



## DOSSIERS THÉMATIQUES DU CNRS

# LA CYBERSÉCURITÉ AU CNRS



# LES LABORATOIRES EN CYBERSÉCURITÉ

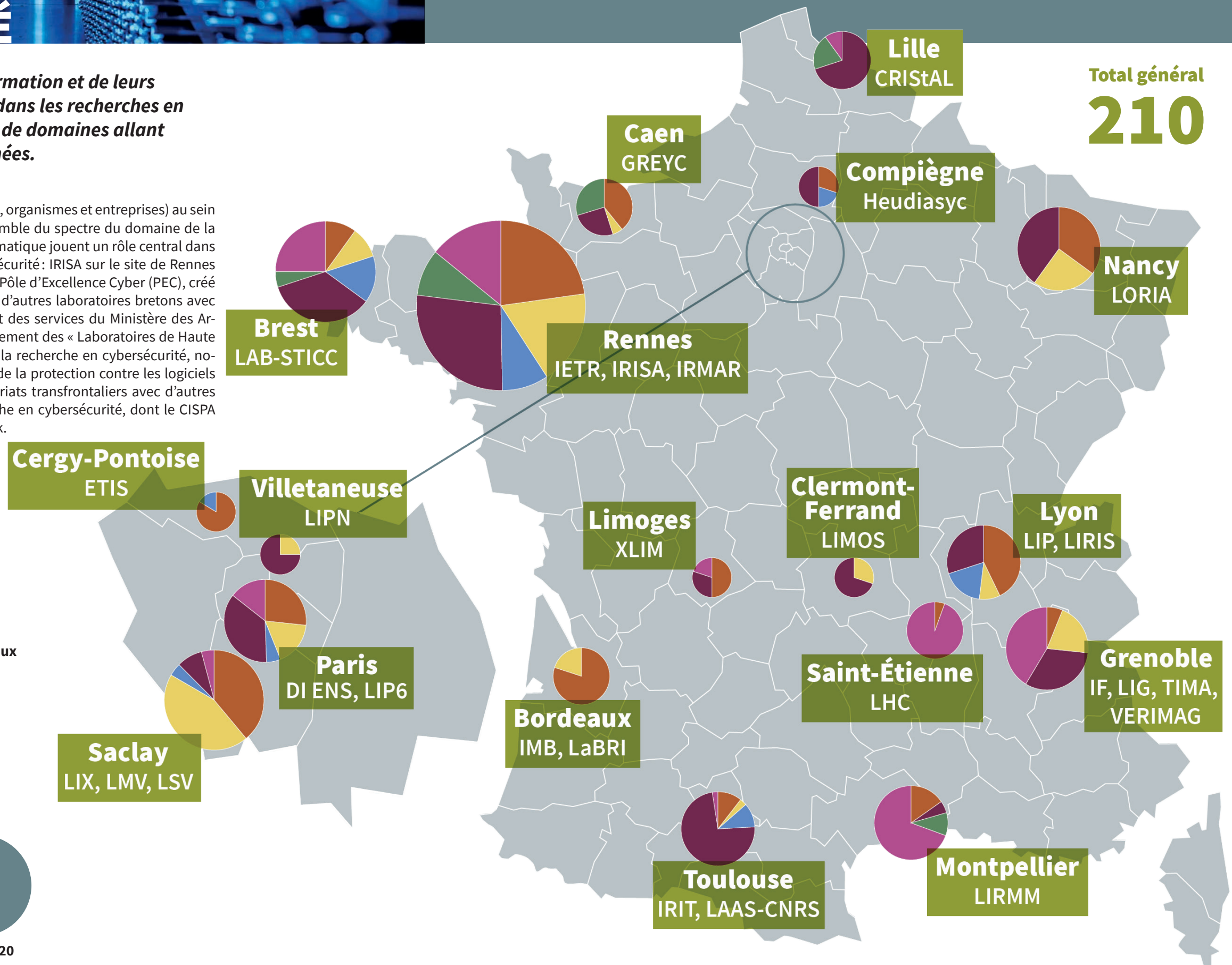
À travers l'Institut des sciences de l'information et de leurs interactions (INS2I), le CNRS est investi dans les recherches en cybersécurité et couvre un large spectre de domaines allant de la cryptologie à la protection de données.

Le CNRS mène, avec ses partenaires (universités, écoles, organismes et entreprises) au sein des unités mixtes de recherche, des travaux sur l'ensemble du spectre du domaine de la cybersécurité. Deux laboratoires de recherche en informatique jouent un rôle central dans les deux pôles identifiés au niveau national en cybersécurité : IRISA sur le site de Rennes et LORIA sur celui de Nancy. Le site rennais accueille le Pôle d'Excellence Cyber (PEC), créé en 2016, qui structure les partenariats entre l'IRISA et d'autres laboratoires bretons avec des acteurs industriels français de la filière sécurité et des services du Ministère des Armées. Les sites de Rennes et de Nancy accueillent également des « Laboratoires de Haute Sécurité » (LHS) qui constituent des plateformes pour la recherche en cybersécurité, notamment sur le thème de la détection d'intrusions et de la protection contre les logiciels malveillants. Le site de Nancy développe des partenariats transfrontaliers avec d'autres centres d'excellence européens en matière de recherche en cybersécurité, dont le CISP (Helmholtz Center for Information Security) à Sarrebruck.

## Thématiques abordées :

- Codage et cryptographie
- Méthodes formelles pour la sécurité
- Protection de la vie privée
- Sécurité des systèmes, des logiciels et des réseaux
- Sécurité et données multimédia
- Sécurité des systèmes matériels

## Nombre de chercheurs et enseignants-chercheurs en cybersécurité :



Cartographie des laboratoires en cybersécurité au CNRS



# CITATIONS DE RECHERCHE : CHERCHEUSES ET CHERCHEURS EN CYBERSÉCURITÉ

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



**Jean-Yves Marion**  
Professeur à l'Université de Lorraine, directeur du LORIA

« 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 ! »



**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. »



**David Pointcheval**  
Directeur de recherche CNRS, directeur du DI ENS, ERC Advanced Grant 2013

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



**Véronique Cortier**  
Directrice de recherche CNRS au LORIA, 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. »



**Hubert Comon**  
Professeur de l'ENS Paris-Saclay au LSV, médaille d'argent du CNRS 2008

« Proposer un nouveau paradigme en méthodes formelles pour réaliser des preuves de sécurité quel que soit le modèle d'attaquant. »



**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. »

## POLITIQUE SCIENTIFIQUE

Depuis 2015, l'Institut des sciences de l'information et de leurs interactions (INS2I) du CNRS a mené 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 chargés de recherche CNRS. Depuis quatre ans, six jeunes chercheuses et chercheurs ont été recrutés sur cette thématique au sein de l'Institut de recherche en informatique et systèmes aléatoires, du Laboratoire lorrain de recherche en informatique et ses applications, du Laboratoire Hubert Curien et du Centre de Recherche en Informatique, Signal et Automatique de Lille.

### ANIMATION SCIENTIFIQUE

Dans le cadre de son année thématique consacrée au thème de la sécurité en 2016, l'INS2I au CNRS a lancé plusieurs actions destinées à animer la communauté cybersécurité au sein de ses unités, avec, en particulier, la création du Groupement de recherche (GdR) Sécurité informatique (voir focus pages suivantes). L'institut a également co-piloté avec Inria, au sein de l'alliance des sciences et technologies du numérique ALLISTENE, la réalisation en 2016-2017 de la cartographie nationale des recherches en cybersécurité.

### SOUTIEN AUX THÉMATIQUES ÉMERGENTES EN SÉCURITÉ

En marge des recherches sur la sécurité informatique classique, l'INS2I-CNRS soutient également le thème émergent de la sécurité post-quantique, en particulier à travers la Fédération Paris Centre for Quantum Computing (PCQC) créée en 2014 pour coordonner les actions des équipes des unités IRIF et LIP6. PCQC présente un potentiel unique au niveau national, porté notamment par six chercheurs CNRS dont les travaux ont une très grande visibilité internationale (avec, notamment, deux projets ERC Starting Grant). PCQC est partenaire de deux projets sélectionnés en 2018 pour la phase de lancement du futur flagship européen Technologies quantiques.

Chercheuse expliquant une proposition de protocole de vote électronique. Les équations correspondent au fonctionnement de ce protocole.



## LE GROUPEMENT DE RECHERCHE SÉCURITÉ INFORMATIQUE

**Le GdR (Groupement de recherche) Sécurité Informatique est un outil national d'animation de la recherche créé en 2016 par l'Institut des sciences de l'information et de leurs interactions (INS2I) du CNRS.**

Le GdR rassemble aujourd'hui plus de 1000 participants issus du CNRS, des institutions académiques partenaires et du monde industriel. Le GdR 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.



Directeur du GdR  
**Gildas Avoine**  
Professeur, INSA Rennes  
IRISA



### LES ACTIVITÉS DU GDR S'ORGANISENT SELON SIX GROUPES DE TRAVAIL :

- **Codage et cryptographie (commun avec GdR IM)**  
Responsable : Damien Vergnaud
- **Méthodes formelles pour la sécurité**  
Responsables : Stéphanie Delaune et Sébastien Bardin
- **Protection de la vie privée**  
Responsable : Benjamin Nguyen
- **Sécurité et données multimedia (commun avec GdR Isis)**  
Responsables : Caroline Fontaine et William Puech
- **Sécurité des systèmes, des logiciels et des réseaux**  
Responsables : Aurélien Francillon et Olivier Levillain
- **Sécurité des systèmes matériels (commun avec GdR SOC2)**  
Responsables : Lillian Bossuet et Marie-Lise Flottes

### ANIMATION

Des événements thématiques sont également organisés par les groupes de travail. En 2018, il y a ainsi eu 13 conférences ou journées thématiques organisées par les GT.

**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. Durant toute une semaine en immersion, les doctorants travaillent en groupe afin de résoudre des défis scientifiques proposés par des industriels, aux frontières de la recherche académique et des préoccupations du monde économique.

Cette expérience permet aux doctorants de se confronter à la réalité des problèmes des 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.

## REDOCS

Chaque année, trois ou quatre entreprises sont conviées à REDOCS, qui défient trois ou quatre équipes de quatre doctorants, pendant une semaine très intensive.

Les entreprises qui souhaitent participer à REDOCS doivent contacter le directeur du GdR.

Le GdR publie une Gazette trimestrielle qui laisse 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.

Pour en savoir +  
<http://gdr-securite.irisa.fr/redocs/>

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.

### LES PARTENAIRES 2016-2019 DES REDOCS





## TUTELLES DES LABORATOIRES

Aix-Marseille Université  
Bordeaux INP  
CentraleSupélec  
CY Cergy Paris Université  
École Centrale de Lille  
École Centrale de Lyon  
École Centrale de Nantes  
École des Mines de Saint-Étienne  
École des Ponts ParisTech  
ENGEEES  
ENIB  
ENS  
ENS Lyon  
ENS Rennes  
ENSEA  
ENSICAEN  
ENSTA Bretagne  
Grenoble INP  
IMT Atlantique  
INP Toulouse  
Inria  
INSA Lyon  
INSA Rennes  
INSA Strasbourg  
Institut Polytechnique de Paris  
Sorbonne Université

Université Bretagne Occidentale  
Université Caen Basse-Normandie  
Université Clermont Auvergne  
Université Côte d'Azur  
Université de Bordeaux  
Université de Bretagne-Sud  
Université de l'Artois  
Université de Lille  
Université de Lorraine  
Université de Lyon  
Université de Montpellier  
Université de Nantes  
Université de Rennes 1  
Université de Strasbourg  
Université de technologie de Compiègne  
Université de Toulon  
Université Grenoble Alpes  
Université Gustave Eiffel  
Université Lumière Lyon 2  
Université Paris-Dauphine PSL  
Université Paris-Saclay  
Université Polytechnique Hauts-de-France  
Université Sorbonne Paris Nord  
Université Toulouse 1 Capitole  
Université Toulouse 2 Jean Jaurès  
Université Toulouse 3 Paul Sabatier

Photo de couverture : Bibliothèque de stockage à bandes magnétiques du Centre de calcul de l'Institut de physique nucléaire et de physique des particules (CC-IN2P3). Cette infrastructure de recherche conçoit et opère un système de stockage de masse et de traitement de grandes quantités de données, contribuant ainsi à de nombreuses expériences d'envergure internationale, principalement dans le domaine de la physique et de l'astroparticule. Le centre participe également à des projets transdisciplinaires. Ses deux salles informatiques de 850 m<sup>2</sup> chacune hébergent plusieurs milliers de serveurs ainsi que des bibliothèques robotisées pouvant stocker près de 340 pétaoctets de données sur bandes magnétiques.

© Cyril FRESILLON / CC IN2P3 / CNRS Photothèque

### CNRS

Institut des sciences de l'information et de leurs interactions (INS2I)

3, rue Michel-Ange 75016 Paris

[www.ins2i.cnrs.fr](http://www.ins2i.cnrs.fr)

Contact : [ins2i.secretariat@cnrs.fr](mailto:ins2i.secretariat@cnrs.fr)



Réalisation et mise en page : INS2I Communication  
Impression : CNRS DR1 IFSEM secteur de l'imprimé  
Septembre 2020

Contact :  
[olivier.cappe@cnrs.fr](mailto:olivier.cappe@cnrs.fr)