

PROFESSEURE : Esma Aïmeur
Local : 2361 du Pavillon André-Aisenstadt
Courriel : aimeur@iro.umontreal.ca

Site Internet : <http://www.iro.umontreal.ca/~aimeur/>
Directrice du laboratoire TALENT : <http://www-labs.iro.umontreal.ca/~talent/>

HORAIRE : à déterminer

DESCRIPTION DU COURS

Le but de ce cours intrinsèquement **multidisciplinaire**, est de présenter le traitement des connaissances de différents *types* et selon différents *contextes*.

Je commencerai par une introduction à l'intelligence artificielle de manière générale et aux systèmes d'apprentissage, en particulier « Adversarial learning » et « Reinforcement learning ».

J'aborderai les systèmes de recommandation, les agents conversationnel « chatbots », ainsi que les aspects éthiques de l'intelligence artificielle.

Le cours sera fortement axé sur *l'aspect humain* de la sécurité des données personnelles. Il sera question de menaces informatique, de vol d'identité, de préservation de la vie privée et de « Fake news ».

Je présenterai différentes technologies de l'information et de la communication, notamment les moteurs de recherche, les outils de partage et de diffusion de connaissances, les réseaux sociaux et les applications mobiles.

Avec l'émergence de technologies de plus en plus performantes, une invasion progressive de la vie privée s'est produite. Nous allons présenter les plus invasives et aborder l'aspect éthique de l'usage de ces technologies. Nous verrons notamment les avantages et inconvénients des réseaux sociaux et des forums de discussion.

Une autre partie du cours concerne le commerce électronique (*profiling*, recommandation de produits, négociation, paiement en ligne etc.). Un accent sera mis sur la sécurité des informations collectées qui permettent aux utilisateurs d'accéder aux services en ligne au prix d'une divulgation de leurs données personnelles. Ces dernières sont exploitées à des fins économiques (publicités ciblées, revente...) mettant parfois en danger la vie privée de leurs usagers. Les données personnelles étant devenues des actifs monnayables, nous étudierons les différents impacts sur la société et verrons les changements du comportement que l'on peut observer chez l'individu si ces données venaient à être vendues par leurs propriétaires, ou révélées à des tiers.

Par ailleurs, bien qu'étant le principal moyen pour informer les usagers de l'utilisation de leurs données privées, les politiques de confidentialité sont en général ignorées. Pour causes, les utilisateurs les trouvent trop longues et trop vagues, elles utilisent un vocabulaire souvent difficile à comprendre.

Un cours d'introduction à l'informatique quantique sera présenté pour faire la différence entre l'information classique et l'information quantique. Cette dernière ne peut être lue ni copiée sans être perturbée, elle ne peut être diffusée à plusieurs destinataires et quelques fois elle semble se propager instantanément.

Pour finir, je présenterai l'apprentissage à distance : le e-Learning et l'apprentissage humain (Systèmes Tutoriels Intelligents) en mettant un accent particulier sur l'aspect interaction Humain-Machine, ce qui nous amène à traiter de la coopération, de la collaboration et des conflits entre apprenants dans un contexte où l'apprentissage est devenu désormais informel.

PRÉALABLE

Il est souhaitable mais **non obligatoire** que l'on ait suivi le cours d'intelligence artificielle.

ÉVALUATION

Chaque étudiant(e) aura à faire une synthèse d'articles (rédigée **en français ou en anglais** sous forme d'un article de recherche) accompagnée d'un exposé oral de 15 minutes, et d'un projet à programmer (en équipe).

Les langages possibles sont C, C++, JAVA, Python, PHP ou Ruby On Rails.

- Projet : 50 %
- Synthèse et exposé : 50 % (30 % pour la synthèse et 20 % pour l'exposé oral)

Je ferai appel à quelques conférencier(e)s pour enrichir le cours.

PLAN DU COURS

(Le nombre d'heures consacrées aux sujets est indiqué approximativement entre parenthèses)

1. Introduction (2)

2. Intelligence artificielle (concepts de base) (4)

Historique, Systèmes à base de connaissances, apprentissage symbolique automatique, données cryptées, systèmes de recommandations, « agents conversationnels », chatbots, éthique de l'intelligence artificielle.

3. Connaissances sensibles (8)

Sensibilisation à la sécurité des données personnelles
Principales menaces sur internet (exp : « phishing », « doxing »)
Vie privée (préservation et détection de la violation de la vie privée)
Vol d'identité
"Computer Forensics"
Aspects humains de la sécurité

3. Fake new (2)

Techniques de détection
Techniques de prévention
Apprentissage machine pour Fake news

4. Éthique (2)

Normes et standards
Les principes de persuasion de Cialdini
La manipulation en ligne
(Santé, éducation, finances etc).

5. Technologies de l'information et de la communication (TIC) (8)

Partage et diffusion de connaissances.
Moteurs de recherche, Réseaux Sociaux Applications mobiles :
(Google Search, Youtube, TikTok, Facebook, LinkedIn, Instagram, Pinterest, Snapchat, Google+, Netflix, Spotify etc.)

Géolocalisation
Extraction d'informations sur Web (Web Usage Mining)
Web analytics
Référencement Web

6. Traitement de la connaissance en Commerce électronique (6)

Identification des besoins des clients
Techniques de personnalisation (Profiling)
Recommandation de produits (films, livres, etc.)
Négociation (types de négociation, protocoles de négociation, systèmes de négociation)
Paiement électronique, sécurité (cryptographie : confidentialité et intégrité)
Aspect économique de la vie privée
Marché des données personnelles

7. Information classique versus quantique (2)

Définitions
Propriétés
Applications (cryptographie, calcul quantique, téléportation, pseudo-télépathie)

8. Apprentissage Humain : Systèmes Tutoriels Intelligents (4)

Curriculum
Modèle de l'apprenant
Stratégies tutorielles
Interfaces humain machine
Les systèmes tutoriels intelligents sur Web

9. Traitement de l'information pour l'apprentissage à distance : e-Learning (2)

Learning Management System (LMS)
Learning Content Management System (LCMS)
Virtual Classrooms (Web conferencing)
Authoring tools, Simulation tools, Assessment tools
Universités virtuelles
Plateformes
Préservation de la vie privée en e-Learning

RÉFÉRENCES

Aucun livre n'est obligatoire pour ce cours. Pour celles et ceux qui veulent en savoir plus, je recommande les ouvrages suivants.

Russell, S., Norvig P. (2019). "Artificial Intelligence: A Modern Approach". Prentice-Hall.

Blau, A., Burt, A., Groyberg, B., Yampolskiy, R. (2019). "Cybersecurity: The Insights You Need from Harvard Business Review". Harvard Business Review Press.

Carissa Véliz. (2021). " Privacy is Power: Why and How You Should Take Back Control of Your Data". Bantam Press.

Michael Bazzell. (2020). " Extreme Privacy: What It Takes to Disappear ". Independently published.

Laurent Alexandre. (2018). "La Guerre des Intelligences", Jc. Lattès.

Daniel Kahneman. (2013). "Thinking Fast and Slow" Farrar, Straus and Giroux, New York.

Francois-Bernard Huyghe (2019). " Fake News, la Manipulation en 2019", VA Editions.

Gheraouti, S. (2016) "Sécurité informatique et réseaux", 5^{ème} édition, Dunod.

Yann Lecun. (2019). "Quand la machine apprend", Odile Jacob.

Idriss Aberkane. (2018). "L'Age de la Connaissance", Robert Laffont.

Dominique Boullier. (2019). "Sociologie du Numérique", Armand Collin.

Richard Thaler. (2018). "Misbehaving", 2018. Points.

Hallas, Bruce. (2018). "Re-Thinking the Human Factor: A Philosophical Approach to Information Security Awareness Behaviour and Culture." Hallas Institute.

Collectif (2015). "Sécurité informatique, Ethical Hacking, apprendre l'attaque pour mieux se défendre " Eni Editions.

Pfleeger, C.P., Pfleeger, S.L. and Margulies, J. (2015). "Security in Computing." 5ème édition," Prentice Hall.

Bruce Schneier. (2018). "Click Here to Kill Everybody: Security and Survival in a Hyper-connected World." W. W. Norton & Company.

Evan Selinger, Jules Polonetsky, and Omer Tene. (2018). "The Cambridge Handbook of Consumer Privacy." Cambridge University Press.

Ted Claypoole, Theresa Payton, Swecker Chris. (2016). "Protecting Your Internet Identity: Are You Naked Online?." Rowman & Littlefield Publishers.

Turban, E., King, D., Lee, J.K., Liang, T-P., Turban, D. (2015) Electronic Commerce, A Managerial and Social Network Perspective. 8th edition, Springer.

Byron Reese. (2018). "The Fourth Age: Smart Robots, Conscious Computers, and the Future of Humanity." Atria Books.

Max Tegmark. (2018). "Life 3.0: Being Human in the Age of Artificial Intelligence". Vintage books.

Marc Goodman. (2015). "Future Crimes: Inside The Digital Underground and the Battle For Our Connected World." Doubleday.

Edward Snowden. (2019). " Mémoires Vives" Editions le Seuil.

Cathy O'neil (2017). "Weapons of Math Destruction ", Broadway Books.

Rayna Stamboliyska. (2019). "La Face Cachée d'Internet", Larousse.

Richard Bloom (2013). "Foundations of Psychological profiling, Terrorism, Espionage and Deception", CRC Press.