Université de Montréal

Faculté des arts et des sciences
Département de science politique

POL 3605 – Pouvoir et résistance dans le cyberespace

Hiver 2024

Horaire : mercredi, 8h30 à 11h30

Description et objectifs

L'internet, les médias sociaux et les technologies numériques facilitent le partage rapide d'informations et le réseautage à grande échelle. Ces avancées technologiques sont vues par certains comme de puissants vecteurs de mobilisation politique, voire de démocratisation (par ex., Howard et Hussain 2013; Manacorda et Tesei 2020). Ces bouleversements se sont néanmoins accompagnés de phénomènes de contrôle et de manipulation. Avec les progrès de l'intelligence artificielle et la sophistication grandissante des logiciels (logiciels espions et malveillants, logiciels de reconnaissance faciale et vocale, agents conversationnels – *chatbots*, hypertrucages – *deepfakes*, etc.), les opérations de surveillance, de piratage et de désinformation sont devenues répandues et intrusives. Aux mains de régimes autoritaires, ces technologies peuvent être des outils de censure, de contrôle et de répression. Aux mains de journalistes, d'activistes ou de simples citoyen.nes, ces technologies deviennent des outils de résistance et d'émancipation à l'égard du pouvoir.

Ce cours, structuré en quatre parties, vise à éclairer ces phénomènes. Dans un premier temps, nous examinerons les propositions théoriques, les concepts clés et les principaux débats qui animent ce domaine d'étude. Dans un second temps, nous étudierons l'utilisation de technologies de surveillance par les responsables de régimes autoritaires pour censurer l'accès à l'information, espionner leurs citoyen.nes et museler les opposant.es politiques. Nous porterons aussi une attention aux campagnes de désinformation, de piratage informatique, de même qu'aux cyberattaques mises en œuvre à des fins politiques et militaires par des agent.es à la solde d'États et leurs allié.es.

Dans un troisième temps, nous nous intéresserons au rôle d'internet et des technologies numériques comme vecteurs de mobilisation et de contestation politique au sein de régimes autoritaires et démocratiques. Nous analyserons les stratégies déployées par des membres de la société civile pour contourner la censure et la surveillance en ligne, faire du piratage informatique et relayer des documents confidentiels aux médias pour différents motifs politiques et idéologiques. Nous réfléchirons aussi à l'internet clandestin (*dark web*). Enfin, dans une quatrième partie, nous considérerons les enjeux entourant la cybersurveillance dans un contexte démocratique en nous intéressant entre autres à l'espionnage de

journalistes. Nous examinerons aussi les effets de la désinformation lors d'élections et les enjeux entourant la répression numérique transnationale pour les démocraties comme le Canada. La réflexion sur ces sujets sera éclairée par des études de cas.

Pédagogie

Diverses méthodes de pédagogie active seront employées tout au long de ce cours, incluant des études de cas, des forums de discussion, un jeu de rôle et un jeu de simulation. Ces méthodes seront mises à profit en particulier lors des quatre ateliers. Lors des autres séances, la matière sera présentée de façon magistrale durant la première partie. Après la pause, mais parfois un peu plus tard, des discussions et des exercices en grand groupe ou en petits groupes auront lieu afin de réfléchir de façon critique aux notions théoriques et conceptuelles, ainsi qu'aux études empiriques analysées dans le cours. La lecture et le visionnement de reportages et de courts documentaires alimenteront aussi notre réflexion. La participation active des étudiant.es est fortement encouragée, de même que leur présence, en particulier lors des ateliers.

Diverses activités permettront de compléter l'apprentissage de la matière du cours. Sur Studium, vous pourrez consulter les présentations PowerPoint qui résument des aspects importants de la matière présentée. Les lectures sont accessibles sur Studium ou sur le site web des bibliothèques de l'UdeM. Je vous transmettrai également des informations en lien avec le cours et l'actualité dans l'espace intitulé « Nouvelles » sur Studium. Nous utiliserons aussi Perusall (voir lien sur Studium). Perusall une plateforme de lecture en ligne qui facilite la discussion et l'apprentissage de façon interactive et collaborative afin d'approfondir certains textes. Je vous préciserai la procédure à suivre au début du trimestre. Dans vos échanges avec vos collègues, veuillez s.v.p. faire preuve d'ouverture et de respect, même s'il vous arrive d'être en désaccord.

Évaluation

L'évaluation de l'acquisition des connaissances se fera dans le cadre de **travaux en lien avec les quatre ateliers** du cours et **d'une analyse finale en fin de session.** Les instructions pour les travaux en lien avec les quatre ateliers sont décrites ici.

Atelier #1: étude de cas – quels effets peut-on attribuer aux opérations d'influence menées par la Russie ? – 14 février (20%) – *remise de l'analyse sur Studium le 13 février à 23h30 au plus tard, merci*.

Depuis plusieurs années, la Russie mène une série d'opérations visant à déstabiliser de nombreux pays, dont les États-Unis et ses alliés, en s'ingérant notamment dans leurs processus électoraux pour influencer leurs sociétés. Ces opérations incluent la mise en œuvre de cyberattaques, l'amplification de fausses nouvelles relayées par des usines à trolls et des robots en ligne, l'orchestration de fuites programmées et l'utilisation de l'intelligence artificielle pour créer des photos et des hypertrucages (*deepfakes*) afin de manipuler les publics ciblés. Des médias financés par le régime russe (dont RT et Sputnik) ont aussi été accusés de contribuer à ces campagnes d'influence en relayant des contenus

propagandistes. RT et Sputnik ont d'ailleurs été interdits dans de nombreux pays après l'invasion de l'Ukraine par la Russie. Ces opérations d'influence viseraient à polluer le débat politique, à exacerber les tensions sociales et à désinformer les publics au sein de l'espace médiatique traditionnel et sur internet.

Dans les cercles politiques et médiatiques, on attribue souvent à ces opérations des effets persuasifs importants. Pourtant, la recherche scientifique à ce sujet est encore en émergence et les débats entre chercheur.es se poursuivent. Il importe en ce sens de s'intéresser aux études qui proposent un éclairage empirique naissant sur les effets attribués à ces opérations russes. Pour ce premier atelier, vous réfléchirez à cette question en analysant **deux** des trois recherches suivantes. Vous produirez ensuite une **analyse de quatre pages** à double interligne portant sur les deux études que vous aurez choisies. Dans votre analyse, vous mettrez l'accent sur les observations et les constats des auteur.es qui vous apparaissent les plus importants en effectuant des liens entre les textes.

La première étude aborde l'*astroturfing*, un phénomène appelé « similitantisme » ou « désinformation populaire planifiée[1] » en français. L'*astroturfing* est une stratégie de communication consistant à utiliser différentes techniques de manipulation en ligne (par ex., des robots virtuels qui créent des faux comptes et qui produisent, partagent et amplifient des messages) afin de donner une « fausse impression qu'une opinion particulière a un grand appui populaire » (Zerback, Töpfl & Knöpfle, 2021). Dans leur étude, Zerback et al. (2021) s'intéressent aux effets persuasifs de l'*astroturfing* à des fins propagandistes russes sur internet. Vous examinerez ces effets en lien avec des commentaires typiques d'*astroturfing* sous des contenus de nouvelles sur Facebook. Il n'est pas nécessaire de s'attarder aux analyses statistiques des auteur.es. Expliquez plutôt les principaux constats de leur recherche et votre analyse de ses implications pratiques.

La deuxième recherche porte sur la deuxième édition du livre de Jamieson (2021), dans lequel la chercheure soutient la thèse qu'une campagne d'ingérence russe durant l'élection présidentielle américaine de 2016 a favorisé l'élection de Trump. Après avoir lu l'introduction, où Jamieson présente sa thèse, vous analyserez les chapitres 9 et 11. Dans ces chapitres, Jamieson (2021) explique comment les informations piratées au Parti démocrate et à ses membres ont influencé la couverture médiatique et les deux derniers débats présidentiels par le concours de différents acteurs (Wikileaks, Parti républicain, trolls russes, médias, etc.). Après avoir expliqué la thèse de l'auteure détaillée en introduction, analysez ses observations et constats dans les chapitres 9 et 11. (À noter : l'auteure fait parfois référence à des concepts abordés dans le deuxième chapitre. Je reviendrai sur ces éléments lors de la 2e séance (17 janvier) pour que vous puissiez comprendre ces références).

Le troisième texte est le chapitre cinq d'une recherche de Mazarr et al. (2019) publiée par le *think tank* américain RAND. Dans ce chapitre, Mazarr et al. (2019) examinent les effets des campagnes de manipulation et de désinformation menées par la Russie ces dernières années – et les différentes techniques pouvant être utilisées dans le cadre de celles-ci – sur

[1] Office québécois de la langue française. S.d. *Le grand dictionnaire terminologique*. Québec. https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26529572

différents publics aux États-Unis, au Royaume-Uni, en France, en Allemagne, en Pologne et dans les pays baltes. Vous examinerez les constats des auteur.es qui, à la lumière de diverses sources d'information (enquêtes d'opinion, discours et orientations politiques, etc.), avancent que ces campagnes de la Russie n'auraient pas eu les effets escomptés. Veuillez noter que le texte de Mazarr et al. (2019) a été publié avant l'invasion de l'Ukraine par la Russie, en 2022, avec tous les bouleversements provoqués par ce premier conflit interétatique majeur en Europe depuis la fin de la Seconde Guerre mondiale.

Rappel important : dans votre analyse de quatre pages des deux textes choisis, ne cherchez pas à tout expliquer. Il s'agit d'un exercice de synthèse. Ciblez les éléments clés des textes examinés. Ce faisant, citez les pages où vous puisez vos exemples pour appuyer votre argumentaire. Après avoir restitué les principaux constats des auteur.es et fait des liens entre leurs travaux, vous pouvez partager en conclusion votre regard critique quant aux thèses présentées.

Après avoir rédigé votre analyse, vous partagerez lors de ce 1er atelier vos observations avec vos collègues lors d'une discussion en classe que j'animerai. Pour faciliter les échanges, la classe sera divisée en trois groupes, chacun avec une période préalablement assignée.

L'évaluation de votre travail tiendra compte de votre compréhension des questions soulevées ainsi que de votre capacité à commenter les constats des auteur.es et à effectuer des liens entre leurs enquêtes. La rigueur de votre analyse et la qualité de la langue seront également notées, de même que votre participation à l'atelier. Votre travail doit être sauvegardé dans le fichier « Atelier 1 » sur Studium au plus tard le **13 février à 23h30**.

Atelier #2 : étude du cas iranien – 28 février (5%)

Au cours des dernières années, l'Iran a été le théâtre d'importantes révoltes antigouvernementales, dont une majeure à l'automne 2022. Lors de ces révoltes, les manifestant.es utilisent internet, les médias sociaux et les technologies numériques pour communiquer, s'organiser et contester le régime en place. En contrepartie, ces outils sont utilisés par le régime pour surveiller, censurer et réprimer les manifestant.es et leurs leaders.

Pour la préparation du 2e atelier, je vous invite à réfléchir à ces enjeux en **commentant sur Perusall les deux reportages** assignés pour la séance du 28 février. Le premier reportage fait référence à une période de contestation en Iran à la fin de 2017 et au début 2018. Il détaille le rôle joué par les médias sociaux dans les manifestations (dont Telegram, une plateforme permettant d'envoyer des messages chiffrés qui comptait plus de 40 millions d'utilisateur.trices en Iran lors de cette période selon les estimations). Le deuxième reportage fait état des cybertactiques et du logiciel SIAM utilisé par le régime iranien en 2022 pour traquer et museler ses opposant.es politiques.

Dans votre analyse des deux textes sur Perusall, je vous encourage à mobiliser les auteur.es étudié.es lors des séances précédentes, en particulier celle du 21 février (voir le

PowerPoint). Leurs observations sur différents cas, incluant la révolte populaire en Iran en 2009, alimenteront votre réflexion en prévision de la discussion du 2e atelier.

Pour faciliter les échanges lors de l'atelier 2, la classe sera divisée en trois groupes, chacun avec une période préalablement assignée. Rappelons que Perusall est une plateforme de lecture interactive et collaborative vous permettant de commenter les lectures en ligne, de poser des questions ou de répondre à celle.s d'un.e collègue.

Votre participation sur Perusall (3%) sera évaluée en fonction de la pertinence de vos interventions (questions, commentaires, échanges, etc.). Ces interventions doivent être faites sur Perusall **au plus tard à 8h00 le 28 février**, **avant** le début de l'atelier 2. La qualité de votre participation lors de l'atelier sera également notée (2%).

Atelier #3 : l'internet clandestin, un espace de résistance? – 20 mars (5%)

L'internet clandestin (aussi appelé *dark web* ou *darknet*) est régulièrement dépeint par les médias comme un espace florissant pour la conduite d'activités criminelles les plus sombres. Mais le *dark web* est aussi un lieu d'échanges et de résistance pour des militant.es politiques, des journalistes et des lanceur.ceuses d'alertes. Lors de ce troisième atelier, nous discuterons de ces enjeux. Pour vous préparer, vous lirez et commenterez **sur Perusall** les textes assignés pour la séance. Vous partagerez ensuite vos observations en classe selon le même mode de participation que pour les autres ateliers.

Votre participation sur Perusall (3%) sera évaluée en fonction de la pertinence de vos interventions (questions, commentaires, échanges, etc.). Ces interventions doivent être faites sur Perusall **au plus tard à 8h00 le 20 mars**, **avant** le début de l'atelier 3. La qualité de votre participation lors de l'atelier sera également notée (2%).

Atelier #4 : étude de cas de la controverse entourant l'espionnage de journalistes au Québec (35%) – 3 avril – *remise du travail le 2 avril à 23h30 au plus tard, merci*.

Le 31 octobre 2016, le quotidien *La Presse* révèle que le Service de police de la Ville de Montréal (SPVM) a espionné le téléphone intelligent de son journaliste / chroniqueur Patrick Lagacé. Le reporter a fait l'objet de 24 mandats de surveillance policière autorisés par la justice afin (entre autres) « d'obtenir les appels entrants et sortants » sur son iPhone et d'activer le système GPS « afin de savoir exactement où il se trouvait » (Teisceira-Lessard 2016). Cette histoire constituait le début d'une série de révélations faisant état de l'espionnage de nombreux journalistes par des forces policières au Québec. Dans la foulée de ce scandale, deux projets de loi sur la protection des sources journalistiques ont été adoptés à Ottawa, en 2017, et à Québec, en 2018.

Cette controverse soulève plusieurs questions entourant la pratique du journalisme en démocratie dans un contexte de surveillance. Pour vous préparer à ce quatrième atelier, vous produirez un travail **de 6 pages** à double interligne afin d'examiner les ramifications de ce scandale sur le plan politique, policier, juridique, journalistique et technologique. Prêtez attention aux différents acteurs et actrices de ces évènements, ainsi qu'à leurs

motivations et leurs stratégies. Utilisez les quelques références suggérées à la séance 13 (3 avril) comme point de départ pour votre recherche. Cette histoire a été abondamment couverte et vous ne manquerez pas de sources journalistiques, de rapports et autres travaux, dont ceux d'une Commission d'enquête (la « Commission Chamberland »), pour analyser le sujet. Vous pouvez aussi faire des liens avec les travaux d'auteur.es de ce cours, dont l'article de Lyon (2017).

Lors de la discussion en classe, nous effectuerons un exercice s'apparentant à un jeu de rôle pour mieux comprendre les motivations et les rapports de force des parties prenantes de cette controverse (forces policières, journalistes espionné.es, responsables de médias et politicien.nes).

Votre travail sera évalué en tenant compte de votre compréhension des enjeux soulevés par cette controverse sur le plan politique, policier, juridique, journalistique et technologique, ainsi que votre capacité à expliquer les motivations des parties prenantes. La rigueur de votre analyse et la qualité de la langue seront également notées, de même que votre participation à l'atelier. Veuillez sauvegarder votre travail dans le fichier « Atelier 4 » sur Studium le **2 avril à 23h30h** au plus tard.

Enfin, à la fin de la session, vous effectuerez une **analyse finale** portant sur la matière vue dans l'ensemble du cours. Les questions de l'analyse vous seront transmises le **mercredi 17 avril 2024** via Studium. Je vous poserai des questions à développement qui porteront sur la matière vue lors des séances et les lectures assignées pour ces séances. Vous pourrez consulter vos notes, les présentations PowerPoint et les lectures pour répondre aux questions. La collaboration n'est pas permise. L'analyse finale comptera pour **35 %.** Vous aurez une semaine pour la compléter, c'est-à-dire jusqu'au **24 avril avant 23h30.** Vous remettrez votre analyse finale sur Studium en la sauvegardant en format PDF dans le dossier intitulé « Analyse finale. »

L'**évaluation** de l'analyse finale se fera selon une grille d'évaluation qui tiendra compte de la compréhension de la matière, de la clarté du propos, de la pertinence de l'analyse et de la qualité de la langue.

Propriété intellectuelle et droit à l'image

Les activités d'enseignement dans le cadre de ce cours sont protégées par les droits d'auteur et le droit à la vie privée, dont le droit à l'image. Il est interdit de faire une captation audio ou vidéo du cours, en tout ou en partie, sans le consentement écrit du professeur.
Le professeur est titulaire des droits d'auteur sur ses œuvres qui incluent, notamment, l'ensemble de ses outils pédagogiques (plans, présentations PowerPoint, vidéos, questions, exercices, etc.). Les outils pédagogiques mis en ligne par les professeur.es le sont pour le bénéfice personnel des étudiant.es et ne sont pas destinés à être retransmis ou autrement publiés ou redistribués. L'usage de tout document déposé sur Studium est assujetti à l'engagement de chaque étudiant.e à respecter la propriété intellectuelle et le droit à l'image du professeur.

Rappel de règlements pédagogiques

Veuillez prendre note que le trimestre commence le 8 janvier et se termine le 30 avril 2024 (incluant la période des examens) et que la présence physique est attendue à tous les cours. Aucune demande d'examen différé ne sera acceptée sans motif valable. Nous entendons par motif valable, un motif indépendant de votre volonté, tel que la force majeure, le cas fortuit ou une maladie attestée par un certificat de médecin.

Absence à un examen

Il est de votre responsabilité de motiver, en remplissant le formulaire disponible dans le **Centre étudiant**, toute absence à une évaluation ou à un cours faisant l'objet d'une évaluation continue dès que vous serez en mesure de constater que vous ne pourrez pas vous présenter à une évaluation. Vous devez obligatoirement fournir les pièces justificatives **dans les sept jours suivant l'absence.**

Délai pour la remise d'un travail

Vous devez motiver, en remplissant le formulaire disponible dans le **Centre étudiant**, toute demande de délai pour la remise d'un travail et fournir les pièces justificatives dès que vous êtes en mesure de constater que vous ne pourrez pas remettre à temps le travail.

La pénalité imposée pour les retards dans la remise des travaux est de 10 points de pourcentage par jour. Cette pénalité est calculée en déduisant 10 points de pourcentage à la note obtenue pour le travail en question (par exemple, la pénalité sera de 4 points par jour de calendrier pour un travail valant 40 points). Il s'agit de la politique « par défaut » du Département; le corps enseignant est libre d'imposer une pénalité plus élevée s'il le désire. La personne étudiante qui remet son travail après 23h30 sur Studium le jour de la remise est réputée les avoir remis le matin du jour ouvrable qui suit et les jours non ouvrables sont comptés comme des jours de retard.

Prévention du plagiat

Le Département porte une attention toute particulière à la lutte contre le plagiat, le copiage ou la fraude lors des examens. Le plagiat consiste à utiliser de façon totale ou partielle, littérale ou déguisée le texte d'autrui en le faisant passer pour sien ou sans indication de référence à l'occasion d'un travail, d'un examen ou d'une activité faisant l'objet d'une évaluation. Cette fraude est lourdement sanctionnée.
Tous les étudiant.es sont invité.es 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.**

Bibliothécaire et règles bibliographiques

Il est obligatoire de respecter les règles de présentation et de citations/références (modèle de Chicago pour les travaux et examens maison du Département de science politique). Deux guides à cet effet sont disponibles sur le site du département aux adresses suivantes:

Pour la présentation des travaux:
https://bib.umontreal.ca/economie-politique-relations-industrielles/science-politique

Pour les citations et références:
https://bib.umontreal.ca/citer/styles-bibliographiques/chicago

N'hésitez pas à profiter des services de la bibliothécaire spécialisée en science politique Julia Généreux Randall. Vous pouvez la rejoindre à son bureau (local 3017 de la Bibliothèque des lettres et sciences humaines, Pavillon Samuel-Bronfman) ou lui envoyer un courriel. La BLSH met aussi à disposition un Guide internet, point de départ idéal pour toute recherche documentaire en science politique.

Le harcèlement, y compris à caractère sexuel

Il incombe à chaque membre de la communauté universitaire de se conduire avec respect en tout temps envers tout le monde. En particulier, le Département de science politique s'engage à créer un milieu accueillant et sécuritaire pour toutes et tous, quelle que soit leur identité. Les documents suivants ont des démarches pratiques à suivre : Si vous pensez que vous vivez du harcèlement : https://respect.umontreal.ca/obtenir-de-laide/vous-vivez-une-situation-difficile/. Si on s'est confié à vous ou si vous êtes témoin de harcèlement : https://respect.umontreal.ca/obtenir-de-laide/vous-avez-ete-temoin-dune-situation/. Pour toute autre question : https://respect.umontreal.ca/accueil/

Besoin d'écoute? Situation de détresse?

Vous pouvez faire appel à plusieurs **lignes d'écoute** ou d'urgence. Vous avez accès à un service 24 heures/7 jours offert par l'Alliance pour la santé étudiante au Québec. Le numéro est le suivant : 1-833-851-1363. Vous retrouverez les services d'aide disponibles sur le site du Service à la vie étudiante : https://toutlemondeadesbas.ca/
Vous pouvez aussi faire appel à une **sentinelle.** La sentinelle est employée par l'UdeM, formée et disponible pour vous accueillir, vous écouter et vous orienter vers les bonnes ressources. Son accueil est spontané, respectueux et strictement confidentiel. Le service est offert en plusieurs langues. Bottin des sentinelles :
http://cscp.umontreal.ca/activiteprevention/sentinelle.htm

Si vous souhaitez discuter avec des pairs du stress que peut occasionner la vie étudiante, le local du **PASPOUM** au C-3144 est ouvert (3e étage, Pavillon Lionel-Groulx). Une personne étudiante formée à l'écoute active pourra vous orienter vers des ressources appropriées. Le local du PASPOUM est aussi un espace où vous pouvez déconnecter pendant quelques instants. Consultez les heures d'ouverture et les activités du PASPOUM sur la page Facebook. Vous pouvez vous abonner au compte Instagram du même nom pour suivre les actualités.

Calendrier des séances et des lectures assignées

1. Introduction : présentation du cours, des objectifs et des modalités d'évaluation – 10 janvier

PARTIE I – Mise en contexte, propositions théoriques et concepts clés

2. Présentation de concepts clés et réflexion sur le phénomène de surveillance – 17 janvier

Lyon, David. 2017. « La surveillance globale dans un monde post-Snowden. » *Communiquer*, no. 20: 49-65. https://bit.ly/3aWa1cJ

Lecture suggérée pour réfléchir aux théories et concepts en lien avec la lecture de Jamieson (2021) pour le premier atelier :

Hébert, Virginie, Gabrielle Sirois et Émile Tremblay-Potvin. 2015. « Les effets des médias à l'ère du 2.0 ». Rapport de recherche présenté au Centre d'études sur les médias, sous la direction de Thierry Giasson. https://bit.ly/3ijXVBm

Visionnement d'un reportage sur le phénomène de surveillance avec Edward Snowden.

3. Technologies de « libération » ou technologies de contrôle, de répression et de désinformation ? Retour sur les visions cyberoptimiste et cybersceptique – 24 janvier

Diamond, Larry. 2010. « Liberation Technology. » *Journal of Democracy* 21 (3): 69-83.

Tucker, Joshua A., Yannis Theocharis, Margaret E. Roberts et Pablo Barberá. 2017. « From Liberation to Turmoil: Social Media and Democracy. » *Journal of Democracy* 28 (4): 46-59.

PARTIE II – Régimes autoritaires : cybersurveillance et répression

4. Le marché de la surveillance en ligne – 31 janvier

Deibert, Ronald J. 2023. « The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. » *Foreign Affairs*, January/February.

Reporters sans frontières. 2020. « RSF inaugure « La Bibliothèque libre » - un centre numérique de la liberté de la presse au sein d'un jeu vidéo. » https://bit.ly/3jOr2K2

5. La Chine : contrôle, censure et surveillance de masse – 7 février

Qiang, Xiao. 2019. « The Road to Digital Unfreedom: President Xi's Surveillance State. » *Journal of Democracy* 30 (1): 53-67.

Visionnement d'un reportage sur la surveillance de masse en Chine et discussions.

6. Atelier #1 : étude de cas – quels effets peut-on attribuer aux opérations d'influence menées par la Russie ? – 14 février (20%) – *remise de l'analyse sur Studium le 13 février à 23h30 au plus tard, merci*.

Veuillez consulter dans la section « Évaluation » du plan de cours les instructions pour l'Atelier 1 et le travail de 4 pages à produire en préparation pour cet atelier.

Jamieson, K. H. 2021. *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't and do know*. New York: Oxford University Press (p. 1-16; 159-178 et 187-195). (Accédez au livre numérique en recopiant le titre dans l'outil de recherche Sofia).

Mazarr, Michael J. et al. 2019. « Does Hostile Social Manipulation Work? Measures of Success in Russian Activities in Europe and the United States ». Dans *Hostile Social Manipulation : Present Realities and Emerging Trends*. Sous la direction de Michael Mazarr et al., p. 167 à 224. Santa Monica, CA: RAND Corporation. https://bit.ly/3WRZghQ

Zerback, Thomas, Florian Töpfl et Maria Knöpfle. 2021. « The disconcerting potential of online disinformation: Persuasive effects of astroturfing comments and three strategies for inoculation against them ». *New Media & Society* 23 (5): 1080-1098.

PARTIE III – Résistance en ligne au sein de régimes autoritaires et démocratiques

7. Médias sociaux et mobilisation politique : le printemps arabe et autres cas d'étude – 21 février

Faris, David. M. 2012. « La révolte en réseau : le **«** printemps arabe » et les médias sociaux. » *Politique étrangère, no.* 1: 99-109. https://bit.ly/3WKmeqW

Poell, Thomas et Josée van Dijck. 2017. « Social Media and New Protest Movements. » Dans *The SAGE Handbook of Social Media*, sous la direction de Jean Burgess et al., 546-61. London : SAGE Publications.

8. Atelier #2 : étude du cas iranien – 28 février (5%)

*Veuillez consulter dans la section « Évaluation » du plan de cours les instructions pour l'Atelier 2. Les lectures suivantes doivent être lues et commentées sur la plateforme Perusall (voir le lien dans Studium) **au plus tard à 8h00 le 28 février**, **avant** le début de l'atelier 2.*

Biddle, Sam et Murtaza Hussain. 2022. « Hacked documents: how Iran can track and control protesters' phones. » *The Intercept*, 27 octobre. https://bit.ly/3WQuoxY

CBC. 2018. « Social media plays 'extremely important' role in Iranian protests despite censorship. » *CBC News*, 4 janvier. https://bit.ly/3QfTMe9

9. Semaine de lectures – 6 mars (pas de cours)

10. Cyberactivisme: les cas de Wikileaks, d'Anonymous et de DDoSecrets – 13 mars

Loveluck, Benjamin. 2021. « Les ruses du hacktivisme, aux frontières de l'engagement politique : retour sur Anonymous. » *Quaderni* 2 (103) : 71-88. https://bit.ly/3uSydHj

11. Atelier #3 : l'internet clandestin, un espace de résistance? – 20 mars (5%)

Veuillez consulter dans la section « Évaluation » du plan de cours les instructions pour l'Atelier 3. Les lectures suivantes doivent être lues et commentées sur la plateforme Perusall (voir le lien dans Studium) ***au plus tard à 8h00 le 20 mars****,* ***avant*** *le début de l'atelier 3.*

Kumar, Aditi et Eric Rosenbach. 2019. « La vérité sur le Dark Web: conçu pour protéger les dissidents politiques, il dissimule aussi des activités illicites ». *Finance et Développement*, septembre : 22-25. https://bit.ly/3ihbJMW

Dimitrios, Kavallieros et al. 2021. « Using the Dark Web » Dans *Dark Web Investigation*, sous la direction de Babak Akhgar et al., 27-48. Sheffield, UK : Springer https://bit.ly/3Qk6nNe

Autre lecture suggérée (facultative)

Coutu, Simon. 2022. « Canadian HQ, le *darknet* bien de chez nous: Comment le CRTC a fermé le plus gros marché canadien du web clandestin ». *Radio-Canada*, 30 novembre. https://bit.ly/3ZhnnIn

PARTIE IV – Surveillance, désinformation et répression numérique en démocratie

12. Démocratie, désinformation et répression numérique transnationale – 27 mars

Bennett, Lance W. et Steven Livingston. 2018. « The disinformation order: Disruptive communication and the decline of democratic institutions ». *European Journal of Communication* 33 (2): 122-139.
Al-Jizawi, Noura et al. 2022. « Psychological and Emotional War: Digital Transnational Repression in Canada ». *Citizen Lab Research Report No. 151*, University of Toronto, March 2022. https://bit.ly/3X3vFkU

Lecture suggérée sur les solutions éducatives à l'enjeu de la désinformation:

Landry, Normand. 2018. « Alphabétiser à l'actualité : examen des réponses éducatives aux fausses nouvelles. » Dans *Les fausses nouvelles, nouveaux visages, nouveaux défis*, sous la

direction de Florian Sauvageau, Simon Thibault et Pierre Trudel, 173-94. Québec : PUL. (Accédez au chapitre en recopiant le titre de ce livre numérique dans Sofia).

13. Atelier #4 : étude de cas sur l'espionnage de journalistes au Québec – 3 avril (35%)

Veuillez consulter dans la section « Évaluation » du plan de cours les instructions pour l'Atelier 4 et le travail de 6 pages à produire en préparation pour cet atelier.

Pistes de recherche :

Canada. 2017. *Loi sur la protection des sources journalistiques*. L.C. 2017, ch. 22. https://bit.ly/3vypYxK

Québec. 2017. *Commission d'enquête sur la protection de la confidentialité des sources journalistiques*. Québec. https://shorturl.at/wCGRU

Québec. 2018. *Loi sur la protection de la confidentialité des sources journalistiques*. Chapitre P-33.1. LégisQuébec. https://bit.ly/3eLP6u5

Radio-Canada. 2018. « Commission Chamberland. » https://bit.ly/3xQT25M

Trudel, Pierre. 2016. « Journalisme et démocratie. » *Le Devoir*, 1er novembre 2016. https://bit.ly/3eR9fPk

TVA. S.d. « Journalistes espionnés. » *TVA Nouvelles*. https://bit.ly/3ug86rh

14. Conclusion : jeu de simulation sur la désinformation, retour sur la matière et perspectives – 10 avril

15. Affichage des questions de l'analyse finale (35%) sur Studium – 17 avril

*L'analyse finale doit être remise **le 24 avril avant 23h30**, dans le fichier « Analyse finale » sur Studium (séance 15).*