

Sigle : CYB1083 Gr. 01

Titre : Géopolitique du cyberspace

Session : Hiver 2026 Horaires et local

Professeur : Djerboua, Cherif

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera en mesure d'appréhender les enjeux et de comprendre les doctrines géopolitiques dans le cyberspace.

Contenu

Développement d'Internet, du dark web et du cyberspace. Contrôle et régulation du cyberspace. Respect des libertés individuelles dans le cyberspace. Conflits géopolitiques dans le cyberspace (guerre économique, combats militaires, renseignement, politique d'influence diplomatique et culturelle). Cyberconflitualité et cyberterrorisme, groupes APT. Doctrine de cyberdomination. Enjeux de souveraineté numérique et stratégies développées par les États pour renforcer leur contrôle et leur puissance dans le cyberspace.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Au terme de ce cours, l'étudiant.e sera en mesure d'analyser les enjeux géopolitiques du cyberspace et de comprendre les principales doctrines, stratégies et mécanismes de pouvoir qui y sont déployés par les acteurs étatiques et non étatiques.

3. Stratégies pédagogiques :

Le cours est offert en présentiel et s'appuie sur des exposés magistraux, des études de cas et des activités de discussion.

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

Communication par courriel (cherif.djerboua@uqo.ca). Consultation sur rendez-vous.

5. Plan détaillé du cours sur 15 semaines :

| Semaine | Thèmes | Dates |
|---------|---|--------------|
| 1 | Séance 1 – Introduction au cyberspace et à ses fondements géopolitiques <ul style="list-style-type: none"> Émergence et évolution historique du cyberspace Dimensions techniques, politiques et géographiques du cyberspace Cyberspace comme nouveau champ de rivalités internationales et de projection de puissance | 15 jan. 2026 |
| 2 | Séance 2 – Développement d'Internet, du dark web et des espaces numériques alternatifs <ul style="list-style-type: none"> Développement et architecture d'Internet Origines et usages du dark web Enjeux liés à l'anonymat, au contrôle et à la fragmentation de l'espace numérique | 22 jan. 2026 |
| 3 | Séance 3 – Gouvernance, contrôle et régulation du cyberspace <ul style="list-style-type: none"> Gouvernance d'Internet aux niveaux national et international Rôle des institutions, normes techniques et cadres juridiques Tensions entre régulation, souveraineté étatique et libertés individuelles Étude de cas non-évaluée | 29 jan. 2026 |
| 4 | Séance 4 – Libertés individuelles, surveillance et droits fondamentaux <ul style="list-style-type: none"> Protection de la vie privée et des données personnelles Surveillance étatique et privée dans le cyberspace Cadres juridiques et enjeux liés aux droits numériques | 05 fév. 2026 |

| | | |
|----|--|--------------|
| | | |
| 5 | Séance 5 – Acteurs étatiques et non étatiques du cyberspace <ul style="list-style-type: none"> • États et stratégies nationales dans le cyberspace • Entreprises privées et fournisseurs d'infrastructures • Groupes APT, organisations criminelles, hacktivistes et organisations internationales Étude de cas #1 | 12 fév. 2026 |
| 6 | Séance 6 – Cyberconflits et guerre économique <ul style="list-style-type: none"> • Cyberespionnage et opérations de renseignement • Guerre économique et sabotage numérique • Opérations d'influence et cyberopérations à visée militaire Énoncé du projet | 19 fév. 2026 |
| 7 | Séance 7 – Cyberterrorisme & APT <ul style="list-style-type: none"> • Définitions et distinctions : cyberterrorisme, cybercriminalité, cyberconflit • Menaces persistantes avancées (APT) : modes opératoires et objectifs • Impacts stratégiques et sécuritaires du cyberterrorisme | 26 fév. 2026 |
| 8 | Semaine d'études | 05 mar. 2026 |
| 9 | Examen de mi-session | 12 mar. 2026 |
| 10 | Séance 8 – Doctrines de cyberdomination et stratégies nationales <ul style="list-style-type: none"> • Doctrines cyber des grandes puissances • Concepts de dissuasion, résilience et cyberdéfense • Intégration du cyberspace dans les stratégies de sécurité nationale | 19 mar. 2026 |
| 11 | Séance 9 – Souveraineté numérique et contrôle de l'information <ul style="list-style-type: none"> • Concepts et enjeux de souveraineté numérique • Contrôle des infrastructures, des données et des flux informationnels • Stratégies étatiques visant à renforcer l'autonomie et la puissance numériques Étude de cas #2 | 26 mar. 2026 |
| 12 | Séance 10 – Droit international et normes du cyberspace <ul style="list-style-type: none"> • Applicabilité du droit international au cyberspace • Normes, responsabilités et attribution des cyberopérations • Limites du droit face aux conflits et opérations numériques | 02 avr. 2026 |
| 13 | Séance 11 – Géopolitique des technologies émergentes <ul style="list-style-type: none"> • Intelligence artificielle et rivalités stratégiques • 5G, semi-conducteurs et chaînes d'approvisionnement critiques • Informatique quantique et impacts sur la sécurité internationale Étude de cas #3 | 09 avr. 2026 |
| 14 | Séance 12 – Perspectives futures et enjeux stratégiques du cyberspace <ul style="list-style-type: none"> • Évolution des menaces et des conflits numériques • Défis futurs en matière de gouvernance et de sécurité • Enjeux émergents pour les libertés individuelles et l'ordre international | 16 avr. 2026 |
| 15 | Examen Final | 23 avr. 2026 |

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

- Études de cas : 15 %
- Projet : 20 %
- Examen de mi-session : 30 %
- Examen final : 35 %

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- 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](https://uqo.ca/biph) ou écrivez-nous au Biph@uqo.ca

8. Principales références :

1. **Mueller, M. L. (2010)**
Networks and States: The Global Politics of Internet Governance – MIT Press
2. **Broeders, D. & van den Berg, B. (Eds.) (2020)**
Governing Cyberspace: Behavior, Power and Diplomacy – Bloomsbury
3. **Amoretti, F. (2024).**
Internet Diplomacy: Shaping the Global Politics of Cyberspace. Rowman & Littlefield / Bloomsbury.

9. Page Web du cours :

<https://moodle.uqo.ca>