# Diplôme d'études supérieures spécialisées en cybersécurité - 1454

## RESPONSABLE :

### Gatineau

**Luigi Logrippo**
**Responsable de programme d'études de cycle supérieur**

**Pour de plus amples informations :**

Téléphone : 819 595-3900, poste 1614
Courriel : csinfo@uqo.ca

## SCOLARITÉ :

30 crédits, Deuxième cycle

## OBJECTIFS :

Objectifs généraux
Le programme de DESS en cybersécurité a pour objectif de préparer les futurs diplômés à une carrière professionnelle technique de haut niveau dans le domaine de la cybersécurité. Il fournit une formation de pointe pour concevoir, développer et implémenter des solutions de cyberdéfense ou pour mener des investigations numériques.

Objectifs spécifiques
Au terme de cette formation, la personne étudiante sera en mesure de :

• Comprendre les concepts théoriques et les aspects pratiques liés au domaine de la cybersécurité;
• Effectuer une analyse sur les cybermenaces;
• Sélectionner les techniques appropriées pour résoudre des problèmes spécifiques de cybersécurité;
• Appliquer des techniques avancées de l'IA pour concevoir des solutions de cybersécurité;
• Comprendre et appliquer les techniques d'analyse pour détecter des défauts dans les logiciels;
• Connaître les techniques de cryptographie et leurs applications;
• Maîtriser les techniques de cyberenquêtes;
• Se familiariser avec enjeux sociétaux et légaux concernant la cybersécurité et la protection de la vie privée;
• Savoir documenter, présenter et valoriser les résultats d'une analyse de cybersécurité, rédiger des rapports techniques et préparer des communications orales;
• Mettre en pratique ses connaissances avec la réalisation d'un stage ou la rédaction d'un essai pour la résolution de problèmes dans des domaines variés;
• Renforcer ses compétences pratiques à travers la mise en œuvre de projets d'envergures en cybersécurité.

## INFORMATIONS SUR L'ADMISSION :

| Lieu d'enseignement | Régime | Trimestres d'admission | | |
|---|---|---|---|---|
| | | Automne | Hiver | Été |
| Gatineau | TC | ✓ | ✓ | |
| | TP | ✓ | ✓ | |

TC : Temps complet
TP : Temps partiel

## CONDITIONS D'ADMISSION :

**Base études universitaires**

Être titulaire d'un baccalauréat dans l'un des domaines suivants: informatique, mathématiques, génie informatique, logiciel ou électrique ou l'équivalent obtenu avec une moyenne cumulative d'au moins 3,0 (sur 4,3) ou l'équivalent. La personne candidate doit avoir des connaissances de base en informatique et en mathématiques équivalentes aux exigences du cours MAT1023.

Tout dossier de candidature avec une moyenne inférieure à 3,0, mais supérieure ou égale à 2,8 sur 4,3 sera étudié par le sous-comité de programme et pourrait, dans certains cas, faire l'objet d'une recommandation d'admission.

Les dossiers des personnes candidates détentrices d'un baccalauréat obtenu avec une moyenne cumulative inférieure à 2,8 sur 4,3, mais égale ou supérieure à 2,5 sur 4,3 (ou l'équivalent) seront étudiés par le sous-comité de programme, à la condition de posséder une formation additionnelle et pertinente d'au moins 15 crédits universitaires (ou l'équivalent) complétés avec une moyenne cumulative d'au moins 3,0 sur 4,3 (ou l'équivalent). Ces dossiers pourront faire, dans certains cas, l'objet d'une recommandation d'admission.
Le comité d'admission du programme se réserve le droit d'imposer des cours d'appoint ou une propédeutique à la candidate ou au candidat qui ne répond pas entièrement aux conditions d'admission du programme.

Posséder une connaissance adéquate du français conformément à la politique linguistique applicable à l'UQO.

Posséder une compréhension suffisante de l'anglais.

**Base expérience**

La personne candidate n'ayant pas fait d'études universitaires, mais qui a complété des études collégiales, pourra être admis à un programme de deuxième cycle si elle ou il a au moins douze années d'expérience de travail à la fois pertinente et significative, eu égard à la discipline ou au champ d'études du programme pour lequel elle sollicite l'admission. La personne candidate doit avoir des connaissances de base en informatique et en mathématiques équivalentes aux exigences du cours MAT1023.

Dans le cas de la personne candidate qui, sans avoir complété un baccalauréat, a néanmoins obtenu des crédits universitaires, le nombre d'années d'expérience requis sera modulé en fonction des crédits obtenus et des résultats scolaires. La candidate ou le candidat pourrait devoir se soumettre à une entrevue. Elle ou il pourrait également se voir imposer des cours d'appoint ou une propédeutique.

Nonobstant ce qui précède, un dossier dont la qualité est jugée exceptionnelle pourrait être considéré pour l'admission.

## PLAN DE FORMATION :

**Cours obligatoires (24 crédits)**

| | | |
|---|---|---|
| | INF5163 | Méthodologie de recherche en informatique |
| | CYB6033 | Renseignement sur les cybermenaces et analyse de risques de cyberattaques |
| | CYB6003 | Techniques de cryptographie |
| | CYB6043 | Atelier pratique en cybersécurité |
| | CYB5006 | Stage en cybersécurité |
| | CYB6006 | Rapport de stage en cybersécurité |
| ou | CYB6012 | Essai en cybersécurité |

**Cours optionnels (6 crédits)**

| | |
|---|---|
| | Choix de deux cours dans le bloc A : Techniques avancées en cyberdéfense |
| ou | Choix de deux cours dans le bloc B : Investigation numérique |

**Bloc A : Techniques avancées de cyberdéfense**

| | |
|---|---|
| CYB6053 | Sécurité des systèmes embarqués et de l'internet des objets |
| CYB6063 | Méthodes avancées en cybersécurité basée sur l'intelligence artificielle |
| CYB6073 | Analyse statique du logiciel pour la cybersécurité |
| CYB1173 | Sécurité du logiciel (INF1563 ou INF1653) |

**Bloc B : Investigation numérique**

| | |
|---|---|
| CYB6023 | Forensique numérique avancée et réponse aux incidents |
| CYB6083 | Cadres législatifs en cybersécurité |
| CYB1073 | Cybersécurité comportementale |

## CYB1073

**Cybersécurité comportementale**

**Objectifs :** Au terme de ce cours, l'étudiant.e sera en mesure de comprendre les principaux facteurs humains de risques en cybersécurité et de décrire différentes techniques d'ingénierie sociale et les mécanismes d'influence sur lesquels ils s'appuient.

**Contenu :** Éléments de base de cybersécurité. Facteurs humains de risque en cybersécurité : erreurs et négligence, limitations et biais cognitifs. Profilage des cyberattaquants et des cyberdéfenseurs : motivations, comportements. Ingénierie sociale : mécanismes d'influence, tromperie, éléments de théorie des jeux comportementale. Risques liés aux médias sociaux et santé mentale : phénomènes de bulles, désinformation, cyberintimidation, pédo-piégeage. Problématiques psychologiques et sociales liées aux mécanismes d'authentification, choix et réutilisation des mots de passe, acceptabilité sociale de la biométrie. Techniques défensives basées sur le comportement (pots de miel, stéganographie, etc.).

## CYB1173

**Sécurité du logiciel**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura une compréhension de la problématique et des solutions pour la construction et l'évaluation de logiciels fiables dans des environnements possiblement hostiles.

**Contenu :** Vulnérabilités et faiblesses des logiciels, leur identification et gestion. Principes de conception de logiciels sécuritaires dans un environnement hostile. Attaques et robustesse contre les attaques. Gestion de la mémoire et vérification des limites. Sécurité par conception dans toutes les phases de développement, des besoins au code. Choix et utilisation de composantes fiables, identification et bonification de code faible ou vulnérable. Méthodes formelles, analyse formelle et vérification formelle de propriétés de sécurité. Méthodes de test de propriétés de sécurité. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

## CYB5006

**Stage en cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura développé des compétences pratique en milieu de travail liée aux connaissances en cybersécurité acquises dans le programme. Selon le choix de l'étudiant, le stage peut se dérouler en industrie, ou un organisme public ou parapublic.

**Contenu :** Réalisation d'un stage en milieu de travail. Par le biais d'un projet de recherche ou de développement portant sur un sujet relié à un besoin du milieu de travail et conforme aux objectifs du programme, l'étudiant devra s'initier aux méthodes de travail de l'employeur en expérimentant ses connaissances théoriques pour contribuer de manière significative aux pratiques professionnelles du milieu. Normalement, le stage est complété dans un ou deux trimestres et il conduit nécessairement à un rapport de stage.

## CYB6003

**Techniques de cryptographie**

**Objectifs :** Au terme de ce cours, l'étudiant.e sera initiée aux concepts de la cryptographie et de son application dans le domaine de la sécurité des données. Elle/Il pourra analyser différents algorithmes cryptographiques en évaluant leur sécurité, efficacité et complexité, ainsi que d'acquérir une compréhension générale des méthodes de cryptanalyse.

**Contenu :** Introduction à la cryptographie. Exemples historiques des techniques de cryptologies classiques : le chiffrement de Vigenère, le chiffrement de Hill; la cryptanalyse des crypto-systèmes classiques. La cryptographie moderne. Cryptographie à clé secrète; D.E.S., triple DES, AES, etc.; modes d'opération des chiffrements par blocs. Cryptographie à clé publique : RSA, El-Gamal, etc. Protocoles cryptographiques : authentification, distribution de clés. Fonctions de hachage : algorithmes SHA-1 et MD5.

## CYB6006

**Rapport de stage en cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura rédigé un rapport portant sur un projet réalisé lors du stage qui démontre qu'elle/il a réalisé une étude approfondie d'un sujet en cybersécurité de nature appliquée. Elle/il aura réalisé une présentation orale de son projet.

**Contenu :** Complémentaire à l'activité de stage, le rapport de stage est un exposé écrit qui documente les résultats du projet en cybersécurité réalisé lors du stage. Pour ce faire, le rapport doit démontrer une bonne connaissance des techniques et méthodes de développement dans un milieu professionnel et faire preuve des habiletés de rédaction scientifique. Il doit décrire les fondements méthodologiques des réalisations du stage, présenter les réalisations et faire état de leur évaluation en faisant montre d'un esprit critique. Le rapport de stage est suivi par une présentation orale.

## CYB6012

**Essai en cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura démontré son appropriation critique des connaissances acquises à travers un travail de recherche et de développement sur un sujet de nature théorique ou appliquée. L'étudiant.e aura développé ses compétences de rédaction et de présentation.

**Contenu :** L'essai est un exposé écrit faisant état des résultats d'un travail de recherche et de développement. L'essai doit démontrer une maîtrise des techniques et méthodes de recherche ou de développement, de la rédaction et la présentation scientifiques. Pour ce faire, l'étudiant devra décrire les fondements méthodologiques des réalisations du travail, en plus d'en réaliser une analyse critique. Normalement cette activité sera réalisée sur une période de deux trimestres, et sera complétée par une présentation orale.

## CYB6023

**Forensique numérique avancée et réponse aux incidents**

**Objectifs :** Au terme de ce cours, l'étudiant.e maîtrisera les concepts théoriques, les méthodologies et processus pour résoudre des problèmes pratiques liés au domaine de la criminalistique numérique et de la réponse aux incidents.

**Contenu :** Portrait de la cybermenace et de la cybercriminalité. Méthodologies et les processus nécessaires pour détecter les cyber-incidents. Méthodologies d'enquêtes sur les ordinateurs et les réseaux : identification, récupération et évaluation d'éléments de preuves digitaux. Étapes du processus de réponses aux incidents liés à la cybersécurité.

## CYB6033

**Renseignement sur les cybermenaces et analyse de risques de cyberattaques**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura maitrisé et mis à l'épreuve les techniques de détection, de réponse et de lutte contre les menaces persistantes avancées (APT) et les campagnes de logiciels malveillants.

**Contenu :** Introduction au concept du renseignement, métier d'analyste de risque et niveaux de renseignement sur les menaces. Planification, direction et génération des besoins en matière de renseignement. Évaluation du risque d'intrusions adverses : chaîne de destruction, modèle diamant, comportement adverse, indicateur de compromission. Sources de données pour l'analyse d'intrusion : open source intelligence (OSINT), etc. Structuration et stockage d'information sur les renseignements : techniques-tactiques-procédures (TTP), Malware Information Sharing Platform (MISP), MITRE ATT&CK, etc. Outils analytiques. Dissémination du renseignement aux niveaux tactique, opérationnel et stratégiques. Études de cas.

## CYB6043

**Atelier pratique en cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e aura réalisé un projet pratique d'envergure en cybersécurité intégrant les connaissances acquises dans les cours du programme.

**Contenu :** Le contenu du projet est variable selon les intérêts des étudiant.e.s et de l'expertise professorale disponible.

## CYB6053

**Sécurité des systèmes embarqués et de l'internet des objets**

**Objectifs :** Au terme de ce cours, l'étudiant.e sera en mesure de réaliser une analyse poussée sur menaces et des vulnérabilités associées aux systèmes embarqués et connectés dans l'internet des objets et de préserver la sécurité des applications, des données et des protocoles de communication.

**Contenu :** Introduction aux systèmes embarquées et aux architectures des systèmes dans l'internet des objets. Technologies les plus utilisées et les principales plateformes pour l'internet des objets. Vulnérabilités et menaces spécifiques aux systèmes embarqués dans l'internet des objets. Mécanismes d'authentification décentralisés. Sécurité dans les réseaux Ad-hoc : partage de secret, certification, etc. Sécurité des protocoles de communication : norme zigbee, etc. Études de cas : domotique, villes intelligentes, etc.

## CYB6063

**Méthodes avancées en cybersécurité basée sur l'intelligence artificielle**

**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.

## CYB6073

**Analyse statique du logiciel pour la cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e sera en mesure d'appliquer des techniques d'analyse statique de code et d'utiliser des outils qui implémentent ces techniques à diverses fins.

**Contenu :** Rappel du langage C et mesure de complexité d'un programme C. Objectifs d'analyse du code : exploration, compréhension, détection de défauts, etc. Défauts logiciels et conséquences sur le fonctionnement : division par zéro, décisions erronées, dépassement de la mémoire, etc. Analyse des domaines des variables, analyse du flot d'exécution. Technique et outils d'exécution symbolique de code C et application au test, à la vérification et à la cybersécurité. Réduction de la complexité du code. Introduction à l'interprétation abstraite.

## CYB6083

**Cadres législatifs en cybersécurité**

**Objectifs :** Au terme de ce cours, l'étudiant.e se sera approprié les

différentes normes et règlementations dans le domaine de la cybersécurité.

**Contenu :** Étude du problème de la cybercriminalité : infractions contre les ordinateurs et les données, fraudes et extorsions, contenu défendu, infractions contre la personne et les organisations, la cybercriminalité organisée. La loi de l'investigation informatique. La protection de la vie privée et la protection des données dans les institutions privées et gouvernementales. Les droits d'auteur. Ce cours est enseigné tenant compte de différents cadres normatifs entre l'Europe et l'Amérique du Nord.

### INF5163

**Méthodologie de recherche en informatique**

**Objectifs :** Permettre à l'étudiante ou l'étudiant de développer ses aptitudes à mener de manière efficace des travaux de recherche en informatique, ainsi que préparer des rapports, publications et présentations scientifiques de bonne qualité.

**Contenu :** Introduction aux différents types de recherche en informatique (fondamentale vs appliquée, théorique vs empirique, mémoire ou essai/stage). Méthodologie de recherche et projet de recherche : élaboration des objectifs et de la problématique, planification et gestion de la recherche et diffusion des résultats. Recherche documentaire et analyse critique de documents scientifiques. Développement, prototypage, documentation et exploitation d'algorithmes et de logiciels. Rédaction technique (rapport de progrès, mémoire, rapport d'essai ou de stage en milieu de travail, articles, demande de bourse, etc.). Présentation de quelques outils de rédaction et de présentation scientifiques. Présentation technique (ex. orale, affiche, vulgarisation). Intégrité, éthique et plagiat. Propriété intellectuelle (documents, logiciels, brevets, etc.). Partage et libre distribution de codes et de données. Aspects d'ÉDI (équité, diversité et inclusion). Valorisation des résultats et transferts technologiques. Carrières de chercheuse ou de chercheur.