



DOSSIERS THÉMATIQUES DU CNRS

LA CYBERSÉCURITÉ AU CNRS

LES LABORATOIRES EN CYBERSÉCURITÉ

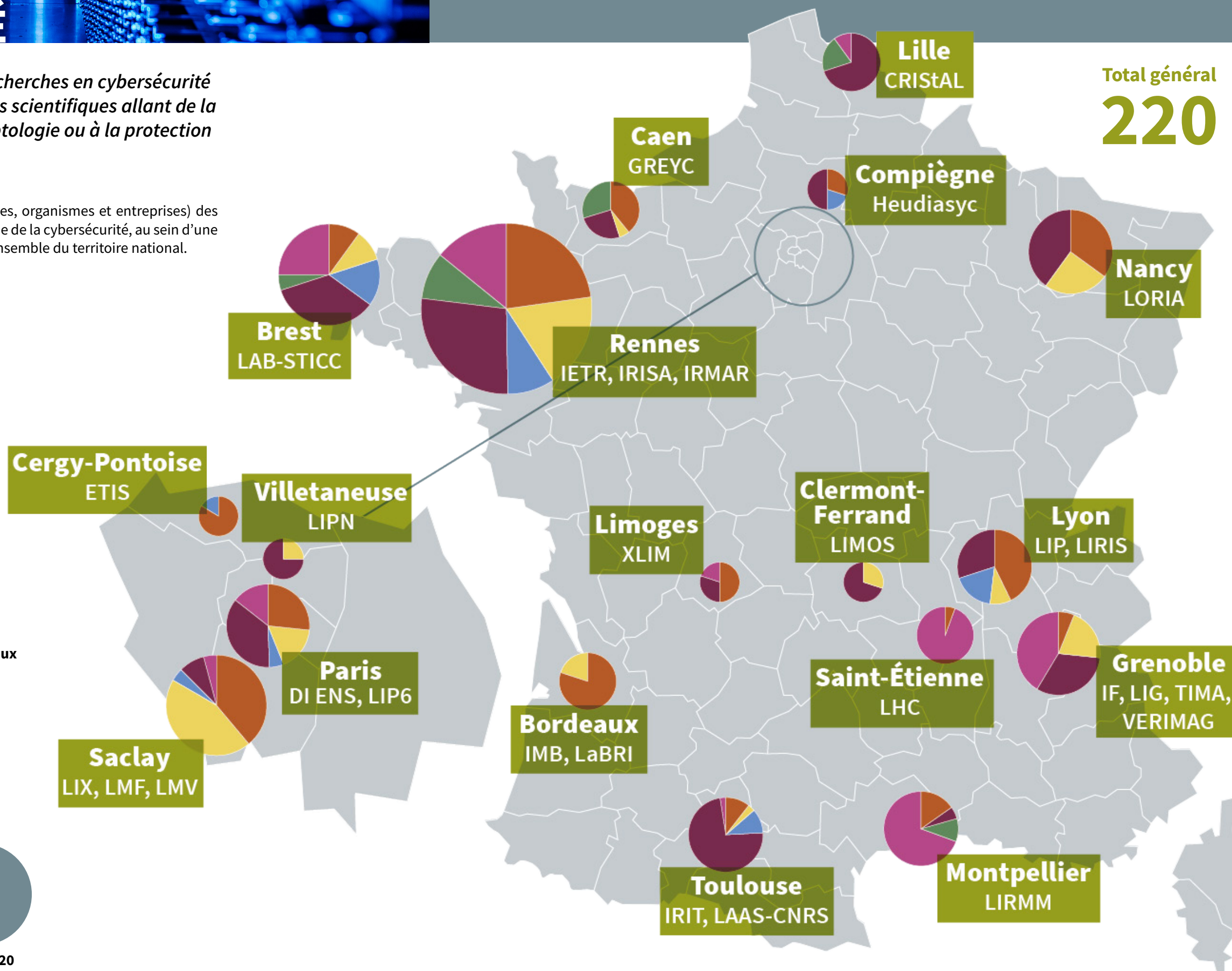
Le CNRS est fortement investi dans les recherches en cybersécurité et couvre un large spectre de thématiques scientifiques allant de la sécurité des systèmes matériels, à la cryptologie ou à la protection de données à caractère personnel.

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 réparties sur l'ensemble du territoire national.

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.



© Inria/Photo Kaksonen

« 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 ! »

Jean-Yves Marion
Professeur à l'Université de Lorraine, directeur du LORIA, porteur du Labcom Cybermallix



© Inria/Photo Kaksonen

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

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



© Inria/Photo N. Dohr

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

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



© Inria/Photo D. Grandmougin

« 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. »

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



Crédit photo : Clémentine Maurice

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

Clémentine Maurice
Chargée de recherche CNRS au CRISTAL



© 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. »

Pierrick Gaudry
Directeur de recherche CNRS au LORIA

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 chargés de recherche CNRS. Depuis cinq ans, dix jeunes chercheuses et chercheurs ont ainsi été recrutés en sécurité informatique.

ANIMATION SCIENTIFIQUE

Dans le cadre de son année thématique consacrée au thème de la sécurité en 2016, l'Institut des sciences de l'Information et de leurs interactions (INS2I) du CNRS 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).

PEPR CYBERSECURITE

Le PEPR (« Programme et Équipements Prioritaires de Recherche ») Cybersécurité est une des mesures phares de la stratégie nationale d'accélération en cybersécurité annoncée par le Président de la République en février 2021. 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 responsabilité de la conception et du suivi de ce programme, doté de 65 M€ de budget, est assurée par Gildas Avoine, Professeur Insa Rennes à l'IRISA et ancien directeur du GDR Sécurité informatique. 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.

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.

Contact :
nicolas.porquet@cnrs.fr

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.

Après avoir été dirigé par Gildas Avoine de 2016 à 2021, le GDR est maintenant dirigé par Caroline Fontaine. Il rassemble aujourd'hui plus de 1300 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.



Directrice du GDR
Caroline Fontaine
Directrice de recherche CNRS, LMF



GROUPES DE TRAVAIL

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

- 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)

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 la directrice du GDR.

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

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.

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

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.

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.

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.

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 le 7 décembre 2021, suite à un partenariat 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.

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.

ALGODONE

Algodone est une start-up créée en 2015 issue des travaux du LIRMM. Elle fournit des plateformes de sécurité flexibles et clés en main dédiées à la gestion des réseaux d'objets connectés. Il s'agit d'une infrastructure complète pour gérer de manière sécurisée le cycle de vie d'objets connectés et proposer des schémas de monétisation disruptifs.

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.

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 Paris Saclay
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 m² 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

Contact : ins2i.secretariat@cnrs.fr

Réalisation et mise en page : INS2I Communication

Impression : CNRS DR1 IFSEM secteur de l'imprimé

Mai 2022



Contact :

olivier.cappe@cnrs.fr