GEODE

Géopolitique de la datasphère

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

IFG Institut Français de Géopolitique

FORMATION

DIPLÔME DE FORMATION SUPÉRIEURE SPÉCIALISÉE D'UNIVERSITÉ

RÉVOLUTION NUMÉRIQUE : ENJEUX STRATÉGIQUES ET GÉOPOLITIQUES

Ouverture février 2021

www.geode.science

A propos

Géopolitique de la Datasphère (GEODE) est un centre de recherche et de formation pluri-disciplinaire sur les enjeux stratégiques de la révolution numérique, **présélectionné pour le label «Centres d'excellence» du Ministère des Armées**. Il est également le plus important bénéficiaire du programme *Cyber Initiative* de la **Fondation William et Flora Hewlett**.

Au sein de l'Université Paris 8, GEODE rassemble des chercheurs de l'Institut Français de Géopolitique, des Écoles de Saint-Cyr Coëtquidan, de l'Université de Savoie Mont Blanc, de l'ENS, de l'Université de Paris, de l'INALCO, et de l'INRIA.

Une double ambition :

- Étudier la datasphère comme un objet géopolitique à part entière
- Utiliser les ressources de la datasphère pour faire de l'analyse géopolitique

*Avec l'interconnexion globale des systèmes d'information et de communication, des pans entiers des activités humaines sont transformés en données numériques, et celles-ci se retrouvent de plus en plus au cœur des **processus de décision**. Or, ces évolutions suscitent l'émergence de **nouvelles opportunités** (économiques, politiques, organisationnelles) comme de **nouvelles menaces** (cyberattaques, cybercriminalité, actions informationnelles). Elles favorisent la montée en puissance de nouveaux acteurs non-étatiques aux activités transfrontalières et à l'ubiquité inédite qui défient la souveraineté des États. Mais elles offrent également aux États de nouveaux moyens d'exercer leurs pouvoirs régaliens. Elles transforment ainsi les rapports de pouvoir, à la fois entre les États, mais aussi entre les États, la société civile et le secteur privé.*

Objectifs de la formation

Former aux grands enjeux géopolitiques et stratégiques de la révolution numérique de nos sociétés et aux outils qui permettent d'en exploiter les données disponibles en sources ouvertes. Cette formation adossée à la recherche est assurée par des experts de la géopolitique du numérique et des professionnels de la transformation numérique et de la cybersécurité.

- Compréhension et analyse des dynamiques et des rivalités de pouvoir géopolitiques liées à la révolution numérique ;
- Identification des enjeux stratégiques à long terme de la transformation numérique et de la façon dont ils s'appliquent aux entreprises et aux États ;
- Compréhension de l'environnement stratégique dans lequel s'insèrent les organisations, publiques et privées et des principaux risques et menaces de ce nouvel environnement ;
- Compréhension des fondamentaux pour anticiper, mitiger et répondre au risque cyber ;
- Utilisation des ressources numériques pour inférer des stratégies d'acteurs ;
- Maîtrise des outils d'investigation en sources ouvertes.

Public visé

Cette formation s'adresse principalement à des professionnels issus de sciences humaines et sociales, ou de sciences de l'informatique et de l'ingénieur, dont des cadres d'entreprises, de la défense et de la diplomatie.

Elle accueille à la fois :

- Des professionnels à compétences techniques qui souhaitent une formation aux enjeux stratégiques de la datasphère ;
- Des cadres en stratégie qui ont besoin de se former aux questions de cybersécurité et aux enjeux de la révolution numérique.

Compétences

A l'issue de la formation, les participants seront capables de :

- Prendre en compte la révolution numérique dans la stratégie d'un État ou d'une entreprise à moyen et long terme ;
- D'appliquer la méthodologie géopolitique à des situations conflictuelles multi-acteurs et d'en tirer des conséquences stratégiques pour leur organisation ;
- Conduire une analyse de risques cyber, élaborer une analyse stratégique de ces risques, et anticiper les crises potentielles liées à ces risques ;
- Anticiper les modifications de l'environnement stratégique des organisations ;
- Mobiliser des outils de collecte et d'analyse de données en sources ouvertes.

Calendrier

2021

Janvier	*Février*	*Mars*	*Avril*
	Jeudi 11 Vendredi 12	Jeudi 4 Vendredi 5 Jeudi 25 Vendredi 26	Jeudi 8 Vendredi 9 Samedi 10
Mai	*Juin*	*Juillet*	*Août*
Jeudi 20 Vendredi 21 Samedi 22	Jeudi 10 Vendredi 11	Semaine du 5 au 9	
Septembre	*Octobre*	*Novembre*	*Décembre*
	Jeudi 14 Vendredi 15	Jeudi 18 Vendredi 19	Mercredi 15 Jeudi 16 Vendredi 17

2022

Janvier	*Février*
Participation au Forum International de la Cybersécurité et au *Cyber 9/12 Strategy Challenge*	2 jours *(dates à déterminer)*

30 jours de formation

- 165h d'enseignements
- 35h de travaux pratiques réalisés avec un professionnel de la gestion du risque numérique
- Visites sur site
- Rédaction d'un mémoire professionnel

Contenu de la formation

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*.

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

Il s'agit 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 internationales qu'elles génèrent deviennent de nouveaux enjeux géopolitiques.

Module 4 : Cyberguerre : le cyberespace, lieu 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'agit d'étudier les stratégies de puissance mises en place par différents États ou organisations dans l'espace numérique (Chine, Russie, États-Unis, France, Union européenne, États d'innovation numérique : Estonie/Israël).

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 répond 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 renseignement qui peuvent être utilisés à des fins d'analyse 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.

Critères d'admission

L'admission à cette formation se réalise :

- soit sur titre : Master 2 dans les domaines des sciences humaines et sociales (géopolitique, droit, sciences de gestion, communication, géographie, *etc.*) ou des sciences informatiques et de l'ingénieur
- soit sur validation des acquis professionnels et personnels : la VAPP (Décret n° 85-906 du 23 août 1985 modifié par le décret du 19 août 2013 - Articles D.613-38 à D. 613-50) peut être accordée aux personnes ne remplissant pas les conditions précitées après exposé de leurs motivations et étude de la cohérence de leur projet professionnel, et sur justification d'au moins 3 ans d'expérience professionnelle dans le champ du numérique.

Dans les deux cas, l'admission se fait après sélection du dossier de candidature, puis entretien éventuel.

Coût de formation

Entreprise	7 500€
Administration publique	4 000€
Etudiant en formation initiale	Droits de scolarité

Les coûts liés à l'hébergement, à la restauration et au transport sont à la charge du participant ou de son employeur.

Candidatures

Les candidatures se font via le site de l'Université Paris 8, espace Candidature et Admission avant le 15 novembre 2020.
Les candidatures se composent :
- du formulaire d'inscription
- d'une lettre de motivation
- d'un *curriculum vitae*
- d'une copie du dernier diplôme et relevé de notes
- d'une copie d'une pièce d'identité (recto-verso)

Les questions administratives doivent être adressées à Sophie Ghannam (sophie.ghannam@univ-paris8.fr). Toute autre question doivent être adressées à l'adresse du@geode.science.

Informations pratiques

Responsable de formation : Amaël Cattaruzza, Professeur des Universités à Paris 8

Capacité d'accueil : 15 à 20 places

Lieu de formation* : Campus Condorcet, Aubervilliers (Métro ligne 12, RER B)

*En fonction de l'évolution de la situation sanitaire, les cours pourront être suivis à distance.