le cnam
Auvergne – Rhône-Alpes

Cybercriminalités, Cybersécurité et Cyberdéfense (C3)

Cybercriminalités, Cybersécurité et Cyberdéfense (C3)

CRM210

Planning

Période	Modalité
Information Indisponible - Information Indisponible	Formation ouverte et à distance (FOAD)

CONDITIONS D'ACCES / PRÉREQUIS

Ce séminaire ne nécessite pas de pré-requis particuliers. Etant pluridisciplinaire, il aborde aussi bien des sujets de sciences politiques (politiques nationales de cyberdéfense, régulation), des aspects mathématiques (chiffrement), d'ingénierie (informatique, réseau), de stratégie et de droit. Une lecture préalable de quelques sources bibliographiques est recommandée.

OBJECTIFS PÉDAGOGIQUES

Le cours « cybercriminalités, cybersécurité et cyberdéfense» est l'enseignement magistral abordant les questions de sécurité informatique, de criminalité informatique et de cyberdéfense du Master « Sciences Criminelles » du Cnam. Cet enseignement est construit sur un équilibre entre les différentes compétences à l'œuvre dans la compréhension et la maîtrise des phénomènes de criminalité informatique :

- Une ***compétence technique***, permettant aux auditeurs de comprendre, en profondeur et non pas de façon superficielle, quels sont les tenants et les aboutissants techniques des opérations de cybercriminalité, et des systèmes de défense (cybersécurité, et cyberdéfense). Il s'agit ici, non pas de s'arrêter à une typologie ou à des définitions, mais de comprendre quelles sont les étapes d'une intrusion, comment elles sont réalisées, quelles sont les techniques utilisées, et quel est l'état de l'art technique de ces disciplines, offensives et défensives ;

- Une ***compétence organisationnelle, pénale et juridictionnelle***, permettant de comprendre quels sont les capacités et les limites des réponses autorisées par le Droit ; l'organisation de ces réponses pénale et de prévention des crimes informatiques ; incluant le savoir-faire organisationnel de mise en œuvre et de déploiement de réponses adaptées, tant pour des organisations publiques (Etat, collectivités) que privées (industrie).

- Une **compétence *informationnelle*,** permettant de comprendre les mécanismes à l'œuvre dans les campagnes de cybercriminalité s'appuyant sur les savoirs de la psychologie (« psyops »), de la théorie de l'information et des médias (campagnes de social engineering, info-déstabilisation), permettant le travail d'audit (« forensics ») et une compréhension des processus sociologiques et

sociétaux de propagation des techniques (« *hacking communities* »), des mécanismes d'engagement dans le « white hacking », afin de donner aux auditeurs de ce séminaire une perspective juste et équilibrée des enjeux et des pratiques.

La finalité de cet enseignement est de former les auditeurs à la maîtrise des risques de cybercriminalité, mais également à la formulation de politique générale et de politique de réponse adaptées, prenant en compte toutes les dimensions de cette discipline : compréhension sociologique du phénomène communautaire « hacking » (défense du droit d'expression, libertés individuelles, *open source*, logique d'innovation ouverte, etc), bonne maîtrise technique et compréhension des campagnes d'attaque (Man in the Middle, APT, etc), et une véritable compétence stratégique et organisationnelle (management de la sécurité des systèmes d'information, cadres normatifs et réglementaires, enjeux juridiques, enjeux supranationaux et géopolitiques).

Ce cours est animé par un collectif d'enseignants-chercheurs, d'experts provenant de l'industrie, du monde de la communauté « open source » de la cybersécurité et de responsables travaillant au sein d'administrations concernées.

COMPÉTENCES VISÉES

Information Indisponible

Contenu de la formation

Syllabus Général

- **Présentation du domaine de la cybersécurité : histoire, organisation, juridictions**
  - Histoire et fondations
  - Les doctrines nationales de cyberdéfense
  - Le management de la sécurité des systèmes d'information
  - L'organisation de l'Etat : réponses, juridictions
  - Introduction au chiffrement et à la cryptographie
- **La cybercriminalité, sa régulation et les savoir-faire techniques de réponse**
  - Les enjeux futurs de la recherche et de la R&D
  - Les acteurs privés de la cybersécurité : les start-ups
  - La démarche d'enquête forensic et l'interaction avec la justice
- **Enjeux stratégiques, régulation, cyberdéfense et politiques générales**
  - L'incident de sécurité et l'investigation forensic
  - Le continuum défense – sécurité
  - Cybersécurité et rupture technologique :IoT et cybersécurité
  - Le dispositif national

1. **Présentation du domaine de la cybersécurité : histoire, organisation, juridictions**

Cette introduction générale du cours présente un historique du hacking, depuis ses années pionnières au début de 1972, jusqu'aux mouvements cyberlibertaires et aux « start-ups » de cybersécurité des années 2010-2018. Le cours interroge notamment l'évolution de la pratique, ses fondamentaux et les changements de culture organisationnelle et sociétale des activités de hacking, pour analyser leur entrée progressive dans la sphère économique, puis la sphère de puissance des États nations. Le cours est un panorama de la cybersécurité, de la cybercriminalité et des activités de cyberdéfense, et leur impact sur la société.

2. **Les doctrines nationales de cyberdéfense et cybersécurité**

Ce séminaire présente les différentes doctrines et stratégies nationales de cybersécurité, et aborde plus spécifiquement la question de la graduation des réponses, les questions de droit international et d'encadrement, la cyberdiplomatie, ainsi qu'une analyse des

différentes crises internationales récentes.

3. **La sécurité des systèmes d'information**

Ce cours à pour objectif de faire prendre conscience de l'importance de la Sécurité des Systèmes d'Information et de leur management (qualité, conformité, respect des régulations et règles normatives). Le cours présente en particulier les différentes problématiques et menaces liées aux Systèmes d' Information ainsi que les précautions d'ordres techniques, humain et juridique à prendre pour lutter contre la cybercriminalité (- Enjeux juridiques liés à la pénétration d'un SI ; Cadre normatif et réglementaire ; bonnes pratiques de Sécurité des Systèmes d'Informations ; Le management opérationnel et stratégique de la SSI)

4. **Les réponses Etatiques et l'organisation de l'Etat en matière de sécurité des SI**

Ce cours présente les enjeux d'organisation et de gestion des organismes d'Etat en matière de cybersécurité et cybercriminalité, en s'attardant particulièrement sur le rôle et les missions de l'ANSSI.

5. Introduction au chiffrement et à la cryptographie : les principes fondamentaux (I)

Ce cours constitue une introduction aux méthodes de cryptographie et de chiffrement. Il présente les fondements mathématiques du chiffrement, son histoire, pour former les auditeurs à réaliser leur premier chiffrement et déchiffrement.

6. **La gestion des identités, du chiffrement et exemples pratiques et appliqués de cryptographie (II)**

Ce cours est la suite de l'introduction à la théorie de base et la pratique de techniques cryptographiques utilisées dans la sécurité informatique. Nous allons couvrir des sujets tels que le chiffrement (clé secrète et à clé publique), l'intégrité des messages, signatures numériques, l'authentification des utilisateurs, la gestion des clés, hachage cryptographique, protocoles de sécurité de réseau (SSL, IPSec), l'infrastructure à clé publique, la gestion des droits numériques.

7. **Les enjeux futurs de la recherche, de la R&D : le rôle critique de la technologie et de la recherche**

Ce cours présente le rôle central tenu par la recherche en sécurité informatique, aussi bien dans le domaine « open source » et communautaire (white hat), le domaine académique que le domaine industriel. Le cours présente les enjeux techniques futurs, et les « road-maps » potentiellement associées dans le domaine de la sécurité informatique et de la cybersécurité.

8. **Les acteurs privés de la cybersécurité : point de vue d'une start-up innovante**

Les acteurs de l'entrepreneuriat en cybersécurité jouent un rôle décisif dans la diffusion des standards avancés de chiffrement et de sécurité. Guillaume Pontallier, fondateur de la société Tanker, présente l'histoire de Tanker, les questions de certification et de régulation du secteur entrepreneurial, la dynamique d'innovation dans les jeunes start-up françaises à travers l'histoire de Tanker.

9. **La relation entre l'expert forensic et la cour de Justice**

Ce cours présente la conduite d'une enquête Forensic dans le cadre d'une expertise judiciaire, en analysant les contraintes spécifiques des enquêtes de criminalité informatique dans le cadre de procédures de justice.

10. **L'incident de sécurité et les investigations dans le domaine des menaces persistantes avancées**

Ce cours présente la définition et la description des incidents de sécurité, ainsi que la méthodologie d'investigation des menaces persistantes avancées (Advanced Persistant Threats) : le travail d'investigation, les étapes techniques, les défis et enjeux techniques, ainsi qu'un panorama des scénarios d'attaques et des systèmes de réponses.

11. **Le continuum défense - sécurité**

Le continuum défense - sécurité est désormais une évidence dans le monde réel : terrorisme, piraterie, trafics à grande échelle appellent des réponses hybrides qui combinent l'action des forces armées et celle des acteurs de la sécurité intérieure. Dans le cyberespace, ce

continuum s’observe davantage encore. La criminalité et la délinquance opèrent un transfert dans le monde immatériel, tandis que celui-ci devient un nouveau terrain de conflictualité. Dans cet espace sans frontière, il n’y a pas de « champ de bataille », ni de « zone de sécurité prioritaire » où se concentreraient des actions ciblées. La construction maillée du réseau et le développement de la mobilité confèrent à la menace un caractère polymorphe et ubiquitaire.

12.**Le Darknet : acteurs et organisations criminelles**

L’enjeu de ce séminaire est de décrire les technologies et fonctions déployées sur différents réseaux de communication qui ont fait l’objet d’une appellation Darknet et de voir quelles actions criminelles sérieuses y sont menées. Pour cela, il faut avant tout comprendre le territoire social et l’environnement économico-technologique représenté par Internet et les réseaux de communication. Nous caractériserons ensuite les Darknets afin de les regrouper par type de fonctionnalité et étudierons les destinataires de contenu. Ainsi, nous serons en mesure d’expliquer comment certaines activités criminelles invertissent la toile, dans quelle mesure et avec quel résultat. L’étude de certains comportements et techniques criminels sera également réinvestie dans une approche de lutte contre ces mêmes phénomènes subversifs.

13. **Les enjeux de sécurité des objets connectés (IoT)**

Seconde partie de la conclusion du séminaire, cette intervention aborde les questions fondamentales de défense des libertés d’expression, de création, d’invention et du respect de la vie privée dans un contexte de numérisation. Le cours retrace les grands débats, les évolutions (et reculs) des législations françaises et européennes. Le cours met en lumière les objectifs de politique générale d’un Etat dans la défense des citoyens, de leur vie privée, et des contraintes posées par les vulnérabilités des systèmes d’information contemporains. Ce cours est animé par Véronique Legrand, Professeur titulaire de la Chaire Cybersécurité du Cnam

14. **Les stratégies de réponses sectorielles et les stratégies souveraines de réponse aux menaces dites de « cyberdéfense »**

Ce cours constitue la première partie de la conclusion de synthèse au séminaire C3, organisé sous la forme d’une confrontation de différentes perspectives, issues de l’expérience des trois intervenants dans les domaines de R&D industrielle, de la recherche et des grands groupes nationaux.

Modalités de validation et d’évaluation

Contrôle continu: Contrôle de connaissances et de savoirs qui se déroule tout le long du temps de l'enseignement

Mémoire: Ecrit portant sur un sujet validé par l'enseignant

Accompagnement et suivi:

Prise en charge des auditeurs inscrits à une unité d’enseignement, depuis l’inscription jusqu’au déroulement effectif de la formation.

Parcours

Cette UE est constitutive des diplômes suivants:

[{"code":"MR12801A","code_suivi":749,"date_debut_validite":"2022-09-01","date_fin_validite":"9999-08-31","date_limite_utilisation":"9999-08-31","affichable":true},{"code":"MR12802A","code_suivi":1237,"date_debut_validite":"2023-11-20","date_fin_validite":"2025-08-31","date_limite_utilisation":"2025-08-31","affichable":true}]

ECTS: 6

Volume Horaire indicatif	Financement individuel hors tiers financeur et CPF	Tarif de référence (Employeur)
45 heures	450.00	900.00

Infos Pratiques

Durée indicative	Modalité	Période	Date de début des cours	Date de fin des cours
45 heures	Formation ouverte et à distance (FOAD)	Annuel	Information Indisponible	Information Indisponible

Dernière mise à jour: 02/07/2025 10:21:06