Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB6063 Gr. 01
Titre : Méthodes avancées en cybersécurité basée sur l'intelligence artificielle
Session : Hiver 2026 **Horaire et local**
Professeure : Bouhaddi, Myria

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera en mesure d'appliquer des techniques d'intelligence artificielle pour la cybersécurité ainsi que la sécurisation des systèmes basés sur l'intelligence artificielle.

Contenu

Éléments de base de l'intelligence artificielle (IA). Application des techniques d'apprentissage automatique et de raisonnement pour la sécurité des systèmes informatisés : détection de vulnérabilités, détection d'intrusions, classification de malwares, identification et analyse de risques. Systèmes d'attaques et de défenses autonomes basés sur l'IA. Étude des vulnérabilités des algorithmes de l'IA : empoisonnement des données, inférence des données d'apprentissage, inférence des paramètres de modèles, etc. Protection des technologies basées sur l'IA : confidentialité différentielle, génération d'exemples antagonistes, etc.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

3. Stratégies pédagogiques :

La structure pédagogique de ce cours intègre les éléments suivants :

1. **Cours magistraux** : une séance hebdomadaire de 3 heures.
2. **Devoirs** : répartis tout au long du semestre pour renforcer les concepts abordés.
3. **Projet avec présentation orale** : permettant aux étudiants de démontrer leur compréhension et d'appliquer les connaissances acquises.
4. **Deux examens** : Évaluant la maîtrise des compétences et des connaissances couvertes en cours.

4. Heures de disponibilité ou modalités pour rendez-vous :

Communication par courriel (myria.bouhaddi@uqo.ca) et via le forum de discussion.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction à l'intelligence artificielle pour la cybersécurité** • Rôle de l'IA dans la cybersécurité moderne • Typologie des problèmes de sécurité : détection, classification, décision et réponse • Panorama des approches IA utilisées en sécurité	16 jan. 2026
2	**Fondements de l'apprentissage automatique** • Données, features, labels • Apprentissage supervisé, non supervisé, par renforcement • Pipeline ML : collecte, entraînement, validation et déploiement • Surapprentissage, biais, dérive conceptuelle	23 jan. 2026
3	**Méthodes classiques d'apprentissage atomatique en cybersécurité** • Régression logistique, SVM, arbres de décision • Choix des modèles selon le problème • Métriques de performance en sécurité : ○ faux positifs / faux négatifs, précision, rappel, ROC • Étude de cas : Phishing/IDS **Devoir 1**	30 jan. 2026

4	**Détection d'anomalies et vulnérabilités** • Clustering, isolation, modèles statistiques • Détection d'intrusions réseau • Anomalies systèmes et comportements utilisateurs • Études de cas : K-means pour trafic réseau	06 fév. 2026
5	**Classification des malwares et analyse de risques** • Features statiques et dynamiques • ML supervisé vs non supervisé • Modèles hybrides • IA et analyse de risques	13 fév. 2026

6	**Autoencodeurs et détection d'anomalies avancées**
	• Limites des méthodes classiques de détection d'anomalies
	• Principe des autoencodeurs :
	  ○ Encodage / décodage
	  ○ Erreur de reconstruction
	• Autoencodeurs comme outils de détection d'anomalies
	• Étude de cas : détection d'anomalies réseau
	
	(Séance en non présentiel)
		20 fév. 2026

7	**Apprentissage profond appliqué à la cybersécurité** • Réseaux neuronaux profonds : rappel conceptuel • CNN, RNN • Applications : classification de malwares, détection d'intrusions, analyse de logs **Projet de session** **(Séance en non présentiel)**	27 fév. 2026
8	**Semaine d'études**	06 mar. 2026
9	**Examen de mi-session**	13 mar. 2026
10	**Apprentissage par renforcement dans la cybersécurité** • Principe du RL • Environnements, états, actions, récompenses • Problèmes de décision séquentielle en sécurité	20 mar. 2026
11	**Systèmes de défense automatisés basés sur l'IA** • Techniques de défense autonomes et réactives basées sur l'IA. • Détection et réponse automatique aux menaces. • Étude de cas : Développement d'un système de défense basé sur l'apprentissage automatique. **Devoir 2** **(Séance en non présentiel)**	27 mar. 2026
12	**Férié**	03 avr. 2026
13	**Vulnérabilités, attaques et défenses des systèmes d'IA** • Typologie des vulnérabilités des modèles d'IA. • Attaques contre les systèmes d'apprentissage • Défenses associées • Introduction à la confidentialité différentielle • Étude de cas : analyse d'une attaque IA et de ses contre-mesures	10 avr. 2026
14	**Présentation orale des projets**	17 avr. 2026

15	**Examen final**	24 avr. 2026

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes.

Dans le cas spécifique du cours **Méthodes avancées en cybersécurité basée sur l'intelligence artificielle,** l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 25 %**
- **Examen final : 30 %**
- **Travail de session : 25 %**
- **Devoir 1 et 2 : 20 %**

7. Politiques départementales et institutionnelles :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.
Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

1. Diogenes, Yuri, and Erdal Ozkaya. *Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics*. Packt Publishing Ltd, 2018.
2. Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc.", 2018.
3. Halder, Soma, and Sinan Ozdemir. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Packt Publishing Ltd, 2018.
4. Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019.

9. Page Web du cours :

http://moodle.uqo.ca