TELECOM SudParis

IP PARIS

CONFÉRENCE DE PRESSE

8 DÉCEMBRE 2022

CYBERSÉCURITÉ

CONTACTS PRESSE

Charlotte Gabet : 01 76 21 67 54 – cgabet@amalthea.fr

Sophie Rousset : 01 76 21 67 53 – srousset@amalthea.fr

Institut Mines-Télécom

SOMMAIRE

Édito de François Dellacherie,
Directeur de Télécom SudParis _____ page 3
« Avec 10 000 nouveaux ingénieurs Cyber diplômés d'ici 2030,
Télécom SudParis a vocation à contribuer activement
à la stratégie nationale d'accélération pour la cybersécurité »

Illustration sur le volet Formation

- Train Cyber Experts _____ page 4
- 404 CTF en partenariat avec la DGSE _____ page 6

Illustration à travers deux projets de Recherche

- SuperViz : Supervision et Orchestration de la Sécurité _____ page 7
- HEIR : Plateforme holistique de cyber-intelligence pour des environnements de santé sécurisés _____ page 9

Deux portraits Cyber Télécom SudParis

- Nesrine Kaaniche
  Maître de conférences à Télécom SudParis,
  experte en cybersécurité et protection de la vie privée _____ page 11
- Amré Abou Ali
  Alumni, co-fondateur CEO et CTO de Cybershen _____ page 12

Annexe :

- Infographie : Télécom SudParis en chiffres _____ page 13

L'ÉDITO DE
FRANÇOIS DELLACHERIE, DIRECTEUR DE TÉLÉCOM SUDPARIS

En tant que grande école publique d'ingénieurs, reconnue au meilleur niveau des sciences et technologies du numérique, Télécom SudParis souhaite apporter des réponses concrètes aux défis liés à la transformation numérique de notre société.

Avec une ambition : s'appuyer sur une formation académique et des laboratoires de recherche d'excellence, pour former des scientifiques et des ingénieurs ouverts aux évolutions du monde, capables de construire une société numérique de confiance.

Dans ce contexte, la cybersécurité fait plus que jamais partie de nos priorités. Car avec l'évolution des technologies récentes (Cloud, Big Data, Internet des Objets), les vecteurs et opportunités d'attaques numériques se sont eux aussi développés, et même accélérés ces derniers mois, faisant de chacun de nous, entreprises, pouvoirs publics et particuliers, de potentielles victimes.

Pour affronter ces menaces, des solutions technologiques rapides sont attendues, et les ingénieurs sont, une fois n'est pas coutume, en première ligne. C'est pourquoi nous voulons, à Télécom SudParis, renforcer l'impact de l'Ecole sur la sécurité nationale, en contribuant activement à la stratégie nationale d'accélération pour la cybersécurité, qui s'inscrit dans le plan France 2030, et vise notamment à créer 37000 emplois dans le domaine cyber d'ici 2025 et à développer des solutions souveraines et innovantes de cybersécurité.

Notre objectif : diplômer, avec nos partenaires académiques et industriels, 10000 nouveaux professionnels de la cybersécurité d'ici 2030, à Bac+5 ou équivalent.

Pour cela, nous créons de nouveaux supports numériques partageables. Nous développons de nouveaux outils de formation à la cybersécurité. Nous créons des plateformes d'expérimentation permettant de mettre en pratique les compétences acquises, pour les appliquer à différents cas d'usage, dans les domaines par exemple de la santé, du transport, de l'industrie, des télécommunications.

Pour maintenir notre capacité à bâtir un monde numérique de confiance, nous innovons également dans nos laboratoires. Nous menons une recherche de pointe pour inventer de nouveaux standards numériques plus robustes aux cybermenaces. Par exemple, nous utilisons l'intelligence artificielle pour automatiser la détection de vulnérabilités dans les systèmes. Nous coordonnons des projets financés par l'Europe ou par l'Agence Nationale de la Recherche. Nous recrutons et formons de jeunes chercheurs pour faire déboucher ces projets vers des applications concrètes pour la société. Nous demandons à ces mêmes chercheurs de développer de nouvelles formations à l'état de l'art, pour en faire bénéficier l'ensemble de nos apprenants (en formation diplômante et en formation continue).

« Avec 10 000 nouveaux ingénieurs Cyber diplômés d'ici 2030, Télécom SudParis a vocation à contribuer activement à la stratégie nationale d'accélération pour la cybersécurité. »

D'ici 2030, nous allons également renforcer notre action dans l'écosystème de la cybersécurité. Nous allons consolider nos relations avec les acteurs publics Français et Européens de la confiance numérique, et nous lancerons de nouvelles coopérations avec les acteurs industriels, qui mettent sur le marché les produits et services que nous utilisons tous.

Autant d'actions qui mettent la formation des futurs experts de la cybersécurité au cœur de notre mission, pour contribuer, à notre niveau, à renforcer la confiance de la société dans le numérique.•

LA CYBERSÉCURITÉ **ET LES ENJEUX DE FORMATION**

TRAIN-CYBER-EXPERTS, PROJET LAURÉAT FRANCE 2030, **STRATÉGIE D'ACCÉLÉRATION POUR LA CYBERSÉCURITÉ**

Train Cyber Experts a été sélectionné dans le cadre de la stratégie nationale d'accélération pour la cybersécurité «France 2030 » dans l'appel à manifestation d'intérêt « Compétences et métier d'avenir » sur le volet dispositif.
Le Projet a été pensé afin de construire des ressources pédagogiques, sous forme de contenus numériques et de plateformes technologiques, organisées par blocs de compétences, dans une optique de modularité, de réutilisabilité et de pédagogie centrée sur les compétences conduisant à des certifications.

CONTEXTE

Les études de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et de European Cyber Security Organisation (ECSO) démontrent un manque mondial de professionnels formés à la cybersécurité.
En 2021, l'International Information Systems Security Certification Consortium (ISC2), principale organisation à but non lucratif du secteur, estimait que la couverture des besoins à l'échelle internationale aurait supposé d'accroître le nombre de spécialistes en cybersécurité de 65%. En un an, le nombre de postes non-pourvus est passé de 3,12 millions à 2,72 millions dans le monde, ne réduisant que très partiellement le « gouffre entre demande et offre ». En France, on compterait aujourd'hui environ 15000 postes disponibles mais non couverts dans le secteur de la cybersécurité, selon une étude récente d'un cabinet de conseil français*.

*Cabinet de conseil Wavestone, étude du 16 mars 2022, « Cybersécurité : où en sont les grandes organisations françaises ? »

Plusieurs facteurs sont en jeu :

- Une dépendance croissante aux outils et objets numériques,
- Un accroissement de l'activité malveillante,
- Un manque d'attractivité des métiers de la cybersécurité, mal connus et souffrant d'un déficit d'image chez les étudiants, amenant à un nombre de diplômés significativement plus faible que les besoins malgré l'existence de parcours de formation.

Ce constat fait de longue date a amené plusieurs actions sur le sujet au niveau européen sur la Formation Cyber, notamment traité par les 4 projets pilotes européens (Cybersec4eu, Concordia, Echo, SPARTA) préfigurateurs du centre d'excellence en cybersécurité européen et du réseau de centres nationaux.
L'ENISA, agence de cybersécurité européenne installée à Athènes a publié en septembre dernier son référentiel de compétences en cybersécurité. Il met en évidence 12 catégories de métiers cyber afin de créer une compréhension commune des rôles, compétences, aptitudes requises, faciliter la reconnaissance des compétences en cybersécurité ; et soutenir la conception de programmes de formation liés à la cybersécurité.

SUITE PAGE SUIVANTE

LA CYBERSÉCURITÉ **ET LES ENJEUX DE FORMATION**

DIPLÔMER 10000 PROFESSIONNELS DE LA CYBERSÉCURITÉ À L'HORIZON 2030

Train Cyber Experts regroupe des acteurs académiques de premier plan (l'institut Mines-Télécom et ses écoles, Eurecom, Université Paris-Saclay, Université Versailles-Saint-Quentin, CentraleSupélec) disposant d'une expérience de plus de 20 ans dans la formation en cybersécurité. Il inclut plusieurs partenaires industriels apportant leur soutien à l'élaboration des contenus numériques et des plates-formes.

Les participants académiques se donnent pour objectif de diplômer 10000 professionnels de la cybersécurité à l'horizon 2030, au niveau Bac+5 ou équivalent (ingénieur en formation initiale ou en alternance, master, mastère spécialisé, diplôme d'ingénieur de spécialité, etc.).

Les formations développées seront tournées vers l'alternance pour faciliter l'intégration dans le monde professionnel. Elles seront proposées à labellisation SecNumEdu de l'ANSSI pour les rendre visibles des apprenants.

Pour construire cette offre de formation, le projet développera deux types d'outils :

- Des modules de formation numériques mutualisés, pouvant être intégrés dans des parcours de formation. Ils couvriront notamment les pré-requis pour la cybersécurité, sur les domaines technologiques (cryptographie et protection des données personnelles, sécurité des systèmes et des réseaux, programmation sécurisée, sécurité matérielle, …), et de sciences humaines et sociales (gestion de crise, environnement réglementaire et juridique, économie de la cybersécurité, etc.)
- Des plates-formes physiques de formation, permettant de mettre en œuvre les compétences acquises dans des environnements spécifiques et professionnalisants. Ces plates-formes seront associées à des métiers et secteurs d'activité, et permettront d'assurer une forte employabilité des étudiants pour des secteurs en tension. Des plates-formes de cyber-range orientées industrie seront notamment déployées, des plates-formes de production industrielle, des plates-formes de réseau 5G et de mobilité.

TÉLÉCOM SUDPARIS COORDINATEUR DU PROJET TRAIN CYBER EXPERTS

« L'Ecole était déjà fortement impliquée dans le projet SPARTA, réseau de compétences en cybersécurité soutenu par le programme européen H2020, avec notamment la coordination des travaux sur la formation professionnelle. Au sein du projet Train Cyber Experts, Télécom SudParis participera au développement de modules de formation, notamment réseaux, système et protection des données personnelles. L'Ecole développera également plusieurs plates-formes, autour de la cybersécurité des réseaux, de la cybersécurité du bâtiment connecté, et de la cybersécurité du véhicule autonome » **Hervé Debar, Directeur-adjoint en charge de la recherche, membre du conseil scientifique de l'ANSSI et chef de projet de TCE.**

Pour Télécom SudParis, l'enjeu est de déployer très rapidement deux programmes de formation, l'une d'ingénieur par apprentissage (FIPA), l'autre de mastère spécialisé. Ces formations, de 25 à 30 places offertes chaque année, ont pour vocation de former des experts dans le domaine de la cybersécurité, capables de concevoir et de développer des systèmes sécurisés, de les auditer et de les opérer. Ils pourront accomplir des missions de conception, de pilotage et d'audit en début de carrière, et évolueront naturellement vers des fonctions de management, par exemple responsable de la sécurité des systèmes d'information d'une entreprise ou d'une administration.

L'École offrira également des formations certifiantes focalisées sur des enjeux technologiques, comme la cybersécurité pour les réseaux du futur, l'industrie ou la santé. Ces formations plus courtes pourront soutenir les évolutions de carrière des professionnels de la cybersécurité, et former des professionnels d'autres domaines aux enjeux de la cyber (risques, menaces, parades).

Télécom SudParis mettra également en place une offre de validation des acquis de l'expérience (VAE) permettant d'accéder à ces diplômes.

Toutes les formations offertes par Télécom SudParis seront proposées à labellisation SecNumEDU, et SecNumEDU-FC pour les formations courtes spécifiques. •

Train Cyber Experts en chiffres

- ***4,4 millions*** *de dotation*
- ***Former 10 000 professionnels*** *de la cybersécurité à horizon 2030*
- ***5 acteurs académiques au sein du projet :*** *Institut Mines-Télécom et ses écoles, Eurecom, Université Paris-Saclay, Université Versailles-Saint-Quentin, CentraleSupélec*
- ***6 partenaires industriels :*** *dont deux associations professionnelles*
- ***25 à 30 places offertes*** *chaque année à Télécom SudParis*

LA CYBERSÉCURITÉ **ET LES ENJEUX DE FORMATION**

404 CTF, PROJET PÉDAGOGIQUE INNOVANT

CHALLENGE CYBER CONÇU PAR LES ÉLÈVES EN PARTENARIAT AVEC LA DGSE

Dans le cadre de la convention de partenariat signée en 2021 par Télécom SudParis, la Direction Générale de la Sécurité Extérieure (DGSE) et l'Institut Mines Télécom, dans le but de promouvoir la Cybersécurité dans l'enseignement, l'Ecole a proposé aux étudiants un projet pédagogique innovant autour de la Cybersécurité.

Au travers des projets de pédagogie active menés au sein de Télécom SudParis, GATE® (Gestion et de l'Apprentissage du Travail en Équipe) pour les 1ère année et Cassiopée pour les 2e année, les élèves ingénieurs du club de cybersécurité de Télécom SudParis, HackademINT, ont conçu un tournoi Cyber avec la DGSE.

Les élèves ingénieurs ont bénéficié des conseils des enseignants-chercheurs en cybersécurité, de l'expertise de la DGSE, et de l'aide des partenaires pour cet événement de 71 défis qui a réuni 2700 participants durant 3 semaines de compétition.

Afin de rendre les métiers de la cybersécurité plus attractifs mais aussi pour détecter de futurs talents, le 404 CTF était ouvert au grand public et proposait aux participants de se confronter individuellement à divers défis, à travers des missions clandestines d'un agent des services secrets français, pour découvrir l'histoire et les métiers techniques de la DGSE.

Les vainqueurs du challenge cybersécurité ont été récompensés le 23 juin dernier, lors du Salon Vivatech, à l'occasion d'une cérémonie sur le stand de la DGSE. •

Les élèves ingénieurs et organisateurs du 404 CTF nous racontent l'histoire de sa mise en place

Remise de prix du challenge 404 CTF au Salon VivaTech, le 17 juin 2022

« Créer un challenge comme le 404 CTF a été un travail complexe mais très intéressant et gratifiant. Nous avions une importante responsabilité. Quand vous êtes dans une compétition, vous représentez votre école, et en tant qu'élève, vous avez le droit à l'échec. Dans le cas du 404 CTF, Télécom SudParis nous a confié, au travers des projets pédagogiques, la tâche de concevoir ces challenges pour le compte de la DGSE. Nous n'avions pas le droit à l'erreur »

Julien Ribiollet, président HackademINT

« En permettant à nos étudiants de créer un nouveau challenge de cybersécurité de taille majeure, nous renforçons davantage la culture de l'école en matière de Cybersécurité, avec une activité à la fois sérieuse et ludique. Les compétences de pointe de Télécom SudParis en systèmes d'information et systèmes de sécurité, associées aux expertises des équipes de la DGSE, sont autant d'atouts pour relever les défis de la souveraineté numérique »

Francois Dellacherie, Directeur Télécom SudParis

LA CYBERSÉCURITÉ : **ILLUSTRATION À TRAVERS 2 PROJETS RECHERCHE**

SUPERVIZ, SUPERVISION ET ORCHESTRATION DE LA SÉCURITÉ

PROTÉGER LES SYSTÈMES INFORMATIQUES DES ENTREPRISES, GRÂCE AU RENFORCEMENT DES MÉCANISMES DE PROTECTION PRÉVENTIFS.

Le projet SuperviZ est l'un des 7 premiers projets retenus dans le cadre du Programme et équipement prioritaire de recherche (PERP). Il bénéficie d'une aide de l'état gérée par l'Agence Nationale de la Recherche au titre de France 2030 de 1,6 millions d'euros.

CONTEXTE

La supervision de sécurité est un sujet qui a émergé au début des années 1980, sous le terme de « détection d'intrusions ». Le postulat de base considère qu'il est impossible de sécuriser complètement un système d'information, et donc qu'il est nécessaire de mettre en place des mécanismes de détection des attaques. Fondamentale dans le contexte général des systèmes et réseau d'entreprise, la supervision l'est tout autant pour la sécurité des systèmes cyber-physiques. En effet, avec des « objets » (dispositifs de nature et de capacité très hétérogène) qui devraient à terme être tous, ou presque, connectés, la surface d'attaque augmente significativement. La sécurité n'en devient que plus difficile à mettre en œuvre. En ce qui concerne la sécurité, l'augmentation du nombre de composants à surveiller, ainsi que la croissante hétérogénéité des capacités de ces objets en termes de communication, stockage et calcul, rend la détection plus complexe.

OBJECTIFS

Le projet SuperviZ définit un ensemble de verrous scientifiques qui devraient permettre de résoudre les problèmes actuels de la supervision de sécurité et de traiter de nouveaux types d'attaque.

Ces verrous scientifiques, au nombre de 4, sont :

1. Le nombre et la diversité des composants à superviser, bien au-delà des ordinateurs qui étaient l'objet principal de la supervision de sécurité. Nous incluons maintenant des objets connectés de toute forme, capacité et de toute nature, notamment ceux utilisés dans les infrastructures critiques pour les piloter, dans les domaines de l'énergie, du transport, de la santé par exemple. Les mécanismes de détection de nouvelle génération devront être beaucoup plus fiables que précédemment.

2. La complexité des infrastructures à superviser, qui sont de taille très importante, hétérogènes et interconnectées, nécessitent des mécanismes de supervision et de réponse capables de prendre en compte la nature cyber-physique de ces infrastructures, et d'assurer une continuité d'activité sous attaque.

3. La prise en compte d'attaques ciblées de plus en plus complexes et silencieuses (attaque contre la chaine logicielle SolarWinds/Orion, logiciel Pegasus, …) qui demandent une compréhension globale de la menace et des capacités des attaquants, et une amélioration significative du temps de réponse en détection et en remédiation.

4. La prise en compte d'attaques massives et systémiques, qui soumet les utilisateurs des SI à un pilonnage constant de tentatives malveillantes, demande une amélioration des mécanismes de réponse pour limiter les dégâts causés par ces attaques.

TÉLÉCOM SUDPARIS CO-PILOTE LE PROGRAMME

« Il est nécessaire d'améliorer significativement l'efficacité de la chaîne détection-réaction (réponse et remédiation). L'objectif principal du projet est donc d'apporter de SUITE PAGE SUIVANTE

LA CYBERSÉCURITÉ : **ILLUSTRATION À TRAVERS 2 PROJETS RECHERCHE**

Crédits : rawpixel.com sur Freepik

nouvelles solutions et de faire avancer l'état de l'art scientifique actuel. En cohérence avec les objectifs des programmes et équipements prioritaires de recherche (PEPR), nous avons aussi pour objectif de préparer le transfert de nos résultats vers la communauté industrielle nationale. » **Hervé Debar, Directeur-adjoint en charge de la recherche et membre du conseil scientifique de l'ANSSI**

Télécom SudParis conduit des recherches sur la modélisation de la progression d'un attaquant au sein d'un système d'information, afin de proposer à un opérateur de visualiser la progression des attaquants. Cela doit donner à un opérateur la possibilité de choisir le moment où il va bloquer l'attaquant, avant qu'il ne cause des dommages mais également en évitant de perturber le fonctionnement des SI.

L'Ecole pilote également les activités du projet liées à la validation des mécanismes de détection. L'objectif est de s'assurer que les sondes conçues dans le projet sont effectivement efficaces pour détecter les attaques qu'elles doivent détecter, sans envoyer de faux positifs, et de permettre une comparaison entre diverses technologies de sondes. La complexité des attaques demande des techniques de détection également très complexes, utilisant des techniques d'apprentissage et d'intelligence artificielle. De nombreuses technologies existent, mais il est très difficile de comparer leur efficacité sur le problème de la détection. •

SuperviZ en chiffres

- ***5,6 millions d'euros*** *de budget total*
- ***13 Partenaires institutionnels :*** *INRIA, CEA, Université de Lorraine, Institut Mines-Télécom (Télécom SudParis, Télécom Paris, IMT Atlantique), Institut Polytechnique de Grenoble, Eurecom, Centre National de la Recherche Scientifique – Délégation Occitanie Ouest, CentraleSupélec, Université de Rennes 1*
- ***>10 Démonstrateurs et prototypes*** *en cours de développement et bientôt testés en conditions réelles*
- ***4 chercheurs Télécom SudParis*** *impliqués dans le projet*

LA CYBERSÉCURITÉ : **ILLUSTRATION À TRAVERS 2 PROJETS RECHERCHE**

PLATEFORME DE CYBER-INTELLIGENCE POUR DES ENVIRONNEMENTS DE SANTÉ SÉCURISÉS

PROPOSER DE NOUVEAUX MÉCANISMES DE CYBERSÉCURITÉ POUR LES INFRASTRUCTURES DE SANTÉ

Lancé en septembre 2020, le projet HEIR a reçu 5 millions d'euros de financements du programme de recherche et d'innovation Horizon 2020 de la Commission Européenne. Il s'appuie sur un consortium de 16 partenaires, 2 acteurs académiques, 9 entreprises fournissant les technologies de base, et 5 partenaires du domaine de la santé (3 hôpitaux situés en Angleterre et en Grèce, un centre de recherche et l'agence nationale de santé norvégienne).

CONTEXTE

Les environnements de santé sont de plus en plus sensibles aux attaques informatiques, comme le démontre le nombre grandissant d'incidents survenus dans différents centres hospitaliers européens ces années. Les hôpitaux utilisent de nombreux systèmes d'information pour gérer les patients. Les objets de santé sont également très fortement numérisés. Le numérique est au cœur de toutes les plates-formes d'imagerie médicale qui sont malheureusement soumises aux mêmes vulnérabilités informatiques que nos ordinateurs. Les contraintes liées à leur usage rendent plus difficiles les opérations de maintenance classique comme les mises à jour. D'autres objets sont également fortement numérisés, notamment pour observer les patients (mesure de glucose, analyse de sang, mesure de la tension ou du rythme cardiaque) ou leur donner des médicaments (pompe à insuline, seringue connectée, etc.).

La numérisation implique également la génération de gros volumes de données sensibles concernant les patients. Ces données intéressent d'une part les praticiens pour décider des traitements et en suivre l'efficacité et, d'autre part, la recherche médicale pour développer et tester de nouveaux traitements et mieux comprendre le fonctionnement des traitements actuels. SUITE PAGE SUIVANTE

« Nous sommes quotidiennement touchés par des tentatives d'hameçonnage, dont la fréquence et la crédibilité sont susceptibles de mettre à mal notre vigilance. Ces attaques lorsqu'elles réussissent paralysent nos établissements hospitaliers. Il devient donc fondamental de protéger nos équipements et nos données. HEIR a pour objectif d'accompagner au plus près les infrastructures de santé face à la menace cyber, tant pour protéger l'ensemble de l'infrastructure hospitalière que les données qui y résident. »

Hervé Debar, Directeur-adjoint en charge de la recherche,
membre du conseil scientifique de l'ANSSI et chef de projet de HEIR.

LA CYBERSÉCURITÉ : **ILLUSTRATION À TRAVERS 2 PROJETS RECHERCHE**

OBJECTIFS

Le projet travaille sur deux axes :

1. La recherche et l'analyse de vulnérabilités et d'attaques contre les infrastructures informatiques
2. L'accès contrôlé et protégé aux données de santé

HEIR développe tout d'abord une plate-forme de recherche et d'analyse de la menace (Threat Hunting). Cette plate-forme distribuée, installée au sein des réseaux informatiques des hôpitaux, permet de détecter la présence de vulnérabilités et d'attaques. Les traitements effectués permettent de donner un score de risque. Les opérateurs informatiques peuvent ainsi traiter en priorité les risques les plus importants.

Le projet crée également un observatoire de la cybersécurité des environnements médicaux. Les hôpitaux contribuant à cet observatoire remontent des informations anonymisées sur leur niveau de cybersécurité. L'observatoire agrège ces informations pour identifier des problèmes de cybersécurité touchant l'ensemble du secteur médical et pour fournir des recommandations d'actions de remédiation. Cette mesure permet également à un contributeur de se positionner par rapport à l'ensemble du secteur et de traiter ses vulnérabilités spécifiques.

Finalement, le projet développe une plate-forme de protection des données personnelles, permettant un partage tracé d'informations tout en respectant les prescriptions des patients. Chacun d'entre eux participant à une étude de santé spécifie la manière dont ses données peuvent être utilisées. Les utilisateurs des données (médecin, chercheur, régulateur) spécifient dans leurs demandes d'accès l'usage qu'ils feront de ces données. La plate-forme analyse la correspondance entre les souhaits des patients et les demandes d'accès, et retourne les informations, soit de manière anonymisée, soit de manière agrégée, pour respecter le RGPD et les désirs des utilisateurs.

TÉLÉCOM SUDPARIS COORDONNE LE PROJET HEIR

L'Ecole travaille sur l'analyse des données de vulnérabilité des dispositifs médicaux. Depuis 2017, les fabricants de dispositifs médicaux (et autres fournisseurs des opérateurs d'infrastructures critiques) ont l'obligation de publier les données de vulnérabilité de leurs équipements. Ces données sont présentées sous forme de texte et leur exploitation est difficile pour les opérateurs. Télécom SudParis développe des méthodes d'analyse basées sur le traitement du langage naturel et l'intelligence artificielle pour déterminer automatiquement le niveau de risque présenté par ces vulnérabilités, afin de fiabiliser l'établissement du score de vulnérabilité. Télécom SudParis utilise également ces mêmes méthodes pour analyser les mécanismes d'attaque et de remédiation indiqués dans ces documents, pour proposer aux opérateurs des actions permettant de remédier à ces vulnérabilités.•

HEIR en chiffres

- ***5 millions d'euros*** *de budget*
- ***Consortium de 16 partenaires*** *de 10 pays :*
  - ***2 académiques***
  - ***9 entreprises*** *fournissant les* ***technologies de base***
  - ***5 acteurs*** *du domaine de l****a santé***
- ***2 chercheurs*** *au sein de Télécom SudParis*
- ***4 prototypes*** *pilotes testés*

EXEMPLES DE RÉALISATION

Crédits : Universitetssykehuset nordnorge hf

Capteur de glucose

Cet équipement, utilisé par les diabétiques, mesure le taux de glucose dans le sang. La mesure est utilisée pour suivre l'évolution du diabète et injecter de l'insuline. Les données sont collectées par le fabriquant de l'objet sur sa plate-forme, située hors de l'Union Européenne.

>> HEIR développe une solution pour protéger ces données et assurer la conformité au RGPD, sans dégrader la qualité de suivi des patients et l'efficacité opérationnelle des praticiens.

Moniteur mère enfant

Cet équipement est utilisé pour mesurer la fréquence cardiaque et d'autres constantes vitales chez la mère et le nouveau-né au cours de l'accouchement. Cet appareil utilise un système d'exploitation commercial, ayant plusieurs vulnérabilités.

>> HEIR surveille les communications de l'appareil sur le réseau, pour détecter des comportements malveillants ou anormaux, symptomatiques d'attaques.

Crédits : Croydon Health Services National

LA CYBERSÉCURITÉ **2 PORTRAITS TÉLÉCOM SUDPARIS**

NESRINE KAÂNICHE,

MAÎTRE DE CONFÉRENCES À TÉLÉCOM SUDPARIS, EXPERTE EN CYBERSÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE

« POUR RÉUSSIR DANS LA RECHERCHE, RESTEZ CURIEUX ! »

UN PARCOURS SCIENTIFIQUE ET UNE PASSION POUR LA SÉCURITÉ

Après un parcours orienté sur les mathématiques, Nesrine intègre une école d'ingénieur en Tunisie où elle se passionne pour la sécurité. Elle réalise son stage de fin d'étude sur la cryptographie au sein du département Réseaux et Services de Télécommunications de Télécom SudParis. Séduite par le rayonnement de l'Ecole, le sérieux des équipes de recherche et l'ambiance au sein de son laboratoire SAMOVAR, elle rejoint Télécom SudParis en 2011 afin de réaliser sa thèse de doctorat sur la sécurité des données stockées dans le cloud, basée sur des mécanismes cryptographiques, dans la lignée de son stage de fin d'étude. Saluée par ses paires avec le troisième prix de la Thèse SAMOVAR pour la qualité de ses travaux, son parcours scientifique et académique se poursuit à Télécom SudParis avec un post-doctorat, durant lequel elle intègre la chaire Valeurs et Politiques des Informations Personnelles de l'IMT. Elle devient ingénieure de recherche au sein de la chaire où elle traite des données très sensibles et collabore avec des laboratoires de recherche internationaux, notamment l'institut de recherche de Stanford en Californie aux États-Unis, et plusieurs industriels, dont Qwant sur les traces laissées sur le web.

En 2019, elle rejoint le département Informatique de l'Université de Sheffield, en Angleterre, comme enseignante-chercheuse en cybersécurité. Elle prend la responsabilité de développement de la thématique de protection de la vie privée au sein de l'équipe de recherche « Sécurité des Systèmes Avancés » et représente le département au niveau de la faculté au sein du comité de diversité, pour l'égalité des genres.

UN TRAVAIL DE RECHERCHE AXÉ SUR LA PROTECTION DES DONNÉES PERSONNELLES

Nesrine intègre l'équipe «Sécurité Confiance Numérique» du laboratoire SAMOVAR en 2020 : *« A Télécom SudParis, je me suis toujours sentie libre pour identifier de nouveaux enjeux à résoudre et pour approfondir les thématiques fondamentales que sont la Cybersécurité et la protection des données privées ».*

Soutenue depuis le début de l'année par le programme de l'Agence Nationale de la Recherche (ANR), Jeunes Chercheuses et Jeunes Chercheurs, elle consacre ses travaux à une meilleure protection de la vie privée et un traitement «équitable» des données pour les services de santé. *« La crise du Covid a mis en lumière la nécessité de collaborer encore davantage dans le domaine de la santé. L'accès aux données réelles de santé et la collaboration entre plusieurs acteurs sont très difficiles en raison de contraintes à la fois juridiques et éthiques. Avec une sensibilisation croissante du public et les nouvelles législations telles que le RGPD, il est impératif de traiter les enjeux liés à la vie privée afin d'ouvrir la voie à la prochaine génération de systèmes. »*

A la clé de ses travaux ? Concevoir de nouveaux protocoles basés sur des briques cryptographiques afin de sécuriser les échanges et l'agrégation des calculs effectués sur les données collectées puis stockées par différents acteurs de la Santé et sites médicaux. Basé sur ces données de santé, très sensibles, ce calcul reposant sur des algorithmes d'Intelligence Artificielle collaboratifs, dont l'apprentissage fédéré, renforce le respect de la vie privée en ciblant les acteurs fiables adaptées aux besoins spécifiques des tâches de calcul. *« Véritable enjeux stratégiques pour l'Europe, être à la pointe de la protection de la vie privée des citoyens en ligne ne doit pas se traduire par une perte de compétitivité pour développer et bénéficier des nouvelles avancées de l'IA.»*

LA CURIOSITÉ, LE PRINCIPE MÊME DE LA RECHERCHE

Pour Nesrine Kaâniche, la recherche est un travail d'équipe stimulant afin de résoudre des problématiques en lien avec des enjeux de société. *« Il faut avoir une vision sur le long terme, trouver de nouvelles approches. Etre flexible et méthodologiquement ouvert d'esprit. La recherche se déroule rarement comme prévu. Mais avant tout, il faut savoir rester curieux !!! C'est le principe même de la recherche »* •

Podcast Sciences num. consacré aux travaux de Nesrine Kaâniche.

AMRÉ ABOU ALI,

CO-FONDATEUR CEO ET CTO DE CYBERSHEN

« PROPOSER AUX ÉTABLISSEMENTS PUBLICS, PME ET ETI UN ACCOMPAGNEMENT PERSONNALISÉ ET AUTOMATISÉ POUR FAIRE FACE À LA MENACE CYBER »

Amré Abou Ali, démocratise la cybersécurité. Cet ancien étudiant de Télécom SudParis vient de fonder Cybershen avec un autre Alumni de l'École. La Start-up developpe une solution européenne de protection des terminaux pour protéger les entreprises et les entités publiques contre les menaces cyber. Grace à une offre *plug and play,* la société protège en temps réel contre les flux malveillants et avec un système d'accompagnement au durcissement. Une offre qui s'adapte en fonction de la structure de l'entreprise pour ainsi permettre aux PME, ETI et établissements de santé de lutter contre les menaces cyberattaques grandissantes.

UNE PRISE DE CONSCIENCE DU RISQUE CYBER

Lors de sa formation à Télécom SudParis, Amré choisit de se spécialiser en dernière année dans la cybersécurité. Dans le cadre de la labellisation SecNumEdu de l'Ecole, il obtient le titre ESSI (Expert en Sécurité des Systèmes d'Information), délivré par l'ANSSI. En 2017, fraîchement diplômé de Télécom SudParis, il occupe plusieurs postes dans le domaine de la santé. Il rejoint d'abord le Conseil National de l'Ordre des Pharmaciens en tant que Responsable sécurité des systèmes d'information (RSSI) du Dossier Pharmaceutique (DP). Puis il intègre la multinationale américaine IQVA, experte en données de santé, où il assure la mise en conformité de problématiques de sécurité. En 2019, Amré devient RSSI au sein de l'établissement de santé GHU Paris Psychiatrie & Neurosciences. Avec la crise du COVID-19, il prend conscience d'une réelle faille de sécurité pour les établissements de santé et les petites structures et réfléchit à une solution pour mieux accompagner les différents acteurs face au risque cyber.

LA PRISE EN CONSIDÉRATION DU SUJET CYBER TRÈS VARIABLE EN FONCTION DE LA TAILLE DES STRUCTURES

En 2021, avec son ancien camarade de Télécom SudParis, Charles Mure, ils imaginent une offre de cybersécurité accessible à tous. Ils travaillent sur une solution qui s'adapte à toute taille de structure et qui peut être utilisée par des acteurs inexpérimentés. Ils intègrent d'abord le Cyber Booster, premier startup studio français dédié à la cybersécurité en mars 2022 avant de rejoindre l'incubateur de Télécom Paris. Les deux ingénieurs concrétisent la création de société après plusieurs constats : *« S'il existe à l'heure actuelle de nombreuses solutions pour pallier la menace cyber, ces dernières sont généralement destinées à des acteurs de grande taille, ayant déjà une maturité élevée en matière de cybersécurité. L'augmentation des cyberattaques, la généralisation de la menace à tout type de structures depuis la pandémie, l'usage incontournable d'internet, la carence d'expertise cyber et de sensibilisation sont autant de constats qui nous ont amené à la création de Cybershen. »*

Lancée en mars 2022, Cybershen propose aux entreprises et entités publiques n'ayant aucune expertise en matière de cybersécurité une solution de protection des terminaux (postes, mobiles), afin de protéger en temps réel ces acteurs contre les cybermenaces. En délivrant les fondamentaux en matière de cybersécurité, pour accompagner la structure dans la construction de son propre système de sécurité. La plateforme adapte le paramétrage de sécurité en fonction de la structure de l'entreprise ce qui la rend compatible avec tout type d'acteur : ETI, PME, établissement public. Financée en partie grâce au prêt d'honneur de l'Institut Mines-Télécom Cybershen poursuit sa phase de Recherche et Développement. La Start-up est accompagnée par le pôle Systematic Paris DeepTech et la solution devrait être opérationnelle à l'été 2023.

UNE FORMATION COMPLÈTE AUSSI BIEN SUR LES ENJEUX DE LA CYBERSÉCURITÉ QUE DE L'ENTREPRENEURIAT

« Ma spécialisation en cybersécurité n'a pas été une évidence mais elle est, selon moi, aujourd'hui le choix le plus judicieux de mon parcours. La cybersécurité associe une haute maitrise technologique du numérique avec un volet humain extrêmement fort. La formation délivrée à l'école m'a fourni toutes les clés pour saisir les enjeux liés à ce domaine ainsi que les bases technologiques pour évoluer dans différentes structures. »

En parallèle de sa formation, Amré intègre la Junior Entreprise, association étudiante de Télécom SudParis, qui l'a sensibilisé au monde de l'entrepreneuriat et lui a donné les outils pour se lancer sereinement dans cette aventure. *« Cette autre facette m'a apporté la capacité à me lancer. L'intérêt en créant sa Start-up est de pouvoir faire bouger les choses, challenger le statu quo. L'approche projets offerte par Télécom SudParis permet d'avoir une vision globale de l'entreprenariat. Il faut continuer à le promouvoir car il permettrait à la France d'améliorer son statut économique et de lui offrir un avantage compétitif très fort. »* •

Retour au «Sommaire»

ANNEXE
TÉLÉCOM SUDPARIS EN CHIFFRES

1979 Création de l'Institut National des Télécommunications (INT) et de sa section ingénieur

97 Enseignants-chercheurs

Groupe Institut Mines-Télécom (IMT)

EPE Institut polytechnique de Paris (IP Paris)

Ministère de tutelle
Économie, Finances et Relance

961 Étudiantes/étudiants inscrits en 2022-2023

688 Étudiantes/étudiants en formation ingénieurs

207 Diplômées/diplômés ingénieurs en 2021 (FISE + FIPA)

106 Doctorants encadrés par nos enseignants-chercheurs

23% D'étudiantes

29% De boursiers sur critères sociaux

10% D'étudiants issus des filières d'admission parallèle

9% D'étudiants en alternance

93,75% Taux net d'emploi des diplômés ingénieurs (Enquête CGE 2022)

10 400 Diplômées/diplômés

2 Sites : Evry-Courcouronnes et Palaiseau

900 Hébergements

15 Start-ups incubées en moyenne par an

26,9% D'étudiants de nationalité étrangère sur le campus