comprendre l'impact des innovations technologiques sur la délinquance existante et sur l'émergence de nouvelles formes de crimes;
- Identifier les modalités de réponse que les organisations publiques et privées peuvent déployer afin de lutter contre la cybercriminalité;
- Imaginer des politiques, des stratégies et des produits innovants et efficaces de prévention et de contrôle de la délinquance numérique.

Organisation des séances

2 septembre // Présentation du séminaire
Concepts directeurs du séminaire
Présentation des partenaires Desjardins (Élizabeth Legault)
Modalités pédagogiques et d'évaluation
Thèmes des travaux
Composition des équipes de travail

Rutger Leukfeldt (dir.) (2017). *Research agenda: The human factor in cybercrime and cybersecurity*, La Haye: Eleven Publishing. Accessible en ligne à https://www.thehaguesecuritydelta.com/media/com_hsd/report/141/document/Research-Agenda-The-Human-Factor-in-Cybercrime-and-Cybersecurity.pdf

Guides sur le travail en équipe :
http://www.tact.fse.ulaval.ca/fr/html/sites/guide2.html
https://vie-etudiante.uqam.ca/medias/fichiers/conseils-soutien/Travaux_equipe.pdf

Guides sur l'utilisation de Teams:
Teams – Aide & apprentissage : https://support.microsoft.com/fr-fr/teams

9 septembre // Histoire de l'internet, criminologie et cybercrime
Émergence des nouvelles technologies de l'information et de la communication
Propriétés criminogéniques de l'internet
Adéquation des théories criminologiques à la cybercriminalité

David Maimon et Eric Louderback (2019). « Cyber-dependent crimes: An interdisciplinary review », *Annual Review of Criminology*, vol. 2, pp. 191-216.
Benoît Dupont et Chad Whelan (2021). « Enhancing relationships between criminology and cybersecurity », *Journal of Criminology*, pp. 1-17.

Références complémentaires:
Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., et Savage, S. 2012. "Measuring the cost of cybercrime." 11th Workshop on the Economics of Information Security. 25-26 June, 2012.
Yochai Benkler (2006). *The wealth of networks: How social production transforms markets and freedom*, Yale University Press: New Haven.
Manuel Castells (2001). « Chapitre 1 : Ce que nous apprend l'histoire d'Internet », *La galaxie Internet*, Paris : Fayard, pp. 18-49.
Kyung-Shick Choi, Claire S. Lee, et Eric R. Louderback (2020). « Historical evolutions of cybercrime: From computer crime to cybercrime", dans Tom Holt et Adam Bossler (sous la direction de), *The Palgrave handbook of international cybercrime and cyberdeviance*, New York: Springer, pp. 27-43.
Tom Holt (2017), "Identifying gaps in the research literature on illicit markets on-line", *Global Crime*, vol. 18, no. 1, pp. 1-10.
Tom Holt et Adam Bossler (2014), « An assessment of the current state of cybercrime scholarship », *Deviant Behavior*, vol. 35, no. 1, pp. 20-40.

South Park (2008). *L'internet est parti*. Saison 12, Épisode 6, http://kawoa.com/fr/southpark1206internet.
van der Wagen, Wytske, et Pieters Wolters (2015), "From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks", *British Journal of Criminology*, vol. 55, no. 3, pp. 578-595.
Jonathan Zittrain (2008). *The future of the Internet and how to stop it*. Yale University Press: New Haven.

16 septembre // Le vol d'identité, la fraude en ligne et la fraude interne
Les fraudes financières en ligne (fraude nigériane, fraude à la loterie, fraude aux enchères)
Le vol d'identité (hameçonnage, clonage, prise de contrôle de compte, obtention de crédit, etc.)

Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganan, Tom Grasso, Michael Levi, Tyler Moore et Marie Vasek (2019). « Measuring the changing cost of cybercrime », *2019 Workshop on the Economics of Information Security*, Boston, 3-4 juin 2019.
Monica Whitty (2019). « Predicting susceptibility to cyber-fraud victimhood », *Journal of Financial Crime*, vol. 26, no. 1, pp. 277-292.

Références complémentaires:
Heith Copes et Lynne Vieraitis (2008). "The risks, rewards and strategies of stealing identities". In Megan McNally and Graeme Newman (eds.), *Identity Theft and Opportunity, Crime Prevention Studies* (Vol. 23). Monsey: Criminal Justice Press, pp. 87-110.
Heith Copes et Lynne Vieraitis (2009). "Bounded rationality of identity thieves : Using offender-based research to inform policy", *Criminology & Public Policy*, vol. 8, no. 2, pp. 237-262.
Benoit Dupont (2010). "La coévolution du "vol d'identité" et des systèmes de paiement", *Criminologie*, vol. 43, no. 2, pp. 247-268.
Benoit Dupont et Esma Aïmeur (2010). « Les multiples facettes du vol d'identité », *Revue Internationale de Criminologie et de Police Technique et Scientifique,* vol. LXIII, no. 2, 2010, pp. 177-194.
Ian MacInnes, Damani Musgrave et Jason Laska (2005). « Electronic commerce fraud: Towards an understanding of the phenomenon », *Proceedings of the 38th Hawaii International Conference on System Sciences*.
David Modic et Stephen Lea (2014). « Scam compliance and the psychology of persuasion », *SSRN Electronic Journal*, DOI: 10.2139/ssrn.2364464.
Frank Stajano et Paul Wilson (2011). « Understanding scam victims: Seven principles for systems security", *Communications of the ACM*, vol. 54, no. 3, pp. 70-75.

Définition des principales problématiques pouvant être abordées pour le travail de session.

23 septembre // Le piratage et les attaques informatiques
Virus, Chevaux de Troie, Botnets, Attaques par déni de service

Les motivations et les compétences des pirates
Dimensions organisationnelles de cyberdélinquance
Division du travail et rôle de la confiance

NCA (2017). *Pathways into cyber crime*, National Crime Agency, Londres.
Benoît Dupont, Anne-Marie Côté, Jean-Ian Boutin et José Fernandez (2017). « Darkode : recruitment patterns and transactional features of 'the most dangerous cybercrime forum in the world' », *American Behavioral Scientist*, vol. 61, no. 11, pp. 1219-1243.

Références complémentaires:
Nicolas Auray et Danielle Kaminsky (2006). « Les trajectoires de professionnalisation des hackers : La double vie des professionnels de la sécurité », Working papers in economics and social sciences, Télécom Paris.
Benoît Dupont (2014). "Skills and trust: A tour inside the hard drives of computer hackers", dans Carlo Morselli (sous la direction de), *Illicit networks*, Oxford: Routledge, pp. 195-217.
Steven Furnell (2010). "Hackers, viruses and malicious software", dans Yvonne Jewkes et Majid Yar (eds.), *Handbook of Internet crime*, Cullompton: Willan, pp. 173-213.
Cormac Herley et Dinei Flôrencio (2009). "Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy", *8th Workshop on the Economics of Security*, Londres: University College, 24-25 Juin.
Thomas Holt (2007). « Subcultural evolution? Examining the influence of on-line and off-line experiences on deviant subcultures », *Deviant Behavior*, vol. 28, no. 2, pp. 171-198.
Tim Jordan et Paul Taylor (1998). « A sociology of hackers », *The Sociological Review*, vol. 46, no. 4, pp. 757-780.
Jonathan Lusthaus (2013). "How organised is organised cybercrime?", *Global Crime*, vol. 14, no. 1, pp. 52-60.
Parmy Olson (2012). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous and the Global Cyber Insurgency*, New York: Little, Brown and Company.
Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Chris Kruegel, Giovanni Vigna (2009). *Your botnet is my botnet: Analysis of a botnet takeover*. University of California Santa Barbara Technical report, Santa Barbara.

30 septembre // La sécurité de l'information dans les organisations
Les pertes et les vols de données : causes et conséquences
Les menaces internes et menaces externes
L'impact de l'insécurité de l'information sur la vie privée et l'économie numérique

Howard Bilodeau, Mohammad Lari et Mark Uhrbach (2019). *Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017*, Ottawa: Statistique Canada.

Amy Ertan, Georgia Crossland, Claude Heath, David Denney et Rikke Bjerg Jensen (2018). *Everyday cyber security in organisations*, Londres: Royal Holloway University.
À survoler pour les tableaux: Verizon Business RISK Team (2021). *2021 data breach investigations report*, Verizon Business.

Références complémentaires :
Eirik Albrechtsen et Jan Hovden (2009). "The information security digital divide between information security managers and users". *Computers and Security*, vol. 28, no. 6, pp. 476-490.
Sara Kraemer, Pascale Carayon et John Clem (2009). "Human and organizational factors in computers and information security: Pathways to vulnerability", *Computers and Security*, vol. 28, no. 6, pp. 509-520.
Ponemon Institute (2009). *Trends in insider compliance with data security policies*, Ponemon Institute: Traverse City.

7 octobre // La sécurité physique de l'information
Présentation de cas par un expert Desjardins (Cindy Martel)

Période de questions-réponses animée par les étudiants

14 octobre // La protection des données
Présentation de cas par un expert Desjardins (Jocelyn Bouchard)

Marisa Reddy Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli et Andrew Moore (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Pittsburgh: Software Engineering Institute.

Période de questions-réponses animée par les étudiants

21 octobre // Semaine de lectures

28 octobre // La gouvernance en sécurité
Présentation de cas par un expert Desjardins (Martin Labelle)

Période de questions-réponses animée par les étudiants

4 novembre // Prévention et régulation de la cybercriminalité
L'économie de la sécurité
La théorie de la réglementation graduelle
Les partenariats public-privé

David Wall (2007). "Policing cybercrimes: situating the public police in networks of security within cyberspace". *Police Practice and Research*, vol. 8, no. 2, pp. 183-205.
Tyler Moore (2010). "The economics of Cybersecurity: Principles and policy options", *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103-117.

Références complémentaires:

Johannes Bauer et Michel van Eeten (2009). « Cybersecurity: Stakeholder incentives, externalities and policy options », *Telecommunications Policy*, vol. 33, no. 10-11, pp. 706-719.

Roderic Broadhurst (2006). "Developments in the global law enforcement of cyber-crime", *Policing: An international Journal of Police Strategies & Management*, vol. 29, no. 3, pp. 408-433.

Lawrence Lessig (2006). "Chapitre 7: What things regulate". *Code version 2.0*. New York : Basic Books, pp. 120-137.

Tyler Moore et Richard Clayton (2008). « The consequence of non-cooperation in the fight against phishing », *3rd APWG eCrime researchers summit*, 15-16 octobre.

Milton Mueller (2010), « Chapitre 8: Security governance on the internet ». *Networks and States: The global politics of internet governance*. Cambridge: The MIT Press, pp. 159-183.

Graeme Newman et Ronald Clarke (2003). "Chapitre 7: Policing e-commerce". *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan, pp. 145-177.

Johnny Nhan et Laura Huey (2008). "Policing through nodes, clusters and bandwith", dans Stéphane Leman-Langlois (ed.), *Technocrime: Technology, crime and social control*, Cullompton: Willan, pp. 66-87.

Sécurité Publique Canada (2018). *Stratégie nationale de cybersécurité: Vision du Canada pour la sécurité et la prospérité dans l'ère numérique.* Gouvernement du Canada : Ottawa.

11 novembre, 18 novembre et 25 novembre // Travail de groupe et consultations avec le professeur et les experts Desjardins

Préparation du projet
Partage d'expérience sur le travail de groupe
Stratégies de présentation

2 décembre // Présentation des projets au Comité sécurité de Desjardins

Présentation de chaque équipe, accompagnée de 10 minutes de questions
Rétroaction du jury et évaluation
Cocktail de clôture [si permis par la santé publique]

Remise du rapport de projet par chaque équipe

Évaluation

- Une recension **individuelle** de la littérature de 1500-2000 mots complémentaire de la stratégie choisie par l'équipe et qui comptera pour 25% de la note finale. Cette recension devra être remise **au plus tard le 28 octobre 2021**.

- Un poster et une note de synthèse (environ 5 pages) qui devront décrire un programme visant à rehausser la confiance des membres et clients d'une institution financière fictive (CoopR) envers cette

dernière sur la cybersécurité de leurs données. Desjardins préparera une étude de cas sur cette entreprise (proche de la réalité corporative) qui servira de mise en contexte pour le travail de session. L'étude de cas présentera le problème défini en collaboration avec les répondants Desjardins, le contexte théorique, empirique et corporatif de ce problème, ainsi que la solution proposée. Cette dernière devra être accompagnée d'une justification ayant conduit à ce choix, d'une description du programme ou des outils proposés, ainsi que d'indicateurs d'évaluation pouvant être utilisés pour en mesurer les effets. Le poster et la présentation vidéo enregistrée de 10 minutes qui l'accompagnera devront être remis le **25 novembre 2021 (à minuit)**, et la note de synthèse qui détaillera l'approche adoptée devra être déposée le **2 décembre 2021**. Ils compteront pour 50% de la note finale (répartis en 25% pour la note de synthèse et 25% pour le poster).

- Une note individuelle de commentaires de rétroaction d'environ 1000 mots qui comptera pour 25% de la note finale, qui devra identifier les forces et les faiblesses du travail d'équipe et du programme ou de la solution proposée. Cette note pourra contenir des réflexions contextuelles, conceptuelles et organisationnelles sur l'adéquation entre le problème identifié et le résultat obtenu, ainsi que sur le processus du travail d'équipe. Cette note sera à remettre le **9 décembre 2021**.

Ressources en ligne

ANSSI Guide d'hygiène informatique @ https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
Trousse cybersécurité Desjardins @ https://cybereco.ca/trousse-entreprise/
Workshop on Security and Human Behaviour @ https://www.lightbluetouchpaper.org/?s=shb
Ars Technica @ http://arstechnica.com/security/
Chaire de recherche en Prévention de la cybercriminalité @ https://www.prevention-cybercrime.ca/
Computer World @ http://www.computerworld.com
F-Secure @http://www.f-secure.com/weblog/
Internet Actu @ http://www.internetactu.net/
SERENE-RISC @ http://konnect.serene-risc.ca/
The Register @ http://www.theregister.co.uk/security/
Risks Digest @ http://catless.ncl.ac.uk/risks
Bruce Schneier @ www.schneier.com/blog/
Sophos Lab @ http://nakedsecurity.sophos.com/
Threatpost @ https://threatpost.com/
Wired News @ www.wired.com
Krebs on security @ http://krebsonsecurity.com/

Services offerts par les bibliothèques

Guide de recherche en criminologie
https://bib.umontreal.ca/criminologie-psychologie-travail-social/criminologie

Barème de notation

Grille de conversion des pourcentages

Grille de conversion des pourcentages			
Points	Note littérale	Valeur	Pourcentage
4,3 4 3,7	A+ A A-	Excellent	87 [90] 83 [85] 80
3,3 3 2,7	B+ B B-	Très bon	77 73 70
2,3 2 1,7	C+ C C-	Bon	65 60 57
1,3 1	D+ D	Passable	54 50
0	E	Échec	-de 50

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 pédagogique de la Faculté des études supérieures et postdoctorales
https://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/reglement-pedagogique-de-la-faculte-des-etudes-superieures-et-postdoctorales/

Notamment les dispositions sur les retards, la révision de l’évaluation, le plagiat et la fraude.