CRI 6720 : IMPACT DES TECHNOLOGIES DE SÉCURITÉ

Plan de cours – Automne 2026

12h30 - 15h3[redacted]

Arnaud Moderie
École de criminologie – Université de Montréal

arnaud.moderie@umontreal.ca

Disponibilités : sur rendez-vous par courriel

1. Introduction

Ce cours porte sur les transformations qu'ont connues les institutions de sécurité avec l'arrivée du New Public Management. Cette approche a amené les organisations publiques à accorder davantage d'importance à l'efficacité, à la reddition de comptes et à l'atteinte de résultats, alors même que leurs ressources sont souvent limitées. Dans ce contexte, les organisations de sécurité ont dû revoir certaines de leurs façons de faire, notamment en partageant davantage les responsabilités et en intégrant de nouveaux outils technologiques, comme l'intelligence artificielle, les systèmes de prédiction, les caméras portées par les policiers et la reconnaissance faciale.

Le cours invite également à dépasser l'idée selon laquelle les technologies seraient de simples outils neutres. Leur développement et leur utilisation doivent être étudiés en tenant compte du contexte social, politique, économique et idéologique dans lequel elles prennent place. Une attention particulière est accordée à leurs effets possibles, notamment aux biais, aux discriminations et aux inégalités qu'elles peuvent produire ou renforcer. Le cours analyse aussi la façon dont les personnes et les organisations utilisent ces technologies, se les approprient, les adaptent, les contournent ou les détournent de leur fonction initiale. Enfin, il s'intéresse aux liens entre les technologies récentes et les outils plus traditionnels, comme les dossiers et les fichiers papier, qui demeurent présents dans les pratiques de sécurité.
Remarque : Ce cours ne couvre par les enjeux de cybercriminalité tels qu'abordés dans le séminaire CRI 6234 : Nouvelles technologies et crime.

2. Objectif général du cours

Le cours a pour objectif de sensibiliser les étudiant·es aux principaux enjeux et de stimuler leur réflexion sur les principaux enjeux qui caractérisent la formulation, le déploiement, l'appropriation et l'impact d'une technologie de sécurité, tant d'un point de vue social qu'individuel. Comme l'indique l'intitulé du cours, il s'agira de fournir un cadre pour appréhender et comprendre l'impact des technologies de sécurité et développer une réflexion critique et intégratrice des dimensions historique, politique, sociale et performative (effets) – et parfois inattendues – des technologies de sécurité.

3. Pédagogie et enseignement

Le séminaire se déroulera **dans la salle C-4141 le mercredi de 12h30 à 15h30.** Selon le principe qui caractérise la formation étudiante aux 2e et 3e cycles, son bon déroulement repose largement sur la responsabilité des étudiant.es **dont la présence et la participation sont nécessaires**. Les séances sont principalement alimentées par les interventions et réflexions des étudiant.es, aussi **ils/elles ont la responsabilité de lire et travailler les textes prévus pour chacune des séances.** Ces textes sont indiqués ci-dessous et sont disponibles sur la plateforme StudiUM. Il est donc crucial de faire les lectures puisqu'une grande partie des séances sera alimentée par les réflexions, commentaires, questions des étudiant.e.s. Le professeur, quant à lui, apportera des éléments théoriques, conceptuels et méthodologiques nécessaires au déroulement des discussions.

Un duo d'étudiant.e.s sera désigné.e pour chaque séance[1] qui aura la responsabilité d'en faire l'animation à partir des lectures identifiées et avec l'aide de tout autre support (documentaire, extraits de séries, articles de presse, balado, etc.) qu'il jugera utile. Chaque duo se composera d'une personne qui devra réaliser un **rapport intégratif des lectures** pour la séance (précisions ci-dessous) et d'une personne qui réalisera **une critique du rapport** du / de la collègue, sur le mode de la complémentarité. Fonctionnant par équipe, le duo **aura pour responsabilité d'animer la séance**, de poser des questions à l'ensemble des participants du séminaire et d'animer la discussion autour des textes, avec l'aide du professeur (ex. par des illustrations ou des cas d'actualité, à partir d'expériences personnelles ou d'enjeux sociaux et politiques, etc.). Le duo peut également s'appuyer sur des extraits de documentaires ou films pour illustrer des points de présentation. Cette organisation vise à animer et provoquer l'interaction et des apprentissages dynamiques et ne fait pas l'objet d'évaluation formelle.

4. Évaluation

L'évaluation se fera **en quatre temps**.

[1] Pour des raisons logistiques, il se peut qu'il y ait plus qu'un duo pour certaines séances.

1. Premièrement, les étudiant.es sont évalué.es sur leur participation (prise de parole, participation aux débats, commentaires sur les lectures, animation du séminaire) (10%).
2. Deuxièmement, chaque étudiant.e doit réaliser un rapport intégratif et critique des lectures indiquées pour une séance (max. 5 pages), basé sur une grille indicative présentée lors de la première séance du cours et disponible sur StudiUM (20%). Ce rapport, en format Word, doit être envoyé par courriel au professeur au plus tard le samedi midi (12h00) précédent le cours. Il est aussitôt rendu disponible sur StudiUM.
3. Une troisième évaluation consiste à rédiger un commentaire / critique d'un rapport du / de la collègue (max. 3 pages) (20%) également présenté lors de la séance. La personne qui rédige le rapport écrit, ainsi que la personne rédigeant le commentaire, forment le duo responsable d'animer la séance. Cette critique est remise au professeur au plus tard au début de la séance (format Word).
4. Enfin, une quatrième évaluation consiste à livrer un travail de fin de session – 20 pages maximum, interligne 1,5 – traitant d'un sujet libre de choix pour autant qu'il soit en lien avec à l'impact des technologies en sécurité. À titre d'exemple, ce travail peut traiter d'une technologie, d'un acteur, d'une politique, d'un marché, d'un enjeu social, etc. Ce travail comptera pour 50% de l'évaluation du cours et devra être remis en version électronique (Word) le 16 décembre 2026 à 17h00.

Selon la politique de l'École de criminologie, les travaux remis en retard seront pénalisés de 10% le premier jour et 5% par jour supplémentaire de retard (incluant samedi et dimanche ainsi que les jours fériés). Seules des raisons médicales accompagnées d'un billet du médecin feront exception à cette règle. Ce délai ne peut dépasser 5 jours.

5. Calendrier des rencontres

Séance 1 | 2 septembre 2026 – Introduction, présentation du cours
Présentations des participants et du plan de cours ; organisation de la session (choix des textes par les étudiant.e.s pour la répartition des rapports/commentaires) ; présentation de la grille de rédaction de rapport / commentaire ; introduction à la question de l'impact des technologies en sécurité intérieure.

Séance 2 | 9 septembre 2026 – penser la technologie en sécurité intérieure
Concepts et enjeux préliminaires pour penser la technologie et la science des données; modernité et technologie; technologie et démocratie; évolution de la conception de la technologie; développement de la technologie dans la médiatisation des rapports humains; sécurité, technologie et utilisation des données dans la définition des priorités et des cibles en application de la loi. *Ce cours sera dispensé sur Teams

Lectures :

- Ceyhan, Ayse (2006), « Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitude », *Cultures & Conflits*, 64 : 1-21.

- Feenberg, Andrew (1999), "The Limits of Technical Rationality", in Feenberg, A, *Questionning Technology*, Londres, New York: Routledge, pp. 75 – 100.
- La démocratie peut-elle reprendre le contrôle de la technique ? avec Andrew Feenberg (14 juin 2018 France culture)

Séance 3 | 16 septembre 2026 – Déterminisme ou neutralité de la technologie ?
Quel statut donner à la technologie : la thèse du déterminisme technologique et le principe de neutralité technologique ; questionnement sur l'autonomie et la performativité des technologies de sécurité ; floutage de la frontière entre machines et humains. Étude de cas du service de police de Tampa *Ce cours sera dispensé sur Teams

Lectures :

- Latour, B. (2007), « Le dédale de la médiation technique », in *L'espoir de Pandore. Pour une vision réaliste de l'activité scientifique*, Paris : La Découverte, pp. 183-227.
- Norocel, O. C. (2022), « Gendering Web2.0 Sociotechnical Affordances of Far-Right Metapolitics". *Social Media & Society*, accès avancé: 1-11.
- Écoutez Donna Haraway parler de cyborgs sous un arbre – Le code a changé (Podcast Radio *France 17 août 2024)*
- *Clemmow, C., Schumann, S., Rubini, S., Martinsone, A., & Rottweiler, B. (2026). Pathways into Violence-focused* Online Communities: Examining Configurations and Temporal Patterns of Motivational Drivers and Risk Factors.

Séance 4 | 23 septembre 2026 – Évolution linéaire ou reconfiguration permanente de la technologie ?
Le barbelé et les murs de sécurité : « succès » persistant d'anciennes technologies dans les dispositifs de sécurité actuels ; les mécanismes d'articulation entre anciennes, nouvelles technologies (low-tech / high-tech) et style de raisonnement humain dans la gestion et l'anticipation du risque ; automation de la prise de décision.

Lectures :

- Bonelli, L. & Ragazzi, F. (2014). « Low-tech security: Files, notes and memos as technologies of anticipation ». *Security Dialogue*, 45: 476-493.
- McGuire, M. R. (2021), The laughing policebot: automation and the end of policing, *Policing & Society* 31(1): 20-36.

***** Congé universitaire le 30 septembre 2026 – Journée nationale de la vérité et de la réconciliation *****

Séance 5 | 7 octobre 2026 – Espace de formulation et de conception de technologies de sécurité
Entre critères techniques et arbitrages politiques, le processus de choix et de sélection d'une technologie de sécurité ; une constellation d'intérêts et de conflits de rationalité : le processus de

fabrication et d'installation d'une technologie de sécurité ; la technologie comme instrument de l'action publique.

Lectures :

- Follis, Karolina (2017), "Vision and Transterritory: The Borders of Europe", *Science, Technology and Human Values*, 42(6): 1003-1030.
- Klauser, F. (2022), "Policing with drones: Towards aerial geopolitics of security". *Security Dialogue*, 53(2): 148-163.

Séance 6 | 14 octobre 2026 – Mobilisation, appropriation et résistance aux technologies : prédiction et système de justice criminelle.

Réflexion sur les 'manières de faire' et les opérations des usagers de technologie de sécurité ; penser la « consommation » ou l'usage d'une technologie comme une forme de production ; l'importance du contexte d'action et de mobilisation d'une technologie ; le cas du Big Data et de la prédiction dans le système de justice criminelle.

Lectures :

- Brayne, Sarah (2017), "Big Data Surveillance: The Case of Policing", *American Sociological Review*, 85(5): 977-1008.
- Brayne, Sarah & Angèle Christin (2021), "Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts", *Social Problem*, 68: 608-624.

***** Semaine de lecture : du 19 au 25 octobre 2026 *****

Séance 7 | 28 octobre 2026 – Intelligence artificielle et algorithmes en sécurité intérieure : le cas canadien et les droits de la personne

Discussion pratique et réflexion collective autour de l'utilisation de l'intelligence artificielle dans le contexte domestique canadien en matière de sécurité; droits de la personne; données personnelles, vie privée et intelligence artificielle; Directive sur la prise de décisions automatisée du Canada; débats, ainsi que l'émergence d'applications policières concrètes, notamment la production automatisée de rapports ou d'analyses assistées par l'IA intégrées aux caméras corporelles.

Lectures :

- Gouvernement du Canada (2021), *Directive sur la prise de décisions automatisée.*
- Robertson, Kate; Cynthia Khoo & Yolanda Song (2020), *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*. Citizen Lab, Munk School of Global Affairs, pp: 36-149.
- Zuzanna Labedzka, P., Peters, D., J Dudley, J., & Zilka, M. (2026). Human-AI Interaction for Time-Critical Sensemaking in Missing Persons Investigations. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (pp. 1-15).

Séance 8 | 4 novembre 2026 – Conférence d'un intervenant du milieu de la sécurité intérieure sur l'impact des technologies sur les enquêtes - À confirmer/Ou travail autonome avec consultation du professeur

Séance 9 | 11 novembre 2026 – La technologie et ses biais : the New « Jim Code »?
Enjeux liés à la conceptualisation de la technologie et de ses impacts en matière de discrimination et de biais; « code culturel » et technologie; « impensés » en matière de conceptualisation de la technologie et conséquences sur le public.

Lectures :

- Benjamin, Ruha (2019), « Coded Exposure. Is Visibility a Trap?", in *Race After Technology: Abolitionist Tools for the New Jim Code*, Cambridge: Polity: 97-136.
- Raji, Inioluwa Deborah; Timnit Gebru et al. (2020), "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", *Proceedings of the 2020 AAAI/ACM Conference* on AI, Ethics and Society (AIES '20), 7-8 février 2020, New York, NY, USA: 1-7.
- Zilka, M., Sargeant, H., & Weller, A. (2022). Transparency, governance and regulation of algorithmic tools deployed in the criminal justice system: A UK case study. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society : 880–889,

Séance 10 | 18 novembre 2026 – Technologie, pensée magique, automation et travail humain
Réflexion sur le rôle et la place dans la technologie dans les politiques publiques en matière de sécurité ; effets pervers des technologies ; éthique de l'interaction entre humains et machines ; automation et travail humain.

***Lectures* :**

- Mann, Monique; Peta Mitchell & Marcus Foth (2022), "Between surveillance and technological solutionism: A critique of privacy-preserving apps for COVID-19 contacttracing". *New Media & Society*, prépublié: 1-19.
- Casilli, Antonio A. (2019), "Les humains vont-ils remplacer les robots? » (chap. 1), in. *En attendant les robots. Enquête sur le travail du clic*. Paris : Seuil : pp. 31-62.
- Avec Alain Damasio, on refait la science-fiction (et le monde aussi) – Le code a changé (29 juin 2024 Podcast Radio France)
- Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19

Séance 11 | 25 novembre 2026 – Conférence Anthony Amicelle, maître de conférence à Sciences Po Bordeaux (technologie, sécurité et flux financiers) – À confirmer

Lecture :

- Amicelle, A. (2022), « Big data surveillance across fields: Algorithmic governance for policing & regulation", *Big Data & Society*, accès avancé, pp: 1-12.

Séance 12 | 2 décembre 2026 –(Dés)information, démocratie, technologie et sécurité Rôle et impact de l'information et des technologies de l'information en sécurité intérieure; désinformation; usages des technologies de l'information comme arme de distraction massive; le cas du complotisme et du conspirationniste.

***Lectures* :**

- Golebiewski, Michael & danah boyd (2019), *Data Voids: Where Missing Data Can Easily be Exploited*, Data & Society, New York, NY.
- Hannah, Matthew, N. (2021), "A Conspiracy of Data: QAnon, Social Media, and Information Visualization", *Social Media & Society*, Juillet-Septembre: 1-15.

Séance 13 | 9 décembre 2026 – Impact des technologies sur la mobilisation, l'(h)activisme et l'extrémisme violent.

Participation sociale, influenceurs, micro-célébrités et outils numériques ; le web comme espace d'activisme, de (dés)information et d'incubation' ; usages des technologies de l'information dans la propagation de la haine et la mobilisation des idées et des personnes.

***Lectures* :**

- Gaudette, Tina; Ryan Scrivens; Garth Davis & Richard Frank (2021), « Upvoting extremism: Collective identity formation and the extreme right on Reddit", *New Media & Society*, 23(12): 3491-3508.
- Lumsden, Karen (2019), "I want to kill you in front of your children" is not a threat. It's an expression of desire: Discourses of online abuse, trolling and violence on r/MensRight, in Lumsden, Karen et Emily Harmer (dirs.), *Online othering. Exploring digital violence and discrimination on the web*. Londres, New York: Pelgrave McMillan: 91-115.

16 décembre 2026 | REMISE DU TRAVAIL FINAL (17H00) – FORMAT WORD

Bibliographie sélective :

Aas, K. F. ; Gundhus, H. O. & Lomell, H. M. (eds.) (2009), *Technologies of Insecurity*. London : Routledge.

Andrejevic, M. & K. Gates (2014), Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2): 185-196.

Amicelle, A. (2021), "Policing et big data : la mise en algorithmes d'une politique internationale », *Critique internationale*, 92 : 23-48.

Amicelle, A. & G. Grondin (2021), « Algorithms as suspecting machines : financial surveillance for security intelligence ». In D. Lyon & D. Murakami-Wood (eds.), *Security intelligence and surveillance in the big data age*. Vancouver: UBC Press.

Aradau, C. & T. Blanke (2017), "Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data. *European Journal of Social Theory*, 20(3): 373-391.

Ball, K. ; Lyon, D. & Haggerty, K. (eds.) (2012), *The Routledge Handbook of Surveillance Studies*. London, New York : Routledge.

Benkler, Y. ; R. Faris & H. Roberts (2018), *Network propaganda : manipulation, disinformation, and radicalization in American politics*, New York : Oxford University Press.

Benjamin, R. (2019), *Race After Technology. Abolitionist Tools for the New Jim Code*. Cambridge: Polity.

Bennet Moses, M. & J. Chan (2018), "Algorithmic prediction in policing: assumptions, evaluation, and accountability", *Policing and Society*, 28(7): 806-822.

Bennet, C. (2011), *Security Games*. New York : Routledge.

Boullier, D. (2016), *Sociologie du numérique*. Paris : Armand Colin.

Browne, S. (2015), *Dark Matters. On the Surveillance of Blackness*. Durham & Londres: Duke University Press.

Burgess, P. (2010). *The Routledge Handbook of New Security Studies*. New York : Routledge.

Cardon, D. (2018), « Le pouvoir des algorithmes », *Pouvoirs,* 164(1) : 63-73.

Casilli, Antonio A (2019), *En attendant les robots. Enquête sur le travail du clic*. Paris : Seuil.

Chan, J. & L. Bennet-Moses (2017), "Making Sense of Big Data for Security", *The British Journal of Criminology*, 57(2): 299-319.

Chavalarias, D. (2022). *Toxic data : Comment les réseaux manipulent des opinions*. Flammarion.

Cheney-Lippold, J. (2017), *We are data : algorithms and the making of our digital selves*. New York : New York University Press.

Clemmow, C., Schumann, S., Rubini, S., Martinsone, A., & Rottweiler, B. (2026). Pathways into Violence-focused Online Communities: Examining Configurations and Temporal Patterns of Motivational Drivers and Risk Factors.

Crettiez, X., & Piazza, P. (dirs.) (2006), *Du papier à la biométrie : identifier les individus*. Paris : Les Presses de SciencesPo.

Ducol, B. (2015), A Radical Sociability : In defense of an off-line/on-line multidimensional approach to radicalisation, in Bouchard, M. (dir.), *Social Networks, Terrorism and CounterTerrorism : Radical and Connected Account*. Londres : Routledge : 87-107.

Ellul, J. (1988), *Le bluff technologique*. Paris : Hachette.

Ellul, J. (1954), *La technique ou l'enjeu du siècle*. Paris : Armand Colin.

Evans, C. L. (2018), *Broad Band. The Untold Story of the Women Who Made the Internet*. Londres: Penguin.

Feenberg, A. (1999), *Questioning Technology*. Londres, New York: Routledge.

Grobois, P. (2018), *Les batailles d'Internet. Assauts et résistances à l'ère du capitalisme numérique*, Montréal : Écosociété.

Hargittai, E. & C. Sandvig (dirs.) (2015), *Digital research confidential : The secrets of studying behavior online*. Cambridge MA. : MIT Press.

Halpern, C. ; P. Lascoumes & P. Le Galès (2014), *L'instrumentation de l'action publique.* Paris : Les Presses de SciencesPo.

Hälterlein, J. (2021), "Epistemologies of predictive policing: Mathematical social sience, social physics and machine learning", *Big Data & Society*, Janvier-juin: 1-13.

Huysmans, J. (2014). *Security Unbound. Enacting Democratic LImits*. London : Routledge.

Kotliar, D. M. (2021), « Who Gets to Chose? On the Socio-algorithmic Construction of Choice", *Science, Technology & Human Values*, 46(2): 346-375.

Lavornia, A. & P. Ugwudike (2021), « The datafication revolution in criminal justice : An empirical exploration of frames of protraying data-driven technologies for crime prevention and control", *Big Data & Society*, Juillet-Décembre: 1-15.

Lupton, D. (2015), *Digital Sociology*. London & New York : Routladge.

Lyon, D. (2015), *Surveillance After Snowden*. Cambridge : Polity Press.

Marx, G. (2001), Technology and Social Control : The Seacrh for the Illusive Silver Bullet, in N. J.. Smelser & P. B. Balte (eds.), *International Encyclopedia of the Social and Bahavioural Sciences*. New York : Elsiver.

Manning, P. K. (2011). *The Technology of Policing*. New York : NYU Press.

Milivojevic, S. (2021). *Crime and punishment in the future internet : Digital frontier technologies and criminology in the twenty-first century*. Routledge.

Misa, T. J.; P. Brey & A. Feenberg (2003), *Modernity and Technology*. Cambridge, M. A.; Londres: The MIT Press.

Norris, C. & Armstrong, G. (1999). *The Maximum Surveillance Society : the Rise of CCTV*. Oxfrod : Berg.

Pasquale, F. (2020), *New Laws of Robotics. Defending Human Expertise in the Age of AI*. Cambridge, MA: Harvard University Press.

Pasquale, F. (2015), *The Black Box Society: The Secret Algorithm s that Control Money and Information*. Cambridge, MA: Harvard University Press.

Pötzsch, H. (2015), « The emergence of iBorder: bordering bodies, networks, and machines », *Society and Space*, 33, pp. 101-118.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology : Crime and justice in digital society*. Routledge, Taylor & Francis Group.

Scrivens, R. & A. Amarasingam (2019), “Haters Gonna ‘Like’: Exploring Canadian Far-Right Extremism on Facebook”, in Lumsden, Karen et Emily Harmer (dirs.), *Online othering. Exploring digital violence and discrimination on the web*. Londres, New York: Pelgrave McMillan: 63-89.

Simondon, G. (1958), *Du mode d’existence des objets techniques*. Paris : Aubier.

Singer, P.W. & E. T. Brooking (2018), *Like War : The Weaponization of Social Media*. Boston, New York : An Eamon Dolan Book, Houghton Mifflin Harcourt.

Winner, L. (1977). *Autonomous Technology : Technics Out-Of-Control as a Theme in Political Thought*. Cambridge, MA. : New Press.

Zilka, M., Sargeant, H., & Weller, A. (2022). Transparency, governance and regulation of algorithmic tools deployed in the criminal justice system: A UK case study. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (pp. 880–889). ACM

Zuckerberg, D. (2018), *Not All Dead White Men. Classic Misogyny in the Digital Age.* Cambridge, Londres: Harvard University Press.

Zuzanna Labedzka, P., Peters, D., J Dudley, J., & Zilka, M. (2026). Human-AI Interaction for Time-Critical Sensemaking in Missing Persons Investigations. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (pp. 1-15).