Les technologies numériques concourent à la compétitivité et à la croissance économique, mais dans le même temps elles constituent de nouvelles formes de risques et de menaces.
Jamais, sans doute, le prédateur n'a été aussi près de sa victime puisque au moyen d'Internet, des smartphones et des objets connectés il est partout et constamment avec elle, bénéficiant d'une capacité de nuisance inégalée dans l'Histoire. Ainsi, au mois de mai 2017, un seul virus a permis d'attaquer plus de 150 pays entraînant l'arrêt de plusieurs usines et causant des centaines de milliers d'euros de préjudice.
L'espace cyber bouleverse donc les pratiques professionnelles et les comportements individuels. Si la vie sans le numérique paraît impossible, pour autant, il convient de ne pas se laisser submerger par la vague des innovations et ainsi à s'abandonner sans défense à ces nouveaux outils.
C'est pourquoi, en vue de répondre à ces cybermenaces ainsi qu'aux inquiétudes et aux difficultés rencontrées par les professionnels des secteurs public et privé, l'ISPEC ouvre un nouveau diplôme destiné à fournir des outils pratiques et des méthodologies simples d'emploi visant à prévenir et protéger leur activité de manière efficace et à moindre coût.
Ce diplôme s'adresse à tous ceux, professionnels et étudiants, niveau master, qui souhaitent acquérir les actes réflexes, juridiques et opérationnels en matière de sécurité économique et de cybersécurité afin de mieux affronter les défis contemporains.

- Cours sur 2 jours à partir d'octobre (vendredi et samedi)
- 121 heures de cours
- Examen sous forme d'examen final écrit et mémoire
- Tarifs : Formation Continue : 1 500€ / Formation Initiale : 1 000€
- Niveau Master

Faculté de Droit et de Science Politique
Aix*Marseille Université

I-S-P-E-C

INSTITUT DE SCIENCES PENALES ET DE CRIMINOLOGIE

DIPLÔME D'ETUDES SUPERIEURES UNIVERSITAIRES « Management de la Sécurité Economique et de la Cybersécurité »

Sous la direction de Muriel GIACOPELLI, Professeur à Aix-Marseille Université et la direction adjointe de Xavier LEONETTI, Magistrat

CONTACT ISPEC
Christiane CAPPELLO
04.42.64.61.58 / christiane.cappello@univ-amu.fr
2 AVENUE Henri PONCET – 13090 Aix-en-Provence
http://ispec-facdedroit.univ-amu.fr/
Facebook : Institut de Sciences Pénales et de Criminologie – ISPEC

PROGRAMME DE LA FORMATION

UNITE 1 : Droits et stratégies juridiques (33h)

- Intelligence économique : de l'information au renseignement
- Développement des processus de veille
- Lutte contre l'insécurité et sentiment d'insécurité
- Sciences criminelles à l'ère numérique
- Criminologie et lutte contre la radicalisation
- Lutte contre la criminalité financière et organisée : ressources des réseaux et organisations criminelles
- Droit pénal des affaires : protéger l'activité économique par le droit
- Droit pénal spécial : Evolution de la matérialité des infractions
- Droit des médias et des télécommunications : respect du droit dans les espaces virtuels
- La protection pénale de la vie privée sur internet

UNITE 2 : Management de la sécurité économique (35h)

- Mondialisation de l'économie et compétitivité des nations / les enjeux de l'Intelligence économique
- Les systèmes nationaux de l'Intelligence économique
- Le recours aux données prédictives
- Droit de l'intelligence économique
- La fonction protection dans l'entreprise
- Management du risque
- Les dangers du numérique
- Les enjeux de la cybersécurité : bilan et perspectives
- L'action de l'Etat en matière de cybersécurité
- Insécurité et pensée extrême – Le cyberespace, lieu de radicalisation
- Le risque image et e-réputation
- Le cyberprotection dans l'entreprise

UNITE 3 : Prévention et lutte contre les cybermenaces (35h)

- La criminalité économique : escroqueries et autres abus de confiance
- La politique pénale du parquet en matière de lutte contre les infractions éco-fi et la cybercriminalité
- Propriété intellectuelle, lutte contre la contrefaçon et nouvelles technologies : définitions, droits et enjeux
- Renseignement douanier et lutte contre la contrefaçon
- La lutte contre la contrefaçon dans un grand groupe
- Gendarmerie nationale et prévention des cybermenaces

- La lutte contre la cyber pornographie
- Les atteintes à l'image, à la réputation et à la loi sur la presse
- Droit pénal et procédure pénale en matière de lutte contre le terrorisme

- Le piratage et le délit d'atteinte au système de traitement automatisé de données (STAD) et les nouveaux délits : les extorsions numériques, l'envoi massif de message « Spam » et les actions en déni de service, le téléchargement illégal.
- Les guides d'hygiène numérique et de la préservation de la preuve en matière cyber

UNITE 4 : Les stratégies d'influence et de gestion de la réputation (18h)

- Management et technologies de l'information
- Communication de crise
- Les dérives sectaires dans l'entreprise
- Droit et éthique de l'entreprise
- Stratégies d'influence et de lobbying : les risques informationnels liés à la e-réputation