Révolution numérique : enjeux stratégiques et géopolitiques - DFSSU

PROGRAMME

La formation sera structurée autour de 10 modules thématiques, faisant alterner cours théoriques, méthodologiques, ateliers, travaux pratiques, exercices sur scénario et travail de recherche (rédaction d'un mémoire professionnel). Des visites sur site seront également organisées, ainsi, qu'une participation au Forum International de la Cybersécurité et au Cyber 9/12 Strategy Challenge.
Les enseignements mobiliseront une approche résolument pluridisciplinaire, permettant de mettre en lumière les différents enjeux de la révolution numérique qu'ils soient techniques, géopolitiques, diplomatiques, juridiques, ou sociaux. Au cours de la formation, les modules se déclineront ainsi :

Module 1 : Du cyberespace à la datasphère : les enjeux de la révolution numérique

Il s'agît d'introduire les principaux enjeux de la transformation numérique pour la société, les entreprises, l'État et les organisations : enjeux sécuritaires et stratégiques, ubérisation, intelligence artificielle, enjeux concurrentiels, impacts sociétaux, défis pour la démocratie, questions de confiance.

Module 2 : Géopolitique des technologies numériques et enjeux de souveraineté

Ce module montre en quoi les technologies numériques – Datacenter, Cloud computing, cryptographie – posent aujourd'hui des enjeux de souveraineté pour les États et les diverses solutions qu'ils mettent en place, que ce soit sur le plan technique, logique ou juridique, pour y faire face.

Module 3 : Géopolitique des technologies numériques : Les technologies de rupture

Les enseignements de ce module proposent d'aborder la question des technologies de rupture (IA, 5G, Blockchain, Quantum computing) pour comprendre, à travers les grandes lignes de leur fonctionnement, comment elles pourraient modifier les rapports sociaux et politiques au sein de nos sociétés, et comment la concurrence et la compétition internationale qu'elles génèrent deviennent de nouveaux enjeux géopolitiques.

Module 4 : Cyberguerre : un espace de conflictualité

Ce module s'intéresse aux nouveaux enjeux de la conflictualité numérique (modes d'actions, nature des menaces, stratégies d'acteurs, surprises et ruptures stratégiques, études de cas).

Module 5 : Stratégies de puissance des États dans l'espace numérique

Il s'agît d'étudier les stratégies de puissance mise en place par différents États ou organisations via l'espace numérique (Chine, Russie, États-Unis, France, Union européenne, États d'innovation numérique : Estonie/Israël).

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Module 6 : Sécurité et stabilité du cyberespace : les enjeux de la régulation internationale

Ce module montre en quoi le cyberespace est devenu un enjeu majeur des négociations diplomatiques, comment se construit la sécurité collective à l'ère numérique (GGE, OSCE, Code of Conduct (OSC), initiatives privées, Global Commission on the Stability of Cyberspace, London process), et comment le droit international évolue pour répondre aux défis de la révolution numérique.

Module 7 : Stratégies de cybersécurité et gestion du risque numérique

Ce module assuré par des professionnels aborde les principales questions de cybersécurité qui se posent pour les entreprises et les industriels : comment analyser les risques ? comment gérer son risque cyber ? quel est l'écosystème de la cybersécurité en France ? Il se conclut par l'élaboration de scénarios d'attaque et des mises en situations.

Module 8 : Cartographier la datasphère : comment représenter l'espace numérique

La cartographie de la datasphère est un outil particulièrement performant d'aide à la décision. Ce module présente les bases méthodologiques permettant de mettre en œuvre et d'interpréter des cartes géographiques et géopolitiques de l'espace numérique.

Module 9 : Cartographier la datasphère : investigations dans l'espace numérique

Les réseaux sociaux, ainsi que l'ensemble des données en sources ouvertes sont devenus de puissants instruments de renseignements – qui peuvent être utilisés à des fins d'analyses stratégique et géopolitique (cartographie d'influence informationnelle, réseaux d'acteurs, etc.). Ce module pratique présentera des outils permettant de mettre en œuvre ce type d'investigation.

Module 10 : Révolution numérique : les données au cœur du pouvoir

Ce module présente les grands enjeux sociétaux des technologies numériques, du fait de leur capacité à réguler et anticiper des phénomènes complexes (pollution, consommation d'énergie, diffusion d'un virus, etc.) et des transformations qu'elles induisent dans les relations d'acteurs à tous niveaux. L'usage de ces outils posent néanmoins de nouvelles questions éthiques et politiques (données personnelles, vie privée, démocratie, etc.) qu'il convient de prendre en considération.

Module 11 : Forum international de la cybersécurité et participation au Cyber 9/12 Strategy Challenge

La participation à cet évènement clef de la cybersécurité internationale et au Cyber 9/12 Strategy challenge permet de fournir une vision panoramique des acteurs français et européens de la sécurité informatique et de la cyberdéfense.

Module 12 : Restitution des travaux de recherche

La restitution des travaux de recherches des stagiaires de la promotion sortante fera l'objet d'un évènement particulier, permettant de présenter aux stagiaires de la nouvelle promotion les grands enjeux et les résultats de cette formation.

Retrouvez le détail de la formation sur le site web **www.geode.science**

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

METHODES PEDAGOGIQUES

Les enseignements sont organisés en module qui comprennent :

- des cours théoriques,
- des travaux pratiques sur les outils (OSINT, cartographie),
- des travaux dirigés,
- un exercice sur scénario,
- des visites sur site,
- une participation au Forum International de la Cybersécurité et au Cyber 9/12 Strategy Challenge.