PÔLE D'EXCELLENCE
CYBER

PANORAMA DES ORGANISMES FRANÇAIS ET EUROPÉENS

DU SECTEUR DE LA CYBERSÉCURITÉ

V1.0

NOVEMBRE 2021

Région BRETAGNE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Avertissements :

Les organismes sont classés par rubriques selon leur nature et l'autorité à laquelle ils sont rattachés. Au sein de ces rubriques, les organismes sont classés par ordre alphabétique.

Les fiches concernant les sous-directions de l'ANSSI ont été fournies par M.C. Cevaer, Délégué Régional de l'ANSSI, il s'agit de copies du contenu du site de l'ANSSI.

Patrick ERARD
Délégué Général adjoint - Chef de projet - Conception - Réalisation
Pôle d'excellence cyber

Copyright Pôle d'excellence cyber©. Édition de novembre 2021.
Cette œuvre est mise à disposition sous licence Attribution - Pas d'Utilisation Commerciale - Pas de Modification 3.0 France.
Pour voir une copie de cette licence, visitez http://creativecommons.org/licenses/by-nc-nd/3.0/fr/
ou écrivez à Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Sommaire

Avant-propos
Arnaud Coustillière, Président du Pôle d'Excellence Cyber 4

PARTIE I : Organismes français du secteur de la cybersécurité 7

I. Organismes étatiques de cybersécurité 8
Cabinet du Premier Ministre 8
Secrétariat d'État chargé de la transition numérique et des communications électroniques 12
Secrétariat général à la défense et la sécurité nationale (SGDSN) 13
Ministère des Armées 18
Renseignement 21
État-major des Armées 24
État-major de l'armée de Terre 27
État-major de l'armée de l'Air et de l'espace 30
État-major de la Marine 33
Ministère de l'Intérieur 34
Police judiciaire 35
Gendarmerie nationale 38
Ministère de l'Europe et des Affaires Étrangères 41
Ministère de l'Économie et des Finances 42
Ministère des Solidarités et de la Santé 45

II. Organismes indépendants de la cybersécurité 46
Autorités administratives indépendantes 46
Associations 49
Organismes de recherche 67

PARTIE II : Organismes européens de la cybersécurité 69

Avant-propos

Le Guide des organismes cyber est le premier ouvrage qui offre un panorama des principaux acteurs public et privé de la cybersécurité et cyberdéfense française et européenne. Cette cartographie de l'environnement a été menée par le Pôle d'excellence cyber. Il a sollicité les différents organismes pour qu'ils y décrivent leurs structures et leurs activités. Ce guide démontre le dynamisme du Pôle quant à produire des écrits de référence pour promouvoir le secteur de la cybersécurité.

Ce guide montre à quel point le cyber-espace français et européen se structure autour d'une communauté d'acteurs complémentaires, telle l'Union Européenne, le cabinet du Premier ministre (SGDSN, ANSSI), le ministère de l'Intérieur (Police Nationale, Gendarmerie Nationale), le ministère des Armées (COMCYBER, DGA-MI, COMSIC), des autorités de régulation des activités, des associations et des acteurs privés.

Le rôle central de l'Agence Nationale de la Sécurité des Systèmes d'Information dans la structuration de cet espace, dans la gestion des cyber-menaces et des crises qui peuvent s'y produire, est consolidé par l'ensemble des autres acteurs. Le Pôle d'excellence cyber a pour ambition de structurer la filière souveraine et européenne de la cybersécurité. Ce guide permet de prendre conscience de la richesse, de l'intrication et de la complémentarité des parties prenantes de cet écosystème.

Arnaud Coustillière

Président du Pôle d'Excellence Cyber

ORGANISMES FRANÇAIS DU SECTEUR DE LA CYBERSÉCURITÉ

1 ORGANISMES ÉTATIQUES DE CYBERSÉCURITÉ

CABINET DU PREMIER MINISTRE

CONSEIL NATIONAL DE L'INDUSTRIE (CNI)

www.conseil-national-industrie.gouv.fr

Dans le cadre de la politique nationale de « reconquête industrielle », le Conseil National de l'Industrie (CNI) appuie le gouvernement à travers la structuration des filières industrielles françaises sous la forme de Comités stratégiques de filière (CSF). Ces Comités stratégiques de filière ont pour objet de favoriser le dialogue entre l'État, les entreprises et les représentants des salariés dans le but de faire converger les compétences et les savoir-faire. Le Conseil National de l'Industrie labellise dix-huit Comités stratégiques de filière (CSF), spécialisés selon les secteurs visés.

La cybersécurité constitue un enjeu transverse de chacun de ces Comités stratégiques de filière, mais trois d'entre eux sont directement liés au numérique : le CSF « Infrastructures du numérique », le CSF « Électronique » et le CSF « sécurité ».

Le CNI est présidé par le Premier ministre.

CONTACT

contact.cni@finances.gouv.fr

Nouveaux CSF

Infrastructures du Numérique

COMITÉ STRATÉGIQUE DE FILIÈRE « INFRASTRUCTURES DU NUMÉRIQUE »

www.conseil-national-industrie.gouv.fr

La filière des infrastructures du numérique est aujourd'hui pleinement mobilisée face aux défis que posent la généralisation de la connectivité à très haut débit, le déploiement de la 5G, la croissance de l'Internet des objets ou encore de l'intégration de l'intelligence artificielle dans les réseaux. Afin de soutenir l'innovation, l'emploi et l'export dans ce domaine, le CSF « Infrastructures du numérique » a ainsi été créé en 2018. Ce Comité fédère l'ensemble des acteurs de la filière, des fabricants d'équipements et de matériaux (câbles de communication, équipements de radiocommunications) aux fournisseurs de services (opérateurs télécoms) en passant par les centres de recherche.

Le CSF « infrastructures du numérique » se concentre sur quatre objectifs principaux :

- 5G : définir les enjeux liés au déploiement des réseaux 5G (calendrier des usages, identification des freins à lever…) et mettre en place un réseau de plateformes 5G multi-sites ;
- Territoires intelligents : accompagner les collectivités territoriales dans leurs projets et poursuivre le Plan France très haut débit (THD) pour densifier les infrastructures ;
- Emploi et compétences : anticiper les besoins futurs liés à l'aboutissement du Plan France très haut débit (THD) pour pérenniser les emplois ;
- Offre à l'exportation : promouvoir le savoir-faire de la filière à travers la Team France Export et Bpifrance.

Le CSF « Infrastructures numériques » est présidé par Didier Casas.

COMITÉ STRATÉGIQUE DE FILIÈRE « INDUSTRIES DE L'ÉLECTRONIQUE »

www.filiere-electronique.fr

La filière industrielle électronique est un acteur essentiel de la révolution digitale puisqu'elle est au cœur du développement de l'Internet des objets, dont la croissance est en pleine expansion, à travers les technologies de la nanoélectronique et de l'électronique de puissance. Ce CSF « industries de l'électronique » a été créé en 2019 et rassemble les fabricants de composants, les fabricants d'équipements de test et mesure et de production électronique, les entreprises développant des systèmes et des logiciels embarqués mais également les laboratoires de recherche et les établissements de formation de ce secteur.

Le CSF « industries de l'électronique » s'articule autour des axes de travail suivants :

- Innovation : soutenir les programmes de recherche et développement notamment dans les technologies de la nano-microélectronique, les composants semi-conducteurs avancés, les systèmes cyber-physiques, les logiciels embarqués… ;
- Industrie électronique du futur : faire tendre la filière vers l'industrie 4.0 à travers la digitalisation et la robotique ;
- Diffusion de l'électronique : accompagner la transformation numérique des PME/ETI/Start-ups à travers des réseaux performants (création d'un Digital innovation hub – DIH) en mesure de leur offrir des produits et services adaptés ;
- Compétences et emplois : promouvoir les formations existantes et renforcer l'offre de formation continue et initiale ainsi que l'alternance dans la filière électronique ;
- Rayonnement international : favoriser l'internationalisation des entreprises à travers le financement de l'export tout en assurant leur indépendance ;
- Intelligence artificielle : encourager le développement de processeurs dédiés à l'intelligence artificielle ainsi que la coopération entre les acteurs de la filière.

Le CSF « Industries de l'électronique » est présidé par Thierry Tingaud.

CONTACT

Délégué permanent
Jacques Roujansky
jroujansky@cics-org.fr

www.filiere-electronique.fr/actualites-et-publications/

CSF Industries de Sécurité

CONTACT

Délégué permanent
Jacques Roujansky
jroujansky@cics-org.fr

COMITÉ STRATÉGIQUE DE FILIÈRE « INDUSTRIES DE SÉCURITÉ »

www.conseil-national-industrie.gouv.fr/comites-strategiques-de-filiere/industries-de-securite

Lancé en 2018 par le Premier ministre, le Comité stratégique de filière « Industries de sécurité » succède au Comité de la filière industrielle de sécurité (CoFIS) mis en place en 2013. Ce nouveau Comité de filière rassemble l'ensemble des acteurs publics et privés œuvrant au développement de produits et de services dans le secteur de la sécurité. Ce comité a pour objet la protection des entreprises et des citoyens ainsi que la dynamisation économique de la filière industrielle de sécurité. Il agit de façon opérationnelle à travers des projets structurants qui engagent l'État et l'industrie. Ces projets répondent très concrètement aux enjeux de souveraineté face aux risques liés aux technologies critiques et aux technologies de rupture dans ce secteur à fort potentiel économique, mais également à ceux de la formation de la main d'œuvre.

Parmi les projets du CSF « industries de sécurité », quatre sont directement liés au numérique :

- « Cybersécurité et sécurité de l'internet des objets » : réunir et mobiliser les acteurs concernés autour des enjeux suivants ; emplois et compétences, recherche et innovation, accès au marché ;
- « Identité numérique » : favoriser le développement d'une identité numérique forte, des usages et de l'écosystème au profit de la lutte contre la fraude, la protection des données personnelles et la souveraineté numérique ;
- « Territoires de confiance » : développer des solutions pour les collectivités territoriales concernant la ville intelligente et connectée ;
- « Numérique de confiance » : structurer des offres industrielles répondant aux besoins des entreprises et de l'État, notamment en matière de Cloud de confiance.

Le CSF « Industries et sécurité » est présidé par Marc Darmon.

DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE (DINUM)

www.numerique.gouv.fr

La Direction interministérielle du numérique (DINUM), qui succède à la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) à partir de 2019, est un service du Premier ministre à vocation interministérielle. Ainsi, la DINUM a pour but d'accompagner les ministères dans leur transformation numérique, conseiller le gouvernement et développer des services et ressources partagées. La DINUM est chargée de plusieurs missions :

- Élaboration et mise en œuvre de la stratégie numérique de l'État : développement d'infrastructures, de services et de ressources numériques partagés (réseau interministériel de l'État) ;
- Accompagnement des administrations dans leur transformation numérique : promotion de l'innovation en termes de méthodes de travail et pratiques professionnelles dans le domaine du numérique, promotion de la dématérialisation des formalités administratives en tenant compte des besoins des usagers et des agents publics ;
- Coordination de l'exploitation et de la circulation des données de l'État et des organismes placés sous sa tutelle ;
- Définition des principes et règles de construction des systèmes d'information publics ;
- Conception et mise en œuvre d'opérations de mutualisation entre administrations ;
- Conseil et expertise sur les systèmes d'information, projets informatiques ou services numériques.

L'actuel directeur interministériel du numérique est Nadi Bou Hanna.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Direction interministérielle du numérique

SECRÉTARIAT D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

CONSEIL NATIONAL DU NUMÉRIQUE (CNNUM)

www.cnnumerique.fr

Le Conseil national du numérique, créé en 2011, est une commission consultative placée auprès du Secrétaire d'État chargé du numérique, qui traite les questions relatives au numérique par délégation du Premier ministre. Le CNNum a pour objet d'éclairer les décisions du Gouvernement sur toute question ayant trait au numérique : transition numérique de la société, de l'économie, des organisations, de l'action publique, des territoires... A ce titre, le CNNum peut être saisi par le Premier ministre et par le Secrétaire d'État chargé du numérique, avec les ministres concernés.

Le CNNum est chargé de trois missions principales :

- Conseiller le Gouvernement sur les projets de disposition législative ou réglementaire pouvant avoir un impact sur l'économie numérique ;
- Participer au débat public dans le domaine du numérique et contribuer à l'élaboration des positions de la France aux niveaux européen et international ;
- Formuler des recommandations relatives à l'économie numérique.

CONTACT

01 44 97 25 08
info@cnnumerique.fr

ADRESSE

Conseil national
du numérique

Bâtiment Condorcet,
Teledoc 322,
6 Rue Louise Weiss,
75703 Paris Cedex 13

SECRÉTARIAT GÉNÉRAL À LA DÉFENSE ET LA SÉCURITÉ NATIONALE (SGDSN)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

www.ssi.gouv.fr

L'évolution rapide des usages numériques et des menaces qui y sont liées peuvent mettre en péril la sécurité des systèmes d'information des administrations, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE), portant ainsi atteinte à la souveraineté nationale. De fait, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009 dans le but de protéger ces acteurs essentiels des actes de cybermalveillance. Ce service à compétence nationale est rattaché au SGDSN.

L'ANSSI dispose de prérogatives en matière de prévention, de détection et de réaction aux attaques informatiques dirigées contre les administrations et les acteurs économiques, avec une action renforcée auprès des OIV. Ses attributions recouvrent six missions principales :

- Élaborer les mesures de protection des systèmes d'information critiques de l'État et des OIV et en contrôler l'application ;
- Détecter les évènements susceptibles d'affecter la sécurité des systèmes d'information des services de l'État et coordonner la réaction à ces évènements ;
- Prévenir la menace en matière de cybersécurité en proposant des produits et services de confiance (par le biais du Visa de sécurité) pour les administrations et les acteurs économiques ;
- Assister, conseiller et fournir une expertise aux administrations et aux OIV en matière de SSI ;
- Sensibiliser les acteurs économiques et le grand public aux menaces qui pèsent sur les SSI ;
- Former à la sécurité des systèmes d'information.

En outre, une Cellule d'anticipation cyber (CAC), placée auprès du directeur général, coordonne les travaux d'anticipation des enjeux, menaces et opérations de cyberdéfense afin d'apporter un soutien à la prise de décision au plus haut niveau.

L'ANSSI compte environ 600 agents (dont 79% de contractuels, 14% de fonctionnaires, 7% de militaires).

L'actuel directeur général de l'ANSSI est Guillaume Poupard.

CONTACT

secretariat.anssi@ssi.gouv.fr

ADRESSE

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale,

51, boulevard de La Tour-Maubourg,
5700 Paris 07 SP

SOUS-DIRECTION DES OPÉRATIONS (SDO)

La Sous-direction des opérations (SDO), anciennement Centre opérationnel de la sécurité des systèmes d'information (COSSI), assure la mise en œuvre de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la nation dévolue à l'ANSSI.

La SDO est chargée de trois missions principales :

- Centraliser et diffuser la connaissance des menaces et des vulnérabilités des systèmes numériques des administrations et des OIV ;
- Concevoir et mettre en œuvre la capacité nationale de détection des attaques informatiques ;
- Répondre aux incidents de sécurité par une anticipation constante et une réaction adéquate.

La SDO est composée de plusieurs unités :

- La Division connaissance et anticipation (DCA) acquière, développe, capitalise et partage la connaissance de la cybermenace et des vulnérabilités en ce qui concerne le périmètre de compétences que couvre l'ANSSI ;
- La Division détection (DD) est en charge de la conception et de la mise en œuvre de la capacité nationale de détection et opère le service de supervision de la sécurité (SOC) au profit des services de l'État ;
- La Division réponse (DR) met en œuvre la chaîne de réponse aux incidents de sécurité, du signalement à la remédiation ;
- La Cellule partenariat et capacités opérationnels (PCO) développe et entretient les relations opérationnelles avec les partenaires de l'ANSSI ;
- La Cellule État-major (EM- assure une mission de synthèse, de conseil et de soutien opérationnel et d'appui au commandement.

Au sein de la SDO, le Centre de cyberdéfense est une composante qui regroupe les entités de la SDO consacrées aux activités de veille sur la cybermenace, de pilotage des opérations et de gestion des relations opérationnelles avec l'ensemble des partenaires de la SDO. Le Centre de cyberdéfense, disponible 24 heures sur 24, est chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et du traitement des menaces majeures telles que la déstabilisation, l'espionnage, le sabotage ou encore la cybercriminalité.

L'actuel sous-directeur des opérations est François Deruty.

SOUS-DIRECTION EXPERTISE (SDE)

La sous-direction Expertise (SDE) porte la mission globale d'expertise et d'assistance technique de l'agence. Elle apporte son soutien à l'ensemble des autres sous-directions de l'ANSSI, aux ministères, aux industriels et prestataires de la sécurité et aux opérateurs d'importance vitale.

La SDE est organisée de la manière suivante :

- La division Scientifique et technique (ST) chargée de définir les référentiels techniques de l'agence et d'apporter un soutien technique aux autres structures de l'ANSSI dans leurs actions. Pour cela, la division doit connaître et maîtriser l'état de l'art de la sécurité des technologies et des systèmes d'information. À ce titre, elle anticipe les évolutions des technologies, les opportunités et les menaces et propose les innovations nécessaires ;
- La division Produits et services de sécurité (PSS) chargée d'améliorer, en quantité et en qualité, et de promouvoir l'offre notamment nationale en matière de produits et de services de sécurité ;
- La division Assistance technique (DAT) destinée à assister les administrations et les opérateurs d'importance vitale dans la sécurisation technique de leurs systèmes d'information ;
- Le bureau Cryptologie appliquée, qui remplit également la fonction de Cellule gouvernementale de surveillance des systèmes déchiffrement gouvernementaux des satellites (CGS), ayant la mission d'assurer la génération sécurisée des éléments secrets et d'en garantir la protection;
- Le centre de formation à la SSI (CFSSI) chargé de développer et mettre en œuvre la politique de formation de l'ANSSI.

L'actuel sous-directeur expertise est Renaud Labelle.

SOUS-DIRECTION STRATÉGIE (SDS)

La sous-direction Stratégie (SDS) anime, de manière transverse, le processus de planification stratégique, la contribution de l'agence à l'élaboration et à la mise en œuvre des politiques publiques en faveur de la sécurité du numérique, communique vers l'ensemble des publics de l'ANSSI et développe l'animation du réseau de ses partenaires-clés.

La SDS est organisée de la manière suivante :

- La division Communication (COM) informe et assure la promotion des activités de l'agence et de ses recommandations.
- La division Coordination sectorielle (COS) coordonne et rend compte de l'ensemble des activités de l'agence pour la prise en charge des enjeux de sécurité du numérique selon une action sectorielle, auprès des ministères et infrastructures critiques.
- La division Coordination territoriale (COT) accompagne la prise en compte des enjeux de sécurité numérique dans les territoires en agissant au plus près des acteurs locaux.
- La division Coordination internationale (DCI) est en charge de développer, animer et coordonner l'activité internationale de l'agence.
- La division Méthodes de management de la sécurité numérique (MSN) est en charge d'élaborer, d'accompagner et de promouvoir le cadre méthodologique et normatif qui vise à développer une organisation et une gestion efficace de la sécurité numérique.
- La cellule de planification stratégique (CPS) anime le processus de planification stratégique de l'agence et assure un rôle de référent méthodologique et de conseil interne au profit des différentes entités de l'agence sur les questions liées à la stratégie
- La cellule des chargés de mission rassemble les fonctions transverses, de coordination ou de conseil auprès du sous-directeur.
- La cellule des officiers de liaison issus d'autres administrations assurent un suivi permanent des échanges et des activités.

L'actuel sous-directeur stratégie est Yves Verhoeven.

SECRÉTARIAT GÉNÉRAL À LA DÉFENSE ET LA SÉCURITÉ NATIONALE (SGDSN)

SOUS-DIRECTION ADMINISTRATION (SDA)

A vocation transverse, la sous-direction administration (SDA) est responsable de la programmation et de l'exécution des activités de soutien et d'administration de l'ANSSI en lien étroit avec le SAG, Service de l'Administration Générale du SGDSN.

Organisation :

- La Division des ressources humaines (BRH) qui met en œuvre la politique des ressources humaines de l'ANSSI, participe au processus de recrutement et de mobilité de son personnel civil et militaire et assure sa montée en compétence ;
- Le Bureau Finances qui prépare la programmation budgétaire de l'ANSSI et assure le suivi de son exécution. Il élabore et renseigne les tableaux de bord destinés à la direction de l'ANSSI. Il assure, en lien avec les sous-directions de l'ANSSI, l'expression des besoins et la rédaction des cahiers des clauses techniques dans les procédures de la commande publique ;
- Le Bureau du Contrôle et de la Qualité qui porte la politique de la qualité de l'ANSSI, comme outil d'amélioration du fonctionnement de l'ANSSI ;
- Le Bureau des Affaires Juridiques qui apporte à la direction et aux sous-directions de l'ANSSI l'assistance juridique générale nécessaire à l'exercice de leurs missions ;
- Le Bureau de la Logistique qui met en œuvre l'exécution des tâches logistiques de l'ANSSI et participe aux dispositifs d'élaboration et de suivi de l'ensemble des grands projets transverses et intégrés, de nature logistique et immobilière ;
- La fonction Secrétariat et Courrier qui relève de la responsabilité fonctionnelle de l'adjoint du sous-directeur Affaires Générales.

L'actuel sous-directeur admistration est Michel Babeau.

CENTRE GOUVERNEMENTAL DE VEILLE, D'ALERTE ET DE RÉPONSE AUX ATTAQUES INFORMATIQUES (CERT-FR)

www.cert.ssi.gouv.fr

Le CERT-FR soutient la sous-direction des opérations de l'ANSSI concernant la gestion technique des incidents informatiques touchant les administrations et les OIV. Cette structure d'alerte et d'assistance assure une veille, met en place les moyens de protection nécessaires et prépare la réponse aux attaques informatiques. Ainsi, le CERT-FR complète l'approche préventive de l'ANSSI par son action curative. Il assure également la liaison avec le réseau mondial des CERT.

L'actuelle représentante du CERT-FR est Chloé Chabanol.

CONTACT

cert-fr.cossi@ssi.gouv.fr

ADRESSE

Secrétariat général
de la défense et de la
sécurité nationale,

ANSSI/CERT-FR,
51, boulevard
de La Tour-Maubourg,
75700 PARIS 07 SP

CENTRE DE FORMATION À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (CFSSI)

Le CFSSI assure la mission de formation à la sécurité des systèmes d'information de l'ANSSI. Il propose des formations courtes, ouvertes aux agents publics et aux personnels des OIV et OSE, et une formation longue, accueillant chaque année 10 à 12 étudiants, permettant d'obtenir le titre d'expert en sécurité des systèmes d'information (ESSI).

D'autres programmes, portés par l'ANSSI et le CFSSI, ont été développés pour promouvoir la formation à la sécurité des systèmes d'information :

- SecNumEdu, un programme de labellisation des formations spécialisées en sécurité informatique par le biais de son programme (pour plus d'informations : www.ssi.gouv.fr/secnumedu) ;
- CyberEdu, une association de labellisation des formations supérieures en informatique non spécialisées en SSI (pour plus d'informations : www.cyberedu.fr) ;
- SecNumAcadémie, une formation en ligne gratuite sur la sécurité informatique (pour plus d'informations : www.secnumacademie.gouv.fr).

Le CFSSI rejoindra en septembre 2021 le Campus Cyber.

CONTACT

cfssi@cfssi.gouv.fr

ADRESSE

Centre de Formation à
la Sécurité des Systèmes
d'Information,

51, boulevard
de la Tour-Maubourg,
75700 Paris 07 SP

MINISTÈRE DES ARMÉES

DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (DGNUM)

CONTACT

09 88 68 61 42

ADRESSE

Ministère des Armées,
60 boulevard du général
Martial Valin, CS 21623,
75509 Paris Cedex 15

La DGNUM, qui succède à la Direction générale des systèmes d'information et de communication (DGSIC) à partir de 2018, a pour objet de poursuivre la transformation numérique du ministère des Armées en assurant la cohérence globale des systèmes d'information et de communication de ce dernier. Dans ce but, la DGNUM est chargée de plusieurs missions au sein du ministère des Armées :

- Assistance et conseil aux états-majors, directions et services du ministère ;
- Contrôle de l'application de la politique ministérielle par états-majors, directions et services du ministère en matière de systèmes d'information et de communication ;
- Promotion, coordination des actions relatives à la transformation numérique et à l'innovation en matière de technologie de l'information et de la communication ;
- Proposition des orientations générales en matière de sécurité des systèmes d'information ;
- Élaboration de la politique générale en matière d'utilisation du spectre de fréquences de la défense, tant au niveau national qu'international.

L'actuel directeur général du numérique et des systèmes d'information et de communication est Nicolas Fournier.

La DGNUM est composée d'environ 50 agents, civils et militaires.

LA FABRIQUE NUMÉRIQUE DÉFENSE CONNECT

Sur le modèle de l'incubateur de services numérique beta.gouv.fr de la DINSIC*, inaugurée le jeudi 10 janvier 2019, la Fabrique Numérique est physiquement hébergé par l'Innovation Défense Lab (Agence Innovation Défense) constitué d'une équipe qui accompagne le projet d'un intrapreneur du ministère selon la méthode «agile», avec pour objectif la livraison d'un premier produit viable en six mois (PMV : Product Minimum Viable). Les projets sont à ce stade uniquement sur internet.

Sous la direction de l'ASC Frédéric Bardolle (DIRISI), une équipe d'experts est à l'écoute du porteur de projet, lui permettant de cadencer son projet, lui fournir les outils méthodologiques, prendre en compte l'ergonomie du service, le développement de l'application ou du site internet, etc. Parmi elle, on trouve le Commando Numérique Défense Connect, composé des quatre experts suivants :

> Une UX Designer qui aide à concevoir le produit pour et avec l'utilisateur final ;

> Un Data Analyst qui fait parler les données disponibles ;

> Une Product Owner, qui fait le lien entre l'utilisateur final et le projet ;

> Un Coach Agile, qui va prendre le rôle de formateur à la méthode agile, de facilitateur, de coach du projet.

Deux projets actuellement incubés

Le projet «Civils de la Défense», porté par la DRH-MD*, vise à simplifier et accélérer le recrutement de contractuels en élaborant et publiant dans l'outil des offres d'emploi plus visibles, en facilitant la constitution du dossier de candidature et en gérant le parcours du candidat dans l'outil pour un meilleur suivi par tous ses acteurs. Actuellement en phase d'expérimentation sur des offres réelles et avec un nombre réduit d'employeurs, le site sera officiellement ouvert en février (www.civilsdeladefense.fabnum.fr).

Le second projet incubé s'intitule «e-Chauffeur», est porté par le commissariat des Armées (SCA) et apporte une solution pour la mobilité à l'intérieur des bases militaires grâce à un service proche des systèmes VTC via une application sur smartphone. Le service entrera en service au premier trimestre 2019.

Perspectives d'avenir

Alors que la transformation numérique fête fin janvier sa première année d'existence, la Fabrique Numérique capitalise sur ces excellents résultats. Elle planifie ainsi de monter en puissance, passant de deux à six projets incubés, réfléchissant également à l'approfondissement de la phase d'industrialisation succédant à celle d'idéation et d'incubation.

Vous êtes intrapreneur du ministère ? Votre idée peut résoudre un irritant ? N'hésitez pas à contacter le Directeur de Transformation digitale (DTD) ou les Référents Digitaux (RD) de votre organisme. La DGNUM (Mme Valérie Dagand et M. Hervé Cicchéléro) ainsi que la DIRISI (M. Bardolle) sont également à votre disposition.

MINISTÈRE DES ARMÉES

DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

EXPERT TECHNIQUE EN CYBERDÉFENSE

La DGA est l'expert technique référent du ministère des Armées en matière de cyberdéfense. De l'anticipation de la menace à la mise en œuvre de cyber-solutions pour la défense et les hautes autorités de l'État.

La DGA assure, depuis la conception d'algorithmes cryptographiques et de produits de sécurité jusqu'aux analyses de risques de niveaux capacitaire et système :

- un rôle de conseil et de soutien dans tous les domaines de lutte cyber (lutte informatique défensive, lutte informatique offensive, lutte informatique d'influence) du ministère des Armées,
- le développement et l'évaluation de produits de Cybersécurité et de Cyberdéfense, avec une expertise sur les fonctions de protection, de défense et d'action cyber,
- la prise en compte de la cybersécurité et de la cyberdéfense dans les programmes d'armement,
- l'animation de la R&T cyber en lien avec les autres entités étatiques, l'industrie et le monde de la recherche,
- une intervention directe par une partie de ses équipes de haut niveau au profit des unités opérationnelles du COMCYBER et des Armées ainsi que de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour l'analyse des attaques les plus complexes détectées sur les réseaux et des menaces potentielles les plus dangereuses.

Pour disposer d'une capacité d'expertise à la hauteur des enjeux majeurs portés par la cyberdéfense et pour faire face à l'évolution rapide des menaces, la DGA poursuit le recrutement, sur le site de DGA Maîtrise de l'information à Bruz, d'ingénieurs de très haut niveau, spécialisés dans l'analyse et la prévention des attaques informatiques, ainsi que dans la conception de systèmes et d'outils de cybersécurité et d'armes cyber. Nos ingénieurs travaillent le plus souvent en boucle courte avec les équipes opérationnelles en charge de conduire les opérations cyber dans les différents domaines de lutte informatique.

DGA MI poursuit sa montée en puissance en recrutant massivement des experts dans tous les métiers de la cyberdéfense : analyses de risques et scénarii d'attaques, détection d'intrusion, analyse de malwares, architecture de sécurité, cryptographie, développement logiciel cyber, évaluations fonctionnelles et de sécurité, automatisation et aide à la décision pour la conduite des opérations de cyberdéfense. Le recours aux technologies de l'IA et du Big data est aussi au cœur des moyens mis en œuvre par les experts de DGA MI.

Les équipes CYBER de DGA MI sont passées de 250 personnes en 2014 à plus de 500 personnes en 2021 avec pour objectif d'embaucher encore 250 experts et architectes d'ici 2025.

La montée en puissance de la DGA en matière de cyberdéfense se traduit également, en lien avec l'Agence d'Innovation de Défense, par le renforcement de la recherche amont et un soutien accru aux PME, start-up et aux laboratoires de recherche qui interviennent dans ce domaine.

Plus largement, que ce soit au plan régional (Bretagne) ou national, au travers du Pôle d'Excellence Cyber et de la Cyberdéfense Factory, la DGA participe activement à l'animation d'une filière d'excellence cyber tant sur le plan de la formation et de la recherche que sur celui du développement des entreprises françaises innovantes.

CONTACT

02 99 42 91 51

ADRESSE

DGA Maîtrise de l'information,
BP 7, 35998 Rennes Cedex 9

RENSEIGNEMENT

DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE (DGSE)

La Direction générale de la sécurité extérieure s'inscrit dans l'héritage des services de renseignement extérieurs issus de la Seconde Guerre mondiale afin d'« assurer à nos autorités une capacité autonome d'appréciation pour conserver en tout temps notre autonomie stratégique »[1]. Créée en 1982, la DGSE relève du Ministère des Armées et a une vocation interministérielle. La DGSE se présente à la fois comme un service de renseignement extérieur, qui recueille et analyse des informations liés aux intérêts de la France, un service spécial, qui complète l'action diplomatique, et un service intégré, qui maîtrise la totalité des méthodes de renseignement. Ainsi, l'action de la DGSE est principalement tournée vers la lutte contre le terrorisme et la lutte contre la prolifération d'armes de destruction massives. Plus largement, le Service œuvre également à la protection des intérêts fondamentaux de la France, aussi bien dans les domaines économique, politique et diplomatique que militaire.

Dans le domaine de la cyberdéfense plus particulièrement, la DGSE développe des installations destinées à la lutte informatique offensive au profit du Ministère des Armées afin de lui fournir des capacités en matière de recueil de renseignement, de soutien aux engagements militaires, de riposte et d'entrave face aux agressions envers la France. Par ailleurs, dans un souci de préservation de son autonomie technique, la DGSE est en mesure d'assurer la protection de ses propres systèmes d'information.

L'actuel directeur général de la sécurité extérieure est Bernard Emié.

Les effectifs de la DGSE s'élèvent à environ 5700 personnes (dont environ 23% de militaires, 46% de fonctionnaires civils et 31% de contractuels) avec 421 métiers différents, dont une part importante de métiers techniques (architectes cyber, spécialistes de la cryptographie, data scientists, spécialistes des intrusions et recherche de vulnérabilités, experts en communications sécurisées, administrateurs réseau, spécialistes des supercalculateurs, experts du calcul à haute performance (HPC)…)

CONTACT

01 56 06 34 80

ADRESSE

141 Boulevard Mortier,
75020 Paris

ADRESSE POSTALE

Ministère des armées,
CASE n°51 - AP 203,
1 place Joffre,
75700 PARIS SP 07

1 Bernard Emié, directeur général de la sécurité extérieure, dans un entretien au Figaro le 17 juin 2020.

DIRECTION DU RENSEIGNEMENT MILITAIRE (DRM)

La Direction du renseignement militaire, comme son nom l'indique, est tournée vers les armées : elle recueille et analyse du renseignement d'intérêt militaire. Née de la réforme du renseignement militaire en 1992, la DRM relève du Chef d'état-major des Armées et conseille le Ministre des Armées.

Une double mission anime la DRM :

- Appuyer la planification stratégique et la conduite des opérations et contribuer à l'orientation tactique de la manœuvre ;
- Éclairer la prise de décision des hautes autorités politiques et militaires (Président de la République, Ministre des Armées, Chef d'état-major des Armées, grands commandements).

La DRM investit le domaine de la cyberdéfense avec son Centre de recherche et d'analyse cyber (CRAC).

La DRM est constituée d'environ 2000 agents, majoritairement militaires, avec des profils techniques variés (experts des menaces cyber, analystes réseaux, investigateurs en sources ouvertes, spécialistes de l'analyse des smartphones ou ordinateurs récupérés sur les théâtres d'opérations, data scientists, architectes réseaux…)

L'actuel directeur de la DRM est le général de corps aérien Jean-François Ferlet.

CONTACT

01 80 50 14 00

drm.communication.fct
@intradef.gouv.fr

ADRESSE

231 Boulevard
Saint-Germain,
75007 Paris

ADRESSE POSTALE

SIEM-G,
60 boulevard du
Général Martial Valin,
CS21623, 75509
Paris Cedex 15

CENTRE DE RECHERCHE ET D'ANALYSE CYBER (CRAC)

L'exploitation du renseignement issu du cyberespace est nécessaire en ce que seulement 4% des informations sur internet seraient directement accessibles depuis les moteurs de recherche traditionnels comme Google, d'après le directeur de la DRM, le général Ferlet. Le Centre de recherche et d'analyse cyber a ainsi été créé en 2015 afin d'investir le nouveau champ de confrontation que représente le cyberespace. Le CRAC est rattaché à la sous-direction « Recherche » de la DRM.

Les activités du CRAC sont orientées vers deux domaines :

- La recherche et l'exploitation du renseignement d'origine cyber, issu de sources ouvertes (web, réseaux sociaux) ou non (deep web et dark web) et de supports numériques (clés USB, cartes SIM, disques durs…) ;
- L'évaluation de la menace et des systèmes d'armes adverses.

Les effectifs du CRAC s'établissaient à environ 90 personnes en 2018.

DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE (DRSD)

www.drsd.defense.gouv.fr

La Direction du renseignement et de la sécurité de la défense, anciennement Direction de la protection et de la sécurité de la défense (DPSD) depuis 1981, est placé sous l'autorité directe du Ministre des Armées. Ce service de renseignement est spécialisé dans la contre-ingérence des forces, qui vise à protéger les forces en opération, et la contre-ingérence économique, qui vise à protéger le patrimoine scientifique et technologique de la Nation et la base industrielle et technologique de défense (BITD). Dans ces deux sphères, la DRSD a pour mission de déceler, identifier et neutraliser toute menace résultant de services de renseignement étrangers, d'organisations, d'agents ou d'individus dans les domaines du terrorisme, de l'espionnage, du sabotage, de la subversion et du crime organisé.

La contre-ingérence cyber constitue un domaine transversal, qui s'intègre à la fois dans la sphère militaire et la sphère industrielle, pour lequel la DRSD s'appuie sur ses moyens propres et coopère avec d'autres organismes (ANSSI, COMCYBER). La DRSD s'emploie à identifier les vulnérabilités et les menaces susceptibles de porter atteinte aux personnes, aux matériels ou aux informations sensibles du ministère des Armées.

Le directeur général de la DRSD est le général de corps d'armée Eric Bucquet.

La DRSD emploie environ 1400 agents (dont une majorité de militaires) avec des profils techniques recherchés en vue des nouvelles orientations du service vers la cyber (experts en sécurité des réseaux, en forensic (investigation numérique), développeurs, techniciens télécoms, spécialistes cyberdéfense…).

CONTACT

01 80 50 14 00

drsd-dcpm.contact.fct
@intradef.gouv.fr

ADRESSE

27 boulevard Stalingrad,
92240 Malakoff

ADRESSE POSTALE

Case 44,
14 rue Saint-Dominique,
75700 Paris SP 07

ÉTAT-MAJOR DES ARMÉES

COMMANDEMENT DES FORCES DE CYBERDÉFENSE DES ARMÉES FRANÇAISES (COMCYBER)

La création du Commandement de la cyberdéfense, en 2017, illustre la prise en compte récente de l'enjeu de la cyberdéfense au sein des armées, avec la nécessité d'intégrer un volet offensif à la stratégie cyber. Le COMCYBER est l'unité opérationnelle interarmées responsable de l'ensemble des forces de cyberdéfense des armées. A ce titre, il est directement rattaché au chef d'état-major des armées et conseille le Ministre des armées. Le COMCYBER est chargé de plusieurs missions :

- Lutte informatique défensive : protection et défense des systèmes d'information et des réseaux placés sous la responsabilité du chef d'état-major des Armées et du Ministère des Armées (sauf DGSE et DRSD) ;
- Lutte informatique offensive : conception, planification et conduite des opérations militaires de cyberdéfense ;
- Contribution au développement de coopérations bilatérales et multilatérales dans le domaine de la cyberdéfense entre la France et des États alliés ;
- Contribution à la politique des ressources humaines de cyberdéfense et l'animation de la réserve de cyberdéfense ;
- Définition des besoins techniques spécifiques à la cyberdéfense.

L'actuel commandant de la cyberdéfense est le général de division aérienne Didier Tisseyre.

Les effectifs du COMCYBER s'élèvent à environ 3400 cyber-combattants, avec un objectif de 4000 agents d'ici 2025, dont les profils sont variés (ingénieurs en informatique, techniciens, analystes géopolitiques, sociologues...).

GROUPEMENT DE LA CYBERDÉFENSE DES ARMÉES

Depuis le 1er septembre 2020, le Groupement de la cyberdéfense des armées réunit le Centre d'analyse en lutte informatique défensive (CALID), le Centre d'audits de la sécurité des systèmes d'information (CASSI) et le centre des réserves de la préparation opérationnelle de cyberdéfense (CRPOC).

CENTRE D'ANALYSE EN LUTTE INFORMATIQUE DÉFENSIVE (CALID)

Le Centre d'analyse en lutte informatique défensive, créé en 2006, est un organisme interarmées rattaché au COMCYBER depuis 2019. Le CALID, en tant que centre opérationnel en lutte informatique défensive (LID), a pour but de défendre les infrastructures numériques du ministère des Armées et de préserver les missions opérationnelles qui en dépendent. Pour ce faire, le CALID est chargé de plusieurs missions :

- Anticipation des menaces et des attaques potentielles par une veille, une vérification et une évaluation des infrastructures et des procédures de sécurité ;
- Action contre les attaques détectées par le biais des groupes d'action spécialisée qu'il coordonne.

Le CALID travaille en coordination avec la sous-direction des opérations (SDO) de l'ANSSI, dans une logique de partage des méthodes et des outils de travail afin d'améliorer.

CENTRE D'AUDITS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (CASSI)

Le Centre d'audits de la sécurité des systèmes d'information est un organisme interarmées créé en 2008 puis rattaché, comme le CALID, au COMCYBER en 2019. Le CASSI mène des audits de conformité dans les domaines de la sécurité des systèmes d'information (SSI) et des signaux parasites compromettants (SPC). A ce titre, le CASSI a plusieurs missions :

- Vérification et évaluation de la qualité, de l'efficacité et de la cohérence des dispositifs mesurés et des procédures de sécurité ;
- Mise en évidence des vulnérabilités résiduelles.

CENTRE DE LA RÉSERVE ET DE LA PRÉPARATION OPÉRATIONNELLE DE CYBERDÉFENSE (CRPOC)

Le Centre de la réserve et de la préparation opérationnelle de cyberdéfense est un organisme interarmées créé en 2015 et rattaché au COMCYBER depuis 2017. Le CRPOC est chargé du recrutement, de la gestion et de l'entrainement des réserves de cyberdéfense ainsi que de l'entrainement des états-majors, directions et services des armées. De ce fait, il est amené à participer au montage d'exercices nationaux, comme l'exercice annuel interarmées DEFNET, et internationaux, comme l'exercice de l'Alliance atlantique Lock Shields :

- DEFNET est un exercice interarmées qui met en œuvre un scénario réaliste et dynamique visant à tester la coordination entre les différentes unités du ministère en cas d'attaque cyber majeure.
- Lock Shields est un exercice multilatéral de l'OTAN qui vise à évaluer les capacités à défendre un réseau informatique complexe face à des cyberattaques menée par un État fictif.

Plus particulièrement, la réserve de cyberdéfense (RCD) est une unité opérationnelle qui a vocation à être activée pour appuyer les organismes compétents (ANSSI, COMCYBER) en cas de crise cyber majeure qui toucherait les OIV, les administrations de l'État ou des collectivités territoriales. La RCD rassemble des spécialistes de l'informatique de différents niveaux, recrutés et formés par le CRPOC, organisés en unités militaires puis répartis en cellules régionales.

CONTACT

crpoc.cer.fct@intradef.gouv.fr

ÉTAT-MAJOR DES ARMÉES

COMMANDEMENT DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION INTERARMÉES DE THÉÂTRES (COMSICIAT)

Le COMSICIAT est un organe interarmées qui participe pleinement à la sécurité des opérations extérieures de la France. En effet, le COMSICIAT est responsable de la sécurité des systèmes nationaux d'information et de communication (SIC) sur les théâtres d'opération. De ce fait, dès lors qu'un engagement militaire est conduit sur un théâtre d'opération, un détachement du COMSICIAT y est déployé pour superviser et assurer la conduite des SIC sur le terrain. Le commandant d'un COMSICIAT est désigné par le Centre de planification et de conduite des opérations (CPCO), qui coordonne l'action des différents COMSICIAT.

Le COMSICIAT est chargé de plusieurs missions :

- Maintien en condition opérationnelle des SIC et des réseaux et sécurisation des SIC et des réseaux utilisés par les forces déployées en opération ;
- Sécurisation et maintien de la fluidité du transfert de données entre les unités sur le terrain, de même qu'entre le terrain et la métropole ;
- Fixation des priorités en matière d'équipement, en fonction des besoins matériels sur le terrain ;
- Sensibilisation des usagers des réseaux en matière de cyberdéfense.

DIRECTION INTERARMÉES DES RÉSEAUX D'INFRASTRUCTURE ET DES SYSTÈMES D'INFORMATION (DIRISI)

La DIRISI, créée en 2003, est un service de soutien interarmées relevant du chef d'état-major des Armées. La DIRISI est un opérateur de télécommunications au service des forces déployées en opération et du ministère, qui contrôle la sécurité de leurs systèmes d'information et de communication (SIC). Dans la poursuite de cet objectif, la DIRISI est en charge de plusieurs missions :

> Direction, exploitation et soutien des réseaux d'infrastructure et des SIC qui lui sont confiés ;

> Fourniture de services de télécommunications à l'ensemble des organismes du ministère des Armées ;

> Coordination et expertise des SIC du ministère des Armées ;

La DIRISI est composée d'une direction centrale, de directions régionales et de nombreux centres nationaux de mise en œuvre, disposant de relais locaux et de détachements.

Le directeur central de la DIRISI est le général de corps d'armée Jean-Marc Latapy.

La DIRISI compte près de 7300 personnels civils et militaires.

CONTACT

01 56 20 33 83

ADRESSE

Direction interarmées des réseaux d'infrastructure et des systèmes d'information,
Fort de Bicêtre,
BP 07, 94272,
Le Kremlin Bicêtre Cedex

ÉTAT-MAJOR DE L'ARMÉE DE TERRE

quel logo ?

COMMANDEMENT DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (COMSIC)

Dans le cadre de son plan de réorganisation « Au contact », qui répond à la nécessité de s'adapter aux évolutions du monde et des menaces après les attentats de 2015, l'armée de Terre s'est dotée d'un nouveau commandement des systèmes d'information et de communication (COMSIC) en 2016, qui relève du Commandement des forces terrestres (CFT). Le COMSIC est une unité dédiée au combat numérique, à la tête de la chaîne des systèmes d'information et de communication (SIC) de l'armée de Terre dont elle assure la cohérence. À ce titre, le COMSIC est chargé de plusieurs missions :

- Préparation opérationnelle des unités SIC ;
- Gestion des capacités SIC de l'armée de Terre ;
- Conseil au commandement pour l'emploi des SIC.

Le COMSIC est placé sous le commandement du général de division Thierry Lasserre.

Les effectifs du COMSIC s'élèvent à 5000 femmes et hommes, dont 4750 militaires et 150 agents civils.

ÉCOLE DES TRANSMISSIONS (ETRS)

L'école des transmissions (ETRS) fait partie du Commandement des systèmes d'information et de communication (COMSIC) dont elle constitue la division de formation. Née en 1994 de la fusion de trois écoles (ESEAT, EAT et ESOAT), l'ETRS est également la « maison mère de l'arme des transmissions ». L'ETRS, assure la formation du personnel civil et militaire dans les domaines de la guerre électronique et des systèmes d'information et de communication, dont les formations à la cybersécurité.

807E COMPAGNIE DE TRANSMISSIONS (807E CTRS)

La 807e compagnie de transmissions est également une unité SIC de l'armée de Terre. Créée en 2016, elle relève organiquement du COMSIC et fonctionnellement du COMCYBER. La 807e CTRS confère à l'armée de Terre les capacités opérationnelles projetables de lutte informatique défensive. La 807e CTRS est chargée de quatre missions principales :

- Anticipation et analyse des cybermenaces ;
- Supervision de sécurité des systèmes d'information et des systèmes d'armes ;
- Armement des groupes d'intervention cyber (GIR) ;
- Mise en œuvre de la lutte informatique défensive (LID).

CONTACT

02 99 84 32 99

ADRESSE

École des transmissions,
Avenue de la Touraudais,
BP 18,
35512 Cesson-Sévigné

ADRESSE

Armée de Terre,
Quartier La Maltière Stéphan,
Rue Frédéric Benoît,
35136 Saint-Jacques-de-la-Lande

ÉTAT-MAJOR DE L'ARMÉE DE TERRE

785E COMPAGNIE DE GUERRE ÉLECTRONIQUE

CONTACT

01 56 20 33 83

ADRESSE

Armée de Terre,
Quartier La Maltière Stéphan,
Rue Frédéric Benoît,
35136 St-Jacques-de-la-Lande

La 785e compagnie de guerre électronique (785e CGE), créée en 1981, est rattachée au Commandement du renseignement (COMRENS), lui-même sous l'autorité du FCommandement des forces terrestres (CFT). La 785e CGE est l'unité expérimentale de l'armée de Terre en matière de guerre électronique et de transmissions. Elle est chargée à titre principal de l'expérimentation des matériels de guerre électronique.

La 785e CGE est composée d'une centaine de militaires.

CENTRE DE RECHERCHE DES ÉCOLES DE SAINT-CYR COËTQUIDAN (CREC SAINT-CYR)

www.st-cyr.terre.defense.gouv.fr/index.php/crec

CONTACT

02 90 40 40 40

crec-secretariat@st-cyr.terre-net.defense.gouv.fr

ADRESSE

Écoles de
Saint-Cyr Coëtquidan,
56381 GUER Cedex

Le CREC Saint-Cyr, créé en 1998, poursuit deux objectifs principaux : assurer un enseignement de haut niveau aux élèves officiers et promouvoir le rayonnement des écoles de Saint-Cyr par le biais de partenariats avec des universités et des industriels françaises et étrangères. Le CREC Saint-Cyr est composé de quatre pôles de recherche qui s'articulent autour du métier militaire :

- Éthique et environnement juridique : responsabilité du militaire, judiciarisation du champ de bataille ;
- Défense et sécurité européennes : frontières ;
- Mutation des conflits : cyberconflictualité, conflits asymétriques, sociétés militaires privées, robotisation du champ de bataille ;
- Sciences et technologies de défense : mécanique, informatique, électronique (simulation, cryptographie).

Le CREC Saint-Cyr dispose depuis 2012 d'une chaire de cyberdéfense et cybersécurité, en partenariat avec Sogeti et Thales. Les travaux de cette chaire reposent sur cinq thèmes :

- Mutations cyber et forces armées ;
- La territorialisation du cyberespace ;
- Les cyberguerriers ;
- Les stratégies nationales du cyberespace ;
- La menace cyber.

Le CREC est composé d'environ 50 enseignants chercheurs civils et militaires.

LE BUREAU NUMÉRIQUE

Le BNUM a pour missions principales de :

> Satisfaire les besoins de l'armée de Terre en équipements informatiques, en logiciels et en réseaux d'infrastructure pour les systèmes d'information d'administration et de gestion (SIAG) et systèmes d'information opérationnels et de communication (SIOC) non programmatiques ;

> Garantir l'application de la politique de cyberprotection des armées et du règlement général sur la protection des données (RGPD) par le biais d'homologations et d'audits de système d'informations ;

> Renforcer la supériorité opérationnelle et décisionnelle par le biais de la transformation numérique, de la maîtrise stratégique des données et de l'analyse et de la recherche opérationnelle (ARO).

Le chef du bureau numérique est le responsable des systèmes d'information (RSIC) de l'armée de Terre.

Le Bureau Numérique (BNUM) de l'EMAT est placé sous les ordres du colonel Arnaud Volay.

Le BNUM est organisé en trois sections :

SECTION TRANSFORMATION NUMÉRIQUE ET DONNÉES (TND)

Missions :

> Réduire la fracture numérique du soldat dans ses missions comme dans son quotidien ;

> Garantir la maîtrise stratégique des données de l'adT et alléger la charge de saisie et de traitement des données au sein de l'Armée de Terre ;

> Renforcer la supériorité décisionnelle.

SECTION SIAG ET RÉGLEMENTATION (SIAG-RGLT)

Missions :

> Exprimer et suivre la réalisation des besoins de l'adT en matière de SIC (réseaux, matériels, logiciels,...) hors programmes et opérations d'armement ;

> Définir la politique du maintien en condition opérationnelle de l'ensemble des équipements SIAG et SIOC non programmatiques de l'adT ;

> Veiller à l'application, au sein de l'adT, de la politique de cybersécurité des armées ;

> Organiser et contrôler la mise en application du RGPD (règlement général de protection des données).

SECTION ANALYSE ET RECHERCHE OPÉRATIONNELLE (SARO)

Missions :

> Analyser des données numériques, tant organiques qu'opérationnelles, et de toutes natures (RH, finances, liées à la maintenance, aux fonctionnement d'équipements,...) pour présenter des vues objectives et consolidées. Ces techniques permettent d'analyser un problème donné pour identifier (par exemple) des marges de manœuvre, coûts ou gains financiers possibles, des points de tension (RH, financiers,...).

> Diriger la fonction ARO et présider le comité plan de charge de la SARO.

ÉTAT-MAJOR DE L'ARMÉE DE L'AIR ET DE L'ESPACE

BUREAU DU NUMÉRIQUE (BNUM)

Le BNUM, bureau de l'état-major de l'armée de l'Air, assure, au sein de l'armée de l'air, la gouvernance haute de la cyberdéfense militaire sur l'ensemble des travaux air relatifs aux opérations dans l'espace numérique.

COMMANDEMENT DE LA DÉFENSE AÉRIENNE ET DES OPÉRATIONS AÉRIENNES (CDAOA)

Le CDAOA est un commandement opérationnel relevant de l'état-major de l'armée de l'Air. Les missions du CDAOA s'articulent autour de la planification, de la conduite et de la coordination des opérations aériennes :

- Défense de la souveraineté de l'espace aérien national et protection des capacités de l'armée de l'Air ;
- Commandement, conduite et coordination des opérations extérieures ;
- Renseignement d'intérêt Air ;
- Surveillance de l'espace ;
- Préparation opérationnelle : entrainement et formation des forces.

Au-delà de ces missions, le CDAOA intègre le volet opérationnel de la chaîne de cyberdéfense de l'armée de l'Air, avec le Centre air de conduite cyberdéfense (CACC). Cette entité se charge de la planification et de la conduite des opérations de cyberdéfense au sein de l'armée de l'Air. Le CACC assure également la préparation opérationnelle des forces en supervisant leur formation et leur entrainement ainsi que les exercices comprenant un volet cyber.

ADRESSE

Base aérienne
942 Lyon-Mont Verdun

COMMANDEMENT DES FORCES AÉRIENNES (CFA)

Le CFA est un commandement organique relevant de l'état-major de l'armée de l'Air qui assure la préparation et le soutien des bases aériennes et des unités dans leurs missions de dissuasion, de protection, de prévention et de projection.

ADRESSE

Base aérienne
106 Bordeaux-Mérignac

ESCADRON DES SYSTÈMES D'INFORMATION OPÉRATIONNELS ET DE CYBERDÉFENSE (ESIOC)

L'ESIOC, anciennement Groupement aérien de l'informatique opérationnelle (GAIO), de la base aérienne (BA) 118 de Mont-de-Marsan, est l'unité d'expertise de l'armée de l'Air au sein du CFA en matière d'informatique opérationnelle. Il constitue l'échelon d'exécution de la manœuvre cyberdéfense de l'armée de l'Air et, de ce fait, il applique les directives émises par le Centre de conduite cyberdéfense du CDAOA. De plus, l'ESIOC est chargé d'armer le groupe d'intervention rapide (GIR), qui intervient en cas de cyberattaque sur un système de l'armée de l'Air. De ce fait, l'ESIOC est chargé de plusieurs missions :

- Ingénierie logicielle, développement d'applications, soutien des systèmes d'information opérationnels de l'armée de l'Air ;
- Appui aux opérations aériennes : accompagnement des déploiements du Rafale, planification et restitution de l'activité aérienne de chaque plateforme aéronautique ;
- Cyberdéfense des « systèmes métiers ».

L'ESIOC travaille en étroite coopération avec le Centre d'analyse en lutte informatique défensive (CALID) du COMCYBER. Il est également à noter que l'ESIOC est jumelé avec la 591st Signals Units de la Royal Air Force depuis 2016 et, dans ce cadre, les deux unités s'entrainent conjointement autour d'un exercice annuel de lutte informatique défensive dont la première édition a eu lieu en 2020.

CENTRE D'EXPERTISE AÉRIENNE MILITAIRE (CEAM)

Le CEAM, créé en 1933, est placé sous l'autorité du chef d'état-major de l'armée de l'Air. Le CEAM, également appelé « centre de guerre aérienne » (Air Warfare Center), est un centre d'expérimentation qui s'articule autour de trois piliers : la doctrine, les équipements et l'expertise tactique du combattant. De fait, l'innovation est fortement encouragée et soutenue pour mieux répondre aux défis que posent notamment les nouvelles technologies du numérique pour les combats de demain. Le CEAM assure différentes missions visant à préparer les capacités de l'armée de l'Air aux nouveaux enjeux :

- Expérimentation d'équipements, de matériels et de logiciels nouveaux ;
- Préparation globale des futures missions de l'armée de l'Air : identification des besoins, développement et mise en service des équipements, systèmes d'information, liaisons de données tactiques… ;
- Animation du réseau d'innovation opérationnelle : encouragement et accompagnement des projets innovants.

ADRESSE

Base aérienne 118,
1061 Avenue du
Colonel Rozanoff,
40118 Mont-de-Marsan Cedex

ÉTAT-MAJOR DE L'ARMÉE DE L'AIR ET DE L'ESPACE

ÉCOLE DE L'AIR

www.ecole-air-espace.fr

L'École de l'air est un établissement public à caractère scientifique, culturel et professionnel (EPSCP) qui forme les officiers de l'armée de l'Air depuis 1937. L'École de l'air contribue à la recherche dans le domaine de la cyber à travers son Centre de recherche (CReA), le Centre d'excellence cyber ainsi que le Centre d'initiation et de formation des équipages drones (CIFED).

ADRESSE

Base aérienne 701,
Chemin de Saint-Jean,
13661 Salon-de-Provence

CENTRE DE RECHERCHE DE L'ÉCOLE DE L'AIR (CREA)

www.crea.ecole-air-espace.fr

Au sein de l'École de l'air, le CReA a pour objet d'assurer le maintien de l'excellence académique dans le domaine de l'aéronautique militaire à travers un volet enseignement interdisciplinaire et un volet recherche bénéficiant de partenariats diversifiés. Créé en 2002, le CReA rassemble l'ensemble des enseignants-chercheurs et doctorants de l'École de l'Air et porte ses activités de recherche autour des sciences et technologies et des sciences humaines et sociales. En outre, le CReA héberge la chaire « cyber-résilience aérospatiale », qui permet de financer des thèses de doctorat qui se rattachent au domaine de la cyber.

ADRESSE

Centre de recherche de
l'École de l'air,
Chemin de Saint Jean,
13661 Salon-de-Provence Air

CENTRE D'EXCELLENCE CYBER

www.ecole-air-espace.fr/la-recherche/cec/

Afin de développer une expertise de qualité dans le domaine de la cyberdéfense, l'École de l'air a créé en 2018 le Centre d'excellence en cyberdéfense (CEC) du milieu aérospatial. A ce titre, le CEC poursuit un objectif stratégique global : la maîtrise de la cyberdéfense dans la conduite des opérations aériennes. Les trois missions principales du CEC sont les suivantes :

- Soutien à la formation : développement de formations dans le domaine cyber ;
- Promotion de l'innovation et de la recherche : développement de partenariats et de travaux de recherche ;
- Mobilisation et renforcement du réseau des acteurs opérationnels de la cyberdéfense.

ÉTAT-MAJOR DE LA MARINE

CENTRE SUPPORT CYBERDÉFENSE (CSC)

Le CSC est un centre d'entrainement qui vise à préparer les unités opérationnelles de la Marine à réagir à de potentielles attaques informatiques qui affecteraient les systèmes d'armes, les systèmes d'information et de commandement ou les systèmes de contrôle de propulsion des bâtiments. Il s'agit également d'un centre de recherche qui met à profit son expertise pour concevoir de nouveaux outils de cyberdéfense et partager les pratiques à adopter dans la Marine. Créé en 2015, il est sous l'autorité de l'ALCYBER et est rattaché à la Force d'action navale (ALFAN). Le CSC II est chargé de deux missions principales :

- Préparation opérationnelle des unités de la Marine nationale (entraînements à terre, stages MECO (mise en condition opérationnelle)) ;
- Formation, entrainement et mise à disposition des groupes d'intervention rapides (GIR), destinés à être projetés sur une unité où interviendrait un incident de cyberdéfense.

Le CSC dénombre environ 40 entraineurs, militaires et civils, avec un objectif de 55 entraineurs à la fin 2020. Il dispose d'une antenne à Brest et d'une autre antenne à Toulon.

ÉCOLE NAVALE

www.chaire-cyber-navale.fr

L'École navale dispose depuis 2014 d'une chaire de cyberdéfense des systèmes navals, spécialisée « SCADA » (Supervisory control and data acquisition), dont les travaux de recherche visent à améliorer les connaissances et l'appréciation des unités opérationnelles, à terre ou embarquées. La chaire dispose de partenariats variés avec des industriels et des écoles d'ingénieurs du secteur. Les activités de la chaire s'articulent autour de la formation et de la recherche :

- Formation et sensibilisation des acteurs des systèmes d'information à la cybersécurité (officiers de la Marine nationale, experts en cybersécurité dans le domaine maritime) ;
- Recherche autour de la protection des informations sensibles et de l'analyse de la fiabilité et de la sécurité des données.

CONTACT

IRENAV

chairecyber@ecole-navale.fr

ADRESSE

Chaire de cyberdéfense
des systèmes navals,
École navale BCRM Brest,
CC 600, 29240 Brest Cedex 9

MINISTÈRE DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

MINISTÈRE DE L'INTÉRIEUR

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

L'INHESJ est un organisme de formation et de recherche placé sous la tutelle du ministre de l'Intérieur.

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

La DGSI, héritière de la Direction centrale des renseignements généraux de 1907, a été créée en 2014 et relève du ministère de l'Intérieur. La DGSI, comme la DGSE, est un service de renseignement à compétence générale. Ce service dispose d'un réseau de services territoriaux qui disposent de compétences interdépartementales ou départementales.

Dans le cadre de ses compétences en matière de renseignement et de police judiciaire, les missions de la DGSI sont nombreuses :

- Contre-espionnage : détection et neutralisation des menaces visant la souveraineté nationale et de la sécurité des institutions et résultant d'ingérences étrangères ;
- Lutte contre le terrorisme et les extrémismes violents : détection des menaces, protection et sauvegarde de l'intégrité du territoire national, interpellations ;
- Protection économique : protection du patrimoine scientifique, lutte contre l'ingérence économique, cyberdéfense, protection du secret de la défense ;
- Contre-prolifération : identification des programmes de développement d'armes de destruction massive, sensibilisation des industriels, contrôle des biens duaux, détection des réseaux d'acquisition ;
- Lutte contre la cybercriminalité : enquête sur les attaques visant les intérêts fondamentaux de l'État et les OIV.

La DGSI emploie près de 3800 personnels et recrute activement dans les domaines de la protection des SIC, la cyberdéfense et la captation des données.

CONTACT

01 77 92 50 00

POLICE JUDICIAIRE

BRIGADE DE LUTTE CONTRE LA CYBERCRIMINALITÉ (BL2C)

Créée en 1994, la Brigade de lutte contre la cybercriminalité (BL2C), anciennement Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), est un service de police judiciaire de la sous-direction des affaires économiques et financières de la Préfecture de Police. Ce service spécialiste de la lutte contre la cybercriminalité est compétent sur la zone géographique de Paris et sa couronne.

La BL2C est en charge de trois missions principales :

- Investigations sur les infractions à la Loi informatique et libertés, sur les atteintes aux systèmes de traitement automatisé de données (STAD) et à la propriété intellectuelle numérique ;
- Assistance technique et matérielle aux services de police via l'analyse des données informatiques saisies lors des enquêtes ;
- Sensibilisation des personnels du secteur public et des professionnels du secteur privé à la cybercriminalité.

La BL2C dispose d'un effectif de 50 enquêteurs spécialisés dans les nouvelles technologies, répartis entre trois groupes d'enquête et un groupe d'assistance.

CONTACT

01 55 75 26 19

pppj-befti-information@interieur.gouv.fr

ADRESSE

36 Rue du Bastion,
75017 Paris

POLICE JUDICIAIRE

SOUS-DIRECTION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ (SDLC)

Face à l'augmentation de la cybercriminalité, c'est-à-dire les infractions commises au moyen des nouvelles technologies du numérique, la Direction centrale de la police judiciaire (DCPJ) a mis en place la Sous-direction de la lutte contre la cybercriminalité (SDLC) en 2014. La SDLC est un service tourné vers l'action judiciaire et la formation, compétent sur l'ensemble du territoire national, dont le maillage est assuré par ses seize Laboratoires d'investigation du numérique. La SDLC est compétente pour les infractions telles que les piratages, les fraudes au moyens de paiement, les escroqueries téléphoniques ou sur internet. Dans le cadre d'enquêtes dépassant le cadre national, la SDLC est amenée à travailler avec les agences européennes Europol et Eurojust.

La SDLC est ainsi chargée de plusieurs missions :

- Mise à disposition de son expertise et des moyens spécialisés dont elle dispose au profit d'autres services dans les enquêtes se rapportant à la cybercriminalité : aide à l'exploitation des supports numériques, conception de nouveaux outils d'investigation numérique pour les enquêteurs ;
- Formation à la lutte contre la cybercriminalité et animation du réseau de « référents cybermenaces » de la police judiciaire ;
- Assistance aux témoins et victimes de cybercriminalité grâce à la centralisation des signalements à travers les plateformes en ligne « Thésée » (signalement des e-escroqueries), « Pharos » (signalement des contenus et comportements illicites) et la plateforme téléphonique « Info Escroqueries ».

La SDLC compte environ 130 personnels.

CONTACT

Info Escroqueries
0 805 805 817

ADRESSE

101 Rue des Trois Fontanot,
92000 Nanterre

DIVISION DE L'ANTICIPATION ET DE L'ANALYSE (D2A)

La D2A est une unité de la SDLC dédiée au renseignement cybercriminel, dont l'analyse technique est indispensable aux unités opérationnelles chargées des enquêtes. Cette unité intègre le Centre de réponse aux incidents de la police judiciaire française (CSIRT-PJ). La D2A est également un interlocuteur important pour les entreprises du secteur privé qui ne sont pas des opérateurs d'importance vitale (OIV), auxquelles elle fournit des informations et une prévention des risques cyber.

Les principales missions de la D2A sont les suivantes :

- Veille numérique, collecte et analyse des renseignements au profit des unités en charge des enquêtes judiciaires ;
- Prévention et anticipation des cybermenaces telles que les rançongiciels à travers le CSIRT-PJ.

L'actuel dirigeant de la D2A est le commissaire François Beauvois.

La D2A compte 11 personnels.

OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITÉ LIÉE AUX TECHNOLOGIES DE L'INFORMATION DE LA COMMUNICATION (OCLCTIC)

L'OCLCTIC est l'unité opérationnelle de la SDLC, avec trois brigades chargées de la répression des atteintes aux systèmes de traitement automatisé de données (STAD), des escroqueries sur internet et des atteintes aux systèmes de paiement.

L'OCLCTIC est chargé des missions suivantes :

- Investigation ;
- Pilotage des plateformes de signalement « Pharos » et « Thésée ».

L'actuel responsable de l'OCLCTIC est le commissaire divisionnaire François-Xavier Masson.

L'OCLCTIC concentre la majorité des effectifs de la SDLC avec 61 personnels.

GENDARMERIE NATIONALE

Le Commandement de la gendarmerie dans le cyberespace -COMCYBERGEND- a été créé par arrêté du 25 février 2021, publié au Journal Officiel le 16 mars dernier. Sa vocation est de placer les unités de la gendarmerie exerçant une mission dans le cyberespace sous une bannière de coordination unique parfaitement identifiable.

COMCYBERGEND, placé sous l'autorité d'un officier général, est directement rattaché au directeur général de la gendarmerie nationale et incarne la composante numérique que toute mission de la gendarmerie comporte désormais. Il exerce ses missions sur l'ensemble du territoire national et en appui ou au profit de l'ensemble des unités de la gendarmerie nationale.

Le COMCYBERGEND se veut compétent pour connaître et traiter les missions suivantes :

- les investigations judiciaires touchant de près comme de loin à Internet, aux réseaux de communication électronique ou à l'utilisation de l'outil informatique, le renseignement criminel d'intérêt cyber et le traitement de la preuve numérique ;
- la veille des espaces numériques visant, d'une part, la recherche du renseignement à caractère opérationnel sur Internet et, d'autre part, la recherche d'infraction sur Internet ;
- les actions de prévention et de protection contre les cybermenaces en lien avec ses partenaires ;
- la gestion des crises numériques d'ampleur nationale : la coordination des moyens opérationnels mis en œuvre pour le périmètre de la gendarmerie nationale, sous l'autorité des préfets, et dans le respect des prérogatives du parquet de Paris en cas de crises numériques d'ampleur nationale.

Implanté à compter du 1er juin 2021 au Plessis-Robinson avant de rejoindre le Campus cyber dès son avènement, ce commandement se composera de 4 divisions :

1°- la division de la stratégie, de la prospective et des partenariats chargée de la construction de partenariats territoriaux comme nationaux, de la planification des opérations et de l'analyse de la menace cyber ;

2°- la division des opérations numériques formée du centre de lutte contre les criminalités numériques (C3N) et des capacités techniques visant la recherche d'infractions sur Internet ;

3°- la division de l'appui numérique aux opérations, qui comprend l'aide à la relation avec les acteurs de l'Internet, la projection d'experts de la preuve numérique et le développement d'outils d'investigation ;

4°- la division de la proximité numérique formée notamment de la brigade numérique (BNum) et s'appuyant sur le réseau territorial CyberGEND au plus près de la population.

Le COMCYBERGEND appuiera en outre les structures de gestion de crise de la gendarmerie, à l'échelon national ou territorial, pour la prise en compte de leur dimension numérique ou lorsqu'elles se déroulent en tout ou partie dans l'espace numérique.

CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES (C3N)

Le C3N, qui découle du Département de lutte contre la cybercriminalité créé en 1998, témoigne de l'adaptation de la Gendarmerie nationale à la criminalité numérique. Le C3N est une unité interne. Cette unité d'investigation dispose d'une compétence judiciaire nationale. Le C3N intervient notamment dans le cadre d'infractions complexes relatives au haut du spectre de la délinquance dans le cyberespace telles que les atteintes aux systèmes de traitement automatisé de données, les ventes illicites en ligne, la pédocriminalité et l'apologie du terrorisme.

Le C3N échange régulièrement avec le centre national d'expertise numérique (ancien département informatique électronique de l'IRCGN) afin de bénéficier de son expertise et de ses équipements. Il est également amené à travailler avec les autres services d'enquête et les services de renseignement français ainsi qu'avec les institutions internationales Europol, Eurojust ou Interpol.

Le C3N est chargé de plusieurs missions :

- Investigation : le C3N enquête en moyenne sur une centaine d'affaires chaque année ;
- Pilotage de la lutte contre la cybercriminalité de la Gendarmerie et animation du réseau CyberGEND ;
- Veille numérique et étude de l'évolution de la cybercriminalité à partir de l'analyse des comptes rendus de police judiciaire des unités de gendarmerie qui entrent dans le champ de la cybercriminalité ;
- Assistance permanente aux unités territoriales.

Face à l'augmentation continue des infractions, les effectifs du C3N sont en évolution. Environ 50 militaires y sont affectés.

Le C3N dispose de onze antennes implantées au cœur des grandes métropoles afin de renforcer la proximité des enquêteurs spécialisés.

ADRESSE

C3N,
5 Boulevard de l'Hautil,
TSA 36810,
95037 Cergy Pontoise Cedex

GENDARMERIE NATIONALE

CYBERGEND

@CyberGEND

Le COMCYBERGEND anime et coordonne le réseau CyberGEND, réseau décentralisé de gendarmes enquêteurs spécialisés créé en 2014 et répartis sur l'ensemble du territoire national, en métropole et en outre-mer. Le réseau CyberGEND est composé de différents maillons formant la chaîne cyber de la Gendarmerie :

- Les primo-intervenants en nouvelles technologies (P-NTECH) recueillent les plaintes relatives aux infractions de droit commun employant les systèmes d'information et de communication et procèdent à la saisie simple de preuves ;
- Les correspondants en technologie numérique (C-NTech) sont chargés de recueillir les plaintes, procéder à la préservation et à la saisie de preuves, conduire des investigations simples au profit d'une unité d'enquête, de réaliser les premières opérations de criminalistique numérique notamment en matière de téléphonie ;
- Les enquêteurs en technologie numérique (N-Tech) conduisent des investigations numériques plus complexes au profit d'une unité d'enquête ;
- Au bout de cette chaîne, le C3N intervient en cas d'affaire complexe.

Effectifs : le réseau CyberGEND est fort de plus de 7000 gendarmes, avec 265 enquêteurs N-Tech, 6000 correspondants C-Tech, 250 enquêteurs sous pseudonymes. Les élèves gendarmes sont formés en tant que primo-intervenants en nouvelles technologies numériques (P-NTech).

CENTRE NATIONAL D'EXPERTISE NUMÉRIQUE

Le centre national d'expertise numérique est une unité du COMCYBERGEND au service des enquêteurs et magistrats dans le traitement et l'analyse de la preuve numérique.

Pour ce faire, le centre national d'expertise numérique a recours à l'extraction de données conservées sur tous types de supports, au traitement de l'information, ou encore à la veille des réseaux et télécommunications. Dans le cadre de ses missions de soutien opérationnel, le centre national d'expertise numérique est amené à assister les enquêteurs et magistrats sur le terrain ou à distance. Il également amené à travailler au profit d'autres services de la Gendarmerie nationale comme les enquêteurs en technologies numériques (N-TECH) du C3N ainsi qu'avec des institutions internationales comme Interpol ou Europol.

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

AMBASSADEUR POUR LE NUMÉRIQUE

La diplomatie numérique française est incarnée par l'Ambassadeur pour le numérique, placé près du ministre des Affaires étrangères. L'Ambassadeur pour le numérique, qui a une vocation interministérielle, coordonne l'élaboration des positions de la France sur les questions internationales relatives à la transformation numérique et les promeut auprès des partenaires internationaux et de acteurs publics et privés.

L'Ambassadeur pour le numérique assure les missions suivantes :

- Garantir la sécurité du cyberespace à travers le renforcement de l'autonomie stratégique européenne et la promotion de la stabilité du cyberespace dans les instances internationales ;
- Réguler les contenus en ligne et les plateformes numériques ;
- Contribuer à la gouvernance et au caractère ouvert de l'Internet en œuvrant pour le respect du principe de neutralité du net ;
- Promouvoir les droits de l'homme, les valeurs démocratiques et la langue française dans le cyberespace ;
- Renforcer l'influence et l'attractivité des acteurs français du numérique ;
- Devenir leader des technologies de rupture, en particulier sur la question de l'intelligence artificielle.

L'actuel Ambassadeur pour le numérique est Henri Verdier.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

DIRECTION NATIONALE DE RENSEIGNEMENT ET DES ENQUÊTES DOUANIÈRES (DNRED)

CONTACT

Info Douane Service
08 11 20 44 44

ADRESSE POSTALE

2 Mail Monique Maunoury,
TSA90313,
94853 Ivry-sur-Seine Cedex

En matière de lutte contre la fraude douanière, qu'il s'agisse de trafics d'armes, de stupéfiants, de tabac, d'espèces protégées, d'œuvres ou de contrefaçons, la DNRED est le service compétent sur l'ensemble du territoire national. La DNRED, créée en 1988, est un service de renseignement relevant de la Direction générale des douanes et droits indirects (DGDDI) qui met en œuvre la politique du renseignement, des contrôles et de lutte contre la fraude définie par la DGDDI.

La DNRED travaille de concert avec TRACFIN sur de nombreux dossiers. Ses principales missions sont les suivantes :

- Collecte, analyse et diffusion du renseignement d'origine douanière ;
- Enquêtes anti-fraude au sein des entreprises ;
- Lutte contre la contrebande.

La DNRED dispose d'environ 700 personnels.

CYBERDOUANE

Le cyberespace constitue une difficulté supplémentaire pour les services douaniers dans la lutte contre la fraude puisqu'il permet l'anonymisation des vendeurs et acheteurs, l'hébergement de sites web à l'étranger, le morcellement des transactions ou encore l'expédition directe de produits illicites au client final (« dropshipping »), tout cela à l'échelle internationale. Afin de mieux répondre au développement de la fraude sur Internet, la DNRED s'est dotée d'un service douanier spécialisé dans la lutte contre la cyberdélinquance en 2009. Le cellule Cyberdouane vise à détecter les transactions illicites sur Internet, principalement en matière de trafics de contrefaçons, d'anabolisants, de stupéfiants, de médicaments, d'armes, de tabac et cigarettes. L'action de Cyberdouane vise directement l'offre de produits illicites et non seulement les flux.

Les missions de Cyberdouane se concentrent autour des activités de renseignement, qui peuvent aboutir au déclenchement d'une enquête de la DNRED ou du service national des douanes judiciaires (SNDJ) :

- Collecte, exploitation et diffusion du renseignement en matière de fraude sur Internet ;
- Identification des personnes physiques ou morales vendeuses de produits illicites.

Cyberdouane travaille en collaboration avec les autres services nationaux en charge de la cyberdélinquance comme l'OCLCTIC, notamment à travers la plateforme de signalement « Pharos », ainsi qu'avec les institutions internationales comme Europol et Interpol.

SERVICE DE L'INFORMATION STRATÉGIQUE ET DE LA SÉCURITÉ ÉCONOMIQUES (SISSE)

Dans la mesure où les TPE et PME représentent la majorité des entreprises nationales, leur sécurité numérique est un enjeu majeur pour l'économie nationale. Le SISSE, service à compétence nationale créé en 2016, vise ainsi à assurer le pilotage interministériel de la politique publique de sécurité et d'intelligence économique, avec un accent sur la défense de la souveraineté numérique. Le SISSE est placé sous l'autorité du Commissaire à l'information stratégique et à la sécurité économique (CISSE), qui définit cette politique. Le SISSE est également chargé d'animer le réseau des délégués régionaux à l'information stratégique et à la sécurité économiques (DISSE), qui constituent le relai du SISSE à l'échelon local.

Les missions du SISSE d'articulent autour de trois axes principaux :

- Missions d'information stratégique : identification des secteurs, technologies et entités d'intérêt économique, industriel et scientifique ; détection menaces provenant des acteurs, des pratiques d'affaires, des dispositions légales et information des autorités compétentes ;
- Missions de sécurité économique : sensibilisation des acteurs ; détection et suivi des opérations d'investissement étranger dont l'autorisation préalable est obligatoire ;
- Promotion des intérêts économiques, industriels et scientifiques de la Nation : identification et appui des actions susceptibles d'y contribuer ; information des acteurs économiques.

L'actuel directeur du SISSE est Joffrey Célestin-Urbain.

TRAITEMENT DU RENSEIGNEMENT ET ACTION CONTRE LES CIRCUITS FINANCIERS CLANDESTINS (TRACFIN)

CONTACT

01 57 53 27 00

ADRESSE POSTALE

10 Rue Auguste Blanqui,
93186 Montreuil-sous-Bois
Cedex

Créé en 1990, TRACFIN est un service de renseignement financier à compétence nationale placé sous l'autorité du ministre de l'Action et des comptes publics, près du ministère de l'Économie et des Finances. Ce service dédié à la lutte contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme est chargé d'établir la nature, la provenance et la destination des flux financiers suspectés. TRACFIN peut être saisi suite aux déclarations transmises par les professionnels soumis au Code monétaire et financier, mais e aucun cas par les particuliers. Toutefois, il n'est pas compétent en matière de police judiciaire : en cas de mise en évidence de l'infraction, le procureur de la République prend le relai.

TRACFIN est chargé de plusieurs missions :

- Collecte, traitement et diffusion du renseignement relatif aux infractions telles que le financement du terrorisme, le blanchiment d'argent, le détournement de fonds ou la fraude fiscale et sociale ;
- Animation et coordination des moyens d'investigation des services du ministère de l'Économie et des finances pour les infractions susnommées ;
- Étude de l'évolution de ces infractions ;
- Développement de l'action internationale de lutte contre ces infractions.

TRACFIN intègre la menace liée aux nouvelles technologies pouvant être le support de fraudes financières à travers la division d'enquête spécialisée dédiée à la cybercriminalité financière de son Département des enquêtes et grâce au pôle Data Science de son Département des systèmes d'information.

TRACFIN dispose d'environ 170 personnels.

L'actuelle directrice de TRACFIN est Maryvonne Le Brignonen.

DIVISION D'ENQUÊTE SPÉCIALISÉE DÉDIÉE À LA CYBERCRIMINALITÉ FINANCIÈRE

Au sein du Département des enquêtes de TRACFIN, la division d'enquête spécialisée sur la cybercriminalité financière a été créée en 2018 afin d'améliorer le traitement des données numériques et notamment l'analyse de transactions en crypto-actifs. Cette cellule est chargée de trois missions :

- Développement des capacités d'analyse des transactions enregistrées sur les blockchains publiques ;
- Renforcement des liens de TRACFIN avec les services d'enquête de la Gendarmerie (C3N) et des douanes (Cyberdouanes) ;
- Développement des partenariats de TRACFIN à l'international dans le domaine des crypto-actifs.

PÔLE DATA SCIENCE

Au sein du Département des systèmes d'information de TRACFIN, le pôle Data Science effectue des traitements de masse (« Big Data ») en vue de valoriser les données du service et de mieux détecter les fraudes à travers des méthodes avancées d'analyse réseaux, d'intelligence artificielle ou de traitement du langage.

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

AGENCE NUMÉRIQUE EN SANTÉ (ANS)

www.esante.gouv.fr

CONTACT

01 58 45 32 50

ADRESSE

9-11 Rue Georges Pitard,
75015 Paris

L'ANS, anciennement « Agence des systèmes d'information partagés de santé », a pour objet d'encourager le développement des services et outils numériques utilisés dans le cadre de la prise en charge sanitaire et du suivi social et médico-social des usagers du système de santé. L'ANS est un groupement d'intérêt public créé en 2009 et placé sous l'autorité de la délégation ministérielle du numérique en santé (DNS), qui définit la stratégie nationale du numérique en santé mise en œuvre par l'ANS.

L'ANS est chargée de trois missions principales :

- Régulation du numérique en santé : labellisation et certification en matière d'urbanisation, d'interopérabilité, de sécurité et d'éthique des systèmes d'information ;
- Conduite de projets numériques d'intérêt national : télémédecine, répertoire opérationnel des ressources… ;
- Accompagnement du déploiement national et territorial d'outils et de services numériques au bénéfice des usagers et des professionnels.

L'actuelle directrice de l'ANS est Annie Prévot.

ACCOMPAGNEMENT CYBERSÉCURITÉ DES STRUCTURES DE SANTÉ (ACSS)

www.cyberveille-sante.gouv.fr

Dans le secteur de la santé, la sécurité des données et des systèmes d'information est primordiale, notamment pour assurer la sauvegarde du principe du secret médical. Dans ce cadre, la cellule ACSS, créée en 2017, est une structure nationale d'assistance et d'appui aux structures de santé en matière de sécurité des systèmes d'information, qu'il s'agisse d'établissements de santé, de laboratoires de biologie ou encore de centres de radiologie. A ce titre, cette entité est chargée de plusieurs missions :

- Suivi des incidents de sécurité des systèmes d'information des structures de santé ;
- Information et sensibilisation des acteurs à la menace ;
- Partage de bonnes pratiques en matière de prévention et de réponses aux incidents.

2 ORGANISMES INDÉPENDANTS DE LA CYBERSÉCURITÉ

AUTORITÉS ADMINISTRATIVES INDÉPENDANTES

AUTORITÉ DE RÉGULATION DES COMMUNICATIONS ÉLECTRONIQUES, DES POSTES ET DE LA DISTRIBUTION DE LA PRESSE (ARCEP)

www.arcep.fr

CONTACT

01 40 47 70 00

ADRESSE

14 Rue Gerty Archimède,
75012 Paris

L'ARCEP, anciennement Autorité de régulation des télécoms (ART), a été créée par la Loi du 26 juillet 1996. Cette autorité administrative indépendante, initialement dédiée à l'ouverture du secteur des télécommunications à la concurrence, s'est développée pour intégrer la régulation du secteur postal, la protection de la neutralité ou encore la couverture numérique du territoire national. Dans le secteur des télécommunications comme dans le secteur postal, l'ARCEP a une fonction de régulation et de contrôle. Concernant les télécommunications particulièrement, elle est chargée de plusieurs missions :

- Définir la réglementation applicable aux opérateurs de télécommunications ;
- Attribuer des ressources en fréquences ou en numérotation ;
- Veiller au financement et à la fourniture du service universel ;
- Mettre à profit son expertise par le biais d'avis au Gouvernement, au Parlement ou autres autorités de régulation ;
- Édicter des actes de droit souple (lignes directrices ou recommandations) ;
- Veiller au respect du principe de la neutralité du net : mise en place d'une plateforme de signalement des entorses à ce principe www.jalerte.arcep.fr (ralentissement ou blocage de l'accès à certains services ou contenus par le fournisseur d'accès).

L'actuel président de l'ARCEP est Sébastien Soriano.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

www.cnil.fr

La CNIL est une autorité administrative indépendante créée par la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle agit au nom et pour le compte de l'État dans le but de préserver les droits et libertés individuelles ou publiques ainsi que la vie privée des personnes face au traitement de données à caractère personnel. La CNIL dispose d'un réel pouvoir propre puisqu'elle peut contrôler la mise en œuvre des traitements de données à caractère personnel et imposer des mesures correctrices et des sanctions aux responsables de traitement ou à leurs sous-traitants.

La CNIL exerce quatre missions principales :

- Informer les personnes de leurs droits et obligations ;
- Veiller à la conformité de la mise en œuvre des traitements de données à caractère personnel avec le droit en vigueur ;
- Labelliser les produits et services qui contribuent à la protection des données à caractère personnel, accompagner les délégués à la protection des données (DPO) désignés par leurs organismes auprès de la CNIL et faciliter la certification leurs compétences ;
- Suivre l'évolution des technologies de l'information au regard des droits et libertés individuelles ou publiques et de la vie privée des personnes et conseiller les autorités de l'État en la matière.

En matière de cybersécurité plus particulièrement, un ensemble d'articles et de tutoriels sur les bonnes pratiques à adopter est accessible dans la rubrique « cybersécurité » dédiée à la protection du patrimoine informationnel des personnes sur le site de la CNIL.

L'actuelle présidente de la CNIL est Marie-Laure Denis.

AUTORITÉS ADMINISTRATIVES INDÉPENDANTES

HAUTE AUTORITÉ POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES DROITS SUR INTERNET (HADOPI)

www.hadopi.fr

ADRESSE

4 Rue du Texel,
75014 Paris

La HADOPI est une autorité publique indépendante créée en 2009 dans le but de favoriser la diffusion et la protection de la création sur Internet. Cette API ne dispose pas de pouvoir de sanction mais elle peut néanmoins adresser des avertissements aux internautes qui commettraient des infractions au droit de la propriété intellectuelle (téléchargement illégal, contrefaçon...).

Les missions de la HADOPI :

- Encourager le développement de l'offre légale d'œuvres et objets protégés par un droit de propriété : labellisation et référencement des offres, plateforme de signalement des œuvres introuvables, sensibilisation des usagers ;
- Répondre graduellement aux atteintes portées au droit de la propriété intellectuelle : avertissements voire saisine de l'autorité judiciaire au bout de trois avertissements ;
- Réguler les mesures techniques de protection et d'identification des œuvres et objets protégés par un droit d'auteur ou droit voisin.

Le président de la HADOPI est Denis Rapone.

ASSOCIATIONS

ALLIANCE POUR LA CONFIANCE NUMÉRIQUE (ACN)

CONTACT

01 45 05 70 48

ADRESSE

17 Rue de l'amiral Hamelin,
75116 Paris

L'ACN est une association créée en 2013 dans le but de fédérer et de promouvoir la filière de la confiance numérique en France. Le secteur de la confiance numérique englobe les entreprises de la sécurité numérique (identité numérique, systèmes et sous-systèmes électroniques) et de la cybersécurité (produits, logiciels et services), qu'elles soient des leaders mondiaux, des ETI ou des PME. A travers son Observatoire de la confiance numérique, l'ACN recense les entreprises de ce secteur afin de dresser un panorama de la structure de cette industrie et de suivre son évolution. Dans son dernier rapport de 2019, l'Observatoire de la confiance numérique faisait état d'environ 2100 entreprises françaises réalisant 12,4 milliards d'euros de chiffre d'affaires.

L'ACN vise plusieurs objectifs :

- Représenter la filière de la confiance numérique française auprès des institutions nationales et internationales ;
- Participer à l'élaboration de livres blancs, de fiches techniques et autres contributions ainsi qu'aux projets de règlements nationaux et européens ;
- Participer aux débats nationaux et internationaux ;
- Coordonner des actions de développement de marchés et de solutions.

Le délégué général de l'ACN est Yoan Kassianides.

ASSOCIATION FRANÇAISE DES CORRESPONDANTS À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (AFCDP)

ADRESSE

1 Rue de Stockholm,
75008 Paris

L'AFCDP est une association à but non lucratif qui rassemble les professionnels de la protection des données, dont les délégués à la protection des données (DPO) désignés par leurs organismes auprès de la CNIL, afin de favoriser les échanges et la mise en commun des bonnes pratiques. L'AFCDP s'appuie sur des groupes de travail régionaux qui se réunissent annuellement.

L'AFCDP vise les objectifs suivants :

- Favoriser les échanges et la réflexion entre les membres autour du statut et des missions des DPO ;
- Favoriser la concertation entre les entreprises, la CNIL et les autorités nationales ;
- Participer aux initiatives nationales et internationales relatives aux DPO ;
- Assurer une veille concernant les enjeux des DPO ;
- Informer et sensibiliser les personnes sur les DPO ;
- Défendre les intérêts des DPO auprès des autorités nationales et leur soumettre des recommandations et avis.

ASSOCIATIONS

ALLIANCE FRANÇAISE DES INDUSTRIES DU NUMÉRIQUE (AFNUM)

CONTACT

contact@afnum.fr

ADRESSE

17 rue de l'Amiral Hamelin
75016 Paris

L'AFNUM est un syndicat professionnel créé en 2015, qui résulte de la fusion des syndicats Gitep TICS (technologies de l'information et de la communication), SFIB (technologies de l'information), Simavelec (matériels audiovisuels et électroniques) et USPII (photographie). L'AFNUM a pour objet de représenter les industriels des réseaux, des terminaux de l'électronique grand public, de la photographie et des objets connectés. Ces industriels sont réunis au sein de Commissions-métier en fonction de leur secteur d'activité principal. Des groupes de travail réunissent également les entreprises adhérentes concernées par les sujets traités, comme l'intelligence artificielle ou la sécurité des données, pour favoriser la réflexion commune autour des enjeux qu'ils suscitent.

L'AFNUM se donne trois objectifs pour représenter au mieux la filière industrielle :

- Se positionner en interlocuteur privilégié auprès des instances nationales et être force de propositions ;
- Faciliter le développement des industries numériques en France ;
- Promouvoir l'écosystème français des acteurs de l'industrie du numérique.

Le président de l'AFNUM est Georges Karam.

ASSOCIATION FRANÇAISE POUR LE NOMMAGE INTERNET EN COOPÉRATION (AFNIC)

CONTACT

01 39 30 83 00

ADRESSE

1, Rue Stephenson,
Hall A2, 3ème étage,
78 180 Montigny le Bretonneux

Gestionnaire historique des noms de domaine correspondant au territoire français (extension « .fr » et extensions ultramarines « .re », « .pm », « .tf », « .xf » et « .yt »), l'AFNIC est une association à but non lucratif créée en 1997 par l'INRIA, qui gère aujourd'hui plus de trois millions et demi d'extensions. L'AFNIC a pour objectif global de contribuer au développement de l'Internet en France à travers une stratégie en triptyque : assurer un service sûr et stable, favoriser le développement de l'innovation, aider les acteurs français à jouer un rôle de premier plan. L'AFNIC a également été désignée opérateur technique de registre pour le compte des entreprises et des collectivités territoriales qui disposent de leur propre domaine générique, comme l'extension « .bzh » pour la région Bretagne.

L'AFNIC se charge de trois missions principales pour accomplir ses objectifs :

- Promouvoir et accompagner la présence en ligne des entreprises et des particuliers à travers l'extension « .fr », dans le cadre de son rôle d'office d'enregistrement de cette extension ;
- Offrir des services de registres agiles, performants, innovants et sûrs, dans le cadre de son rôle d'opérateur technique de registre ;
- Renforcer la démarche responsable de l'association en optimisant les bénéfices sociaux, économiques et écologiques du Domain Name System (DNS).

Le directeur général de l'AFNIC est Pierre Bonis.

ASSOCIATION DES RÉSERVISTES DU CHIFFRE ET DE LA SÉCURITÉ DE L'INFORMATION (ARCSI)

www.arcsi.fr

CONTACT

secretariat@arcsi.fr

ADRESSE

21 Bis, Rue des Plantes,
75014 Paris

Créée en 1928, l'ARCSI était initialement dédiée aux officiers de réserve de l'Armée de Terre avant de s'ouvrir progressivement à l'ensemble des personnels du domaine du Chiffre et de la sécurité des systèmes d'information. Il s'agit d'une association à but non lucratif qui a pour principal but de favoriser le partage de savoirs et de compétences. L'ARCSI publie chaque année un bulletin composé de travaux de recherche relatifs à la cryptologie et à la sécurité des systèmes d'information.

L'ARCSI a plusieurs objectifs :

- Maintenir et développer le réseau de membres ;
- Favoriser le partage d'expérience sur les enjeux de sécurité des systèmes d'information et promouvoir la réflexion autour de ces questions ;
- Informer ses membres des évolutions dans le domaine de la cryptographie et de la sécurité des systèmes d'information et leur permettre de développer leurs compétences dans ces domaines ;
- Valoriser le patrimoine historique de l'association en le diffusant plus largement.

L'ARCSI regroupe environ 350 membres.

Le président de l'ARCSI est le général (2S) Jean-Louis Desvignes.

ASSOCIATION POUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DE SANTÉ (APSSIS)

www.apssis.com

CONTACT

06 29 36 59 95
secretaire@apssis.com

ADRESSE

84 Rue du Luart,
72160 Duneau

L'APSSIS est une association à but non lucratif créée en 2010 qui a pour objet de promouvoir la sécurité des systèmes d'information de santé à travers son réseau de professionnels du monde de la santé et des SSI.

Les principales finalités de l'APSSIS sont les suivantes :

- Contribuer à la sécurisation des systèmes d'information de santé et au déploiement des bonnes pratiques relatives aux technologies du numériques grâce à la mise à disposition de l'expertise de l'association ;
- Mettre en place des formations à la sécurité des systèmes d'information à destination des professionnels de santé ;
- Produire des contenus collaboratifs dans la domaine de la sécurité des systèmes d'information de santé ;
- Organiser des évènements, dont un congrès annuel, autour de la sécurité des systèmes d'information de santé.

L'actuel président de l'APSSIS est Vincent Trely.

ASSOCIATIONS

CENTRE EXPERT CONTRE LA CYBERCRIMINALITÉ FRANÇAIS (CECYF)

www.cecyf.fr

Dans le domaine de la lutte contre la cybercriminalité, le CECYF permet de fédérer l'ensemble de l'écosystème national, des services chargés de l'application de la loi aux chercheurs en passant par les établissements d'enseignement, afin de favoriser les échanges dans le but de faire naître des projets innovants. Le CECYF est une association à but non lucratif créée en 2014 dans le cadre du projet européen 2CENTRE (Cybercrime Center of Excellence Network for Training Research and Education).

Les objectifs du CECYF s'articulent principalement autour de la formation et de la recherche dans la lutte contre la cybercriminalité :

- Promouvoir l'offre de formation auprès des membres de l'association et produire des supports pédagogiques ;
- Encourager et faciliter la recherche à travers des dispositifs d'aide (analyse de besoin, recherche de financement, réponse aux appels d'offre, mise à disposition de moyens…) dans divers domaines : technique, sociologique, juridique ;
- Assurer une veille technique, scientifique, criminologique et juridique ;
- Sensibiliser le public à la cybercriminalité ;
- Animer le réseau d'acteurs engagés dans la lutte contre la cybercriminalité (organisation et participation à divers évènements, contribution à des publications…).

Le président du CECYF est le général (2S) Marc Watin-Augouard.

CONTACT

contact@cecyf.fr

ADRESSE

10 Rue de Penthièvre,
75008 Paris

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS (CLUSIF)

www.clusif.fr

Le CLUSIF est une association à but non lucratif créée en 1992 qui a pour objet de promouvoir la cybersécurité en animant un réseau d'entreprises et d'administrations et en facilitant les échanges de bonnes pratiques entre ces acteurs. L'association rassemble équitablement offreurs de solutions de sécurité et utilisateurs issus de quinze secteurs différents (administration, assurance, commerce, télécommunications, transport…) afin d'assurer la diversité des profils et des idées. Le CLUSIF dispose de relais au niveau international, avec les clubs de la sécurité internationaux (CLUSI), et au niveau local, avec les clubs de la sécurité régionaux (CLUSIR).

Les principaux objectifs du CLUSIF sont les suivants :

- Favoriser le partage d'expériences et d'idées entre ses membres dans le cadre de groupes de travail mensuels, où utilisateurs et offreurs se rencontrent autour de thématiques choisies par les membres (« cloud et sécurité », « cybersécurité des systèmes industriels », « sécurité de l'internet des objets »…) ;
- Sensibiliser à la sécurité des systèmes d'information ;
- Réaliser des synthèses sur l'état des techniques actuelles relatives à la sécurité des systèmes d'information.

Le président du CLUSIF est Jean-Marc Gremy.

CONTACT

01 53 25 08 80
clusif@clusif.fr

ADRESSE

11 Rue de Mogador,
75009 Paris

CLUB DES EXPERTS DE LA SÉCURITÉ DE L'INFORMATION ET DU NUMÉRIQUE (CESIN)

www.cesin.fr

Le CESIN est une association à but non lucratif, créée en 2012, envisagée comme un club d'échange tourné vers les entreprises, qui s'adresse aux professionnels exerçant des fonctions liées à la sécurité de l'information et du numérique. Le CESIN vise plusieurs objectifs orientés vers la sécurité de l'information et du numérique :

- Faciliter le partage de connaissances et d'expériences et la coopération entre experts de la sécurité de l'information et du numérique ainsi qu'avec les instances nationales ;
- Soutenir les entreprises innovantes en leur apportant des solutions de sécurité ;
- Sensibiliser les dirigeants d'entreprises aux enjeux de sécurité de l'information ;
- Représenter les professions de la sécurité de l'information et du numérique au sein du processus décisionnel : émettre des propositions au regard des évolutions réglementaires ou lors de la production de guides et référentiels concernant la sécurité de l'information et du numérique.

Le CESIN est également membres du Groupement d'intérêt public « Action contre la cybermalveillance » (GIP « ACYMA ») et apporte son soutien au dispositif Cybermalveillance.gouv.fr.

La présidente du CESIN est Mylène Jarossay.

CONTACT

06 09 56 63 17
contact@cesin.fr

ADRESSE

115 Rue Saint Dominique,
75007 Paris

CLUB EBIOS

www.club-ebios.org

Le Club EBIOS, créé en 2006, est une association à but non lucratif orientée vers la gestion des risques appliquée à la cybersécurité et à la protection de la vie privée. L'association rassemble des experts de la sécurité de l'information ainsi que des organismes publics et privés. Le Club EBIOS organise régulièrement des réunions autour de thématiques liées à la gestion des risques.

Le Club EBIOS participe à la publication de la méthodologie de gestion des risques « EBIOS » (Expression des besoins et indentification des objectifs de sécurité) en collaboration avec l'ANSSI. Ce document se présente comme un référentiel de la sécurité des systèmes d'information à destination des administrations publiques et des entreprises devant leur permettre d'identifier les risques à travers différents scénarios, de les analyser et de les traiter à travers des actions appropriées.

CONTACT

06 29 36 59 95
secretaire@apssis.com

ADRESSE

84 Rue du Luart,
72160 Duneau

ASSOCIATIONS

CLUB 27001

www.club-27001.fr

Le Club 27001 est une association à but non lucratif qui vise à promouvoir le partage de connaissances sur les normes ISO 27000 relatives à la sécurité de l'information. A ce titre, l'association réunit les professionnels de la sécurité de l'information et est également ouverte aux particuliers ayant un intérêt pour les normes ISO 27000 afin de former des groupes d'études sur différentes thématiques. Le Club 27001 dispose d'antennes dans plusieurs villes de France où ses membres se réunissent périodiquement en vue d'échanger sur l'évolution des normes et des certifications dans le domaine de la sécurité de l'information. Le Club 27001 organise également une conférence annuelle.

CONSEIL DES INDUSTRIES DE LA CONFIANCE ET DE LA SÉCURITÉ (CICS)

www.cics-org.fr

Afin de relever les multiples défis sécuritaires que pose la transformation numérique, l'industrie française de sécurité est encouragée à investir dans l'innovation pour développer de nouvelles technologies de sécurité. Pour mieux accompagner cette industrie dans la recherche de solutions et d'outils de confiance, le CICS fédère l'ensemble des PME, ETI et grandes entreprises de la sécurité. Le CICS, association à but non lucratif, a été créé en 2013 par quatre syndicats professionnels (GICAT, GICAN, GIFAS et FIEEC) dans le but de porter les intérêts des industriels de la sécurité au sein du COFIS, auquel a succédé le Comité stratégique de filière « Industries de la sécurité ». In fine, l'objet du CICS est de valoriser l'industrie de la sécurité auprès des instances nationales et de la promouvoir à l'exportation. Pour ce faire, le CICS favorise le travail collaboratif entre les acteurs de la filière autour de projets structurants : la création de l'Observatoire économique de la filière industrielle de sécurité et l'élaboration d'une politique industrielle de sécurité ont ainsi été lancés en 2017.

Le CICS a formulé des propositions pour réaliser son objectif global de renforcement de la souveraineté de l'industrie de sécurité :

- Développer une offre de Cloud de confiance permettant de protéger les données sensibles et les outils collaboratifs ;
- Déployer la CNIE en trois ans pour sécuriser les transactions à distance ;
- Déployer des plateformes d'intégration de données de sécurité au profit des collectivités territoriales ;
- Mettre en œuvre les expérimentations du programme de sécurité des JO Paris 2024 ;
- Financer un plan d'équipement cyber et continuité d'activité des centres hospitaliers universitaires du territoire national.

Le président du CICS est Marc Darmon.

CAMPUS CYBER

Initié par le Premier ministre à l'été 2019, le projet d'un Campus Cyber destiné à fédérer et faire rayonner l'écosystème français de la cybersécurité devrait se concrétiser au premier semestre 2021. Il s'agit de créer une communauté cyber susceptible de s'ériger en vitrine internationale du secteur et capable de rivaliser avec les grandes nations de la cybersécurité telles que les États-Unis d'Amérique, la Russie, Israël ou encore la Chine. Si la localisation du Campus à Paris est privilégiée, des antennes devraient voir le jour en région. Ce Campus Cyber réunira l'ensemble des acteurs publics, privés et académiques au sein d'un même lieu afin qu'ils partagent leurs compétences.

Le Campus Cyber sera centré sur quatre activités principales :

- La formation en cybersécurité ;
- La recherche et l'innovation ;
- L'accompagnement des entreprises et des administrations dans l'application des moyens de sécurité ;
- Le renforcement de la coopération opérationnelle, notamment avec un accroissement des échanges entre CERTs.

CYBERLEX

www.cyberlex.org

Parmi les nombreuses questions que soulève la transformation numérique, les enjeux juridiques recouvrent l'ensemble des sujets : protection des données personnelles, libertés numériques, responsabilité des plateformes, contrefaçon en ligne… CYBERLEX est une association centrée sur le droit du numérique, créée en 1996, qui réunit l'ensemble des acteurs du marché des technologies numériques : juristes d'entreprise, avocats, magistrats, professeurs de droit… L'association est envisagée comme un think-tank, c'est-à-dire un lieu d'échange sur l'actualité juridique liée aux nouvelles technologies. CYBERLEX entretient des partenariats avec d'autres associations du secteur numérique comme le CLUSIF et le CECyF afin de mener des travaux conjoints dans le cadre de groupes de travail. L'association organise des réunions mensuelles ainsi que des rencontres annuelles autour d'un thème donné.

CYBERLEX est présidé par Elise Dufour.

CONTACT

cyberlex@cyberlex.org

ADRESSE

4, Avenue Hoche,
75008 Paris

CYBER TASK FORCE

www.cybertaskforce.fr

La Cyber Task Force, créée en 2016 est un groupe de réflexion composé d'acteurs publics et privés. Les membres se réunissent environ une fois par mois pour échanger sur la confiance numérique et formuler des propositions visant les instances décisionnelles nationales et européennes.

La Cyber Task Force a défini quatre objectifs :

- Sensibiliser le public sur les enjeux de sécurité du numérique ;
- Informer le public de l'actualité du numérique sur les réseaux sociaux ;
- Décloisonner les acteurs ;
- Agir à travers la formulation de recommandations et de propositions.

CYBER CERCLE

www.cybercercle.com

CONTACT

contact@cybercercle.com

Cyber Cercle est un groupe de réflexion sur la confiance et la sécurité numériques créé en 2011. Il regroupe des acteurs publics et privé, dont des élus locaux et nationaux, spécialistes et non spécialistes de la sécurité des systèmes d'information, qui se réunissent une fois par mois. Le Cyber Cercle organise divers évènements comme les Rencontres parlementaires de la cybersécurité, qui ont lieu une fois par an, ou le Tour de France de la cybersécurité qui donne lieu à des évènements en région.

Les activités du Cyber Cercle sont articulées autour de deux objectifs principaux :

- Diffuser la culture de sécurité numérique au grand public ;
- Participer aux décisions politiques en formulant des recommandations et propositions.

La présidente du Cyber Cercle est Bénédicte Pilliet.

FÉDÉRATION DES INDUSTRIES ÉLECTRIQUES, ÉLECTRONIQUES ET DE COMMUNICATION (FIEEC)

www.fieec.fr

CONTACT

01 45 05 72 04
contact@fieec.fr

ADRESSE

17, Rue de l'Amiral Hamelin,
75116 Paris

La FIEEC, créée en 1997, est le résultat de l'intégration successive des syndicats professionnels des industries électriques, électroniques, puis de la communication. Elle regroupe aujourd'hui 28 organisations professionnelles de ces trois secteurs en vue de valoriser l'industrie française.

La FIEEC se donne cinq objectifs principaux :

- Promouvoir les industries électriques, électroniques et de communication afin de soutenir leur développement ;
- Être force de proposition quant aux évolutions réglementaires touchant les industries soutenues par la FIEEC ;
- Accompagner les entreprises en partageant les bonnes pratiques à adopter dans le respect des règles techniques et juridiques ;
- Rassembler l'ensemble des acteurs du secteur sous la bannière d'un interlocuteur unique en mesure de porter une vision unitaire et prospective sur l'industrie de demain ;
- Représenter les industries électriques, électronique et de communication auprès des instances nationales et européennes.

Le président de la FIEEC est Laurent Tardif.

GROUPEMENT INTERPROFESSIONNEL POUR LES TECHNIQUES DE SÉCURITÉ DES INFORMATIONS SENSIBLES (GITSIS)

www.gitsis.asso.fr

Le GITSIS, association à but non lucratif créée en 1991, rassemble les entreprises, dont des opérateurs d'importance vitale (OIV), spécialisées dans les systèmes d'armes, l'aéronautique, le nucléaire, les télécommunications et les technologies de pointe (électronique, informatique embarqué). L'objet du GITSIS est de fédérer ce réseau restreint d'entreprises ayant à charge la sécurité d'informations sensibles afin de leur permettre d'échanger et collaborer en toute confiance. En particulier, le GITSIS offre un cadre de coopération permettant à ces entreprises de se prémunir contre le risque de fuite du savoir-faire et du capital intellectuel. Le GITSIS représente ces entreprises auprès des instances nationales et européennes. Des travaux d'intérêt commun sur la protection des informations sensibles sont menés lors des réunions organisées par le GITSIS au profit des entreprises et du secret de défense.

La présidente du GITSIS est Valérie Levacque.

ASSOCIATIONS

GROUPEMENT DES INDUSTRIES DE CONSTRUCTION ET ACTIVITÉS NAVALES (GICAN)

www.gican.asso.fr

CONTACT

01 56 59 15 15
contact@gican.asso.fr

ADRESSE

10 Rue Treilhard,
75008 Paris

Le GICAN est un syndicat professionnel qui rassemble les industriels du secteur naval, aéronaval et maritime français. Le GICAN représente ses membres auprès des instances nationales et européennes dans le but de défendre les intérêts de l'industrie maritime et de promouvoir son savoir-faire à l'international. Le syndicat est organisé en comités spécialisés qui se réunissent régulièrement et réalisent des travaux en lien avec la problématique traitée par le groupe (défense, énergies marines renouvelables, sûreté/sécurité maritime…).

Dans le domaine du numérique plus particulièrement, le GICAN a défini des objectifs stratégiques pour l'industrie maritime française :

- Faire émerger les technologies nécessaires aux navires et structures du futur ;
- Relever le défi de la révolution numérique et de l'industrie du futur ;
- Assurer la sécurité des systèmes d'information, de commandement et de contrôle par le développement de la cybersécurité.

Le président du GICAN est Hervé Guillou.

GROUPEMENT DES INDUSTRIES FRANÇAISES DE DÉFENSE ET DE SÉCURITÉ TERRESTRE OU AÉROTERRESTRE (GICAT)

www.gicat.com

Le GICAT est un syndicat professionnel créé en 1978, qui réunit les industriels et les instituts de recherche du secteur de la défense et sécurité terrestre et aéroterrestre. Anciennement « Groupement des industries concernées par les matériels de défense terrestre », centré exclusivement sur l'industrie de défense, le GICAT a élargi son périmètre d'activités à la sécurité en 2011, un marché en croissance. Le GICAT a pour objet de représenter ses adhérents et de porter les intérêts de l'industrie de défense et sécurité terrestre et aéroterrestre auprès des institutions nationales et européennes.

Le GICAT organise ses activités autour de quatre objectifs :

- Se positionner en interlocuteur privilégié auprès des instances nationales et européennes pour défendre les intérêts de l'industrie de défense et de sécurité terrestre et aéroterrestre ;
- Accompagner le développement de ses adhérents en France et à l'international à travers la mise à disposition d'une offre de services (communication et affaires publiques, information stratégique, soutien export) ;
- Favoriser les échanges entre industriels du secteur ;
- Valoriser les savoir-faire et promouvoir l'offre industrielle, notamment à travers les salons internationaux organisés par sa filiale COGES (Eurosatory, ExpoDefensa, ShieldAfrica, Platinum Security Exhibition).

En matière de numérique, le GICAT a participé au lancement du cluster « Data Intelligence » en 2017, qui vise à développer des solutions françaises pour le renseignement et le traitement massif des données (big data).

Le président du GICAT est Marc Darmon.

DATA INTELLIGENCE CLUSTER

Site web : www.dataintelligencecluster.com

Le cluster Data Intelligence, lancé en 2017, regroupe 25 entreprises françaises innovantes (grands groupes, ETI, PME, Start-ups) développant des solutions de renseignement et de traitement massif des données. Cette initiative industrielle permet de proposer un guichet unique répondant aux besoins spécifiques d'acteurs institutionnels (services de renseignement, agences nationales de sécurité). Les entreprises membres disposent en effet de capacités opérationnelles complémentaires et proposent des produits et services innovants. Ainsi, le cluster propose une offre large, souveraine et adaptée de « solutions de bout en bout » : capteurs, data center mobiles, logiciels d'analyse, calculateurs hautes performances, stockage de données via des Clouds souverains, coffres-forts souterrains…

PLAQUETTE

https://www.gicat.com/wp-content/uploads/2019/01/PlaquetteData-FR.pdf

CONTACT

01 44 14 58 20

ADRESSE

3 Avenue Hoche,
75008 Paris,

GROUPEMENT DES INDUSTRIES FRANÇAISES AÉRONAUTIQUES ET SPATIALES (GIFAS)

www.gifas.fr

Le GIFAS, syndicat professionnel établi depuis 1975 sous son nom actuel, est le fruit de l'évolution de l'industrie aéronautique française. Le GIFAS fédère la filière aéronautique et spatiale autour d'intérêts communs tels que la recherche et l'innovation dans le but de favoriser son rayonnement à l'international. Le groupement est organisé en commissions et comités spécialisés qui permettent à leurs membres d'échanger sur diverses thématiques et de formuler des propositions qui, une fois approuvées par le Conseil d'administration, sont mises en œuvre par les membres permanents du GIFAS.

Le GIFAS vise trois missions principales :

- Représenter l'ensemble des acteurs de la filière aéronautique et spatiale française auprès des instances nationales, européennes et internationales et être force de propositions ;
- Défendre les intérêts communs de ses membres (recherche et développement, relations transatlantiques, marchés publics, environnement…) en collaboration avec l'État et les collectivités territoriales ;
- Promouvoir le savoir-faire de la filière grâce au soutien à la formation et à travers le Salon international de l'aéronautique et de l'espace organisé par sa filiale SIAE, qui a lieu tous les deux ans au Bourget à Paris.

Le président du GIFAS est Éric Trappier.

ASSOCIATIONS

GROUPEMENT D'INTÉRÊT PUBLIC «ACTION CONTRE LA CYBERMALVEILLANCE» (GIP «ACYMA»)

CONTACT

contact@cybermalveillance.gouv.fr

ADRESSE

GIP ACYMA,
6 rue Bouchardon
CS 50070
75481 Paris cedex 10

Au-delà des infrastructures de l'État, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE), les actes de cybermalveillance touchent également les citoyens français au quotidien. En 2015, le Premier ministre s'est saisi de cet enjeu dans sa Stratégie nationale pour la sécurité du numérique. Afin de proposer une assistance de proximité aux victimes de cyberattaques, le Groupement d'intérêt public « Action contre la cybermalveillance » (GIP « ACYMA ») a ainsi été créé en mars 2017, avec l'appui de l'ANSSI.

Le GIP « ACYMA » est un partenariat public-privé constitué d'une quarantaine de membres, qui rassemble les acteurs de la cybersécurité autour d'une mission d'intérêt général : la sécurité numérique. Le GIP oriente ses actions autour de trois axes :

- L'assistance aux victimes d'actes de cybermalveillance à travers le dispositif Cybermalveillance.gouv.fr ;
- L'information et la sensibilisation du public sur la sécurité numérique ;
- L'observation et l'anticipation du risque numérique.

L'actuel directeur général du GIP « ACYMA » est Jérôme Notin.

CYBERMALVEILLANCE.GOUV.FR

www.cybermalveillance.gouv.fr

CONTACT

contact@cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr, lancé en 2017 par le GIP « ACYMA », est un dispositif national de sensibilisation, de prévention et d'assistance aux victimes d'actes de cybermalveillance hors OIV et OSE. Cette plateforme s'adresse donc aux particuliers, entreprises et collectivités territoriales, hors périmètre d'intervention de l'ANSSI. La plateforme propose un diagnostic personnalisé du problème et une mise en relation de la victime avec un prestataire susceptible de le solutionner. L'outil de diagnostic se présente sous la forme d'un formulaire en ligne accessible aux particuliers et aux professionnels qui pensent être victimes de cybermalveillance.

HEXATRUST

Site web : www.hexatrust.com

CONTACT

contact@hexatrust.com

ADRESSE

118 Rue de Tocqueville,
75017 Paris

Hexatrust est une association créée en 2014, qui regroupe des entreprises aux profils variés, dans le but de promouvoir la sécurité des systèmes d'information. L'association a ainsi pour objet de réunir des sociétés de pointe dans leur domaine afin de proposer une offre complète de solutions souveraines en mesure de répondre aux besoins de cybersécurité et de cloud de confiance. Hexatrust organise des réunions mensuelles entre ses membres et travaille en lien avec Systematic.

Hexatrust a défini cinq engagements qui orientent ses actions en matière de cybersécurité et de cloud de confiance :

- Faciliter les échanges entre acteurs de la sécurité des systèmes d'information ;
- Sensibiliser le public sur la réglementation et promouvoir les bonnes pratiques ;
- Créer un cadre de référence valorisant les domaines d'expertise des membres de l'association à destination des utilisateurs ;
- Établir des schémas d'évaluation et de certification ;
- Agir en coordination avec les autres organismes du secteur afin de promouvoir conjointement les intérêts de ses membres.

Le président d'Hexatrust est Jean-Noël de Galzain (Wallix).

LA QUADRATURE DU NET

www.laquadrature.net

CONTACT

09 72 29 44 26
contact@laquadrature.net

ADRESSE

60, rue des Orteaux,
75020 Paris

La Quadrature du Net est une association à but non lucratif créée en 2013, qui a pour but de défendre les droits et les libertés fondamentales dans l'environnement numérique. L'association milite pour un maintien de l'Internet libre, neutre et décentralisé, offrant à ses utilisateurs un espace d'émancipation individuelle et collective à travers le partage des connaissances. Plus particulièrement, la Quadrature du Net investit les thématiques de la censure, de la surveillance ou encore de la protection des données personnelles pour réaliser des analyses et agir en faveur des libertés fondamentales à travers des recours ou des actions politiques.

La Quadrature du Net emploie trois principaux modes d'action pour réaliser ses objectifs :

- La sensibilisation et la formation de tout public aux enjeux sécuritaires du numérique et aux bonnes pratiques en informatique ;
- La réflexion, l'étude et la production d'analyses autour des enjeux politiques et juridiques du numérique ;
- L'action politique et juridique auprès des instances nationales et internationales compétentes (participation à des évènements, propositions auprès des décideurs politiques, actions juridiques…) afin de peser dans le débat public et ainsi favoriser l'évolution de la législation française et européenne sur le numérique.

ASSOCIATIONS

OBSERVATOIRE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DES RÉSEAUX (OSSIR)

www.ossir.org

L'OSSIR est une association à but non lucratif, créée en 1996, qui a pour objet de rassembler les utilisateurs portant un intérêt particulier à la sécurité des systèmes d'information et des réseaux. L'OSSIR dispose de trois groupes régionaux, avec des antennes à Paris, à Toulouse et en Bretagne, qui organisent des rencontres autour de l'actualité de la sécurité de l'information et des réseaux et proposent des présentations portant sur ces sujets ainsi que des solutions de sécurité pour les particuliers et les professionnels. L'OSSIR organise également chaque année une journée de la sécurité des systèmes d'information (JSSI) autour d'un thème particulier.

CONTACT

secretariat@ossir.org

ADRESSE POSTALE

45, Rue d'Ulm,
75230 Paris Cedex 5

OBSERVATOIRE DES LIBERTÉS ET DU NUMÉRIQUE

Face aux menaces que font peser les technologies de l'information et de la communication sur les droits et libertés individuelles, l'Observatoire des libertés et du numérique se donne pour objectif de mieux protéger les citoyens en complétant les actions menées par la CNIL. L'OLN a été créé en 2014 par cinq organisations syndicales et associatives (Ligue des droits de l'homme, Syndicat des avocats de France, Syndicat de la magistrature, Centre d'études sur la citoyenneté, l'informatisation et les libertés, Creis Terminal). En particulier, l'Observatoire s'intéresse aux thématiques de l'internet des objets, des dispositifs de surveillance (vidéosurveillance, écoutes, biométrie…), du fichage (fichiers FNAEG et FAED), ou encore de la neutralité du Net.

L'OLN se concentre sur les actions suivantes :

> Sensibilisation et information du public sur les risques liés à l'atteinte à la vie privée et aux informations personnelles sur Internet ;

> Actions juridiques en faveur de la défense des droits et libertés individuelles.

PÔLE D'EXCELLENCE CYBER (PEC)

www.pole-excellence-cyber.org

Initié en 2014 par le ministère des Armées (pacte défense cyber) et par le Conseil régional de Bretagne (pacte d'avenir) avec une portée nationale et un objectif de rayonnement international, le Pôle d'excellence cyber s'appuie sur le tissu académique et industriel régional ainsi que sur ses partenaires nationaux et européens.

Le Pôle d'excellence cyber a pour mission de faire converger les compétences et de stimuler le développement de :

- L'offre de formation en cybersécurité (initiale, continue, supérieure) ;
- La recherche académique en cybersécurité ;
- La base industrielle et technologique de cybersécurité, avec une attention particulière portée aux PME-PMI innovantes, aussi pour les porter à l'export.

Le Pôle d'excellence cyber répond ainsi à trois enjeux majeurs, au profit de la communauté nationale de cyberdéfense et de cybersécurité :

- Disposer des compétences nécessaires pour répondre aux besoins de développement de la filière ;
- Disposer d'une offre de recherche en adéquation avec les besoins du ministère et des industriels ;
- Disposer de produits et de services de confiance.

Une organisation horizontale, collaborative et en réseau, structurée en association Loi 1901, qui associe des acteurs civils et militaires, publics et privés, académiques et industriels, en s'appuyant sur leurs compétences et leurs champs d'intervention respectifs.

Des groupes de travail spécialisés par thématique (référentiel, formation, plates-formes, recherche, développement industriel, …) réunissent l'ensemble des membres et partenaires du Pôle. Cette approche pragmatique offre au Pôle la meilleure concertation possible entre les différents acteurs, dans un souci permanent de cohérence, d'efficacité, de réactivité et de fonctionnement en mode projet.

Plusieurs chaires industrielles, la chaire de cyberdéfense, la chaire cyber navale, la chaire cyb'air, analyse de la menace, des systèmes industriels critiques, etc. Plus de 20 nouvelles formations créées, un travail de fond avec le Rectorat pour former à la cybersécurité les BTS STI2D, SIO, SN, 12 M€ d'investissement sur 6 ans dans des thèses, des post doc et des séminaires scientifiques, 6,3 M€ d'achat de plates-formes de recherche (CPER) et de formation sont les principales réalisations du Pôle.

Outre le ministère des Armées et la Région Bretagne, et les organismes qui en dépendent, le Pôle d'excellence cyber compte aujourd'hui une soixante dizaine de membres actifs : douze grands groupes (Airbus Cyber Security, Bertin IT, Capgemini, DCI, EDF, La Poste, Naval Group, Nokia, Orange, Safran, Sopra-Steria, Thales), des ETI, des PME/PMI, des laboratoires de recherche, des universités et écoles d'ingénieurs.

CONTACT

contact@pole-execellence-cyber.org

SYSTEMATIC

www.systematic-paris-region.org

Systematic est une association à but non lucratif créée en 2005, qui se définit comme un Pôle européen de compétitivité réunissant des acteurs de l'écosystème des Deep Tech, ou de l'innovation structurante. Une majorité d'entreprises (PME, ETI, Start-ups, Grands groupes) sont présentes parmi les membres de l'association, aux côtés d'acteurs académiques et de collectivités territoriales. Systematic est structuré en six Hubs, ou pôles, qui permettent de réunir les membres afin qu'ils échangent autour de différentes thématiques liées aux ruptures technologiques : intelligence artificielle, cybersécurité, infrastructure digitale et internet des objets, ingénierie digitale, optique et photonique, open source. En plus de ces six pôles, trois groupes travaillent autour des enjeux économiques et sociétaux liés à la transformation numérique sur les thèmes de la société, de l'industrie et service, et des territoires.

Les principales actions menées par Systematic sont les suivantes :

- Accompagner les projets d'innovation à travers une plateforme d'innovation ouverte ;
- Faciliter la mise sur le marché des nouveaux produits, services et usages développés ;
- Apporter un soutien opérationnel aux entreprises afin d'accélérer leur croissance et leur compétitivité à travers cinq volets : visibilité, accès au marché, recherche de financements, management, recrutement ;
- Soutenir le développement économique du territoire et sa valorisation.

Le président de Systematic est Jean-Luc Beylat.

CONTACT

01 69 08 06 8
contact@systematic-paris-region.org

ADRESSE

Site Nano-Innov,
Bâtiment 86,
2 Boulevard Thomas Gobert,
CS 70005,
91127 Palaiseau Cedex

SYNDICAT PROFESSIONNEL DES FABRICANTS DE FILS ET CÂBLES ÉLECTRIQUES ET DE COMMUNICATION (SYCABEL)

www.sycabel.com

Le SYCABEL est un syndicat professionnel créé en 1917, qui a pour objet de représenter l'industrie des fils et câbles électriques et de communication. Cette industrie de haute technologie est stratégique car elle répond à des enjeux transversaux : l'énergie et la communication. De fait, cette industrie recouvre de multiples secteurs comme la construction, les infrastructures de transport ou encore l'équipement industriel. Le SYCABEL est composé de commissions transversales et de comités spécialisés dont les membres travaillent sur des problématiques liées à la filière (développement durable, matières premières, télécommunications...).

Les missions du SYCABEL sont les suivantes :

- Analyser et surveiller le marché du câble et les facteurs influents ;
- Réaliser des études des composantes de coût et des publications d'indicateurs ;
- Développer l'industrie du câble en fonction des besoins sociétaux ;
- Piloter et coordonner la contribution de la filière à l'élaboration de nouvelles normes ;
- Représenter l'industrie du câble auprès des instances nationales et européennes ;
- Entretenir des relations institutionnelles avec les grands acteurs du secteur.

Le président du SYCABEL est Eric Francey (Nexans).

CONTACT

01 47 64 68 10
dg@sycabel.com

ADRESSE POSTALE

17 Rue de l'Amiral Hamelin,
75116 Paris

ASSOCIATIONS

SIGNAL SPAM

www.signal-spam.fr

Signal Spam est une association à but non lucratif, créée en 2005, constituée d'un important réseau d'acteurs publics et privés ayant pour intérêt commun la lutte contre le Spam, c'est-à-dire les communications non sollicitées et importunes. La plateforme en ligne permet aux internautes de signaler les abus constatés sur leur messagerie, qu'il s'agisse de Spam ou de phishing (hammeçonnage). Ces signalements sont ensuite retransmis aux autorités compétentes et aux acteurs concernés afin qu'ils les traitent. De fait, ils peuvent constituer une base de preuves numériques utile aux services de police et de gendarmerie, permettant de compléter les dossiers d'instruction liés à la cybercriminalité.

Ainsi, afin de lutter contre le Spam, Signal Spam assure les missions suivantes :

- Définition, mise en œuvre et suivi du système de traitement informatisé des Spam signalés ;
- Transfert des signalements reçus aux autorités compétentes et aux acteurs concernés(autorités de protection des données, hébergeurs web, routeurs expéditeurs de messages, services de police et de gendarmerie, annonceurs et fournisseurs d'accès internet) ;
- Sensibilisation et information du public concernant les outils et pratiques permettant de lutter contre les Spams ;
- Participation au débat public et aux actions entreprises par les instances nationales et européennes en matière de lutte contre les Spams.

CONTACT

contact@signal-spam.net

ADRESSE

8 Rue du Faubourg Poissonnière,
75010 Paris

ORGANISMES DE RECHERCHE

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNRS)

http://www.cnrs.fr

Le CNRS est un établissement public à caractère scientifique et technologique (EPST) créé en 1939 qui a pour mission d'« Identifier, effectuer ou faire effectuer, seul ou avec ses partenaires, toutes les recherches présentant un intérêt pour la science ainsi que pour le progrès technologique, social et culturel du pays » .

Le président directeur général du CNRS est Antoine Petit.

ADRESSE

2 Rue Michel-Ange,
Paris

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA)

www.inria.fr

À la croisée des mondes académique et industriel, l'INRIA est un est un établissement public à caractère scientifique et technologique (EPST) qui a pour objet de « pourvoir la France en technologies de pointe et développer son autonomie et sa souveraineté ». Initialement créé sous le nom d'IRIA en 1967, l'INRIA existe sous son nom actuel depuis 1979. Depuis ses débuts, l'INRIA a pour objet de décloisonner la recherche pour la mettre au service de l'industrie et de la transformation numérique française. L'INRIA encourage l'innovation autour d'un modèle interdisciplinaire d'« équipe-projet » qui permet de mettre en place des partenariats industriels. Afin de promouvoir la culture numérique, des programmes éducatifs sont mis en place par l'INRIA en lien avec l'Éducation nationale comme Class'Code ou INRIA Learning Lab. Des partenariats internationaux sont également développés.

Les principaux axes de recherche sur lesquels se concentrent les scientifique de l'INRIA sont les suivants :

- Intelligence artificielle ;
- Algorithmes et informatique quantiques ;
- Sécurité numérique ;
- Sciences des données ;
- Calcul haute performance ;
- Numérique frugal ;
- Logiciel ;
- Santé numérique.

2

ORGANISMES EUROPÉENS DE LA CYBERSÉCURITÉ

AGENCE EUROPÉENNE CHARGÉE DE LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION (ENISA)

www.enisa.europa.eu

CONTACT

+30 28 14 40 97 11

ADRESSE DE L'ANTENNE SITUÉE À ATHÈNES

Visilissis Sofias Str 1,
Maroussi 15124, Attiki
GREECE

ADRESSE DU SIÈGE SOCIAL À HÉRAKLION

Nikolaou Plastira 95,
Vassilika Vouton,
70013 Heraklion,
GREECE

L'Agence européenne pour la sécurité (ou European Union Agency for Cybersecurity (ENISA)) a été créée en 2004 dans le but d'accompagner les États membres dans le développement de leurs capacités en matière de cybersécurité et de favoriser la coopération européenne dans ce domaine. Le règlement européen de 2019, connu sous le nom de « Cybersecurity Act », a consolidé l'ENISA et renforcé ses missions en lui octroyant un mandat permanent et en définissant un cadre de certification de cybersécurité dans lequel l'ENISA joue un rôle prépondérant. Ainsi, l'ENISA est un interlocuteur privilégié pour les États membres et un véritable point de référence auprès des institutions européennes en matière de cybersécurité. Son conseil d'administration est composé de représentants des États membres et de la Commission européenne.

L'ENISA assure les missions suivantes :

- Favoriser le développement d'un cadre de coopération effectif entre les grands acteurs de la cybersécurité des différents États membres (organismes publics et privés) et les institutions et agences de l'Union ;
- Favoriser la coopération entre États membres et entre États membres et institutions de l'Union en matière de cybersécurité ;
- Participer à l'élaboration d'une politique commune de cybersécurité recouvrant le large spectre des secteurs concernés par la transformation numérique ;
- Promouvoir le renforcement des capacités et l'émergence des talents en matière de cybersécurité ;
- Apporter une expertise indépendante et transparente reposant sur des normes communes.

EUROJUST

www.eurojust.europa.eu

CONTACT

+31 70 412 5000
info@eurojust.europa.eu

Eurojust est l'agence européenne de coopération judiciaire entre les États membres, qui a pour objet de faciliter la coordination des enquêtes et poursuites judiciaires dépassant le cadre d'un seul État afin de lutter contre les formes graves de criminalité organisée. Cet organe a été créé en 2002 et rassemble des officiers et magistrats de liaison issus des différents États membres de l'Union. De nombreux types de criminalité sont traités tels la criminalité informatique, la fraude et la corruption, la criminalité contre l'environnement…

Les trois principales missions d'Eurojust sont les suivantes :

- Promouvoir et améliorer la coordination entre les autorités policières et judiciaires des États membres ;
- Améliorer l'entraide judiciaire internationale et l'exécution des demandes d'extradition ;
- Soutenir les autorités judiciaires des États membres afin de renforcer l'efficacité de leurs enquêtes et poursuites.

En matière de cybercriminalité, Eurojust est à l'origine du réseau européen anti-cybercriminalité (EJCN) et coopère étroitement avec Europol et l'EC3, notamment au sein du Projet SIRIUS. De plus, l'agence européenne publie chaque année le Cybercrime Judicial Monitor (CJM) à l'attention des autorités judiciaires impliquées dans la lutte contre la cybercriminalité.

RÉSEAU JUDICIAIRE EUROPÉEN EN MATIÈRE DE CYBERCRIMINALITÉ (EJCN)

Le Réseau judiciaire européen en matière de cybercriminalité (ou European Judicial Cybercrime Network (EJCN)) a été créé en 2016 par Eurojust. Il s'agit d'une structure de soutien aux autorités judiciaires des États membres de l'Union qui a pour objet de leur apporter une expertise spécialisée et de promouvoir l'échange d'expériences et de bonnes pratiques en matière de lutte contre la cybercriminalité. L'ECJN se présente comme un facilitateur des échanges entre les parties prenantes contribuant au respect de l'État de droit dans le cyberespace (Europol, Eurojust, ENISA, Interpol, CEPOL), le secteur privé (prestataires de services) et d'autres acteurs concernés.

L'EJCN assure les missions suivantes :

- Diffuser et échanger des informations relatives aux législations nationales, à la jurisprudence, à la coopération internationale, aux savoir-faire et bonnes pratiques aux États membres en matière de lutte contre la cybercriminalité et fournir des outils aux professionnels ;
- Encourager le recours à Eurojust dans les affaires transfrontalières liées à la cybercriminalité et dans les enquêtes utilisant le cyberespace.

PROJET SIRIUS

CONTACT

sirius.eurojust@
eurojust.europa.eu

Le Projet SIRIUS est né d'une initiative commune aux deux agences européennes Europol et Eurojust en 2017 avec un objectif simple : créer une plateforme facilitant les échanges de preuves numériques (e-evidence : courriers électroniques, contenus de messageries instantanées…) dans le cadre des enquêtes et poursuites. En effet, les procédures judiciaires et policières se trouvent parfois entravées par les dénis d'accès aux données situées à l'étranger et fortement complexifiées par la quantité d'informations qui circulent dans le cyberespace.

De fait, SIRIUS assure les missions suivantes :

- Proposer des formations de haut niveau en présentiel et en e-learning à travers la plateforme de l'Agence européenne pour la formation des services répressifs (CEPOL) ;
- Fournir des outils et solutions améliorant l'effectivité des investigations menées dans le cyberespace et faciliter les échanges entre professionnels via plateforme d'Europol pour les experts (ou European Platform of Experts (EPE)).

EUROPOL

CONTACT

+31 70 302 5000

ADRESSE

Europol, Eisenhowerlaan
73, 2517 KK The Hague,
The Netherlands

ADRESSE POSTALE

Europol P.O. Box 908
50, 2509 LW The Hague,
The Netherlands

EUROPOL

www.europol.europa.eu

Europol est l'agence européenne compétente en matière de répression de la criminalité en charge de la coopération policière entre les États membres en matière de lutte contre le trafic de stupéfiants, contre le crime organisé et contre le terrorisme. Créée en 1999, Europol est l'héritière de la structure intergouvernementale TREVI.

Les principales missions assurées par Europol sont les suivantes :

- Veiller à l'application du droit et appuyer les opérations de maintien de l'ordre ;
- Centraliser les informations relatives aux activités criminelles ;
- Apporter une expertise aux autorités chargées de l'application de la loi.

Plus particulièrement, Europol exerce ses compétences en matière de lutte contre la cybercriminalité à travers trois unités spécialisées : le Centre européen de lutte contre la cybercriminalité (EC3), l'Unité de signalement des contenus sur Internet (EU IRU) et la Joint Cybercrime Taskforce (J-CAT).

La directrice d'Europol est Catherine de Bolle.

CENTRE EUROPÉEN DE LUTTE CONTRE LA CYBERCRIMINALITÉ (EC3)

En matière de lutte contre la cybercriminalité, l'Union européenne encourage la coopération policière et judiciaire entre États membres à travers la mise en place d'autorités répressives pour répondre aux nouvelles menaces. Le Centre européen de lutte contre la cybercriminalité (ou European Cybercrime Centre (EC3)) a ainsi été créé en 2013 au sein d'Europol dans le but de coordonner les opérations de lutte contre la criminalité organisée qui prospère dans le cyberespace. Ainsi, l'EC3 s'attache à démanteler les réseaux criminels qui commettent des infractions pénales à l'aide de réseaux de communication électronique et de systèmes d'information et/ou contre ces réseaux et systèmes. En particulier, l'EC3 se concentre sur la lutte contre la fraude en ligne, la maltraitance des enfants sur Internet ou encore les crimes de haute technologie comme les rançongiciels.

Les principales missions de l'EC3 sont les suivantes :

- Centraliser et analyser les renseignements relatifs à la cybercriminalité provenant d'un grand nombre de sources afin d'évaluer l'état de la menace ;
- Apporter une expertise aux États membres afin de favoriser le renforcement des capacités de leurs services de police et de justice ;
- Apporter un soutien opérationnel aux États membres en matière de lutte contre la cybercriminalité à travers la mise en place d'équipes communes d'enquête et la mise à disposition de solutions et d'outils ;
- Représenter les services d'enquête européens spécialisés dans la lutte contre la cybercriminalité auprès d'Interpol et des autres unités internationales.

JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

L'Unité J-CAT a été créée en 2014 au sein du Centre européen de lutte contre la cybercriminalité (EC3). Il s'agit d'une équipe opérationnelle permanente d'officier de liaison spécialisés dans la lutte contre la cybercriminalité et détachés de différents États membres et non-membres de l'Union. De même que le cyberespace ne connaît pas de frontières, les opérations de la J-CAT sont transfrontalières et peuvent s'étendre au-delà des frontières de l'Union.

Cette unité se concentre sur quelques affaires de haute priorité, sélectionnées au préalable parmi les affaires proposées par les officiers de liaison de chaque État. Les affaires sélectionnées font l'objet d'un plan d'action mené par le pays à l'origine de la proposition, avant d'être portées devant les autorités judiciaires compétentes.

UNITÉ DE SIGNALEMENT DES CONTENUS SUR INTERNET (EU IRU)

L'Unité de signalement des contenus sur Internet (ou EU Internet Referal Unit (EU IRU)) est une unité de surveillance de l'Internet créée en 2015, rattachée au Centre antiterroriste européen d'Europol, qui a pour objet d'identifier les contenus illicites partagés sur Internet et sur les réseaux sociaux aux fins de blocage. Pour ce faire, l'EU IRU travaille en coopération avec les acteurs du secteur privé comme les fournisseurs d'accès Internet.

Les missions de l'EU IRU sont les suivantes :

- Apporter un support aux autorités européennes compétentes à travers une analyse stratégique et opérationnelle des contenus terroristes ;
- Signaler les contenus en ligne à caractère terroriste et extrémiste violent et partager ces signalements aux partenaires concernés ;
- Détecter et ordonner le retrait des contenus en ligne utilisés par les réseaux de contrebande pour attirer les migrants et réfugiés.

EUROPEAN CYBER SECURITY ORGANISATION (ECSO)

Site web : www.ecs-org.eu

L'European Cyber Security Organisation (ECSO) est une association à but non lucratif créée en 2016. ECSO représente la Commission européenne pour la mise en place du Contrat de partenariat public-privé pour la cybersécurité (cPPP). A ce titre, ECSO rassemble les principaux acteurs européens de la cybersécurité dans le but de développer l'écosystème européen de la cybersécurité et de le rendre compétitif à l'international.

Les principales missions qu'assure ECSO sont les suivantes :

- Travailler en collaboration avec la Commission européenne et les administrations nationales des États membres de l'Union afin de promouvoir la recherche et l'innovation dans le domaine de la cybersécurité ;
- Proposer un agenda stratégique pour la recherche et l'innovation ainsi qu'une feuille de route régulièrement actualisée ;
- Favoriser le développement du marché européen de la cybersécurité et les investissements dans l'innovation ;
- Encourager la croissance et la compétitivité de l'industrie européenne de cybersécurité à travers des technologies, solutions et services innovants ;
- Prendre part à l'élaboration et à la mise en œuvre des politiques industrielles européennes de cybersécurité pour promouvoir l'autonomie numérique à travers l'utilisation de solutions sécurisées et de confiance ;
- Soutenir le développement et les intérêts de l'écosystème européen de la cybersécurité, y compris le développement des formations et de la recherche.

L'actuel président d'ECSO est Philippe Vannier.

CONTACT

+32 27 77 02 58
secretariat@ecs-org.eu

ADRESSE

10 Rue Montoyer,
1000 Bruxelles,
Belgique

PÔLE D'EXCELLENCE
CYBER

12 B rue du Patis Tatelin
35700 RENNES
France

www.pole-excellence-cyber.org