Potentiel Défi-clé « Institut de Cybersécurité de l'Occitanie »

Périmètre thématique – enjeux (globaux et locaux) – inscription dans les priorités scientifiques partagées entre les acteurs académiques…

Les vingt dernières années ont connu une recrudescence des attaques informatiques qui ont touché différents types de systèmes, allant des objets connectés, aux systèmes et infrastructures critiques, et ont ciblé différents objectifs (attaques vis-à-vis de la disponibilité des services, divulgation et vol de données personnelles, escroquerie, intelligence économique, diffusion de fausses informations sur les réseaux sociaux, cybercriminalité…). Des exemples récents ont ciblé des hôpitaux, des établissements publics, mais également des entreprises. La cybersécurité et la protection vis-à-vis des malveillances informatiques sont ainsi devenues une priorité internationale, mais également une priorité de souveraineté nationale.

En novembre 2018 lors d'un discours à l'UNESCO, le Président de la République, Emmanuel MACRON, lançait l'appel de Paris pour la cybersécurité mondiale qui fut co-signé par 50 pays. Cette initiative s'est concrétisée au niveau national par la mise en œuvre de nombreuses actions. Parmi celles-ci, on peut noter rien qu'en 2020 la mise en place d'un Comité Stratégique de Filière (CSF) «Industrie de sécurité» et d'un projet structurant «Cybersécurité et sécurité de l'IoT» mais aussi le lancement d'un PEPR « Programme et équipements prioritaires de recherche » dédié à la cybersécurité qui s'inscrit dans le PIA4. Au niveau européen, la cybersécurité fait également partie des priorités du nouveau programme Horizon Europe avec un cluster thématique dédié. Un règlement portant sur la mise en place d'un nouveau centre européen de compétences et son réseau, dans les domaines de la cybersécurité, de l'industrie, de la technologie et de la recherche est en cours d'adoption. Il explore les moyens d'une collaboration européenne meilleure et plus intégrée en matière de cybersécurité, préservant et protégeant les valeurs et les libertés européennes, telles que le respect de la vie privée.

Dans un même temps, la Région Occitanie s'est dotée d'outils pour soutenir l'industrie de la cybersécurité dans le territoire. La création de la plateforme Cyber'Occ, les projets de Digital Innovation Hub ou encore la création d'un CERT/CSIRT régional s'inscrivent dans cette dynamique.

Afin de positionner l'Occitanie parmi les leaders de cette thématique en France et de stimuler l'émergence d'une filière d'excellence, nous proposons de créer un Défi-clé « Cybersécurité » qui viendrait renforcer cette dynamique en stimulant la recherche amont, en développant la formation et en favorisant les collaborations et la valorisation des avancées scientifiques pour soutenir les acteurs économiques en Occitanie et plus largement.

La région Occitanie dispose d'un écosystème très riche dans le domaine de cybersécurité, sur les sites de Toulouse, Montpellier et de Perpignan, avec des acteurs académiques et centres de recherche pluridisciplinaires (CEA, ENAC, INP Toulouse, INSA Toulouse, IRIT, ISAE-SUPAERO, LAAS, LIRMM, LERASS, IDETCom, IES, IMT, TSE, UM, UPVD, UT1, UT2, UT3…) et institutionnels, développant des recherches de premier plan au niveau national et international, des formations reconnues (TLS-SEC, SECNUM…), et des acteurs industriels dynamiques, incluant de grands groupes, des PME et startups, par exemple dans le secteur des systèmes embarqués critiques (Airbus, Thales, …) et dans les services (iTrust, Sogeti, SCASSI, SopraSteria, etc.), ainsi que des acteurs institutionnels (ANSSI, Cyber'Occ). Nous avons aussi été précurseurs dans la recherche dans le domaine de la cybersécurité dès le début des années 1980, notamment dans le domaine des architectures de sécurité. Cependant, ce potentiel a besoin d'être renforcé et soutenu fortement pour avoir un pôle de compétences à forte visibilité nationale et internationale, équivalent à celui en Bretagne ou à Paris. Comme peut le montrer la cartographie d'Allistene (https://www.allistene.fr/files/2018/03/VF_cartographie_2017-06-13.pdf) et un dossier récent de l'institut INS2I du CNRS (https://ins2i.cnrs.fr/sites/institut_ins2i/files/ressource-file/livret_cybersecurite_sept2020_mail.pdf), la région Occitanie fait partie du Top 5 des activités en Cybersécurité sur le plan national. Une synergie plus forte et consolidée permettrait à la région Occitanie de disposer d'une visibilité accrue et de prétendre à rentrer dans le Top 3 des pôles en Cybersécurité. Sous la bannière Cybersécurité, nous comptabilisons plus de 150 personnes, sur le domaine de l'ESR, en recherche et formation, si une majorité sont dans les sciences du numérique et les sciences dures, plus d'une vingtaine sont identifiées dans le domaine des sciences sociales.

Objectifs scientifiques

Les systèmes informatiques sont aujourd'hui de plus en plus embarqués dans des systèmes critiques (tels que dans l'avionique et l'automobile) ainsi que dans de multiples objets connectés massivement déployés dans les domiciles et les environnements professionnels. L'accroissement de la connectivité des systèmes via l'utilisation de multiples protocoles de communication hétérogènes, notamment sans fil, a permis le développement de nouveaux services et usages, en introduisant tout autant de nouvelles menaces qui nécessitent le renforcement de la protection vis-à-vis du risque de malveillances informatiques. Les vulnérabilités exploitées par les attaquants touchent les différentes couches des systèmes et de plus en plus les couches basses et le matériel. Les vulnérabilités Spectre et Meltdown identifiées dans les processeurs Intel en sont des exemples récents. Par ailleurs, la protection des données personnelles et de la vie privée est devenue aussi un véritable enjeu scientifique et sociétal à cause de la collecte massive de données et à la multiplication des systèmes de partage d'informations personnelles, désirés ou non par les individus. Les réseaux sociaux sont également devenus un terrain privilégié pour différents actes de cybercriminalité et de désinformation. Ainsi cette proposition se veut pluridisciplinaire en associant différentes communautés des sciences du numérique (Mathématiques, Informatique, Microélectronique, Electronique, Physique) mais également les sciences sociales qui par leur approche amènent une dimension essentielle à la compréhension sociétale de la sécurité, et aussi à la conception de solutions acceptables du point de vue juridique, éthique et économique. La recherche de meilleurs compromis entre efficacité de la protection, utilité et acceptabilité constitue un enjeu fondamental auquel ce défi ambitionne d'apporter des solutions novatrices.

Les recherches en cybersécurité en Occitanie visent à développer de nouvelles solutions de protection vis-à-vis des malveillances et des méthodes expérimentales d'analyse de sécurité permettant de répondre à ces enjeux. Elles couvrent plusieurs volets que nous avons déclinés en 4 thèmes principaux, croisant différentes disciplines.

Thème 1: Renforcer la sécurité matérielle, logicielle et des systèmes
Thème 2: Assurer la sécurité des réseaux et environnements connectés du futur/technologies émergentes
Thème 3: Mieux protéger les données et la vie privée, et améliorer la confiance dans les réseaux sociaux
Thème 4: Améliorer la conception par des approches formelles et étudier l'impact/l'apport de l'intelligence artificielle

Le premier thème majeur de nos travaux porte sur le développement de nouvelles architectures et mécanismes, pour améliorer la sécurité des processeurs et des systèmes en s'appuyant sur des solutions mixtes intégrant des mécanismes de protection matériels et logiciels, diversifiés et reconfigurables dynamiquement, allant du circuit et dispositif matériel aux applications et services. Ces travaux seront complétés par le développement de solutions basées sur la cryptographie légère et post-quantique (et une passerelle pourra être envisagée avec le DEFI Quantique) dédiées à renforcer la protection de systèmes embarqués par exemple pour l'Internet des objets (IoT) vis-à-vis d'attaques physiques. Les champs d'investigation incluent la recherche de nouvelles solutions permettant d'améliorer la protection vis-à-vis d'attaques par canaux auxiliaires et de nouvelles attaques matérielles, ainsi que des techniques d'analyse et de traitement de données visuelles (images, vidéos, objets 3D) par exemple dans une optique de tatouage de ces objets et de protection de propriété intellectuelle. La technologie des blockchains est également un champ de recherche sur lequel nous sommes investis pour développer de nouvelles solutions de sécurité. Une autre dimension importante de nos travaux est de s'assurer de l'utilisabilité des mécanismes de sécurité en maîtrisant leur impact sur l'activité et la performance des utilisateurs. Ces analyses intégrant l'identification des activités et ressources supplémentaires à mobiliser (e.g. temporelles, cognitives, motrices…) sont indispensables pour l'acceptabilité de ces mécanismes.

Le second thème se consacre au domaine de l'Internet des objets (IoT), en particulier aux risques liés au déploiement de multitudes de protocoles sans fils, hétérogènes et vulnérables, dans des espaces privés et professionnels, et plus généralement à la sécurité des futurs réseaux programmables notamment avec la généralisation des techniques de Cloud/Fog/Edge Computing et de virtualisation. L'avènement de nouvelles technologies de communication (5G et bientôt la 6G) et de nouveaux environnements de déploiement complexes intégrant des infrastructures de communication terrestres, mobiles et satellites, et au-delà, des opérateurs tiers (opérateurs de plateformes de services pour l'IoT, opérateurs CDN, etc.) pose également de nouveaux défis vis-à-vis de la sécurité. Nos recherches dans ce contexte portent sur le développement de nouvelles approches de protection basées par exemple sur des techniques de *fingerprinting* et des techniques

de détection d'anomalies et d'intrusion combinant des informations multi-couches (issues de la couche physique mais également des couches réseaux supérieures). Un autre défi important est d'envisager de rendre les systèmes encore plus autonomes face aux attaques en intégrant des mécanismes de réaction associés à la détection. La réflexion intégrera aussi des dimensions stratégiques, de défense, des enjeux internationaux, des dimensions politiques et sociologiques de la cybersécurité, notamment dans le contexte particulier des communications par satellites et dans le domaine spatial.

Le troisième thème a pour ambition d'une part de développer de nouvelles solutions pour la protection des données et de la vie privée basées par exemple sur des techniques cryptographiques avancées permettant de traiter de façon sécurisée des données chiffrées en protégeant l'anonymat des utilisateurs, compatibles avec le RGPD, et d'autre part de rendre sûrs les réseaux sociaux vis-à-vis de différentes formes de malveillances, d'abus et de menaces (cybercriminalité, harcèlement, terrorisme, pratiques abusives de fournisseurs de service, etc.), permettant ainsi au citoyen de naviguer sereinement dans ces réseaux. Ces problématiques seront abordées sous des facettes multiples et pluridisciplinaires combinant des techniques issues des domaines des sciences du numérique, des mathématiques, des sciences sociales, juridiques et économiques. Outre le développement de solutions basées sur des techniques de chiffrement et de protection de vie privée avancées applicables en pratique (chiffrement par attributs, chiffrement complètement homomorphe, distribution sécurisée du traitement de l'information, *differential privacy*…), nos recherches portent notamment sur des problématiques liées à l'acceptabilité, la légalité, l'éthique des moyens de sécurisation, ainsi que sur les moyens de régulation pour susciter la confiance. Ces aspects s'associent au développement de dispositifs innovants de sensibilisation et de prévention de la menace cyber fondés notamment sur des partenariats publics-privés. En effet, les évaluations conduites sur les programmes de réduction des risques liés au numérique (par exemple en milieu scolaire) montrent que la plupart des actions permettent d'améliorer la compréhension des menaces liés aux usages numériques, mais dans la plupart des cas elles s'avèrent peu efficaces pour changer les comportements des usagers et orienter leurs actions. À partir d'une approche axée sur le renforcement du « pouvoir d'agir » des acteurs, cet axe de recherche a pour ambition de proposer des solutions pouvant non seulement accroître le niveau de connaissances relatives aux cybermenaces, mais surtout avoir un impact significatif sur le changement des pratiques des usagers. Deux défis peuvent être mis en avant dans ce contexte : i) le défi de l'acculturation des personnels et des personnes à ces enjeux du champs immatériel et ii) ne pas réduire le cyber espace à une affaire de techniciens, il faut que ce soit un espace raisonné par tous les acteurs et usagers.
Sur le volet économique, l'objectif est de mieux comprendre, de façon théorique, les liens entre concurrence et investissements en cybersécurité, en utilisant par exemple des outils de la théorie des jeux pour modéliser les choix d'investissements d'entreprises en concurrence en fonction de leurs différents business-model. Cette analyse permettra d'identifier les défaillances de marché propres à la cybersécurité et les mesures de politiques publiques les plus à même d'y remédier. Ces travaux trouvent un écho dans plusieurs domaines d'usage tels que la santé et la mobilité. Des interactions sur ce thème avec Occitanie Data/Ekitia et avec l'Institut de Science des Données de Montpellier (ISDM) seront également explorées dans le cadre de ce défi.

Enfin, le quatrième thème est plus transverse, et couvre deux volets principaux. Le premier concerne le développement d'approches formelles pour maîtriser la conception et faciliter la recherche et l'audit de vulnérabilités, en utilisant notamment des approches basées sur la théorie des langages ou des patrons de sécurité et des vérifications formelles. Le deuxième explore plus particulièrement les enjeux liés aux algorithmes d'intelligence artificielle, d'une part comme outil pour renforcer la cybersécurité et d'autre part comme cible d'attaques qu'il faut détecter et prévenir avec une grande efficacité. Nos travaux sur ce sujet sont tout à fait complémentaires aux recherches menées dans le cadre de l'institut d'intelligence artificielle de Toulouse ANITI, dont le périmètre des travaux ne couvre pas la cybersécurité. Nous mettrons à profit les avancées sur les fondements de l'IA au sein d'ANITI pour résoudre des problématiques propres au domaine de la cybersécurité.

Au-delà de ces thèmes qui permettent d'identifier les axes de recherche propres à l'Occitanie, l'objectif de cette proposition est également de renforcer les interactions entre les disciplines, que cela soit entre les sciences numériques et/ou les sciences dures et/ou les sciences sociales. Ainsi une attention particulière sera portée sur les défis scientifiques croisés aussi bien disciplinairement, que géographiquement afin de favoriser l'émergence en Occitanie d'une communauté structurée, traitant différentes facettes pluridisciplinaires de la cybersécurité, avec une forte visibilité nationale et internationale.

Ces recherches intègrent des développements conceptuels, concrétisés par la mise en œuvre de preuves de concepts et des validations expérimentales qui nécessitent le déploiement de plateformes. Nous envisageons notamment la création/consolidation de plateformes, dont la valeur ajoutée sera très importante pour fédérer les travaux de recherche entre nos équipes et aussi pour les travaux des différents membres des équipes Occitanie-ouest et Occitanie-est, en prenant en compte aussi les complémentarités avec les plateformes existantes par exemple au CEA. Les plateformes envisagées concernent l'étude et la caractérisation d'attaques par canaux auxiliaires et l'observation de leurs effets sur la micro-architecture, ou bien l'étude de futures architectures de sécurité pour les réseaux 5G et l'IoT. L'ambition est aussi de mettre en commun des outils et des développements logiciels issus de nos recherches et de favoriser leur diffusion et utilisation auprès de nos partenaires mais aussi en accès libre.

Nos domaines d'application ciblés sont multiples. Ils couvrent notamment les systèmes embarqués critiques et grand public, par exemple pour l'automobile, l'aéronautique et l'espace, les territoires intelligents (valorisation de la donnée métier) et l'internet des objets (smart city, domiciles connectés, industrie du futur), l'optimisation énergétique, la santé et plus généralement les infrastructures pour le numérique (Cloud, Edge Computing…).

Le renforcement de notre potentiel de recherche en cybersécurité en Occitanie grâce aux moyens qui seront déployés dans le cadre de ce défi et la consolidation des interactions entre les différents acteurs participant à ce défi permettront d'accroître notre visibilité au niveau national et international et de démultiplier les opportunités de collaborations conjointes dans le cadre des appels ANR, FUI et DEP. Nous pourrons ainsi tirer profit collectivement des relations étroites que nous avons déjà avec les principaux laboratoires de recherche en France (par exemple avec IRISA, Supelec Rennes et IMT Bretagne, le LIP6 et Telecom Sud Paris, les laboratoires d'informatique de l'ENS et de l'ENS Lyon, le Loria à Nancy, l'Université de Grenoble ou Eurecom à Sophia Antipolis). À l'échelle internationale, nous pourrons nous appuyer sur le réseau CyberSec4Europe et nos partenaires dans les projets européens H2020 et plus largement (Université de Maryland et Université d'Illinois à Urbana-Champaign, États-Unis...).

Les actions à développer

1. Structurer, renforcer les collaborations et rendre visible l'institut de cybersécurité de l'Occitanie, par l'organisation de journées scientifiques et l'accueil en Occitanie d'évènements nationaux et internationaux. Une démarche de communication sera mise en œuvre pour valoriser les compétences et recherches menées en Occitanie. Un programme scientifique de haut niveau sera développé en créant une école Internationale de Cybersécurité, et un programme de chercheurs invités sera également prévu pour accroître la dimension internationale de cet Institut.
2. Renforcer les moyens humains sur la thématique par le financement d'une dizaine d'allocations doctorales co-financées à 50% et d'une dizaine de post-doctorants de 18 mois à 100%, en vue de soutenir l'amorçage de projets nouveaux, notamment académique-industrie, et de renforcer les collaborations entre différents sites en Occitanie (notamment Toulouse-Montpellier). Cet effort sans précédent en termes de moyens humains aura un impact fort sur la visibilité de la Cybersécurité en Occitanie et l'attractivité du site par exemple pour des recrutements au CNRS. Les opportunités de financement complémentaires des thèses seront recherchées via des collaborations avec nos partenaires industriels et des réponses à des appels à projets en France et en Europe. Notre volonté est d'attirer des talents internationaux et de favoriser la mixité et également de démultiplier les opportunités de montage de projets impliquant plusieurs partenaires du site pour renforcer les synergies entre les différentes thématiques de recherche en cybersécurité en Occitanie et améliorer l'attractivité du site.
3. Accompagner le développement de nouvelles plateformes expérimentales (matériels/logiciels, petits et moyens équipements, bancs de mesure…) pour faire émerger ou compléter des plateaux expérimentaux et plateformes structurantes autour de projets collaboratifs, et pour soutenir des actions de formation. En effet, le développement de plateformes de haut niveau fait partie intégrante des moyens nécessaires à accroître pour répondre aux enjeux actuels de la cybersécurité.

4. Établir un réservoir de compétences et d'expertises pour concevoir des contenus personnalisés en matière de gestion de crise dédiés aux entreprises industrielles des filières essentielles et aux collectivités. Ceci servira à accompagner la montée en compétences des acteurs industriels (du dirigeant à l'employé) en matière de sécurité économique pour contribuer à réduire les risques non financiers liés au patrimoine informationnel, à la sécurité des personnes et des biens et aux usages malveillants du numérique, pour mieux gérer une situation de crise. Une feuille de route s'articulera autour de trois phases (avant, pendant, après) à analyser et alimenter en plan d'actions, dans un contexte trans-sectoriel pour embarquer des écosystèmes larges et mobiliser les experts en fonction des axes prédéfinis. Les contributions seront de plusieurs types : un plan blanc pour la cybersécurité, la définition d'une plateforme d'exercices cyber-range et de mises en situation d'une part et l'identification d'un programme de coordination et de partage d'informations et d'expériences décliné en blocs de compétences appelant à une réalisation sous la forme de MOOCs ou de ressources en ligne.

5. Soutenir les actions de formation continue et initiale partagées bi-sites (modules de formation continue de courte durée ciblant des aspects spécifiques de la sécurité, mais aussi des modules communs de formations initiales et doctorales). En complément, des actions de sensibilisation et de diffusion de la culture scientifique et technique en cybersécurité seront mises en œuvre auprès des lycéens et étudiants, notamment avec l'aide du GIP CNFM (Coordination Nationale de la Formation en Micro et nano Électronique), ainsi qu'à destination des écoles primaires et des collèges, en collaboration avec le Rectorat. Notre volonté est également de promouvoir la mixité afin de pallier le faible pourcentage de filles dans les formations scientifiques dans le domaine numérique.

Etat des forces académiques régionales

Nous listons ici les partenaires et laboratoires ayant confirmé leur intérêt pour contribuer à ce défi. D'autres contacts sont en cours.

Établissements partenaires ou Tutelles des laboratoires

CNRS, CEA, ENAC, INP de Toulouse, INSA de Toulouse, ISAE-Supaero, Université de Montpellier, Université de Perpignan, UT1, UT2J, UT3

Laboratoires et équipes de recherche

Les laboratoires et équipes de recherche qui participent aux objectifs de ce défi sont les suivants :

- Montpellier: IMAG (UMR 5149, CNRS/UM), LIRMM (UMR 5506, CNRS/UM), IES (UMR 5214 CNRS/UM), Faculté de Droit (UM - Laboratoire Dynamiques du Droit, Laboratoire de Droit Privé)

- Toulouse : CEA, ENAC (Axe RESCO), IDETCOM (UT1), Institut de droits privé (EA 1920, UT1), IMT (UMR 5219, INSA Toulouse/UT1/UT2J/UT3/CNRS), IRIT (UMR 5505 CNRS/INP/UT3/UT1/UT2J), ISAE-SUPAERO, LAAS-CNRS (UPR 8001), LERASS (EA 827, UT3), TSE-R (UMR 1415 UT1/CNRS/INRAE/EHESS)

On estime les ressources académiques contribuant à ce défi à plus de 150 personnes incluant les permanents chercheurs et enseignants chercheurs, ainsi que les doctorants, post-doctorants et ingénieurs de recherche.

Les laboratoires et équipes impliquées sont pluridisciplinaires et couvrent de multiples facettes de la problématique de la cybersécurité : Technologies de l'information et de la communication - informatique, mathématiques, électronique (CEA, ENAC, IRIT, ISAE, LAAS, LIRMM, IES), sciences humaines et sociales, questions juridiques, stratégiques et économiques (Faculté de droit de Montpellier, IDETCOM, Institut de droit privé, LERASS, TSE-R)

Les laboratoires et équipes de recherche impliquées dans ce défi ont une expertise reconnue et visible au niveau national et international. Les exemples suivants fournissent quelques indicateurs:

- Les chercheurs en Occitanie ont été précurseurs dans la recherche en cybersécurité depuis les années 1980, et publient dans des conférences et revues de premier plan (IEEE Symposium on Security and Privacy, ESORICS, IEEE DSN, Crypto, Eurocrypt, IEEE Transactions on Computers, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Theory…). Plusieurs de nos publications sont très bien référencées par la communauté, par exemple sur la politique de sécurité ORBAC (807 citations dans google scholar), en authentification biométrique (699 citations), sur l'évaluation quantitative de la sécurité (585 citations) ou plus récemment sur le chiffrement homomorphe et la protection de la vie privée (135 citations) ou le chiffrement par attributs (277 citations). Deux des neufs finalistes de la compétition mondiale du NIST sur les algorithmes d'échanges de clés post-quantiques sont issus de Toulouse. Cette reconnaissance est aussi illustrée par des responsabilités importantes au niveau de la communauté scientifique (Présidence du comité de pilotage de la conférence internationale IEEE DSN, Présidence du comité de Pilotage de la conférence RESSI, organisation des conférences IEEE/IFIP DSN-2016, CARDIS 2018, ARES2015, FPS-2019, CyberSecurityForEurope2019, CSNet2020 et CSNet2021, participation à des comités éditoriaux de revues (IEEE Security & privacy, IEEE Transactions on computers, etc.), participation à l'animation du GDR Sécurité, et du GDR SOC2), à noter également la présence de collègues au sein du COFIS (comité de la Filière Industrielle de la sécurité).
- Nous avons de fortes collaborations avec des laboratoires de recherche de premier rang en France et en Europe, concrétisées par plusieurs projets H2020, ANR et FUI (par exemple depuis 2015: IRIT (5 projets H2020, 1 COST Action, 1 FUI, 1 ANR, 1 DGA/DGAC, 1 PEPS); LAAS (2 projets H2020, 1 FUI, 3 ANR, 1 RTRA, 1 DGA RAPID, 1 PIA Région) ; LIRMM (3 projets H2020, 9 ANR, 6 projets FUI, et 4 contrats DGA/CEA, 2 projets PIA Région).
- Nous avons de fortes collaborations avec les partenaires industriels incluant des Grands groupes et des PME (*Thales Avionics, EDF, Continental, APSYS/AIrbus, Renault, Thales CS*, *STmicro, Ninjalab, Orange Labs, Pradeo, Seclab, IOTEROP,..*). (depuis 2015: au LAAS 20 CIFRE/Indus, au LIRMM 12 CIFRE, 1 thèse entreprise à l'IRIT…). A noter également des créations d'entreprises issues de nos laboratoires de recherche et établissements comme la société ALGODONE et la startup Kaino-Security Bootcamp, ou encore l'accompagnement de sociétés innovantes comme IOTEROP, SECLAB, accompagnement par TTT de VCUCIM etc.
- Nous organisons également plusieurs événements en Occitanie rassemblant les acteurs académiques, industriels et institutionnels de la cyber sécurité, et en collaboration avec Cyber'OCC et l'ANSSI (Journée annuelle sur les nouvelles avancées en sécurité *(8 éditions, 150 participants/an), Toulouse Hacking Convention (5 éditions, 250 participations/an), Rencontres Cybersécurité Occitanie, CyberSecurity Business convention, Summer Camp Recherche-MIDI en 2015 et 2016, etc.)*
- Des équipements spécifiques et notamment des plateformes technologiques, comme la plateforme SECNUM à l'Université de Montpellier qui a été initiée en 2008 par la Région et le CNRS.

Formation

La région Occitanie compte dès à présent un nombre significatif de formations en Cybersécurité, à différents niveaux d'études. L'ensemble de ces formations montre d'une part une véritable dynamique en termes de formation en Cybersécurité en Occitanie et d'autre part une richesse dans l'offre de formation puisque les sujets abordés couvrent des thématiques variées des sciences du numérique et abordent également les sciences humaines et les sciences sociales.

On compte, au sein de l'Université de Toulouse, deux formations de niveau IUT (une des deux sera lancée à la rentrée prochaine, le BUT CyberSécurité et IoT, dont la coordination du Programme National du parcours CYBER, l'autre labélisée SecNumEdu), au sein de l'UT3 Paul Sabatier, 3 parcours dans 2 masters dans les sciences du numérique et les réseaux et télécommunications, une formation de niveau ingénieur labellisé SecNumEdu par l'ANSSI et un mastère spécialisé co-portés par trois écoles d'ingénieurs (ENSEEIHT, ENAC, INSA), ainsi que deux masters dans le domaine des sciences sociales portées par l'UT1 Toulouse Capitole, avec notamment une formation axée sur les enjeux stratégiques liés au numérique et aux menaces cyber débouchant sur l'emploi au niveau des administrations centrales et demain certainement au sein des collectivités territoriales mais aussi en entreprises depuis déjà quelques années.

Du côté de l'Université de Montpellier, on compte une licence professionnelle en Réseaux et Télécoms avec un parcours Cybersécurité ayant obtenu la certification SecNumEdu à l'IUT de Béziers. Le passage du DUT au

Bachelor Universitaire de technologie (BUT) va introduire dans les IUT un parcours “Déploiement d’applications communicantes et sécurisées” qui laissera une large place à la sécurité. Le département d’informatique de la Faculté des Sciences va ajouter un nouveau module de cryptographie en première année du master Informatique pour préparer à un module avancé en seconde année. Du côté sécurité matérielle, en plus des deux modules dispensés dans deux formations de niveau BAC+5, il est prévu à la rentrée prochaine l’ouverture d’un diplôme d’établissement niveau BAC+6 à Polytech Montpellier. L’école doctorale I2S de l’UM propose également une formation sur cette thématique.

Outre la formation initiale, nos établissements sont aussi très investis dans des actions de formation continue.

Partenariat avec les acteurs socio-économiques

Nous avons de fortes interactions avec les acteurs industriels et sociaux économiques de la région qui sont investies sur la thématique de la cybersécurité, notamment via notre implication dans cyber’Occ, Digital 113, la mêlée numérique, Captronic, le CLUSIF et le pôle de recherche et de coopération en sécurité digitale Ocssimore qui regroupe en occitanie plusieurs industriels dont la Caisse d’epargne, la Banque Populaire et Pierre Fabre. Notre participation active aux pôles de compétitivité par exemple Aerospace Valley et Eurobiomed, ainsi qu’à différents Clusters tel que TOTEM, ou encore à Digital113, constitue un atout important, d’une part pour échanger sur les besoins des acteurs industriels et les solutions des acteurs académiques en Occitanie, et d’autre part pour construire des partenariats permettant de répondre à ces besoins. La participation à la mise en place du Digital Innovation Hub EDIH Occitanie dont un des sujets d’intérêt porte sur la cybersécurité est aussi une autre opportunité pour renforcer et développer des partenariats avec l’écosystème socio-économique et d'innovation en Occitanie.

Différents niveaux de partenariat existent avec les industriels que ce soit sur des projets coopératifs ou dans le cadre de thèses CIFRE ou de contrats de collaboration avec les industriels. La liste suivante donne des exemples non exhaustifs de nos partenaires industriels en Occitanie:

Airbus, Airbus DS, Activus, APSYS, BoostAerospace, BPCE, CNES, Continental, CS, Cyblex Technologies, Digital Security, IMS Networks, iTrust, Modis, Orange, OCD, Pierre Fabre, Renault Software Labs, Rockwell Collins, Scassi, SecLab Cybersecurity, Sogeti, Sopra-Steria, Thales Avionics, Thales CS, Thales Alenia Space, Thales DIS, Vitesco, Ninjalab, Netheos, Objectif Libre, Lyra Networks, iBP, Great-X, Pradeo, Algodone, Ziwit, …

Une des ambitions de ce défi est de renforcer et élargir ces liens et fédérer les initiatives en cybersécurité en Occitanie intégrant les volets, recherche, formation et innovation. Deux domaines d’application qui sont fortement différenciants pour l’Occitanie, seront privilégiés : 1) l'aéronautique, le spatial et l’automobile, et 2) du vivant et de la Santé. Nous avons un écosystème industriel très riche et dynamique dans ces deux secteurs d’application. Il s’agit également de clairement de profiter des spécificités fortes de l’économie régionale Occitane et d’en devenir des acteurs incontournables sur le plan national. Le rassemblement de nos forces au sein de l’Institut de Cybersécurité de l’Occitanie pour proposer des solutions adaptées aux besoins de ces deux secteurs sera un atout majeur. La cybersécurité est un domaine porteur pour investir et créer de nouveaux emplois, et les besoins en termes de recrutement et de formation sont énormes. A titre d’exemple, les étudiants inscrits dans nos formations initiales ou en doctorat reçoivent généralement plusieurs offres de stage et sont embauchés rapidement à l’issue de leur formation. Un des enjeux est aussi de multiplier les opportunités de création de startup en collaboration avec les différents incubateurs et acteurs de l’innovation en Occitanie.

1ère approche des ambitions & objectifs à 4 ans

L’ambition de l'institut de Cybersécurité de l'Occitanie est claire. Elle consiste à rassembler et fédérer l’ensemble des forces dans le domaine de la Cybersécurité, quelles que soient les disciplines, pour que l’Occitanie, qui a déjà actuellement une place importante sur le plan national, puisse être identifiée dans le TOP 3 des régions dans ce domaine scientifique. Il s’agit également non pas de couvrir forcément l’ensemble des thématiques applicatives, mais bien d’adapter ces forces à des domaines économiques différenciants (aéronautique, spatial, automobile, vivant et santé). Les quatre thèmes de recherche que nous avons développés précédemment représentent les marqueurs forts de notre expertise en Occitanie et des axes de recherche que nous envisageons de renforcer et promouvoir. Nous avons plusieurs objectifs à court et moyen termes.

Il est tout d'abord nécessaire d'accroître les forces en augmentant les capacités de recherche en Occitanie, et en disposant d'expertises scientifiques d'un haut niveau. En particulier, il est nécessaire de renforcer les moyens humains sur la thématique par le financement d'une dizaine d'allocations doctorales co-financées à 50% et d'une dizaine de post-doctorants de 18 mois à 100%. Les post-docs permettront pour moitié environ de favoriser les échanges entre Occitanie-est et Occitanie-ouest et pour moitié de recruter des candidats de haut niveau provenant d'autres régions et d'autres pays. Cet effort au niveau des moyens humains permettra d'accroître l'attractivité et le rayonnement de la région sur cette thématique. La dynamique qui sera impulsée par ce défi Région ouvrira également d'autres perspectives de renforcement de ces moyens via les dispositifs de bourses des écoles doctorales, des bourses CIFRE avec des partenaires industriels qui s'associeront à notre initiative et le montage de projets collaboratifs dans le cadre d'appels nationaux ou européens. L'ambition est de cibler une vingtaine de financements de thèses au total sur 4 ans. Les recrutements de post-doctorants constitueront également un vivier pour proposer d'excellentes candidatures au concours CNRS et aux postes d'enseignants-chercheurs qui seront ouverts au sein de nos établissements pour contribuer à cet effort.

Notre objectif est également de favoriser l'émergence de compétences fortes en soutenant les formations initiales et continues bi-sites, en proposant des nouveaux modules de formation continue à courte durée sur des sujets spécifiques et en menant des actions de sensibilisation auprès des plus jeunes (école, collège). Par ailleurs, les industriels avec lesquels nous nouerons des contacts seront invités à intervenir dans nos formations. C'est déjà le cas dans nos formations, mais cette initiative sera élargie. Enfin, nous proposons la création d'une école thématique sur la cybersécurité, qui aura lieu tous les ans en Occitanie (organisée par exemple en alternance côté Ouest et côté Est), avec un double objectif : contribuer à la montée en compétences sur la cybersécurité en région mais aussi à accroître le rayonnement et la visibilité de la région sur cette thématique.

Beaucoup de travaux menés dans notre région incluent des développements de prototypes et des expérimentations pour lesquels la mise en place de plateformes et des investissements en équipements sont nécessaires. Nous avons pour objectif d'accompagner le développement d'au moins deux plateformes permettant: 1) d'évaluer la sécurité de certains composants matériels vis-à-vis d'attaques spécifiques avancées (canaux de fuite notamment) et de proposer et tester des contre-mesures efficaces et 2) de disposer d'un environnement complet d'expérimentation sur les réseaux de nouvelle génération (5G, SDN, NFV) facilitant les recherches sur l'évaluation de la sécurité de ces réseaux ainsi que la proposition d'architectures de sécurité. L'ouverture potentielle de ces plateformes à des industriels en Occitanie pourrait être explorée, ce qui permet de renforcer les collaborations avec le tissu industriel.

Un des objectifs de notre défi est également d'établir des liens pérennes avec le monde socio-économique, notamment un partenariat fort avec Cyber'Occ qui mobilise des ressources pour communiquer sur les efforts de recherche et de formation auprès du tissu économique. Il s'agit aussi de renforcer les partenariats avec le tissu industriel local, notamment dans le cadre de co-financements des thèses de doctorat ou de dépôt de projets ANR ou projets européens, et l'organisation de séminaires et d'événements scientifiques et d'innovation à forte visibilité. L'ambition est de déposer 2 à 3 projets européens ou internationaux pendant la période visée et de contribuer activement aux réponses aux appels à projets qui seront lancés notamment dans le cadre du PEPR national sur la cybersécurité et de l'ANR. Le renforcement de nos liens avec le tissu industriel permettra aussi de multiplier les opportunités de transfert à travers par exemple le dépôt de projets de Labcom au CNRS, et les différents dispositifs habituels avec le support des SATT Toulouse Tech Transfer et AxLR Occitanie Méditerranée à Montpellier.

Enfin, même si l'implication internationale est aujourd'hui déjà forte dans la région Occitanie, avec des collaborations avec des partenaires internationaux de premier plan, il n'en reste pas moins que nos actions restent morcelées. Ce défi sera un cadre idéal pour coordonner nos actions et mieux valoriser le potentiel de recherche et d'innovation en cybersécurité en Occitanie au niveau international. Des collaborations avec de grands laboratoires de recherche en cybersécurité seront privilégiées, par exemple EPFL en Suisse, UC Louvain en Belgique, TU Darmstadt et le GUF en Allemagne, Université de Lisbonne au Portugal ou bien l'Université Polytechnique de Valence, Universitat Politècnica de Catalunya à Barcelone ou encore l'université de Murcia en Espagne, et le CNR à Pise en Italie.

Le cas échéant, organisation actuelle du consortium, gouvernance, collaborations régionales établies…

La proposition de ce défi clé a été initiée et coordonnée par le LAAS, le LIRMM et l'IRIT.

La gestion administrative sera assurée par le CNRS. Un/une CDD « chef de projet » sera recruté(e) pour la durée des 4 ans du projet. La gouvernance du défi s'inspirera du mode de gouvernance de LabEx. Elle s'appuiera sur un comité exécutif, un comité de pilotage et un conseil scientifique.

Le comité exécutif (CE) rassemblera huit chercheurs académiques occitans représentatifs des laboratoires et des disciplines, d'un représentant de CyberOcc, et d'un représentant de l'ANSSI pour établir le lien avec le milieu socio-économique et la dynamique nationale en Cybersécurité. Il sera en charge de la stratégie. Il précisera et mettra en place le programme annuel d'activités du défi autour de nos quatre thèmes de recherche. Les actions feront en particulier l'objet d'appels d'offres qui seront mis en place par le CE. Il réalisera le processus définitif de sélection. Ses activités seront soutenues par l'embauche d'un CDD « Chef de projet », en charge de coordonner la mise en place des différentes actions, d'assurer le suivi dans la gestion du budget et la communication. Le CE examinera également les opportunités de collaboration et coordonnera des réponses à des appels à projets nationaux par exemple dans le cadre de l'ANR ou du PEPR ou internationaux. Le CE se réunira a minima 4 fois par an et le fonctionnement au jour le jour sera assuré par un bureau composé de responsables du défi (composé de 4 scientifiques : 1 IRIT - 1 LAAS - 1 LIRMM - 1 SHS) et du « chef de projet ». Le CE s'engage d'autre part à rendre compte annuellement des activités du défi et de son avancement auprès des instances signataires et d'experts reconnus dans le domaine, rassemblés au sein d'un comité de pilotage et d'un conseil scientifique.

Le comité de pilotage (CP) se réunira en début de projet et ensuite une fois par an. Il rassemblera des représentants des tutelles (CNRS, UFT, UM, etc.) ainsi que des représentants de la Région Occitanie en charge de la recherche, innovation et enseignement supérieur. Le CP aura pour rôle d'initier et de valider les différentes opérations mises en place, en particulier les appels d'offres internes, les événements et la gestion des crédits.

Le conseil scientifique (CS) sera constitué de personnalités scientifiques extérieures, choisies pour leur reconnaissance dans le domaine et issues du monde académique et industriel. Le CS sera une force de proposition sur les actions à mener, à initier ou à renforcer. Il se réunira une fois par an.