Institut Mines-Télécom

ACTIVITÉS DE L'IMT

DANS LE DOMAINE DES RISQUES ET DE LA CYBERSÉCURITÉ

Initialement, deux sous communautés

- Plutôt séparées entre « Mines » et « Télécom »
- Regroupements car synergies identifiées par les écoles
- Avec les fusions d'écoles, couverture géographique plus homogène

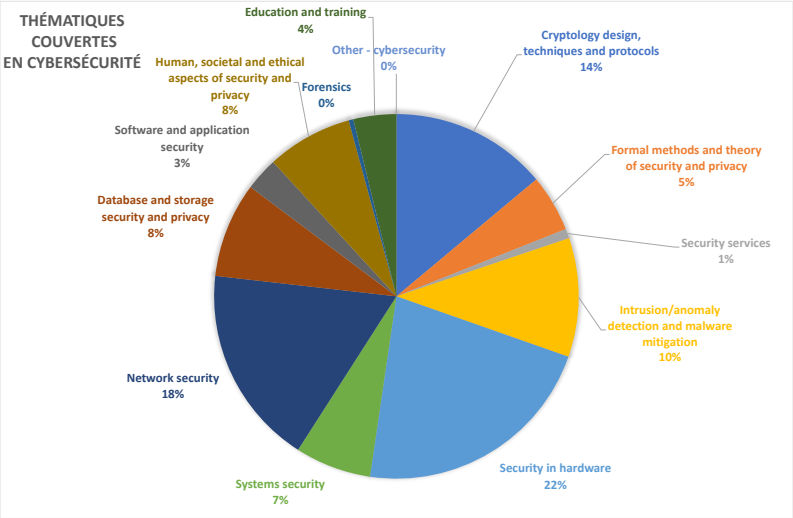
Forte présence dans les appels compétitifs à l'échelon européen

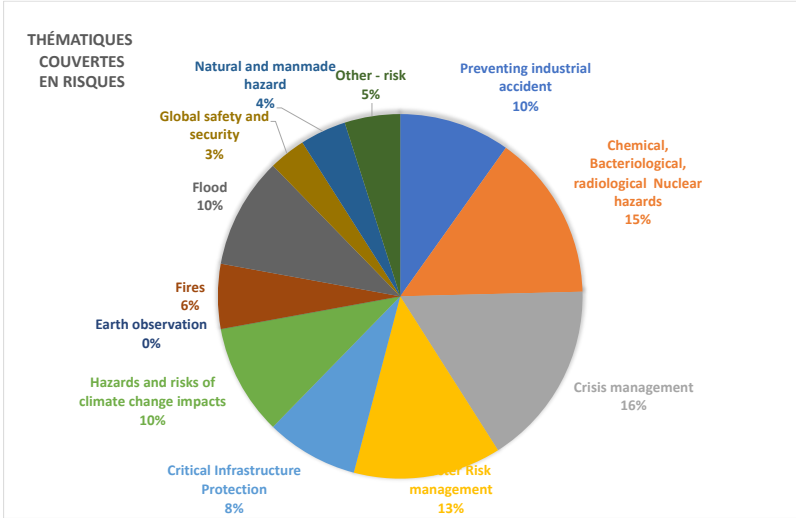
- Coordination et partenariat dans des projets EU et FR
- Présence dans les actions de soutien à la politique EU (expertise, cPPP, …)

Forte demande sociétale

- Formation initiale et tout au long de la vie
- Développement de nouvelles technologies pour relever les grands défis d'aujourd'hui

FORCES PAR GRANDES THÉMATIQUES DE RECHERCHE





- **Interactions entre cybersécurité et risque**
  - Impact des cyberattaques induisant des risques sur des infrastructures critiques
  - Gestion de crise incluant crise « cyber » via infrastructures numériques
  - Impact global du numérique sur nos sujets

- **Application à différents cas d'usage communs**
  - Énergie
  - Santé
  - Immeubles et villes connectés
  - Véhicule connecté
  - Industrie du futur
  - Réseaux du futur (5G&6G, IoT, virtualisation, ...)

- **Plates-formes**

Institut Mines-Télécom

RECHERCHE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

IMT Mines Albi-Carmaux
École Mines-Télécom

IMT Mines Alès
École Mines-Télécom

Institut Mines-Télécom
Business School

MINES
Saint-Étienne
Une école de l'IMT

TELECOM
Paris
IP PARIS

TELECOM
SudParis
IP PARIS

EURECOM

InSIC

Algorithmes cryptographiques

- Cryptographie différentielle; homomorphe
- Fonctions physiques non-clônables (PUF)
- Cryptographie post-quantique

Protocoles cryptographiques et sécurité des données

- Blockchain: laboratoire BART
- Calculs sur données masquées

BART
Blockchain
Advanced Research
& Technologies

Protection des données et des personnes

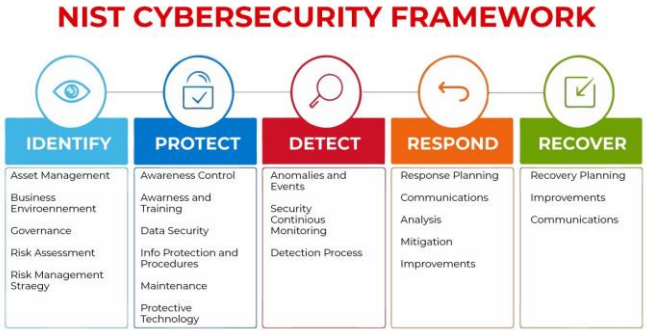
- Chaire Valeurs et Politiques des Informations Personnelles
- Phishing et fraude téléphonique

Tatouage d'images

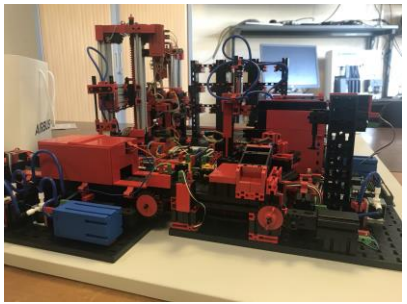
- Applications au multimédia
- Applications à la santé

Institut Mines-Télécom

- **Théorie des jeux**
  - Modélisation des mécanismes d'attaque et de défense
  - Évaluation des systèmes de cybersécurité
  - Optimisation des ressources cyber
- **Analyse de risque**
  - NIST cybersecurity framework
- **Moving Target Defense**
  - Accroissement de la difficulté d'attaque
- **Utilisation des jumeaux numériques pour la cybersécurité**



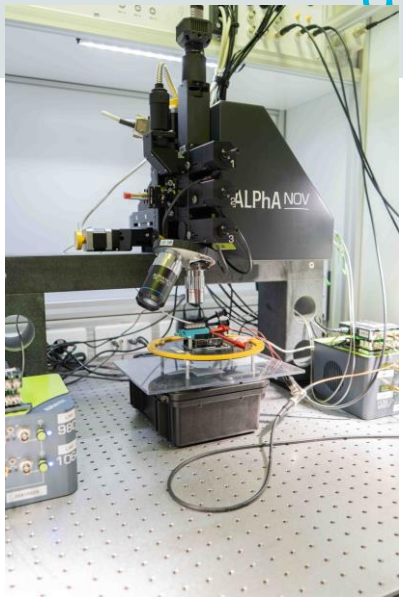
- **Lutte contre les attaques par déni de service**
  - Sécurité des réseaux logiciels (SDN, 5G)
  - Usage de l'IA pour la cybersécurité: détection comportementale
  - Sécurité des algorithmes d'IA
- **Sécurité des objets connectés**
  - Constitution d'une base ouverte de trafic d'objets
- **Sécurité des systèmes cyberphysiques**
  - Cybersécurité pour le véhicule connecté
    - Aspects intra-véhiculaires
    - V2X
  - Cybersécurité pour les protocoles SCADA
- **Analyse de code malveillant (malware)**
- **Analyse de risque, d'impact et remédiation**

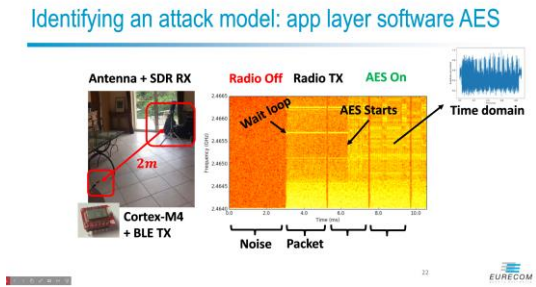


CHAIRE CYBER CNI
Sécurité des infrastructures critiques

Institut Mines-Télécom

- **Sécurité matérielle des systèmes embarqués contre les attaques physiques et cyber**
  - Modélisation des attaques cyber
  - Sécurité « by design »
  - Co-conception cybersécurité et sûreté de fonctionnement
- **Fiabilité matérielle des systèmes embarqués**
  - Architectures et méthodes de conception de systèmes embarqués
- **Confidentialité et intégrité des communications et du stockage externe**
  - Vulnérabilités des firmwares
  - Canaux cachés, fuite d'information
- **Capteurs biométriques**





- **Sécurité des réseaux existants et des réseaux du futur**
  - Lutte contre les attaques par déni de service
  - Déploiement de propriétés dans les environnements virtualisés

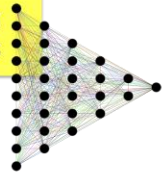
- **Cybersécurité pour l'Internet des objets**
  - Objets industriels
  - Objets connectés de santé

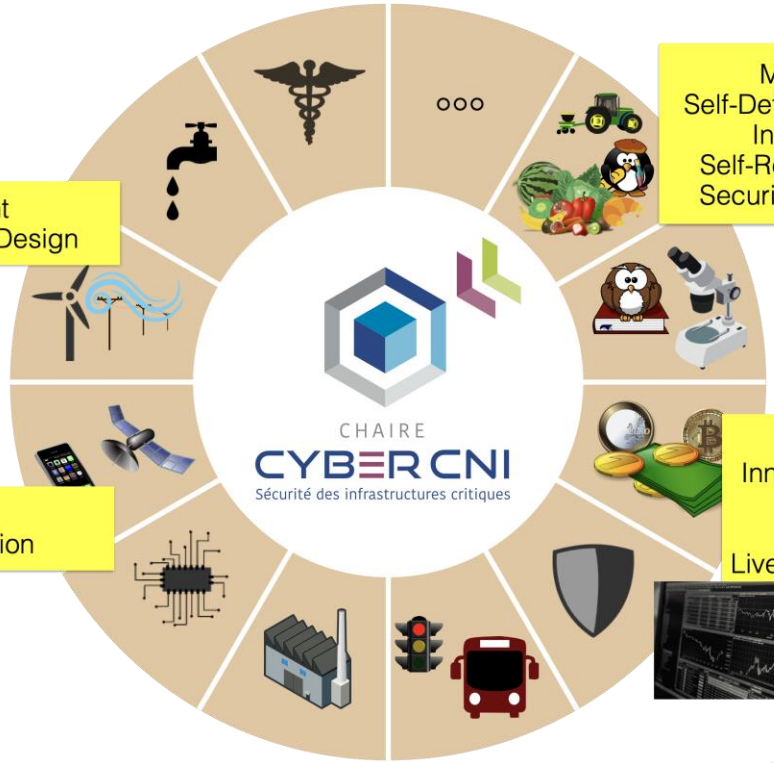
- **Sécurité de la chaîne logistique logicielle**
  - Analyse de vulnérabilités
  - Analyse de provenance
  - Analyse en boîte noire d'implémentation de protocoles cryptographiques

CHAIRE « CYBERSECURITY FOR CRITICAL NETWORKED INFRASTRUCTURES »

Prevent
Security-by-Design

Mitigate
Self-Defend Security Incidents
Self-Recover from Security Incidents





Detect
Anomaly Detection

Human-in-the-loop
Innovative interfaces, Mixed Reality
Data Analytics
Configuration
Live interaction, collaborative actions

14 PhD students | 3 PostDocs | 2 Engineers | 15 Professors

https://cyberCNI.fr

Institut Mines-Télécom

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

TELECOM Paris

TELECOM SudParis

AIRBUS AMOSSYS BNP PARIBAS La banque d'un monde qui change

EDF NOKIA Bell Labs SNCF PÔLE D'EXCELLENCE CYBER

Institut Mines-Télécom

Prévention des risques industriels

- Caractérisation et réduction des aléas
- Incendie, explosion, plateformes d'expérimentation

Plate forme SPARK IMT Mines Ales
explosion de poussières, transfert thermiques, BLEVE

Projet Européen MANIFESTS *: MANaging risks and Impacts From Evaporating and gaseous Substances To population Safety. DG Echo en collaboration avec le Cedre (Coordonnateur, Fr), IMT Mines Ales (Fr),*

Cedre

- la prévention
- ➢ **la préparation**
- la réponse
- le rétablissement

Projet européen eNOTICE

➢ to improve preparedness, resilience and incident response to CBRN attacks and emerging threats through close multi- (stakeholders) and single-discipline (practitioners) interactions.

➢ To improve operational interoperability between all civilian and military CBRN actors

- **Fiabilité des organisation (HRO)**
- **Performance industrielle (Pilotage de la sous traitance)**
- **Planification (amélioration de la fiabilité)**

Chaire RESOH

- La Chaire RESOH, **Recherche en Sûreté, Organisation, Hommes**, est une chaire de recherche et d'enseignement, portée par IMT Atlantique, en partenariat avec **l'ANDRA, Naval Group et l'IRSN**.

- Elle constitue un lieu de production scientifique et académique et d'échange sur le travail dans les organisations à risques, en particulier les mondes du nucléaire

CHAIRE RESOH

- **Ingénierie** des modèles, ingénierie des connaissances, ROP, Sciences des données
- **Industriel, naturels, humanitaires, logistique**

  Exploitation de modèles situationnels à vocation prédictive

Projet européen driver+

- Provide a formal environment to frame European innovation in technology for Crisis Management.
- To develop a Portfolio of Solutions in the form of a database-driven website that aims at documenting all DRIVER+ solutions (the DRIVER integration platform for emerging disaster management technologies).

1. **Analyse et modélisation** : mener une analyse scientifique et technique
2. **Approches numériques** : formaliser et développer des prototypes logiciels
3. Réaliser et interpréter les résultats de campagnes d'**expérimentation**

Plateformes de simulation (IMT Mines Ales, IMT Mines Albi et Mines St Étienne) Simulcrise, CitinCrise, IOmega

- Permetttent aux entreprises, quelle que soit leurs dimensions, leur positionnement et leur expérience, de mener à bien leurs programmes de recherche et développement sur ces thématiques.
- Les sujets traités vont de l'**intelligence artificielle** au service de la décision à l'**entraînement immersif** en passant par la **visualisation de situations complexes**.

Smart Cities

- **H2020 IMPETUS**
- **(TSP et IMT Mines Alès)**
- Gestion de la menace physique (menace biologique)
- et cyber dans la ville connectée

.

❖ H2020 EUNITY: Cybersecurity and privacy dialogue between Europe and Japan

❖ H2020 SPARTA: pilote de centres de compétences

- ➢ Pilotage du programme CAPE (Continuous Assessment for Polymorphic Environments)
- ➢ Pilotage de la tâche sur la formation professionnelle

❖ H2020 SOCCRATES: SIEM pour les infrastructures critiques

- ➢ Détection, prévention, CTI, réaction

❖ H2020 HEIR: Observatoire de la menace pour la cybersécurité des objets connectés de santé

- ➢ Threat hunting
- ➢ Privacy-aware framework

❖ H2020 IMPETUS: Gestion de la menace physique et cyber dans la ville connectée

❖ Cybersécurité et crise des environnements cyberphysiques

- Déjà traité depuis plusieurs années
- Intérêt marquant et continu de domaines d'application complémentaires

❖ Numérisation des infrastructures

- Collecte et analyse de données
- Intelligence situationnelle

❖ Gestion du facteur humain

- Exercices et entraînement

❖ Importance des cas d'usage

- Besoin de comprendre un contexte et de s'adapter à ses contraintes
- Interaction nécessaire avec des sachant du domaine visé

❖ Contribution aux activités des stratégies nationales

- Activités du PEPR Cybersécurité
  - Supervision de sécurité
  - Sécurité matérielle
  - Détection des codes malveillants
- Contributions aux actions/projets cybersécurité dans les PEPR 5G et Cloud

❖ Formation

- Former plus de personnes et mieux
  - Attractivité des métiers ?
- Formation tout au long de la vie
- Appel « Compétences et Métiers d'Avenir » : cybersécurité incluant gestion de crise

Institut Mines-Télécom

QUESTIONS ?

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

IMT Mines Albi-Carmaux
École Mines-Télécom

IMT Mines Alès
École Mines-Télécom

Institut Mines-Télécom
Business School

MINES
Saint-Étienne
Une école de l'IMT

TELECOM
Paris
IP PARIS

TELECOM
SudParis
IP PARIS

EURECOM

InSIC