PLAN DE COURS | CRI6730

Hiver 2026

Les sources ouvertes en criminologie

Prof. David Décary-Hétu | david.decary-hetu@umontreal.ca

Bureau C-4088 | 514-343-6111 #3664

PLAN DE COURS | CRI6730

LES SOURCES OUVERTES EN CRIMINOLOGIE

DESCRIPTEUR DE COURS

Fonctionnement d'internet et technologies utilisées pour communiquer et diffuser des informations en ligne. Impact des médiums utilisés et les sources potentielles de données sur internet. Capacités à collecter et analyser des données en sources ouvertes en criminologie.

OBJECTIFS DU COURS

1) Comprendre le fonctionnement d'internet et des technologies utilisées pour communiquer et diffuser des informations en ligne.
2) Comprendre l'impact des médiums utilisés pour communiquer et diffuser des informations en ligne.
3) Connaitre les sources potentielles de données sur internet et développer des capacités à en identifier de nouvelles.
4) Développer les capacités à collecter et analyser des données en sources ouvertes.
5) Comprendre les droits et responsabilités des chercheurs qui collectent des données en sources ouvertes ainsi que les droits et responsabilités des sujets de qui ces données sont collectées.

PÉDAGOGIE ET ENSEIGNEMENT

Ce cours est basé sur une participation active des étudiants. Dans la plupart des cours, les étudiants seront invités à expérimenter avec des outils de collecte et d'analyse de données et leur présence active sera donc essentielle à la réussite du cours. Le professeur se réservera une partie de chaque cours afin d'expliquer le développement des plateformes étudiées dans le cours, leurs caractéristiques, les façons dont elles ont été étudiées et utilisées dans le passé ainsi que le fonctionnement des outils nécessaires à la collecte et l'analyse de données sur celles-ci. Les implications théoriques et pratiques de l'utilisation de ces plateformes seront aussi explorées.

ÉVALUATIONS

L'évaluation de ce cours se fera selon deux modalités. La première sera un rapport sous la forme d'une demande de subvention. Ce rapport sera accompagné d'une collecte de données sur internet à l'aide des outils présentés dans le cours. L'étudiant devra sélectionner une source de données en ligne et en télécharger le contenu. Cette première partie vaudra 30% de la note finale.

La seconde modalité sera un travail d'analyse basé sur des données collectées en ligne. Dans ce travail, l'étudiant devra utiliser les données collectées dans la précédente évaluation pour expliquer ou décrire un phénomène criminel. Les méthodologies qualitatives ou quantitatives pourront être utilisées. Le travail devra contenir une description précise de la méthode de collecte de données. Cette deuxième évaluation vaudra 70% de la note finale.

Les notes des étudiants seront converties en lettre en suivant approximativement la distribution suivante (ex : les 15% des meilleurs étudiants auront un A+). Le nombre d'étudiants dans chaque catégorie pourrait changer en fonction de la force des étudiants et de la taille du groupe. Tout retard dans la remise des travaux entrainera une pénalité de 10% par période de 24h. Des consignes détaillées des modalités d'évaluation seront disponibles sur Studium.

Conversion des rangs (cycles supérieurs)

Points	Note littérale	Valeur	Rang
4,3	A+	excellent	15%
4	A		35%
3,7	A-		
3,3	B+	Très bon	40%
3	B		
2,7	B-		
2,3	C+	bon	0-10%
2	C		
1,7	C-		
1,3	D+	passable	0%
1	D		
0	E	échec	0%

DÉROULEMENT DU COURS

Cours 1

Présentation du plan de cours et des évaluations.

Concepts fondamentaux en sources ouvertes en criminologie.

Application des sources ouvertes à un cas de fraude.

- Chermak, S. M., Freilich, J. D., Greene-Colozzi, E., & Klein, B. R. (2025). "Open-Source Research in Criminology and Criminal Justice." *Annual Review of Criminology*, 8: 141-170.
- Spruce Point Capital. (2021/2023). "Nuvei Short Seller Reports 1 and 2." *Online: https://www.sprucepointcap.com/research/nuvei-corp.*

Cours 2

Introduction à la programmation en HTML et CSS.

Introduction à l'internet de surface.

- Learn HTML For BEGINNERS!: https://www.youtube.com/watch?v=r136WPQ6mSY
- Learn CSS in 12 Minutes: https://www.youtube.com/watch?v=0afZj1G0BIE

Cours 3

Introduction à la programmation en PHP.

Les outils gratuits et/ou à code source ouvert.

- Learn PHP in 15 minutes: https://www.youtube.com/watch?v=ZdP0KM49IVk

Cours 4

Les moteurs de recherche comme outils de recherche.

Recherches avancées sur des engins de recherches pour différents formats d'information.

- Social-Engineer.org. (2019). "The 2019 Social Engineering Capture The Flag Report". En ligne: https://www.social-engineer.org/wp-content/uploads/2019/11/SECTF-DEFCON27-SECOM-2019.pdf.
- Stubbs-Richardson, M. S., A. K. Cosby, K. D. Bergene & A. G. Cosby. (2018). "Searching for safety: crime prevention in the era of Google". *Crime Science.* 7(1): 1-13.

Cours 5

Fonctionnement de l'internet de surface.

Les forums de discussion comme source ouvertes en criminologie.

Outils et techniques de sources ouvertes appliquées aux forums de discussion.

- Hughes, J., Pastrana, S., Hutchings, A., Afroz, S., Samtani, S., Li, W., & Santana Marin, E. (2024). "The art of cybercrime community research." *ACM Computing Surveys*, 56(6): 1-26.

Cours 6

Évolution, caractéristiques et fonctionnement des réseaux sociaux de Meta.

Outils et techniques de sources ouvertes appliquées aux réseaux sociaux de Meta.

- Sjöberg, J., Cassinger, C., & Rampazzo Gambarato, R. (2024). "Communicating a sense of safety: the public experience of Swedish Police Instagram communication." *Journal of Communication Management*, 28(3): 365-383.

Cours 7

Évolution, caractéristiques et fonctionnement de Telegram.

Outils et techniques de sources ouvertes appliquées à Telegram.

- Lummen, D. L. M. (2023). "Is Telegram the new Darknet? A comparison of traditional and emerging digital criminal marketplaces." *Master's thesis, University of Twente*.

Semaine de lecture

Cours 8

Évolution, caractéristiques et fonctionnement des réseaux sociaux alternatifs.

Outils et techniques de sources ouvertes appliquées à des réseaux sociaux alternatifs.

- Williams, H. J., A. T. Evans, J. Ryan, E. E. Mueller & B. Downing. (2021). "The Online Extremist Ecosystem". *RAND Corporation*. En ligne: https://apps.dtic.mil/sti/pdfs/AD1154178.pdf.

Cours 9

Concepts fondamentaux des monnaies virtuelles.

Traçage des transactions de monnaies virtuelles.

Identification des propriétaires de monnaies virtuelles.

- Botha, J., Pederson, T., & Leenen, L. (2023). "An Analysis of the MTI Crypto Investment Scam: User Case." *European Conference on Cyber Warfare and Security*.
- Wagman, S. (2022). "Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing." *Harv. Nat'l Sec. J.*, 14, 87-101.

Cours 10

Technologies d'anonymat et protection des chercheurs.

Défis et avantages du darkweb pour les sources ouvertes.

Outils et techniques de sources ouvertes appliquées au darkweb.

- Figueras-Martín, E., Magán-Carrión, R., & Boubeta-Puig, J. (2022). "Drawing the web structure and content analysis beyond the Tor darknet: Freenet as a case of study." *Journal of Information Security and Applications*, 68.

Cours 11

Empreintes techniques.

Aspects forensiques des sources ouvertes.

- Krebs On Security Blog Posts.
- Levy, Y. & R. Gafni. (2021). "Introducing the concept of cybersecurity footprint." *Information & Computer Security*. 29(5): 724-736.

Cours 12

La recherche de personnes en sources ouvertes.

Localisation de personnes disparues.

Les sources ouvertes et la police.

- Estellés-Arolas, E. (2022). Using crowdsourcing for a safer society: When the crowd rules. European Journal of Criminology, 19(4), 692-711.

Cours 13

Éthique en collecte de données de sources ouvertes.

Droits et responsabilités des acteurs impliqués.

Gestion et confidentialité des données.

- 🕮 Bayerl, P., Akhgar, B., Raven, A., Gibson, H., & T. Day. (2022). “Future Challenges and Requirements for Open Source Intelligence in Law Enforcement Investigations: Results From a Horizon Scanning Exercise.” En ligne: https://shura.shu.ac.uk/30775/9/Bayerl-FutureChallengesAndRequirements%28VoR%29.pdf.

MATÉRIEL REQUIS

Aucun matériel n'est requis pour le cours.

STUDIUM

Studium (https://studium.umontreal.ca) sera la plate-forme privilégiée pour échanger des informations et des documents. Studium vous permettra de télécharger les notes de cours, de télécharger des guides supplémentaires aux notes de cours, de télécharger les consignes pour les évaluations et aussi de déposer les évaluations. Pour avoir accès à Studium, l'étudiant doit être dûment inscrit à l'Université et être détenteur d'un UNIP.

PLAGIAT ET FRAUDE

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. Notez que l'utilisation total ou partielle, littérale ou déguisée d'un contenu généré par un système d'intelligence artificielle (par ex., ChatGPT) pour un travail faisant l'objet d'une évaluation est interdite.

BIBLIOGRAPHIE

Adams, J., & Roscigno, V. J. (2005). "White supremacists, oppositional culture and the World Wide Web." Social Forces, 84(2), 759-778.

Amarasingam, M. A., & Winter, S. (2021). "How Telegram Disruption Impacts Jihadist Platform Migration." *Centre for Research and Evidence on Security Threats*.

Anderson, T., & Kanuka, H. (2003). E-research: Methods, strategies, and issues. Boston, USA: Allyn & Bacon.

Bancroft, A., & Scott Reid, P. (2016). "Challenging the techno-politics of anonymity: the case of cryptomarket users." Information, Communication & Society, 1-16.

Bergeron, A., J. Donne, & F. Fortin. (2019). "Une publication pour dénoncer, sans plus: description des activités des groupes Facebook s'identifiant au mouvement Anonymous au Canada". Criminologie. 52(2): 33-62

Bérubé, M., Allard, S., Denault, V., Bérubé, M., Allard, S., & Denault, V. (2022). Ensuring the probative value of web searches as digital evidence. *Canadian Criminal Law Review*, *26*(2), 167-173.

Block, L. (2023). "The long history of OSINT." *Journal of Intelligence History*.

Boczkowski, P. J., & Mitchelstein, E. (2012). "How users take advantage of different forms of interactivity on online news sites: Clicking, E-Mailing, and commenting." Human Communication Research, 38(1), 1-22.

Boersma, K. (2023). "So long and thanks for all the (big) fish: exploring cybercrime in Dutch Telegram groups." *Master's thesis, University of Twente*.

Chainey, S. P., & Alonso Berbotto, A. (2021). "A structured methodical process for populating a crime script of organized crime activity using OSINT." *Trends in Organized Crime*.

Chewae, M., Hayikader, S., Hasan, M. H., & Ibrahim, J. "How Much Privacy We Still Have on Social Network?" International Journal of Scientific and Research Publications.

Code Academy. (2016). Make a Website. https://www.codecademy.com/learn/make-a-website.

Code Academy. (2016). PHP. https://www.codecademy.com/learn/php.

Davis, S. & B. Arrigo. (2021). "The Dark Web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology". Crime, Law and Social Change. 76(4): 367-386.

Décary-Hétu, D., & Leppänen, A. (2016). "Criminals and signals: An assessment of criminal performance in the carding underworld." Security Journal. 29(3): 442-460.

Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D., & Schechter, S. (2012). "It's not stealing if you need it: A panel on the ethics of performing research using public data of illicit origin." International Conference on Financial Cryptography and Data Security.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). "An inquiry into the nature and causes of the wealth of internet miscreants." ACM conference on Computer and communications security.

Gerlitz, C., & Rieder, B. (2013). "Mining one percent of Twitter: Collections, baselines, sampling." M/C Journal, 16(2).

Gerstenfeld, P. B., Grant, D. R., & Chiang, C. P. (2003). "Hate online: A content analysis of extremist Internet sites." Analyses of social issues and public policy, 3(1), 29-44.

Ghosh, S., Zafar, M. B., Bhattacharya, P., Sharma, N., Ganguly, N., & Gummadi, K. (2013). "On sampling the wisdom of crowds: random vs. expert sampling of the twitter stream." Proceedings of the 22nd ACM international conference on Conference on information & knowledge management.

Gray, G., & Benning, B. (2019). "Crowdsourcing criminology: Social media and citizen policing in missing person cases." *Sage Open*. 9(4).

Guhl, J., & Davey, J. (2020). "A safe space to hate: White supremacist mobilisation on Telegram." *Institute for Strategic Dialogue*.

Hamilton, R. J. (2022). "Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities." *BCL Rev.*, 63, 1349-1420.

Hassan, N. A. & R. Hijazi. (2016). "Chapter 1: The evolution of open source intelligence". Open Source Intelligence Methods and Tools. New York, États-Unis: Apress.

Hassani, H., Huang, X., Silva, E. S., & Ghodsi, M. (2016). "A review of data mining applications in crime." Statistical Analysis and Data Mining: The ASA Data Science Journal, 9(3), 139-154.

Hutchings, A., & Holt, T. J. (In Press). "A crime script analysis of the online stolen data market." British Journal of Criminology.

La Morgia, M., Mei, A., Mongardini, A. M., & Wu, J. (2021). "Uncovering the dark side of Telegram: Fakes, clones, scams, and conspiracy movements." arXiv preprint.

Martin, J., & Christin, N. (In Press). "Ethics in Cryptomarket Research." International Journal of Drug Policy.

Moore, D., & Rid, T. (2016). "Cryptopolitik and the Darknet." Survival, 58(1), 7-38.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). "An analysis of underground forums." Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

Nair, V., & Kannimoola, J. M. (2022). "A tool to extract onion links from Tor hidden services and identify illegal activities." *Inventive Computation and Information Technologies: Proceedings of ICICIT 2021*.

Natarajan, R. T., Ram, S. S., & Chellappan, C. (2016). "A Tool to Identify an Offensive Gang in Social Networks." International Journal of Engineering Science.

Nguyen, A., & Western, M. (2006). "The complementary relationship between the Internet and traditional mass media: The case of online news and information." Information research, 11(3), 151-183.

Nurik, C. L. (2022). "Facebook and the surveillance assemblage: Policing Black lives matter activists & suppressing dissent." *Surveillance & Society*, 20(1), 30-46.

Paquet-Clouston, M., B. Haslhofer & B. Dupont. (2019). "Ransomware payments in the bitcoin ecosystem". Journal of Cybersecurity. 5(1). 1-11.

Platzer, F., Brenner, F., & Steinebach, M. (2022). "Similarity analysis of single-vendor marketplaces in the tor-network." *Journal of Cyber Security and Mobility*, 205-238.

Rafael, J., & Karsten, M. (2022). "The Effect of Content Moderation on Online and Offline Hate: Evidence from Germany's NetzDG." CEPR Discussion Papers.

Rege, A., & Bleiman, R. (2021). "Collegiate Social Engineering Capture the Flag Competition." *APWG Symposium on Electronic Crime Research*.

Reid, E. M. (1996). "Communication and community on Internet Relay Chat: constructing communities." High noon on the electronic frontier: Conceptual issues in cyberspace.

Rodriguez, A., Chen, Y. L., & Argueta, C. (2022). "FADOHS: framework for detection and integration of unstructured data of hate speech on facebook using sentiment and emotion analysis." *IEEE Access*.

Rossiter, M. (2022). The evolving role of open-source intelligence. Journal of the Australian Institute of Professional Intelligence Officers, 30(1), 19-30.

Schrenk, M. (2012). Webbots, spiders, and screen scrapers: A guide to developing Internet agents with PHP/CURL. New York, USA: No Starch Press.

Sohoraye, M., Gooria, V., Nundoo-Ghoorah, S., & Koonjal, P. (2015). "Do you know Big Brother is watching you on Facebook? A study of the level of awareness of privacy and security issues among a selected sample of Facebook users in Mauritius." International Conference on Computing, Communication and Security.

Tan, Q., Wang, X., Shi, W., Tang, J., & Tian, Z. (2022). "An anonymity vulnerability in Tor." *IEEE/ACM Transactions on Networking*, 30(6), 2574-2587.

Tucker, R., O'Brien, D. T., Ciomek, A., Castro, E., Wang, Q., & Phillips, N. E. (2021). "Who 'tweets' where and when, and how does it help understand crime rates at places? Measuring the presence of tourists and commuters in ambient populations." Journal of Quantitative Criminology. 37(2): 333-359.

Westlake, B., Bouchard, M., & Frank, R. (In Press). "Assessing the validity of automated webcrawlers as data collection tools to investigate online child sexual exploitation." Sexual abuse: a journal of research and treatment.

Yannikos, Y., Heeger, J., & Steinebach, M. (2022). "Data acquisition on a large darknet marketplace." *Proceedings of the 17th International Conference on Availability, Reliability and Security*.

Yip, M., Webber, C., & Shadbolt, N. (2013). "Trust among cybercriminals? Carding forums, uncertainty and implications for policing." Policing and Society, 23(4), 516-539.

Yip, M., Shadbolt, N., & Webber, C. (2013, May). "Why forums?: an empirical analysis into the facilitating factors of carding forums." Proceedings of the 5th Annual ACM Web Science Conference.