Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

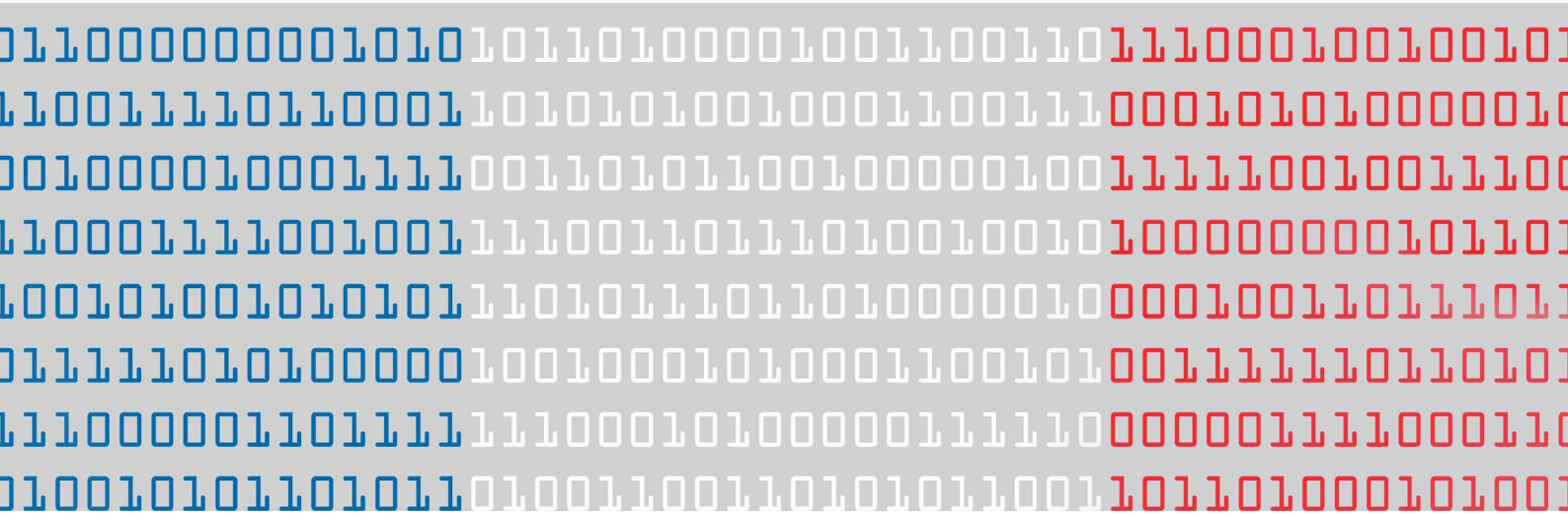
PREMIER MINISTRE

PRÉSENTATION DE LA FORMATION

Session nationale IHEDN-INHESJ

SOUVERAINETE NUMERIQUE & CYBERSECURITE

Septembre 2018 – Juin 2019



Panorama des menaces cyber # Normes, droit et gouvernance du cyberespace et des données # Souveraineté numérique # Gestion du risque cyber : rôle de l'État – Stratégies des entreprises – Coopération public/privé # Coopération internationale

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

CLÔTURE DES INSCRIPTIONS
15 juin 2018

IHEDN

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

SESSION NATIONALE 2018-2019
SOUVERAINETE NUMERIQUE & CYBERSECURITE

IHEDN

OBJECTIFS DE LA FORMATION

Le cyberespace est entré, avec les *Livres blancs sur la défense et la sécurité nationale* de 2008 et de 2013, dans le champ de la sécurité nationale. Il est devenu un terrain de confrontations entre États et un espace dans lequel se développe l'espionnage scientifique, économique et commercial. La généralisation de la cybercriminalité et les possibilités de sabotage de services nécessaires au bon fonctionnement des États et des entreprises sont devenues des menaces majeures.

La *Revue stratégique de défense et de sécurité nationale*, présentée en octobre 2017 au Président de la République, fait de notre souveraineté numérique un enjeu prioritaire. Le Premier ministre a confié au SGDSN le soin d'en préciser les contours à travers la *Revue stratégique de cyberdéfense*.

Conscients de ces enjeux majeurs pour la défense, la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont, avec l'ensemble de leurs partenaires, décidé de proposer une formation de haut niveau à l'attention des cadres dirigeants des secteurs privé et public.

Les auditeurs de cette nouvelle session nationale y acquerront une culture des enjeux de cybersécurité et de souveraineté induits par les transformations numériques. Des présentations académiques, des échanges avec des personnels engagés dans le dispositif national de cybersécurité, alliés à une mission à l'étranger et un exercice de mise en situation de crise, permettront aux auditeurs de développer une vision stratégique "cyber" au service des intérêts de leur entreprise ou de leur administration.

L'INHESJ

L'Institut national des hauts études de la sécurité et de la justice est un établissement public national à caractère administratif placé sous la tutelle du Premier ministre. L'INHESJ intervient dans les domaines de la formation, des études, de la recherche, de la veille et de l'analyse stratégique en matière de sécurité intérieure, sanitaire, environnementale et économique ainsi que dans ceux intéressant la justice et les questions juridiques.

L'IHEDN

Établissement public, à dimension interministérielle, placé sous la tutelle du Premier ministre, l'Institut des hautes études de défense nationale a pour mission de développer l'esprit de défense et de sensibiliser aux questions internationales. Il s'adresse à un large public de civils et de militaires, français et étrangers. La défense, la politique étrangère, l'armement et l'économie de défense, constituent les principaux champs disciplinaires des formations, longues ou courtes, dispensées aux niveaux régional, national et international.

Partenaires et membres du comité de pilotage

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

- ✓ MINISTÈRE L'INTÉRIEUR
- ✓ MINISTÈRE DE LA JUSTICE
- ✓ MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
- ✓ MINISTÈRE DES ARMÉES

DGE DIRECTION GÉNÉRALE DES ENTREPRISES

DIRECTION INTERMINISTÉRIELLE DE NUMÉRIQUE ET DU SYSTÈME D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT

SGDSN

Inria inventeurs du monde numérique

ANSSI

CICS Conseil des Industries de la Confiance et de la Sécurité

Cigref RÉUSSIR LE NUMÉRIQUE

CDSE Club des Directeurs de Sécurité des Entreprises

UNIVERSITÉ Grenoble Alpes

Télécharger le Dossier de candidature

PUBLICS DE RÉFÉRENCE

Les candidats seront reçus par un jury d'admission et seront choisis parmi les grands décideurs du secteur privé et de l'administration publique. Les directeurs des instituts peuvent retenir par ailleurs des personnalités dont la candidature présente un intérêt spécifique.

Une trentaine d'auditeurs, âgés prioritairement de 35 à 55 ans

- ✓ Chefs d'entreprises et cadres dirigeants
- ✓ Hauts fonctionnaires civils et militaires
- ✓ Personnalités représentatives des différents secteurs d'activité économique
- ✓ Personnalités issues du monde politique, de la presse, des syndicats...

Les auditeurs de la session nationale "Souveraineté numérique et cybersécurité " sont désignés par arrêté du Premier ministre, publié au *Journal officiel*.

ORGANISATION PÉDAGOGIQUE DE LA SESSION

L'ensemble des enseignements comporte un volume de 140 heures réparties sur 10 semaines, soit 8 séminaires de 2 jours (jeudi et vendredi), auxquels s'ajoutent 4 jours de mission à l'étranger.

Les cours magistraux ont lieu au siège des instituts à l'École militaire à Paris. Par ailleurs, des visites seront organisées chez des partenaires institutionnels et au sein d'entreprises et pourront occasionner des déplacements en France.

L'ingénierie pédagogique de la session se structure autour

De cours magistraux, de conférences-débats et de retours d'expérience

L'INHESJ et l'IHEDN font appel à un réseau d'enseignants et d'intervenants composé de nombreux experts et praticiens reconnus de la cybersécurité de la sphère institutionnelle et du secteur privé, d'universitaires spécialisés, de hauts fonctionnaires de différents ministères et de grands témoins et décideurs du monde économique et de la société civile.

De visites en institutions et/ou entreprises et d'une mission à l'étranger

Les visites effectuées au sein d'organismes, d'entreprises et d'installations civiles et militaires liées à la cyberdéfense ont vocation à compléter, concrètement, les différents enseignements dispensés. La mission à l'étranger vise à offrir une véritable ouverture et une approche comparée dans l'appréhension des enjeux et problématiques de cybersécurité.

D'une mise en situation de gestion de crise

L'exercice est conduit à partir d'un scénario "entreprise", en temps et en situation réels.
Les auditeurs sont répartis au sein d'une cellule de crise, en responsabilité d'une fonction spécifique, nécessitant des réactions, des analyses et des décisions coordonnées.
L'animation est organisée de manière à placer les membres de la cellule de crise en situation de stress contrôlé. Les auditeurs sont ainsi plongés au cœur d'une cyber attaque en entreprise.

Télécharger le
Dossier de candidature

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

SESSION NATIONALE 2018-2019
SOUVERAINETE NUMERIQUE & CYBERSECURITE

IHEDN

PROGRAMME PRÉVISIONNEL

Le programme est validé par le comité de pilotage présidé par le Secrétaire général de la défense et de la sécurité nationale (SGDSN).

Fin septembre 2018 (date à préciser)

Ouverture conjointe des sessions nationales de l'INHESJ et de l'IHEDN par le Premier ministre

Du 4 au 5 octobre 2018 – 1er Séminaire

Les grands enjeux de la transformation numérique

- ✓ Appréhender la complexité de la société et de l'économie à l'ère du numérique
- ✓ Quels sont les enjeux et perspectives soulevés par la révolution numérique pour les prochaines décennies ? Quelle prospective pour l'économie numérique à 10/20 ans ?
- ✓ Impacts des transformations systémiques, des changements de modèles attribués au numérique (économie collaborative, intelligence artificielle, objets connectés, *Blockchain*…)

Du 22 au 23 novembre 2018 – 2e Séminaire

Panorama des risques et menaces cyber

- ✓ Qu'entend-on par menace cyber ? Quelles en sont les singularités (asymétrie des rapports de force, caractère polymorphe, l'informatique comme cible ou vecteur) ?
- ✓ Les finalités de la menace (espionnage informatique, cybercriminalité, sabotage, attaques informationnelles, déstabilisation et manipulations de l'opinion)
- ✓ Les attaquants et leurs motivations, les vecteurs et modes opératoires
- ✓ Quel est l'état de la menace aujourd'hui en France et en Europe et quelles sont les principales tendances ?
- ✓ Comment se matérialisent ces risques et menaces pour les entreprises et les organisations ? Quels en sont les modes opératoires ? Quels sont les risques systémiques majeurs ?

Du 6 au 7 décembre 2018 – 3e Séminaire

Quelles stratégies pour les entreprises et organisations ?

- ✓ Les grandes phases : prévention et sensibilisation, protection, détection et réponse
- ✓ Quelle gouvernance des systèmes d'information ? Comment intégrer les nouvelles technologies ? Intégration du *Security and privacy by design* ?
- ✓ Résilience et plan de continuité et d'actiivité (PCA)
- ✓ Quelle veille sur les réseaux sociaux ? Quelle réponse à une atteinte à l'image ? Quelle stratégie ? Quels outils juridiques ?
- ✓ Comment figer une scène informatique ?
- ✓ Comment négocier son contrat d'assurance cyber ?
- ✓ Mise en conformité des systèmes d'information

Du 24 au 25 janvier 2019 – 4e Séminaire

Quels rôles et missions pour l'État au niveau national et européen ?

- ✓ L'organisation, la doctrine et le modèle français
- ✓ Quelles missions pour l'Anssi ?
- ✓ Quels rôles pour les services de renseignement ?
- ✓ Quelles missions de police sur internet (cybercriminalité) ?
- ✓ Quel traitement judiciaire, quelle réponse pénale ?
- ✓ Quelles missions pour le ministère des Armées ?
- ✓ Quelles coopérations avec les entreprises ?
- ✓ Quelles responsabilités de l'Union européenne en matière de cybersécurité ?

Du 21 au 22 février 2019 – 5e Séminaire

Cadres et enjeux juridiques

- ✓ Le droit européen face à l'extraterritorialité du droit américain
- ✓ Retour sur la LPM 2013 : la cybersécurité des opérateurs d'importance vitale
- ✓ Les impacts de la transposition de la directive NIS (*Network and Information Security*)
- ✓ Le nouveau RGPD : quelle protection pour les données personnelles ?
- ✓ Les enjeux de normalisation et de certification des services de cybersécurité/Cartographie des acteurs de confiance
- ✓ L'identité à l'heure numérique (règlement eIDAS, loi pour une république numérique)

Du 19 au 22 mars 2019 – Mission à l'étranger

Du 4 au 5 avril 2019 – 6e Séminaire

Gestion des crises cyber

- ✓ Le dispositif national interministériel de gestion des crises : CIC, Vigipirate, Piranet, le centre de coordination des crises cyber (C4), le schéma national de classement des attaques
- ✓ Anssi : quelle management des crises cyber ?
- ✓ La gestion de crise cyber et communication de crise en entreprise
- ✓ Retex de cyberattaques
- ✓ Préparation et exercice de gestion de crise

Du 23 au 24 mai 2019 – 7e Séminaire

Sécurité et stabilité internationale du cyberespace

- ✓ La gouvernance de la cybersécurité (cartographie des institutions internationales compétentes et des différentes initiatives)
- ✓ Quelle régulation du cyberespace vis-à-vis des États et des acteurs privés ? (prévention, réaction, responsabilité)
- ✓ Quels leviers bilatéraux ou régionaux de sécurité pour les États dans le cyberespace : mécanismes de coopération, CERT) ?
- ✓ Quelle cyberdiplomatie pour la France ? Quelle géopolitique à l'ère numérique ?

Du 20 au 21 juin 2019 – 8e Séminaire

Souveraineté numérique

- ✓ Quelle place pour la souveraineté numérique dans la souveraineté nationale ?
- ✓ Quelle dépendance technologique en matière numérique ? Quels sont les enjeux de souveraineté (technologique, économique, politique) pour la France ?
- ✓ Quelles stratégies de puissance des États ? (US, Russie, Chine…)
- ✓ Quels rôle et stratégies des GAFAM ?
- ✓ Les enjeux d'un Cloud souverain
- ✓ Quelle autonomie stratégique européenne ?

CLÔTURE DE LA SESSION

Télécharger le Dossier de candidature

DROITS D'INSCRIPTION

Les droits d'inscription à la session nationale "Souveraineté numérique et cybersécurité" sont fixés à

pour les administrations publiques	**6 000 euros**
pour les entreprises ou les personnes privés	**9 000 euros**

Aucune réduction n'est prévue

Les droits d'inscription sont exigibles dans leur intégralité avant l'ouverture de la session

Les frais afférents à l'hébergement, à la restauration et au transport sont à la charge de l'auditeur ou de son employeur, excepté pour ce qui est prévu par le programme dans le cadre des déplacements.

Formation professionnelle : *L'Institut national des hautes études de la sécurité et de la justice et l'Institut des hautes études de défense nationale sont habilités à percevoir des fonds au titre de la formation professionnelle.*

L'INHESJ et l'IHEDN sont référencés dans Datadock.

Télécharger le Dossier de candidature