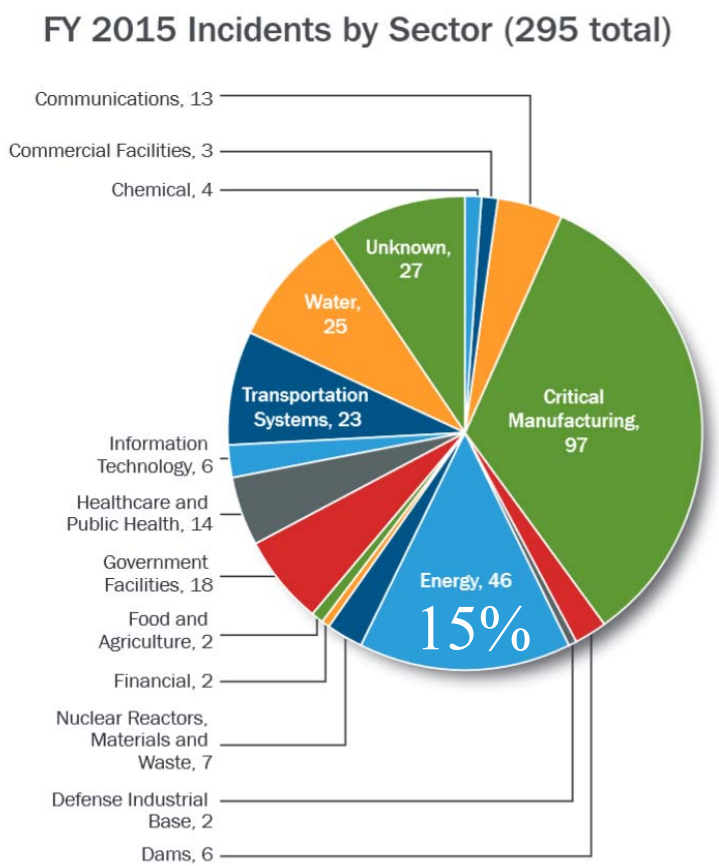
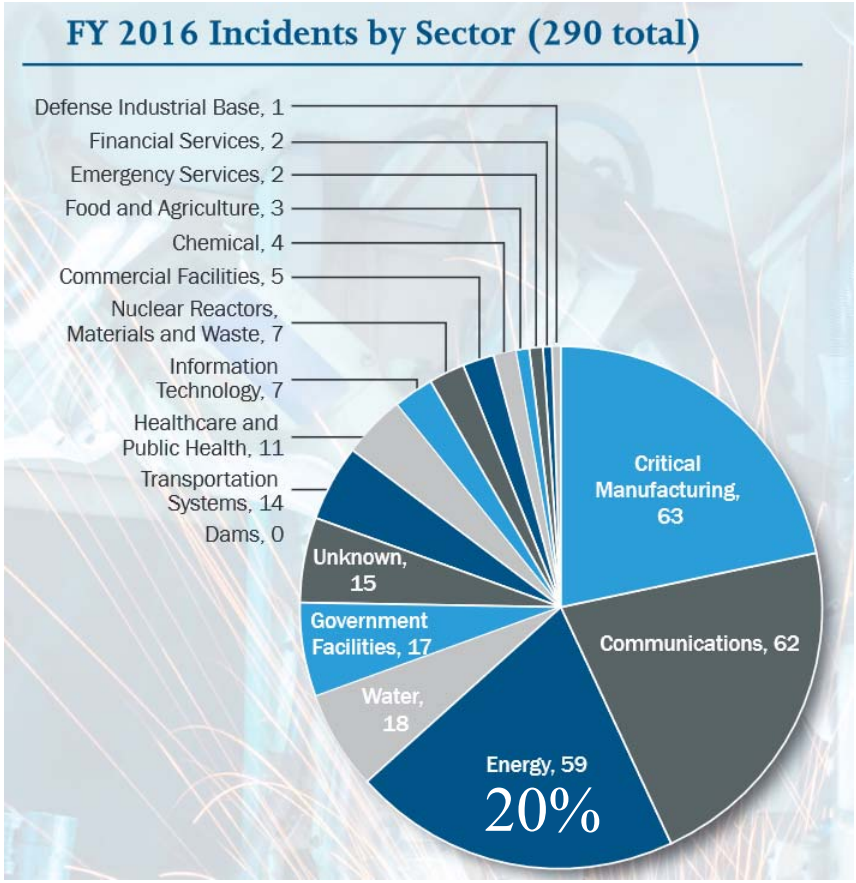
Cybersécurité des smart grids

Stéphane Mocanu
ENSE3/Grenoble-INP
Laboratoire d'Informatique de Grenoble

Motivation

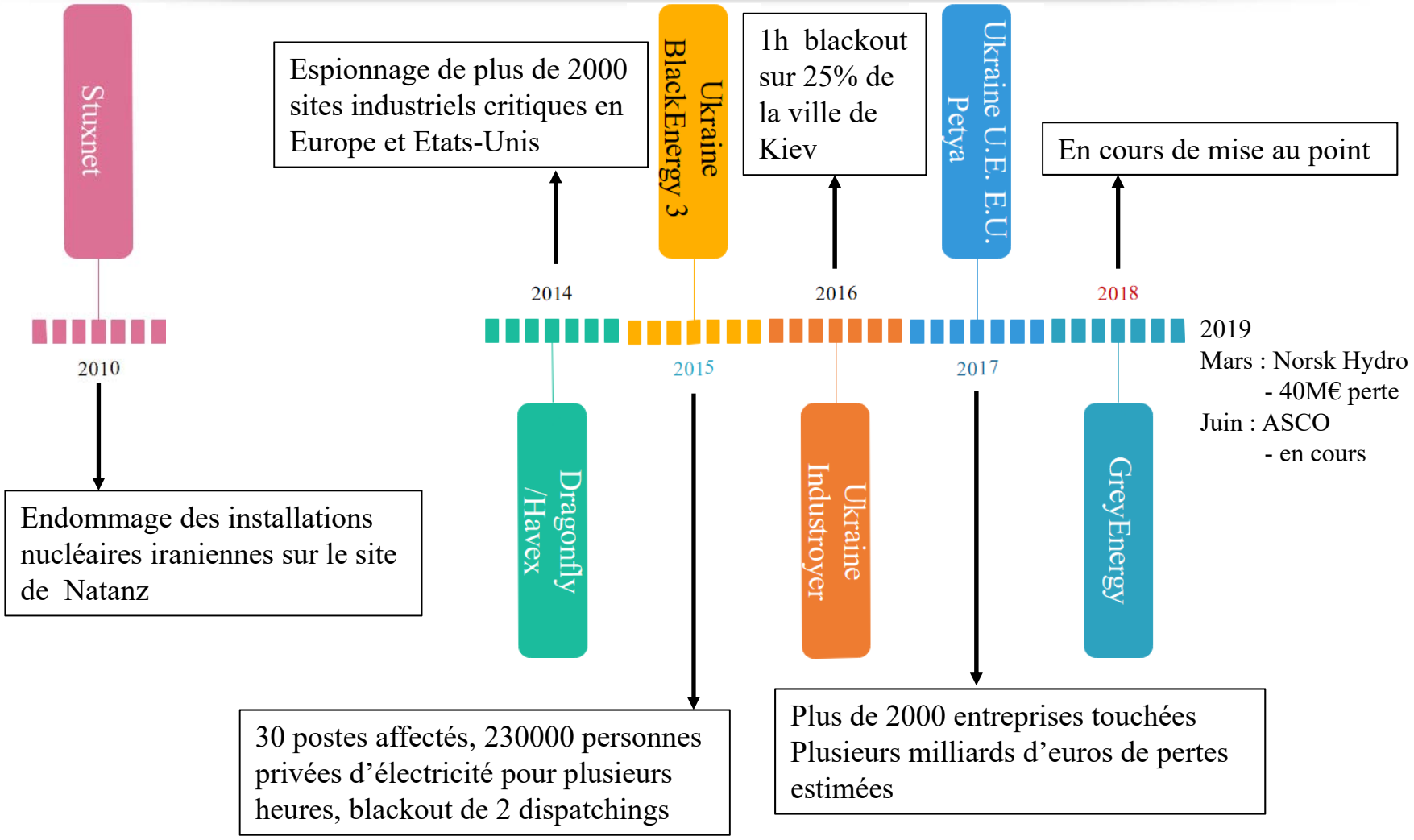
- Le secteur de l'énergie est une cible privilégiée des attaques





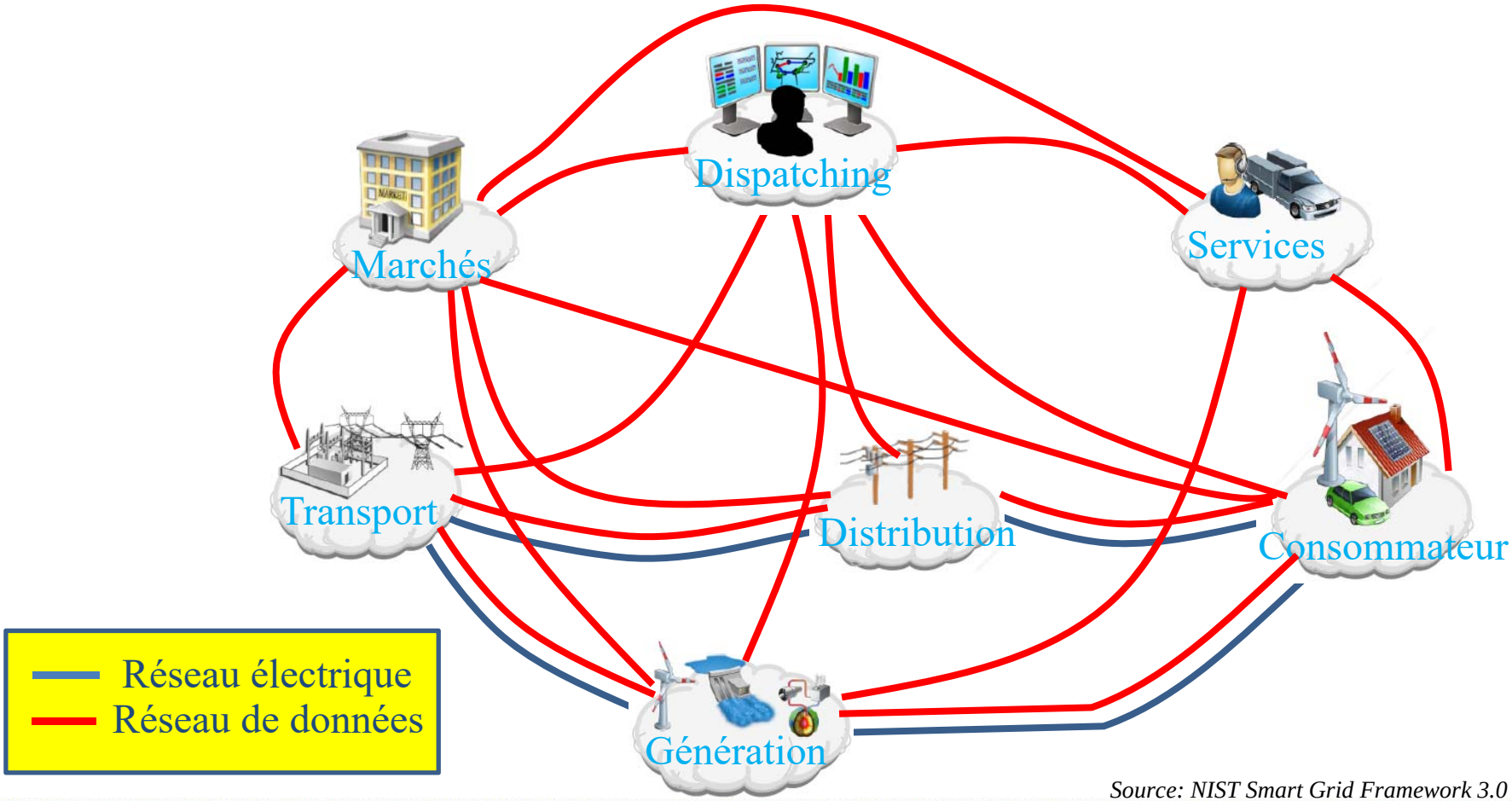
Sources: rapports annuels ICS-CERT https://ics-cert.us-cert.gov/

Attaques et conséquences



Le smart grid : un monde connecté

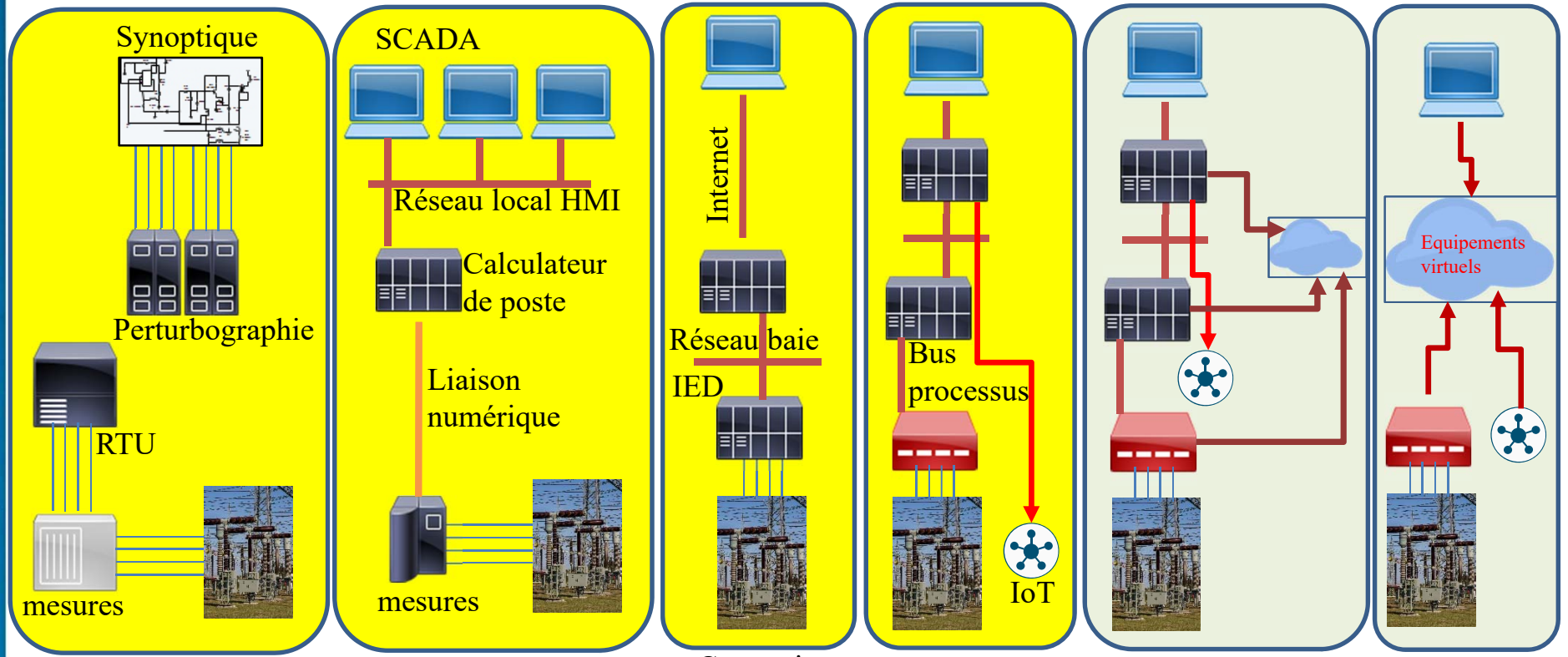
Un « double » réseau : électrique de informatique



Source: NIST Smart Grid Framework 3.0

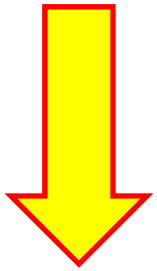
Un monde de plus en plus exposé

- Un exemple : le poste électrique



Etat de lieux

- Les réseaux de données sont indispensables dans les smart-grids
- Le déploiement des technologies Internet ouvre des portes pour les cyberattaques
- Les smart-grids du futur s'appuieront sur le cloud, Big Data, ingénierie de données



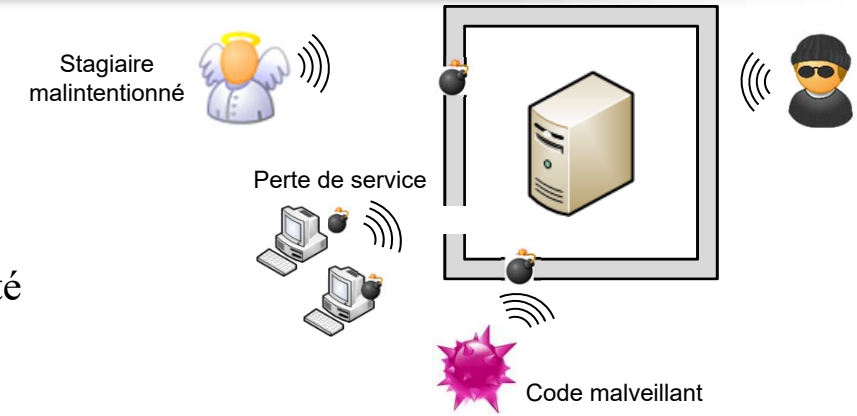
- Le déploiement de la sécurité des systèmes d'information est incontournable

L'énergie étant un Secteur d'Activité d'Importance vitale la SSI est obligatoire (Loi de la Programmation Militaire 2014)

La démarche SSI

Les notions basiques

- Actif primordial
- Menace
- Vulnérabilité
- Attaques = exploitation d'une vulnérabilité
- Intrusion = attaque réussie



Intrusion = exploitation réussie d'une vulnérabilité par une menace

La démarche SSI vise à

- réduire les vulnérabilités
- les rendre difficilement exploitable
- diminuer l'impact des intrusions

Garantir :

- la disponibilité des installation
- l'intégrité des données
- la confidentialité des informations
- la traçabilité des actions

Les guides, les références et les produits

- Normes internationale
  - ISO/IEC 27000 - Systèmes de gestion de sécurité de l'information
  - IEC 62443 Cybersécurité des installations industrielles
  - IEC 62351 Power systems management and associated information exchange - Data and communications security
- Guides et recommandations ANSSI
  - Maîtriser la SSI pour les systèmes industriels
  - Méthode de classification et mesures principales
  - Mesures détaillées
- De produits certifiés et des produits qualifiés
  - Équipements de contrôle/commande
  - Equipements de cyber-sécurité
- ENISA (Agence de l'Union européenne pour la cybersécurité)
  - Mesures de sécurité recommandées pour les smart grids
  - Certification Européenne de Sécurité pour les équipements (Cybersecurity Act – 2019)

Démarche SSI : amélioration continue

- Sensibilisation des personnels
  - Hygiène informatique, prévention des risques
- Cartographie des installations et analyse de risque
  - Matrice gravité/vraisemblance
- Prévention : défense en profondeur
  - Minimiser l'exposition et l'impact
- Surveillance des installations et détection des incidents
- Traitement des incidents
  - Gestion de crise
- Veille sur les menaces et les vulnérabilités
- Les plans de reprise et de continuité d'activité

Deux mesures cruciales

- Sensibilisation des personnels
- Séparation systèmes industriels / Internet

Les 10 principales menaces dans les systèmes industriels	Tendance depuis 2016
Virus sur clé USB ou disque externe	
Virus propagé par Internet ou Intranet	
Erreur Humaine et Sabotage	
Extranet ou Cloud	
Ingénierie Sociale et Hameçonnage	
(D)Déni de Service	
Equipements de Contrôle Commande connectés à Internet	
Intrusion par Access Distant	
Défaillance Technique et Force Majeure	
Smartphones Compromis en Environnement Professionnel	

Source BSI-CS005E Top 10 Threats and Countermeasures 2019

8/10 principaux vecteurs d'attaque peuvent être facilement évités

Le mot de l'enseignant

- Sensibilisation des élèves ingénieurs non-informaticiens aux risques cyber
- Formations sanctionnées par un label national

- ENSE3 : 1ère école d'ingénieurs non-informaticiens labélisée CyberEdu (2018)
  - Filière Automatique
  - Master Smart-Grids et Buildings (en cours)