



# La cybersécurité au CNRS

Dossiers thématiques du CNRS

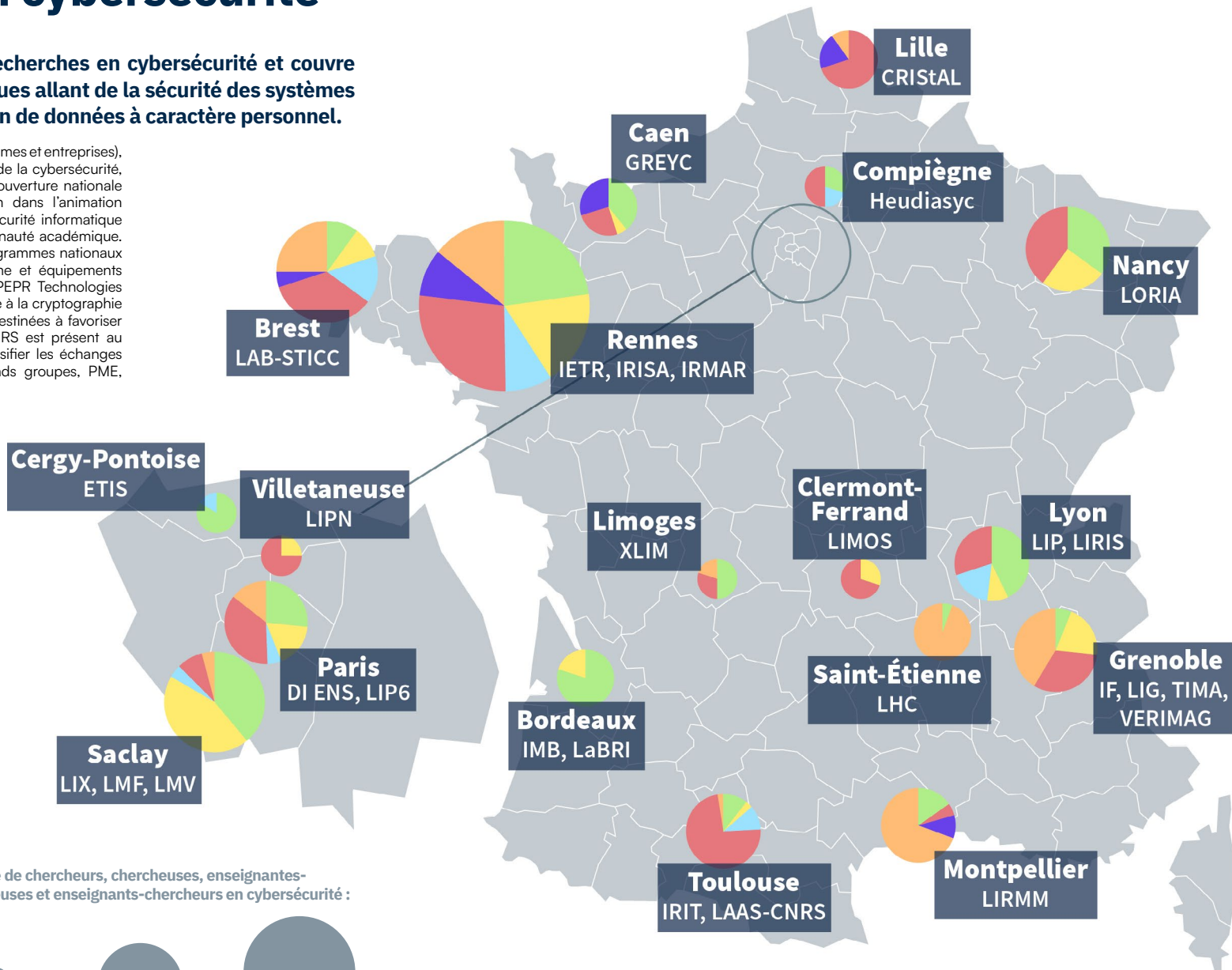
# Les laboratoires en cybersécurité

**Le CNRS est fortement investi dans les recherches en cybersécurité et couvre un large spectre de thématiques scientifiques allant de la sécurité des systèmes matériels, à la cryptologie ou à la protection de données à caractère personnel.**

Le CNRS mène, avec ses partenaires (universités, écoles, organismes et entreprises), des travaux de recherche portant sur l'ensemble du domaine de la cybersécurité, au sein d'une trentaine d'unités mixtes de recherche. Cette couverture nationale large permet au CNRS de jouer un rôle de premier plan dans l'animation scientifique, à travers le Groupement de recherche (GDR) Sécurité informatique qui est devenu, un outil privilégié de l'ensemble de la communauté académique. Le CNRS est également co-pilote avec le CEA et Inria, de programmes nationaux consacrés à la thématique, dont en particulier le programme et équipements prioritaires de recherche (PEPR) Cybersécurité ainsi que le PEPR Technologies quantiques, dont un des projets ciblés est notamment consacré à la cryptographie post-quantique. Enfin, dans le prolongement de ses actions destinées à favoriser l'innovation et le transfert au niveau des laboratoires, le CNRS est présent au Campus Cyber de la Défense, inauguré en 2022, pour intensifier les échanges entre les différents acteurs (laboratoires de recherche, grands groupes, PME, services de l'État) de l'écosystème de la cybersécurité.

## CYBERSÉCURITÉ ET SCIENCES HUMAINES ET SOCIALES

Au CNRS, d'autres laboratoires s'intéressent à la sécurité informatique sous l'angle juridique, économique, politique ou social. Le CIS, à Paris, par exemple, explore les usages du chiffrement par les militants et journalistes dans les contextes de risque élevé. L'IODE, à Rennes, étudie les enjeux juridiques de la stratégie numérique européenne à travers les notions de blockchain et confidentialité, relatives à la gestion des données.



**Cartographie des laboratoires en cybersécurité au CNRS**

# Citations de recherche : chercheurs et chercheuses en cybersécurité

Les laboratoires associés au CNRS abritent plusieurs chercheuses et chercheurs très visibles sur les thèmes liés à la sécurité informatique.



© Mariana Diaz Ramirez

## Véronique Cortier

Directrice de recherche CNRS au LORIA, médaille d'argent du CNRS 2022, ERC Starting Grant 2011, prix Inria-Académie des sciences du jeune chercheur 2015

**Développer Belenios, un logiciel de vote par Internet, disponible sur notre serveur pour tous ceux qui souhaitent organiser un scrutin en ligne librement et gratuitement. »**



© LORIA

## Pierrick Gaudry

Directeur de recherche CNRS au LORIA

**Montrer que les solutions utilisées pour sécuriser les connexions Internet doivent être renforcées suite à la mise en évidence de l'attaque Logjam contre le protocole de chiffrement TLS. »**



© Fabrice / Université de Rennes

## Clémentine Maurice

Chargée de recherche CNRS au CRISTAL, prix de la Femme Cyber chercheuse 2022

**Examiner les sources des failles de sécurité pour repenser la sécurité de nos ordinateurs. »**



© C. Morel / IRISA / CNRS Photothèque

## Stéphanie Delaune

Directrice de recherche CNRS à l'IRISA, ERC Starting Grant 2016

**Produire des protocoles de sécurité véritablement pensés pour les particularités du sans contact. »**



© InriaPhotothèque

## Jean-Yves Marion

Professeur à l'Université de Lorraine, porteur du Labcom Cybermallix

**Développer des techniques d'analyse morphologique, qui correspondent à extraire d'un code sa structure interne, comme si on lui faisait passer une radio pour ne regarder que les os ! »**



© Fabrice Pointcheval

## David Pointcheval

Directeur de recherche CNRS, directeur du DI ENS, médaille d'argent 2021 du CNRS, ERC Advanced Grant et Proof of Concept 2013 et 2020

**Étudier à quel point l'inévitable externalisation des données et des calculs vers le Cloud est compatible avec le respect de la vie privée. »**



# Politique scientifique

Depuis 2016, le CNRS mène une action volontariste sur le thème de la sécurité informatique qui s'est traduite par de multiples actions.

## RECRUTEMENT DE JEUNES CHERCHEUSES ET CHERCHEURS

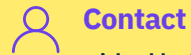
Depuis 2016, la thématique sécurité (cryptologie, sécurité quantique, sécurité matérielle, vie privée, sûreté et sécurité des systèmes, etc.) a été systématiquement présente sous la forme de coloriages thématiques au niveau des concours de recrutement des chargées et chargés de recherche CNRS. Depuis cinq ans, dix jeunes chercheurs et chercheuses ont ainsi été recrutés en sécurité informatique.

## ANIMATION SCIENTIFIQUE

Dans le cadre de son focus thématique consacrée au thème de la sécurité en 2016, CNRS Sciences informatiques a lancé plusieurs actions destinées à animer la communauté cybersécurité, avec, en particulier, la création du Groupement de recherche (GDR) Sécurité informatique (voir focus page suivante).

## SOUTIEN AUX THÉMATIQUES ÉMERGENTES EN SÉCURITÉ

Le CNRS porte également une grande attention aux thématiques de recherche à long terme, susceptibles d'avoir un impact significatif dans le domaine de la sécurité de l'information à horizon de dix à vingt ans. Font notamment l'objet d'un fort soutien les thématiques liées aux technologies quantiques, en particulier sur la cryptographie post-quantique (laboratoires LIP, XLIM, IMB, LAB-STICC, IRISA, LHC, LMV) ainsi que les communications quantiques sécurisées (laboratoires LIP6 et INPHYNI).



Contact

michael.krajceki@cnrs.fr



Chercheuse expliquant une proposition de protocole de vote électronique

## PEPR CYBERSÉCURITÉ

Le Programme et équipements prioritaires de recherche (PEPR) Cybersécurité est une des mesures phares de la stratégie nationale d'accélération en cybersécurité annoncée par le Président de la République en février 2021. Doté de 65 M€ de budget et piloté conjointement par le CEA, le CNRS et Inria, le PEPR vise à développer sur six ans un ambitieux programme de recherche fondamentale, avec un fort impact attendu sur le développement et la compétitivité de la filière industrielle française de la cybersécurité. Pour le CNRS, la direction de ce programme est assurée par Sonia Ben Mokhtar, directrice de recherche CNRS au LIRIS. Le programme de recherche du PEPR Cybersécurité s'appuie à la fois sur des projets collaboratifs prioritaires ciblés (sur les architectures sécurisées, la protection des données personnelles, la sécurité logicielle, les protocoles de sécurité, etc.) et des appels à projets destinés à structurer des communautés scientifiques, notamment autour de la sécurité des données multimédia.

Pour en savoir plus  
<https://www.pepr-cybersecurite.fr/>

Contact  
[contact@pepr-cybersecurite.fr](mailto:contact@pepr-cybersecurite.fr)

## LE CNRS AU CAMPUS CYBER

Le CNRS est également présent au sein du Campus Cyber, lieu totem emblématique de l'ambition française dans le domaine de la cybersécurité, qui accueille sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des associations et des acteurs de la recherche. Au sein du Campus Cyber, le CNRS développe un programme spécifique d'animations et d'événements destinés à intensifier les échanges entre les acteurs du Campus et la recherche menée dans les laboratoires.

Pour en savoir plus  
<https://campuscyber.fr/>

Contact  
[nicolas.porquet@cnrs.fr](mailto:nicolas.porquet@cnrs.fr)



Analyse de protocoles cryptographiques afin d'assurer leur sécurité et la protection de la vie privée

# Innovation

L'augmentation du transfert de connaissances vers les entreprises et plus généralement vers l'ensemble de la société ainsi que l'accroissement de l'impact économique de ce transfert sont des priorités d'actions au CNRS. Le domaine de la cybersécurité offre de nombreuses opportunités d'interaction entre les laboratoires et le monde économique.

## LABCOM

Les laboratoires communs avec les entreprises représentent un modèle intégré de recherche partenariale qui repose sur une gouvernance et un programme scientifique partagés à moyen et long termes.

### CYBERMALLIX

Cybermallix est un laboratoire commun créé en décembre 2021 entre le LORIA et WALLIX, éditeur européen de logiciels de cybersécurité. Ils allient leurs compétences pour renforcer la lutte contre les malwares. L'objectif est de concevoir et de développer des solutions de cybersécurité prédictive, basées sur l'intelligence artificielle, afin de maximiser la détection de logiciels malveillants.

## CRYPTANALYTICS : L'ERC PoC DE DAVID POINTCHEVAL

Une ERC Proof of concept (PoC), un financement qui aide les scientifiques à valoriser et appliquer les résultats d'un précédent ERC, a été accordée à l'équipe de David Pointcheval, directeur de recherche CNRS et directeur du DI ENS, pour ses travaux sur des solutions de cryptographie qui sécurisent le Cloud, où données et calculs sont distribués à distance.

## START-UP

Sur 1400 start-up issues d'unités mixtes de recherche CNRS, 38% relèvent du secteur des technologies de l'information et de la communication, avec une part significative qui concernent l'utilisation de technologies impliquant la cybersécurité.

### FACE-ALIVE

FACE-ALIVE est une start-up créée en 2022 spécialisée dans la sécurité biométrique. Elle est adossée au GIPSA-lab, représenté par Alice Caplier, professeure à Grenoble INP et membre de l'équipe de la start-up. FACE-ALIVE développe des technologies, telles que des systèmes de reconnaissance faciale ou d'empreintes digitales, utilisées par des entreprises et des institutions publiques pour se protéger face aux usurpations d'identité.



Contact

ins2i.valorisation@cnrs.fr

# Focus sur le groupement de recherche sécurité informatique

Le Groupement de recherche (GDR) Sécurité informatique est un outil national d'animation de la recherche créé en 2016 par CNRS Sciences informatiques.

Le GDR rassemble aujourd'hui plus de 1300 participants issus du CNRS, des institutions académiques partenaires et du monde industriel. Il anime la communauté au travers d'activités scientifiques, notamment des rencontres entre académiques et industriels, des écoles pour jeunes chercheuses et chercheurs, des journées nationales et des événements de sensibilisation.

## Co-responsables du GDR

**Caroline Fontaine**

Directrice de recherche CNRS au LMF

**Adeline Roux-Langlois**

Directrice de recherche CNRS au GREYC



## GROUPES DE TRAVAIL

Les activités du GDR s'organisent selon six groupes de travail :

- Codage et cryptographie (commun avec le GDR IM)
- Méthodes formelles pour la sécurité
- Protection de la vie privée
- Sécurité et données multimédia (commun avec le GDR ISIS)
- Sécurité des systèmes, des logiciels et des réseaux
- Sécurité des systèmes matériels (commun avec le GDR SOC2)

## ANIMATION

Des événements thématiques sont organisés par les groupes de travail. En 2022, il y a ainsi eu 10 conférences ou journées thématiques organisées par les GT.

## REDOCS



Les Rencontres Entreprises-DOCTORANTS en Sécurité (REDOCS) constituent un événement annuel important du GDR Sécurité informatique. Ces rencontres permettent de renforcer les liens entre les mondes académiques et industriels.

Cette expérience permet aux doctorants de se confronter à la réalité des problèmes industriels. Elle leur permet aussi de nouer des contacts pour préparer leur après-thèse. Pour les entreprises, les REDOCS permettent d'obtenir des solutions originales à leurs problèmes et de rencontrer des doctorants qui seront potentiellement de futurs collaborateurs, experts en sécurité.

Les entreprises qui souhaitent participer à REDOCS doivent contacter les co-responsables du GDR.

## GAZETTE

Le GDR publie une Gazette trimestrielle qui donne la parole à la communauté scientifique. Au-delà des annonces d'événements, la Gazette propose des interviews de chercheuses et chercheurs et des synthèses des événements du GDR, pour ceux qui n'auraient pas eu l'opportunité d'y assister.

## CLUB DES PARTENAIRES

Le GDR a mis en place en janvier 2020 un club de partenaires industriels dont les objectifs sont notamment de faciliter le rapprochement entre les communautés académiques et industrielles, d'aider les entreprises à maintenir une veille technologique de qualité, ainsi que de mettre en relation recruteurs et jeunes chercheuses et chercheurs.



Pour en savoir plus

<https://gdr-securite.irisa.fr/>



Contacts

[caroline.fontaine@cnrs.fr](mailto:caroline.fontaine@cnrs.fr)

[adeline.roux-langlois@cnrs.fr](mailto:adeline.roux-langlois@cnrs.fr)

# Tutelles des laboratoires cités

Bordeaux INP  
CentraleSupélec  
CNRS  
CY Cergy Paris Université  
École Centrale de Lille  
École des Mines de Saint-Étienne  
ENIB  
ENS - PSL  
ENS Lyon  
ENS Paris-Saclay  
ENS Rennes  
ENSEA  
ENSICAEN  
ENSTA Bretagne  
IMT Atlantique  
INP Toulouse  
Inria  
INSA Lyon  
INSA Rennes  
Institut Polytechnique de Bordeaux  
Institut Polytechnique de Paris

Nantes Université  
Sorbonne Université  
Université Bretagne Occidentale  
Université Bretagne-Sud  
Université Caen Normandie  
Université Claude Bernard Lyon 1  
Université Clermont Auvergne  
Université de Bordeaux  
Université de Lille  
Université de Limoges  
Université de Lorraine  
Université de Montpellier  
Université de Rennes  
Université de technologie de Compiègne  
Université de Versailles Saint-Quentin-en-Yvelines  
Université Grenoble Alpes  
Université Jean Monnet  
Université Paris-Saclay  
Université Rennes 2  
Université Sorbonne Paris Nord  
Université Toulouse 3 Paul Sabatier

**Direction de la publication :** Antoine Petit

**Réalisation et mise en page :** Pôle communication de CNRS Sciences informatiques

**Impression :** CNRS DRI6 IFSEM Secteur de l'imprimé

**Mars 2024**

**Photo de couverture :** Tableau noir : Comprendre les attaques pour améliorer les systèmes de défense. © Christian MOREL / IRISA / CNRS Photothèque



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*





**CNRS**  
 3, rue Michel-Ange  
 75794 Paris Cedex 16  
 + 33 1 44 96 40 00  
[cnrs.fr](http://cnrs.fr) | [X](#) | [LinkedIn](#) | [YouTube](#)

