TELECOM ParisTech

Une école de l'IMT

CONFIANCE NUMÉRIQUE

CYBERSÉCURITÉ, RISQUE ET FIABILITÉ

FORMATION, RECHERCHE, INNOVATION

École de l'IMT, Télécom ParisTech est la première grande école française d'ingénieurs généralistes du numérique. Elle est membre fondateur d'un regroupement de cinq grandes écoles publiques : l'École polytechnique, l'ENSAE ParisTech, l'ENSTA ParisTech, Télécom ParisTech et Télécom SudParis. Ce regroupement amplifiera le rayonnement de la recherche et des formations françaises à l'international. Télécom ParisTech développe chez ses futurs ingénieurs l'ouverture, l'interculturalité, la pluridisciplinarité ainsi qu'une connaissance approfondie des nouveaux modèles économiques, des entreprises innovantes et des défis sociétaux actuels. Elle accueille plus de 1500 étudiants chaque année. Évaluée A+ par le HCERES, sa recherche présente six grands axes thématiques : Sciences des données et intelligence artificielle, Design interaction perception, Innovation numérique, Modélisation mathématique, Très grands réseaux et systèmes et Confiance Numérique.

LA CYBERSÉCURITÉ : UN MARCHÉ EN PLEINE ÉBULLITION

Conscient des enjeux en termes de cybersécurité, le gouvernement français a mis sur pied la loi de programmation militaire dès 2013. Cette loi impose à 200 opérateurs d'importance vitale (OIV) de secteurs très divers (transports, énergie, alimentation ou encore finance) plusieurs obligations : mettre en place des infrastructures spécifiques, se soumettre à des contrôles et déclarer les incidents sérieux à l'Agence nationale de la sécurité des systèmes d'information. Cette loi a généré un besoin très important de spécialistes en cybersécurité.

UNE EXPERTISE AU CŒUR DE TÉLÉCOM PARISTECH

La cybersécurité est au centre des préoccupations de Télécom ParisTech qui en a fait un de ses axes de recherche : l'axe Confiance Numérique. La sécurité et la sûreté y sont étudiés à tous les niveaux hiérarchiques des systèmes : de la couche physique aux applications en passant par les outils mathématiques, les couches logicielles, les réseaux et les aspects sociétaux.

CHIFFRES CLÉS

RECHERCHE

32 enseignants -chercheurs

40 doctorants

3 Chaires de recherche

3 laboratoires communs

16 partenaires industriels

INNOVATION

3 start-up hébergées à l'incubateur

FORMATION

16 cursus de formation

55 diplômés par an

Plusieurs dizaines de stagiaires par an

FORMATION INITIALE

Depuis 2014, le volume d'opportunités d'emplois dans le domaine de la cybersécurité a été multiplié par quatre et on s'attend à une création de 1 400 postes d'ici 2020 en France[1]. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) estime que moins de 30% des besoins en cybersécurité sont couverts et est, elle-même, passée de 500 à 600 collaborateurs depuis la fin de l'année 2017.

CYCLE INGÉNIEUR : FILIÈRE « SÉCURITÉ DES RÉSEAUX ET INFRASTRUCTURES INFORMATIQUES »

La filière SR2I a pour objectif de former des ingénieurs hautement qualifiés en Cybersécurité en leur fournissant les bases nécessaires du point de vue théorique et pratique afin de maîtriser les aspects techniques, organisationnels ainsi que juridiques des infrastructures informatiques et des réseaux dans leurs diverses mutations afin de gérer les risques associés.

Il s'agit de :

- Maîtriser les différents services de sécurité et leurs mécanismes cryptographiques
- Savoir évaluer les risques, les menaces et les conséquences
- Maîtriser l'analyse et la mise en œuvre des attaques
- Maîtriser les outils d'analyse et d'audit
- Maîtriser les techniques de développement d'applications et de protocoles sécurisés
- Mettre en œuvre des infrastructures de confiance

Une maîtrise des concepts et des outils se fait à travers un enseignement théorique renforcé par la pratique sous une forme diversifiée : ateliers, travaux pratiques, projets en groupes, projets individuels.

[1] Source : étude OPIIEC, mai 2017.

« J'ai choisi la filière SR2I pour étudier les questions de sécurité au sein des systèmes. Et quoi de mieux pour protéger les systèmes que d'apprendre à les attaquer ? Nous apprenons ainsi à exploiter les vulnérabilités les plus courantes, ainsi que d'autres plus poussées au cours de projets de développement autour de sujets que nous choisissons ! La filière vise ainsi à former des futurs ingénieurs conscients des problématiques de sécurité, tant techniques qu'organisationnelles, qui sont toujours plus demandés dans les entreprises : c'est passionnant ! »

- Emilien Lavie, promo 2018

FORMATION CONTINUE

Télécom Evolution conçoit et produit des solutions de formation continue innovantes, en intégrant les compétences pédagogiques de trois grandes écoles d'ingénieurs : IMT Atlantique, Télécom ParisTech et Télécom SudParis. Portée par l'adéquation aux besoins réels des entreprises et l'excellence des contenus nourris par des centres de recherche académique, ces formations, certifiantes, en inter-entreprises ou sur mesure, sont l'assurance d'une expérience de formation unique.

CERTIFICAT D'ÉTUDES SPÉCIALISÉES (CES)

Les CES sont des formations certifiantes destinées aux professionnels souhaitant accéder à des métiers ou fonctions spécifiques en forte demande dans le domaine du numérique. Ils sont constitués d'un cursus de formation à haute valeur ajoutée associé à un dispositif de certification. Leur rythme concilie formation et activité professionnelle à raison de 18 à 30 jours répartis sur six à douze mois.

CES « CONSULTANT SÉCURITÉ DES SYSTÈMES ET DES RÉSEAUX »

3 à 5 jours par mois étalés sur 6 mois / Eligible au CPF

Cette formation permet d'apporter les connaissances nécessaires à l'élaboration et à la mise en place d'un plan de sécurité destiné à la protection des ressources vitales de l'entreprise, contre les agressions internes et externes de toute nature : intrusion, destruction, espionnage ou vol.

CES « ARCHITECTURE EN CYBERSÉCURITÉ, RSSI »

5 jours par mois étalés sur 6 mois / Eligible au CPF

Ce CES forme des cadres hautement qualifiés en leur fournissant des connaissances et compétences théoriques, techniques et organisationnelles pour définir, déployer et gérer une architecture de sécurité dans les différents contextes professionnels auxquels ils seront confrontés.

FORMATIONS COURTES

Télécom Evolution propose 12 stages de 2 à 5 jours permettant un focus sur des compétences précises. Quatre d'entre eux offrent un panorama plus général et s'adressent à un public de non spécialistes.

> Comprendre la sécurité numérique pour dialoguer avec les experts (tout public)
> Sécurité des réseaux
> Sécurité des systèmes d'information
> Comprendre la cryptographie et son utilité dans le monde numérique [Nouveau]
> Sécurité des objets connectés et de l'Internet des Objets (IoT)
> Introduction à la sécurité du big data
> Sécurité Web : développer et héberger de manière sûre [Nouveau]
> Sécurité des réseaux et environnements mobiles 2G, 3G, 4G (tout public) [Nouveau]
> Sécurité des systèmes embarqués
> Rétro-ingénierie appliquée à la cybersécurité
> Mécanisme de sécurité des environnements Windows
> Mise en œuvre d'audit de sécurité et de tests d'intrusions [Nouveau]
> Conception d'architecture blockchain
> Mise en œuvre de stratégie blockchain
> Droit, RGPD et protection des données
> Aspects avancés du coud computing avec OpenStack : sécurité et déploiement
> Réseaux et télécommunications : présent et avenir
> WiFi et réseaux sans fil : concepts et mise en œuvre

Pour en savoir plus
www.telecom-evolution.fr/domaines/cybersecurite

FORMATION CONTINUE

Le Mastère Spécialisé® est un diplôme labellisé délivré par un établissement membre de la Conférence des grandes écoles (CGE) dans le cadre d'une formation accréditée. Ce label garantit la vocation professionnelle affirmée, la rigueur et la technicité des enseignements. Il permet aux étudiants de développer leurs meilleurs atouts et constitue un tremplin pour leur carrière professionnelle.

EXECUTIVE MASTÈRE SPÉCIALISÉ® « ARCHITECTE RÉSEAUX ET CYBERSÉCURITÉ »

Durée : 16 mois, dont 10 mois de cours à temps partiel (6 jours de cours par mois) + 4 à 6 mois de stage de thèse professionnelle.

Ce Mastère Spécialisé® forme des architectes dans le domaine des réseaux télécom et de la cybersécurité. L'architecte maîtrise les technologies du réseau et de la sécurité afin de piloter les équipes techniques dans la conception de projets télécom.

APERÇU DU PROGRAMME

> Sécurité des systèmes d'information, de l'internet des objets et du big data
> Piratage informatique de type APT (menace persistante avancée)
> Sécurité des réseaux TCP/IP et WLAN
> Aspects juridiques, cybercriminalité
> Protocoles IPv6
> Réseaux radio-mobiles jusqu'à la 5G
> Référentiel ITIL, certification « Passeport Services »
> Architecture d'une plateforme de services IMS

DÉBOUCHÉS POSSIBLES

> Architecte produits et solutions, services et sécurité
> Concepteur de réseaux et services sécurisés
> Ingénieur exploitation et maintenance, réseaux et sécurité
> Chef de projet dans la transformation numérique

Pour en savoir plus
www.telecom-paristech.fr/architecte-reseaux-securite

MASTÈRE SPÉCIALISÉ® « CYBERSÉCURITÉ ET CYBERDÉFENSE »

Durée : 15 mois, dont 9 mois de cours à temps plein + 4 à 6 mois de stage de thèse professionnelle

Le Mastère Spécialisé® couvre l'ensemble des composantes fondamentales nécessaires à la maîtrise, l'analyse, la conception et la mise en œuvre de solutions de sécurité des systèmes et réseaux informatiques.

APERÇU DU PROGRAMME

> Service de sécurité et mécanisme de cryptographie
> Méthodes, pratiques et Hacking avancé
> Principes, méthodes architecture et protocole, contrôle d'accès et gestion des identités
> Forensic des systèmes et des réseaux
> Sécurité des réseaux et des systèmes informatiques
> Sûreté de fonctionnement et sécurité
> Blockchain et crypto-monnaie : analyse et mise en œuvre

DÉBOUCHÉS POSSIBLES

> Responsable de la Sécurité des Systèmes d'Information (RSSI)
> Responsable du Plan de Continuité d'Activité (RPCA)
> Directeur de programme sécurité
> Chef de projet sécurité, Développeur sécurité

Pour en savoir plus
www.telecom-paristech.fr/cybersecurite-cyberdefense

RECHERCHE

FORCES DISCIPLINAIRES DE RECHERCHE

32
enseignants-chercheurs

40
doctorants

5
ingénieurs

5
post-doctorants

150
publications par an

10
travaux de thèse par an

4 DÉPARTEMENTS, UNE COUVERTURE PLURDISCIPLINAIRE EXHAUSTIVE

IMAGE DONNÉES ET SIGNAL

Thématiques de recherche :
machine learning, détection d'intrusion et de fraudes

COMMUNICATION ET ÉLECTRONIQUE

Thématiques de recherche :
Plateforme Ttool (conception de systèmes embarqués sûrs et sécurisés), sureté de fonctionnement, sécurité des systèmes embarqués (résistance face aux attaques matérielles, et support matériel pour la cybersécurité)

INFORMATIQUE ET RÉSEAUX

Thématiques de recherche :
Théorie des jeux appliquée à la sécurité, communications sécurisées dans les réseaux véhiculaires

SCIENCES ÉCONOMIQUES ET SOCIALES

Thématiques de recherche :
Protection des données personnelles et financières

CHAIRES DE RECHERCHE

Télécom ParisTech, en partenariat avec des entreprises et avec le soutien de la Fondation Mines-Télécom, s'investit dans trois chaires de recherche liées au domaine de la cybersécurité et trois laboratoires de recherche.

CONNECTED CARS AND CYBER SECURITY

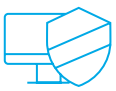
Portée par les professeurs Guillaume Duc et Houda Labiod, la chaire se concentre sur les problématiques de cybersécurité liées à l'émergence d'une nouvelle mobilité qui cristallisent des challenges techniques, sociaux, éthiques, économiques et juridiques parmi les plus pointus et délicats de la transformation numérique. Entreprises partenaires : Nokia, Renault, Thales, Valeo, Wavestone.

www.telecom-paristech.fr/C3S

VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

Chaire de l'IMT, elle bénéficie du mécénat de : Groupe IN, BNP Paribas, Qwant, Sopra Steria, Orange, Dassault Systèmes et d'un partenariat conclu avec la CNIL et la DINSIC. Coordonnée par Claire Levallois-Barth, maître de conférences en droit, elle traite des aspects juridiques, techniques, économiques et philosophiques concernant la collecte, l'utilisation et le partage des informations personnelles.

www.informations-personnelles.org



CYBER CNI SÉCURITÉ DES INFRASTRUCTURES CRITIQUES

Cyber CNI est une chaire de recherche et d'enseignement dans le domaine de la Cybersécurité des infrastructures Critiques. IMT Atlantique, Télécom ParisTech et Télécom SudParis sont partenaires aux côtés de Orange, Airbus Défense, BNP Paribas, Société générale, EDF, Amossys, Nokia et La Poste.

www.chairecyber-cni.org

LABORATOIRES COMMUNS

IDENTITY & SECURITY ALLIANCE (ISA)

Le laboratoire commun de Idemia (ex-Morpho) et Télécom ParisTech prend en charge les défis technologiques associés à la protection de l'identité et à la sécurité des données. Il se consacre au développement et à la généralisation des usages de l'identité dans des conditions qui garantissent la sécurité et la confidentialité.

SEIDO

EDF R&D et Télécom ParisTech ont créé le laboratoire commun de recherche SEIDO, sur l'Internet des Objets et la cybersécurité pour les systèmes électriques. Son enjeu ? Préparer et faciliter le déploiement de services de gestion de la demande en énergie, s'appuyant sur l'interopérabilité d'équipements et ainsi contribuer à assurer la cohérence, l'efficacité et la sûreté de l'ensemble du système.

www.seido-lab.com

BART

L'initiative commune de recherche BART (Blockchain Advanced Research and Technologies) constitue la plus importante équipe de recherche académique sur le sujet de la Blockchain en France. Les chercheurs d'Inria, Télécom ParisTech, Télécom SudParis et SystemX travaillent de concert autour de 6 axes : modèles théoriques, passage à l'échelle et outils de monitoring, sécurité, architectures, confidentialité des données et régulation.

www.bart-blockchain.fr

INNOVATION ET INDUSTRIE

L'INCUBATEUR : PARISTECH ENTREPRENEURS

ParisTech Entrepreneurs est l'incubateur de Télécom ParisTech. En 20 ans, il a accueilli plus de 350 start-up innovantes du numérique. Trois d'entre-elles, spécialisées dans la cybersécurité, y sont actuellement incubées : CYRATING la première agence européenne de notation en cybersécurité, Ogo Security qui propose une solution de protection des sites et applications web pour lutter contre les cyberattaques et Seald qui offre une solution de chiffrement d'e-mails et fichiers intégrée aux outils usuels.

www.paristech-entrepreneurs.fr

UNE RELATION FORTE AVEC LES ENTREPRISES DE L'INDUSTRIE ET DU NUMÉRIQUE

Les liens étroits qu'entretient Télécom ParisTech avec les acteurs économiques en font un témoin privilégié de l'importance de la cybersécurté et de son impact technologique, sociétal, juridique et économique, ainsi qu'un acteur légitime dans le domaine de la formation et de la recherche. Les nombreux partenaires industriels de Télécom ParisTech participent aux enseignements, études de cas, mises en situation professionnelle, tables rondes et séminaires. Ils proposent également des stages, thèses professionnelles, projets « fil rouge » aux étudiants.

Pour plus d'information contactez **relationsentreprises@telecom-paristech.fr**

Pour en savoir plus sur l'axe confiance numérique en formation, recherche et innovation, rendez-vous sur www.telecom-paristech.fr/cybersecurite

Institut Mines-Télécom

CARNOT La recherche pour l'innovation des entreprises

Réalisation graphique – ArtFeelsGood – décembre 2018 Contact : Samantha Bonnet, Direction de la Recherche, Télécom ParisTech