DEF

Stratégie d'accompagnement au Renforcement des capacités

Aspects juridiques du renforcement de la cybersécurité des réseaux électriques

SOMMAIRE

LES INTERVENANTS

BIENVENUE !

Henri Maria

- Juriste en droit de l'énergie
- Expert organisation & régulation secteur électrique

César Clause

- Ingénieur Système électrique
- Expert digital

1

Digital Energy Facility

RAPPELS SUR LA DEF ET SES QUATRE COMPOSANTES

Digital Energy FACILITY

RTEi

1 Digitalisation des opérateurs énergétiques
6,7M€

2 Financement de l'innovation
7,2M€

Financé par l'Union européenne et mis en œuvre par l'Agence française de développement (AFD), ce programme soutient la digitalisation et la modernisation du secteur de l'énergie.

3 Création d'une communauté d'acteurs
1,8M€

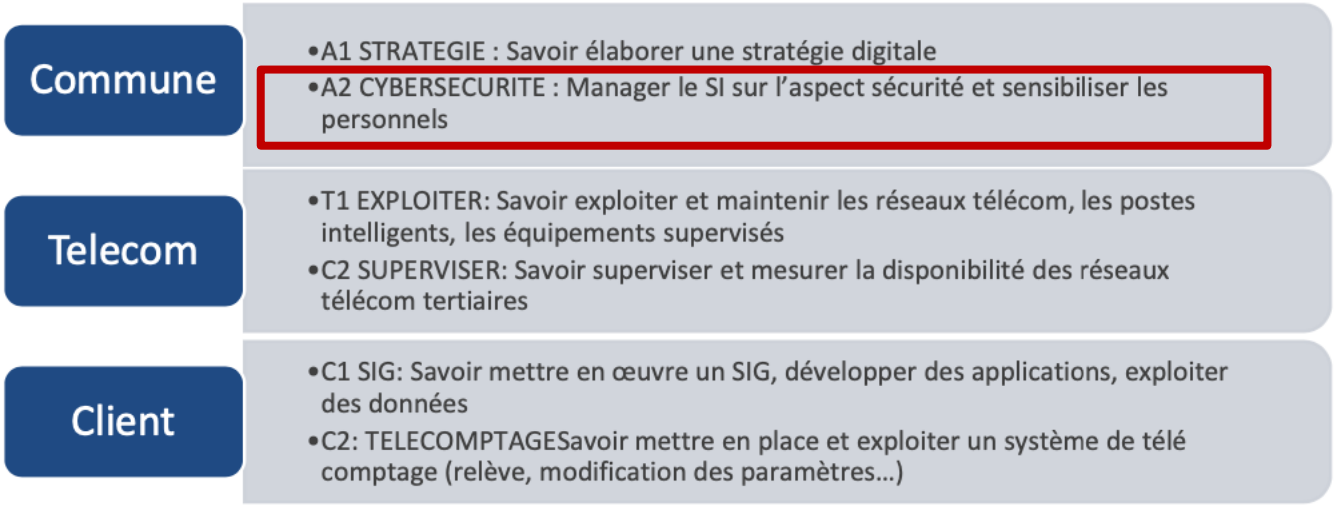
4 Capital amorçage pour des solutions innovantes destinées aux entreprises d'accès à l'énergie
4,8M€ (prêts d'amorçage)

COMPOSANTE 1B DE LA DEF

- **Objectif :** Accompagner le renforcement des capacités des opérateurs
- **Actions financées :** webinaires, ateliers, séminaires, échanges entre pairs, mise en réseau, formations…

LES DOMAINES RETENUS

7 thématiques prioritaires initialement retenues et regroupées en 3 groupes de travail



S1 – Outils collaboratifs pris en compte tout au long du projet

2

Introduction

INTRODUCTION

Propos liminaire

SOMMAIRE

1. DIGITAL ENERGY FACILITY
2. INTRODUCTION À LA CYBERSECURITÉ
3. PANORAMA DES MENACES
4. QUELQUES SPÉCIFICITÉS DU SECTEUR
5. EVALUATION DES VULNÉRABILITÉS
6. CONTREMESURES ET MEILLEURES PRATIQUES
7. CONTEXTE RÉGLEMENTAIRE ET NORMATIF
8. L'EXEMPLE DE RTE

Sommaire du webinaire du 27/06/2023

- Un webinaire **introduisant le sujet de la cybersécurité** a été présenté le 27 juin 2023
- Le présent webinaire est une **présentation complémentaire** → focus sur les **aspects juridiques** de la cybersécurité
- A travers les **exemples français et européens**, montrer l'importance du cadre juridique et institutionnel à mettre en place pour **se protéger des cybermenaces**, et les spécificités dans le domaine des réseaux d'électricité

2.1

Contexte & enjeux

INTRODUCTION

Contexte & enjeux

De nouvelles pratiques destructrices se développent dans le cyberespace :

- Utilisations criminelles d'internet (cybercriminalité), y compris à des fins terroristes,
- Propagation de fausses informations ou manipulations à grande échelle, espionnage à visée politique ou économique,
- Attaques contre les infrastructures critiques (transport, énergie, communication…) à des fins de sabotage, etc.

INTRODUCTION

Contexte & enjeux

- Les risques cyber sont une **menace majeure** : elle est globale (tous les pays), et toutes les personnes (personnes publiques, entreprises, particuliers),

- Les risques cyber peuvent conduire à des **impacts divers potentiellement lourds** : perte financière, risque réputationnel, dommages matériels / corporels, responsabilité civile / pénale, perte de disponibilité du système,

- La sécurité des Système d'Informations vise à protéger la « valeur » d'une entreprise : sécurité des personnes, sécurité des actifs, sécurité de l'information. Elle a une **importance proportionnelle à celle de l'infrastructure ou de l'activité concernée**.

INTRODUCTION

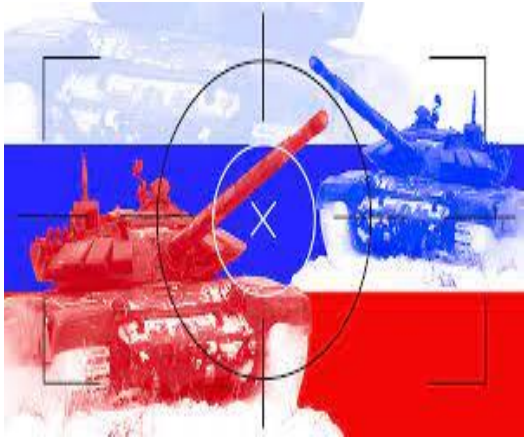
Des impacts potentiellement majeurs pour les Etats

« S'attaquer à nos infrastructures peut entraîner des conséquences sur notre souveraineté, nos libertés fondamentales et la résilience de nos systèmes »

Thierry Trouvé, Directeur général de GRTgaz

INTRODUCTION

L’exemple d’une attaque récente

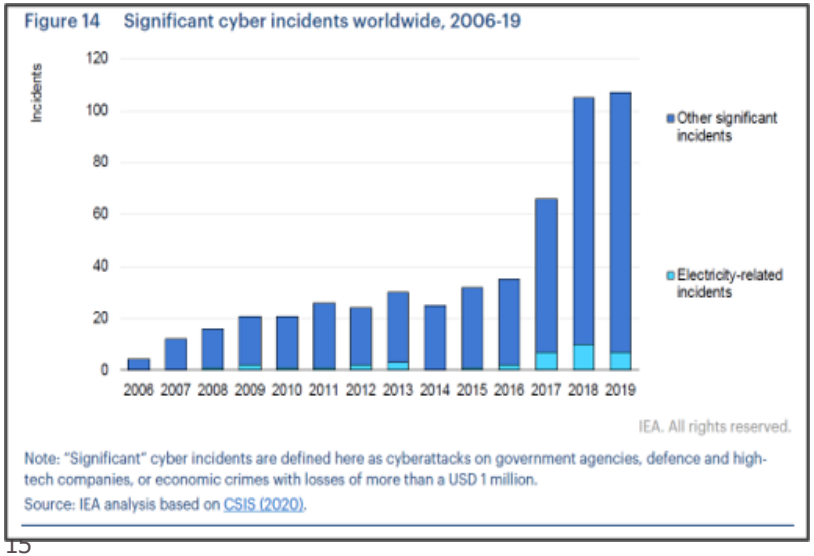


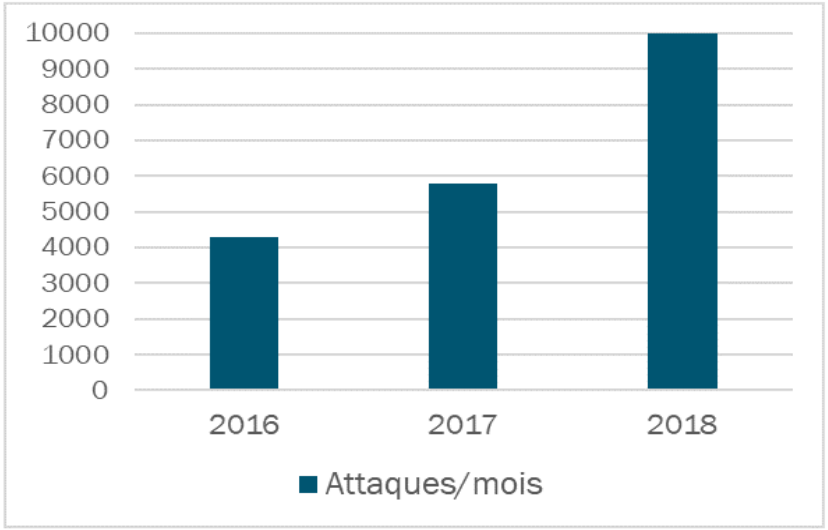
- ***Date:*** 13 avril 2022
- ***Gouvernement ukrainien*** : un piratage du réseau électrique du pays a été évité
- ***Modalités de la cyberattaque :*** Les hackers russes ont pris pour cible l’une des principales entreprises énergétiques du pays, et tenté de désactiver des postes.
- ***En cas de succès***, plus de deux millions de personnes auraient été plongées dans le noir.

INTRODUCTION

Menaces croissantes dans le secteur de l'énergie

Pour les réseaux d'électricité, la menace de cyberattaque est importante et croissante, et les acteurs de la menace deviennent de plus en plus sophistiqués dans la mise en œuvre des attaques.





Attaques "cyber" par mois constatées par RTE (Source : RTE)

INTRODUCTION

Menaces croissantes dans le secteur de l'énergie

L'ENISA a identifié certaines tendances pour 2030, qui concernent en particulier le secteur de l'énergie :

- EC5 Increasing reliance on automation and connectivity of sustainable energy production
- EC7 Increasing danger of resource bottlenecks of critical raw materials for strategic technologies and sectors in the EU
- EN1 The increased usage of new technologies in remote maintenance
- EN7 The emerging use of distributed and alternative energy resources
- EN8 The increasing energy consumption of digital infrastructure

Source : https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

2.2

Une réponse par le droit

INTRODUCTION

Définition juridique

La **cybersécurité** est un écosystème établi pour contrer la menace numérique

En droit européen, la cybersécurité recouvre :

> ***« les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces »***

Article 2 du Règlement (UE) 2019/881 du 17 avril 2019
(« The EU Cybersecurity Act »)

INTRODUCTION

Définition juridique

La **cybermenace :**

« toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »

Article 2 du Règlement (UE) 2019/881 du 17 avril 2019
(« The EU Cybersecurity Act »)

INTRODUCTION

Un droit de la cybersécurité ?

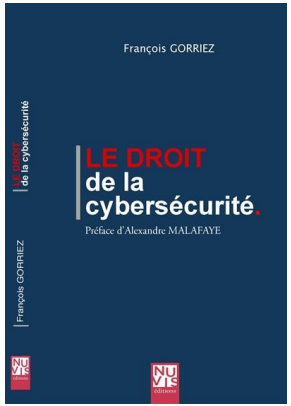
- La cybersécurité est un domaine relativement **récent du droit**
- Son importance a **considérablement augmenté** au cours des dernières décennies avec l'essor d'Internet et des technologies de l'information.
- Ce droit va encore évoluer pour faire face aux **défis croissants** de la sécurité en ligne.
- Un **droit spécifique** au secteur de la cybersécurité de l'énergie se développe.

INTRODUCTION

Un droit de la cybersécurité ?

- La cybersécurité est un sujet de préoccupation qui a émergé assez tôt en France

- Un cadre juridique et institutionnel a été mis en place, ainsi que de la recherche et de la doctrine sur le sujet



INTRODUCTION

Comment le droit s'adapte pour faire face aux menaces spécifiques grandissantes en matière de cybersécurité du secteur de l'énergie et plus particulièrement des réseaux électriques?

France

Union européenne

Monde

3

Un cadre juridique français précurseur

CADRE JURIDIQUE FRANÇAIS

Les activités d'importance vitale

- **LOI n° 2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense**
- **Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale**

Objectif : Assurer la continuité des activités essentielles à la défense et au fonctionnement de la Nation

Comment : Identifier les secteurs d'**activités d'importance vitale** (SAIV), associer à chaque SAIV un ministre coordinateur, charger ce ministre de lister les **opérateurs d'importance vitale** (OIV), imposer aux OIV des obligations spécifiques.

CADRE JURIDIQUE FRANÇAIS

Les activités d'importance vitale

Un secteur d'activités d'importance vitale (SAIV), tel que défini par l'article R. 1332-2 du Code de la Défense, est constitué d'activités :

- Concourant à un même objectif, la production et distribution de biens ou de services indispensables :
  - à la satisfaction des besoins essentiels pour la vie des populations,
  - à l'exercice de l'autorité de l'État,
  - au fonctionnement de l'économie,
  - au maintien du potentiel de défense,
  - ou à la sécurité de la Nation.

- Ou présentant un danger grave pour la population.

CADRE JURIDIQUE FRANÇAIS

Les 12 SAIV et leurs ministres coordonnateurs

Dominante	Secteur d'activités d'importance vitale	Ministère coordonnateur
Régalienne	Activités civiles de l'État	Ministère de l'Intérieur
	Activités militaires de l'État	Ministère de la Défense
	Activités judiciaires	Ministère de la Justice
Humaine	Santé	Ministère chargé de la Santé
	Gestion de l'eau	Ministère chargé de l'Écologie
	Alimentation	Ministère chargé de l'Agriculture
Économique	Énergie	Ministère chargé de l'Énergie
	Finances	Ministère chargé de l'Économie et des Finances
	Transports	Ministère chargé des Transports
Technologique	Communications électroniques, audiovisuel et information	Ministère chargé des Communications électroniques
	Industrie	Ministère chargé de l'Industrie
	Espace et recherche	Ministère chargé de la Recherche

CADRE JURIDIQUE FRANÇAIS

Les opérateurs d'importance vitale

Un opérateur d'importance vitale, tel que défini par l'article R. 1332-1 du Code de la Défense, est une organisation qui :

- Exerce des activités comprises dans un **secteur d'activités d'importance vitale**

- Gère ou utilise au titre de cette activité un ou des **établissements ou ouvrages**, **une ou des installations** dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :
  - d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
  - ou de mettre gravement en cause la santé ou la vie de la population.

CADRE JURIDIQUE FRANÇAIS

Un cadre applicable à RTE

RTE est nommé « opérateur d'importance vitale » en 2008

- Obligation de désigner un délégué pour la défense et la sécurité (interlocuteur privilégié de l'autorité administrative),
- Obligation de former les responsables et leurs directeurs de la sécurité tant au niveau central qu'au niveau local
- Obligation de créer, après une analyse de risques, un **« Plan de Sécurité Opérateur » (PSO)** qui expose la politique de RTE pour faire face aux menaces majeures identifiées par les Services de l'Etat (attentats à l'explosif, sabotages, intrusions, cyber terrorisme…)
- **50 points d'importance vitale (PIV)** ont été identifiés pour lesquels ont été rédigés des **Plans Particuliers de Protection (PPP).**

CADRE JURIDIQUE FRANÇAIS

Focus sur les PIV

- Les points d'importance vitale sont des établissements, ouvrages ou installations qui fournissent les **services et les biens indispensables à la vie de la Nation**.

- Les opérateurs eux-mêmes proposent la liste de leurs points d'importance vitale

- Rédaction de **Plans particuliers de protection (PPP)** pour chacun des points d'importance vitale identifiés.

La France est le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ses infrastructures critiques.

CADRE JURIDIQUE FRANÇAIS

Acteurs et responsabilités

Premier ministre / SGDSN

Le secrétariat général de la défense et de la sécurité nationale assure, par délégation du Premier ministre, le pilotage et la coordination interministérielle du dispositif. Il fixe le cadre de la politique SAIV, notamment en ce qui concerne la méthode et la doctrine.

Il approuve les directives nationales de sécurité (DNS). Il fixe par ailleurs des règles de cybersécurité devant être appliquées par les OIV.

Ministres coordonnateurs

Les ministères coordonnateurs sont chargés de rédiger les DNS de chaque secteur (et sous-secteur) d'activités d'importance vitale en indiquant les enjeux, les vulnérabilités, les menaces qui doivent être prises en compte et en définissant les objectifs de sécurité du secteur.

Les ministères coordonnateurs sont également les points de contacts privilégiés des opérateurs.

Ministère de l'intérieur

Le ministère de l'intérieur est en charge de l'animation territoriale du dispositif pour soutenir l'action des préfets de zone et des préfets de département.

Préfet de zone de défense et de sécurité

Le préfet de zone est l'acteur territorial en charge de la coordination du dispositif SAIV.

Il a un rôle d'animation, d'appui aux préfectures et de relais d'information entre l'échelon central et les échelons départementaux.

Il coordonne également les inspections des PIV situés dans sa zone de compétence.

Préfet de département

Le préfet de département approuve, pour chaque PIV, le plan particulier de protection (PPP) rédigé par l'opérateur.

Il élabore également un plan de protection externe (PPE) comportant les mesures de vigilance et d'intervention prévues en cas de menace ou d'attentat visant ce point d'importance vitale.

Opérateur d'importance vitale

Une fois désignés, les opérateurs doivent répondre à plusieurs types d'obligations : la désignation d'un délégué pour la défense et la sécurité (interlocuteur privilégié de l'autorité administrative), la rédaction d'un plan de sécurité d'opérateur (PSO) qui décrit l'organisation et la politique de sécurité de l'opérateur, la rédaction de plans particuliers de protection (PPP) pour chacun des points d'importance vitale identifiés.

CADRE JURIDIQUE FRANÇAIS

Le Livre Blanc de 2013

- Les cyberattaques : **menace majeure**, à forte probabilité et à fort impact potentiel.
- Les intrusions visant l'État, les opérateurs d'importance vitale, ainsi que les grandes entreprises nationales ou stratégiques du pays **sont quotidiennes**.
- Attaque de **grande envergure** susceptible de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques, et de faire de nombreuses victimes. Elle pourrait donc constituer un véritable **acte de guerre**.

Un renforcement de la sécurité des systèmes d'information est nécessaire. Niveau européen : nécessité de renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques.

CADRE JURIDIQUE FRANÇAIS

La prise en compte des systèmes d'information

Création de la notion de « système d'information d'importance vitale » (SIIV) par la LPM 2014 – 2019 (art. 22)

- Impose aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent
- SIIV : « *systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* »
- Le système électrique est classé « infrastructure d'importance vitale » pour le pays eu égard au rôle crucial de la disponibilité d'électricité et comporte des systèmes d'information d'importance vitale.

CADRE JURIDIQUE FRANÇAIS

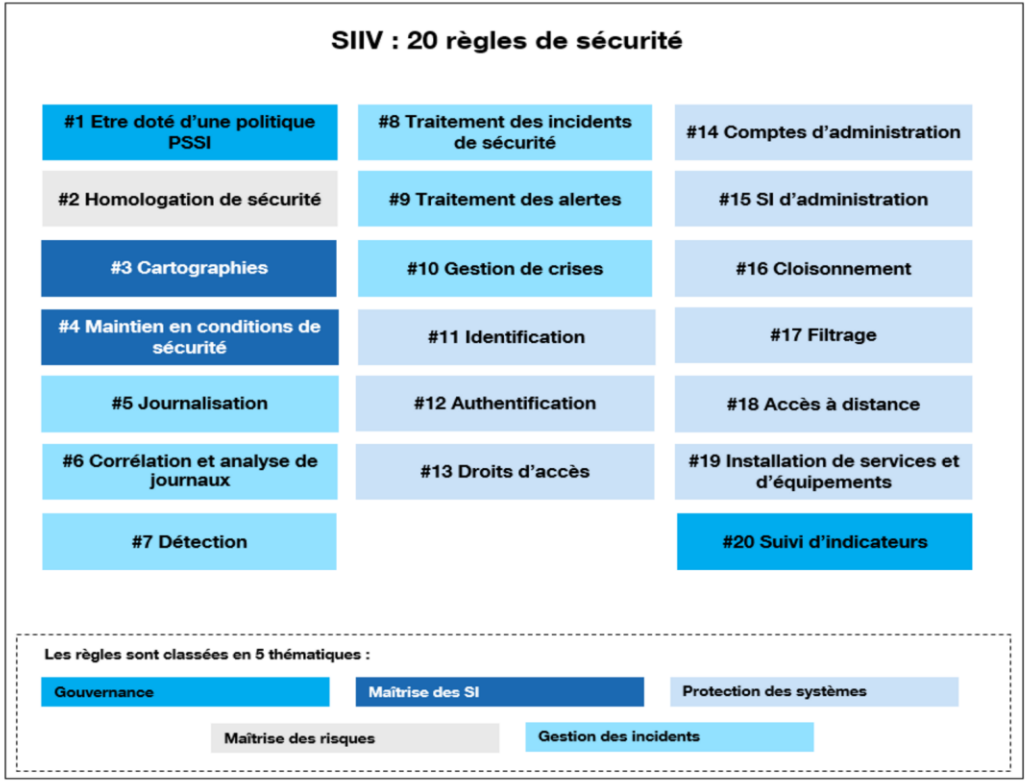
La prise en compte des systèmes d'information

RTE (OIV) dispose de nombreux SIIV. De ce fait, l'entreprise doit respecter les obligations associées :

- Fournir à l'ANSSI la liste de ses systèmes d'information d'importance vitale (SIIV)
- Mettre en place une politique de sécurité des systèmes d'information (PSSI) décrivant les moyens mis en œuvre afin de protéger les SIIV, comprenant une procédure d'homologation du système d'information tous les 3 ans.
- Cartographier les systèmes d'information existants
- Notifier à l'ANSSI tous les incidents de cybersécurité (créer une accidentologie pour mieux anticiper)

CADRE JURIDIQUE FRANÇAIS

Les règles de sécurité des SIIV



CADRE JURIDIQUE FRANÇAIS

L'ANSSI

- Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Créée en 2009 (décret n° 2009-834 du 7 juillet 2009)
- Héritière des organismes de protection des informations de l'Etat
- Budget : 136 millions d'euros
- Environ 600 salariés

L'ANSSI est chargée de la prévention et de la réaction aux incidents informatiques visant les institutions sensibles. Elle participe à la rédaction des normes. Elle organise par ailleurs des exercices de gestion de crises au niveau national.

CADRE JURIDIQUE FRANÇAIS

L'ANSSI

Missions en lien avec les OIV

- L'ANSSI est en charge de piloter la partie cyber du dispositif SAIV et accompagne les OIV dans la mise en œuvre des nouvelles mesures.
- Au sein de l'agence, des coordinateurs sectoriels sont les interlocuteurs privilégiés des administrations et des OIV sur les questions de sécurité et défense de leurs systèmes d'information.
- L'ANSSI peut, au nom du Premier ministre, imposer aux entreprises du secteur de l'énergie de mesures de sécurité et des contrôles de leurs systèmes d'information (SI) les plus critiques.
- Recueille et analyse les déclarations des incidents constatés par les OIV sur leurs systèmes d'information.

CADRE JURIDIQUE FRANÇAIS

Conclusion

3 notions clés
du cadre juridique cybersécurité en France :

Anticipation **Planification** **Concertation**

4

Renforcer la coopération européenne

RENFORCER LA COOPÉRATION EUROPÉENNE

Introduction

L'UE œuvre sur différents fronts pour promouvoir la **cyberrésilience**, **combattre la cybercriminalité** et **stimuler la cyberdiplomatie** ainsi que la **cyberdéfense**.

L'Union européenne a défini une stratégie en matière de cybersécurité afin de renforcer la capacité de l'Europe à lutter contre les cyberattaques et sa résilience face à celles-ci.

- Résilience, souveraineté technique et leadership;
- Capacités opérationnelles de prévention, de dissuasion et de réaction;
- Coopération visant à faire progresser la mondialisation et l'ouverture du cyberespace.

4.1

Cadre général de la cybersécurité européenne

CADRE GÉNÉRAL

L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) créée en 2004 est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe.

- **Conseiller et assister** la Commission et les États membres en matière de sécurité de l'information
- Recueillir et analyser les données relatives aux **incidents**
- Promouvoir des **méthodes d'évaluation et de gestion des risques**
- Favoriser l'**échange de bonnes pratiques** en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées.
- Suivre l'**élaboration des normes pour les produits et services** en matière de sécurité des réseaux et de l'information.

CADRE GÉNÉRAL

Les Directives européennes « NIS » ou « SRI »

La Directive NIS de juin 2016, révisée en 2022, est le texte phare en matière de cybersécurité dans l'Union européenne

- La Directive (UE) 2016/1148 sur la sécurité des réseaux et des systèmes d'information (Directive NIS) a pour objectif d'atteindre **un niveau commun élevé de sécurité des réseaux et des systèmes d'informations** dans toute l'Union Européenne.

- La Directive NIS 2 vient combler les lacunes de la précédente directive NIS pour l'adapter aux besoins actuels.

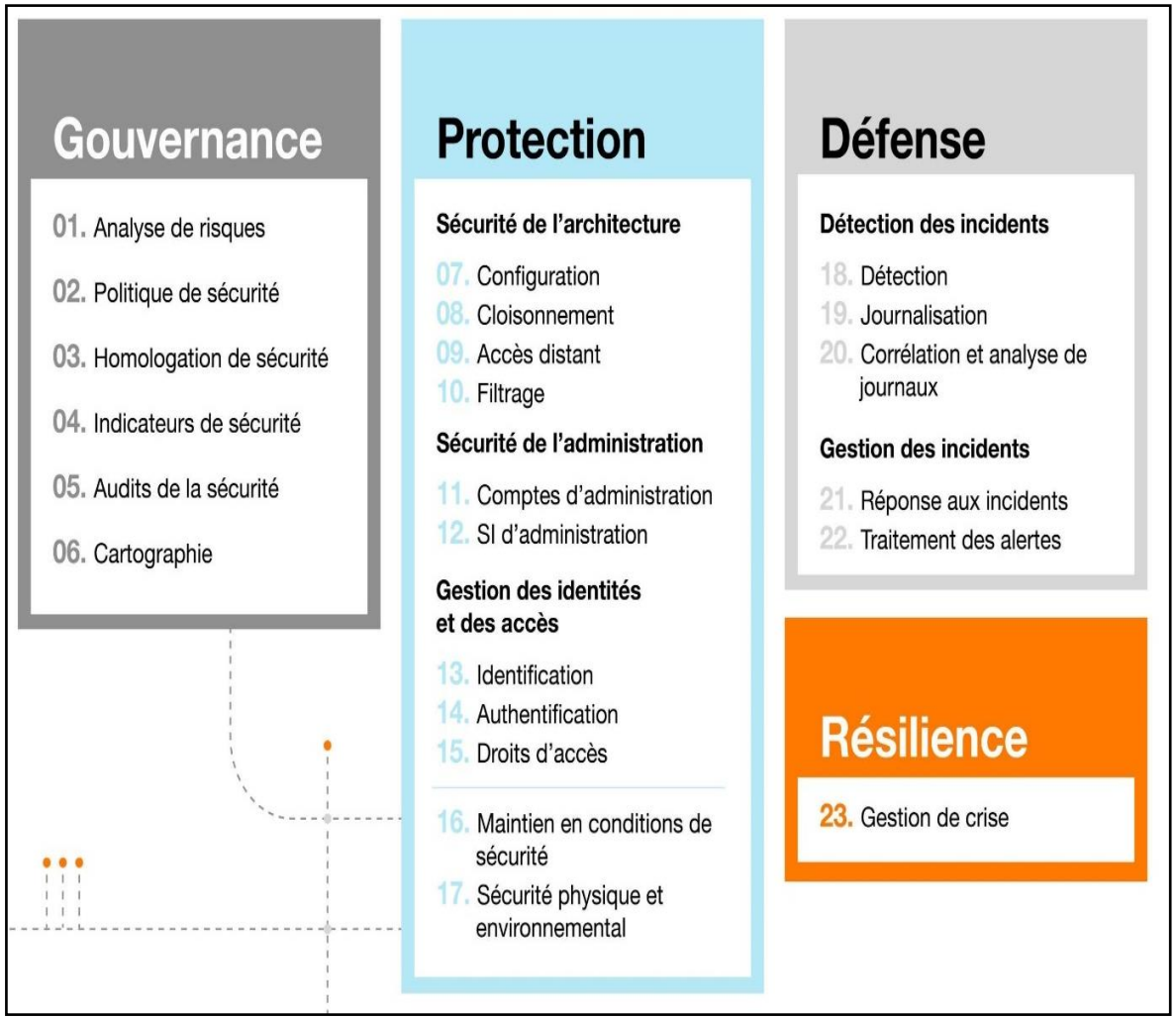
CADRE GÉNÉRAL

Les Directives européennes « NIS » ou « SRI »

La directive européenne NIS répond à 4 enjeux majeurs :

- La création d'un cadre de coopération européen ;
- La mise en place d'un cadre de gouvernance pour chaque État membre (avec notamment la définition d'une stratégie nationale de cybersécurité pour chaque Etat membre, la nomination d'une autorité nationale pour préciser les règles cyber)
- Le renforcement de la cybersécurité des opérateurs de service essentiel (OSE),
- Le renforcement la cybersécurité des fournisseurs de service numérique (FSN).

CADRE GÉNÉRAL



CADRE GÉNÉRAL

Conclusion

- La directive NIS comprend plusieurs dispositions applicables au secteur de l'énergie.

- Cependant, il a été jugé nécessaire de **compléter** ce texte général par des **textes spécifiques au secteur de l'énergie**

  → En 2019, la Commission européenne a publié une **recommandation officielle sur la cybersécurité dans le secteur de l'énergie**, qui a fourni des orientations non exhaustives aux États membres et aux parties prenantes concernées, en particulier les opérateurs de réseaux.

4.2

Code de réseau européen cybersécurité (NCCS)

LE CODE EUROPÉEN CYBERSÉCURITÉ

Introduction

- Les codes de réseau et les lignes directrices sont des règles communes européennes portant sur des questions transfrontalières de gestion du système électrique et des interconnexions entre Etats Membres.

- Les codes de réseau européens définissent, chacun dans leur champ d'application, des exigences techniques ou opérationnelles applicables aux différentes catégories d'acteurs.

- Le Règlement (UE) 2019/943 du Parlement européen et du Conseil sur le marché intérieur de l'électricité prévoit la création d'un code de réseau cybersécurité des flux transfrontaliers d'électricité

LE CODE EUROPÉEN CYBERSÉCURITÉ

Objet

- Le code de réseau sur la cybersécurité vise à établir une norme européenne pour la **cybersécurité des flux électriques transfrontaliers**.

- Il comprend des règles relatives à l'évaluation des cyber-risques, aux exigences minimales communes, à la certification des produits et services en matière de cybersécurité, à la surveillance, à l'établissement de rapports et à la gestion de crise.

- Ce code de réseau fournit **une définition claire des rôles et des responsabilités** des différentes parties prenantes pour chaque activité.

LE CODE EUROPÉEN CYBERSÉCURITÉ

Processus d'élaboration

LE CODE EUROPÉEN CYBERSÉCURITÉ

Sommaire

Le code de réseau contient les parties suivantes :

- Dispositions générales (**Titre 1**)
- De la gouvernance (**Titre 2**)
- De l'évaluation du risque cyber au niveau européen et régional (**Titre 3**)
- De la mise en place d'un cadre commun de cybersécurité (**Titre 4**)
- Gestion du risque au niveau de l'Etat membre (**Titre 5**)
- Gestion du risque au niveau des entités (**Titre 6**)
- Exigences harmonisées en matières de marchés (**Titre 7**)
- Flux d'informations essentielles, incidents de cybersécurité, gestion de crise (**Titre 8**)
- Exercice (**Titre 9**)
- Protection des informations (**Titre 10**)
- Dispositions finales (**Titre 11**)

LE CODE EUROPÉEN CYBERSÉCURITÉ

Des documents complémentaires à produire

Toutes les règles ne sont fixées dans le code. Les « Terms, conditions and méthodologies » (TCMs), seront développés ultérieurement conjointement par l'ENTSO-E, l'EU DSO, les acteurs de marché… Le NCCS prévoit la rédaction des TCMs suivantes :

- Méthodologie d'évaluation des risques de cybersécurité,
- Plans régionaux de traitement des risques de cybersécurité,
- Rapport transfrontalier d'évaluation des risques de cybersécurité,
- Cadre commun de cybersécurité de l'électricité,
- Exigences harmonisées de cybersécurité en matière d'approvisionnement,
- Méthodologie de classification des incidents de cybersécurité.

5

Punir les cybercrimes : sanctions et contentieux

PUNIR LES CYBERCRIMES

Introduction

- La règle de droit a un **caractère obligatoire**, elle s'impose à toute personne, qui a le devoir de la respecter.

- Un individu qui enfreint une règle de droit encourt une **sanction**.

- Les particularités des cybercrimes rendent toutefois très complexe l'application d'un système de sanction efficient car ils :

  - **Se jouent des frontières** et des distances ;
  - **Sont difficilement attribuables** : il est très difficile d'identifier formellement le véritable attaquant (furtivité)
  - Peuvent provenir d'acteurs étatiques comme non-étatiques

PUNIR LES CYBERCRIMES

La responsabilité pénale

Un cybercrime est une « infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ».

Délit

Des atteintes aux systèmes de traitement automatisé de données

Art. 323-1 à 327-7 du code pénal

VS.

Crime

Le sabotage

Art. 411-9 du code pénal

PUNIR LES CYBERCRIMES

L'attaque d'EDF par les « anonymous »

Les faits

- Le 2 juin 2011
- Introduction d'un groupe d'anonymous sans autorisation sur le serveur hébergeant les sites internet d'EDF afin de lancer une attaque de déni de service distribué (DDoS)
- Bloquage du site internet d'EDF, qui est opérateur d'importance vitale (OIV)
- ANSSI et Direction centrale du renseignement intérieur (DCRI) ont été saisis.
- L'un des attaquants a été repéré et identifié par son adresse IP et sa chaine YouTube

PUNIR LES CYBERCRIMES

L'attaque d'EDF par les « anonymous »

La procédure

- Le prévenu a reconnu les faits
- Décision de la chambre correctionnelle du TGI de Paris du 28 septembre 2016
- a été condamné à **6 mois de prison avec sursis et 29.000€ de dommages et intérêts**
  - pour accès et maintien frauduleux dans un système d'information (STAD),
  - entrave à un STAD, et
  - participation à une entente en vue de la préparation à une attaque contre un STAD

- Dommages-intérêts d'EDF :
  - 24 000 euros au titre du préjudice matériel,
  - 5 000 euros au titre du préjudice d'image et commercial

PUNIR LES CYBERCRIMES

Perte de téléconduite chez RTE

Les faits

- 4 salariés de RTE
- Revendication de hausses de salaires
- Entre le 15 juin et le 22 juillet 2022
- Participation à 17 opérations consistant à rompre la communication entre le réseau local dans le Nord et le réseau au niveau national.
- Arrêt de la téléconduite de 25 postes électriques
- Dépôt de plainte de RTE contre X le 26 juillet 2022
- La cellule cybercriminalité de la Direction générale de la sécurité intérieure (DGSI) est saisie

Pour plus d'informations : https://www.rte-france.com/actualites/rte-condamne-actes-malveillance-commis-sur-systeme-electrique-juin-dernier-hauts-france

PUNIR LES CYBERCRIMES

Perte de téléconduite chez RTE

La procédure

- Le 5 octobre 2023 : les salariés sont mis en garde à vue. Motifs : "entrave au fonctionnement d'un système de traitement automatisé de données au préjudice de RTE", « sabotage », «introduction et modification frauduleuse des données d'un système de traitement automatisé en bande organisée »

- Reconnus coupables que du simple délit d'« *entrave au fonctionnement d'un système de traitement informatisé de données* » et condamnés à des peines d'amendes de 5 000 à 10 000 euros.

- Le tribunal de Paris a en revanche écarté les accusations de sabotage et de modification frauduleuse d'un STAD. Il a annulé des auditions menées au début du mois d'octobre et des retranscriptions d'écoutes téléphoniques

- Le parquet de Paris a fait appel de la condamnation

PUNIR LES CYBERCRIMES

Conclusions

- Le système de sanctions juridiques ne peut être complètement efficace compte tenu de la **nature des menaces et de leurs auteurs**
- La répression des cyber attaquants n'a aujourd'hui que **très peu effet dissuasif.**
- Cela ne signifie pas pour autant que le droit est inefficace
- Le droit permet de mettre en place des actions pour **anticiper et minimiser les cybermenaces** et **se technicise** : les règles techniques obligatoires se multiplient.
- Se pose la question de l'**assurance** du risque cyber.

6

Se protéger des cybermenaces : l’assurance cyber

SE PROTÉGER DES CYBERMENACES

Assurer le risque cyber ?

- C’est un enjeu pour les entreprises même si elles n’en ont pas toujours conscience encore aujourd’hui.
- Manque de données pour faire des statistiques et donc créer des produits d’assurance. Risque qui prend différentes formes et mute en permanence.
- Des produits d’assurance sont de plus en plus présents sur le marché
- La Loi d'orientation et de programmation du ministère de l'Intérieur d’avril 2023 (LOPMI) prévoit que toute personne victime d'une cyberattaque doit désormais déposer plainte dans un délai de 72 heures pour prétendre à une indemnisation au titre de son contrat d'assurance.

Pour une société d’électricité ou gestionnaire de réseau, le risque de la coupure généralisée ne pourra a priori pas être assuré en raison de l’ampleur potentiel de ses conséquences

7

Evolution des standards internationaux

7.1

L’évolution des pratiques

EVOLUTION DES PRATIQUES

Des lois cybersécurité adoptées partout dans le monde

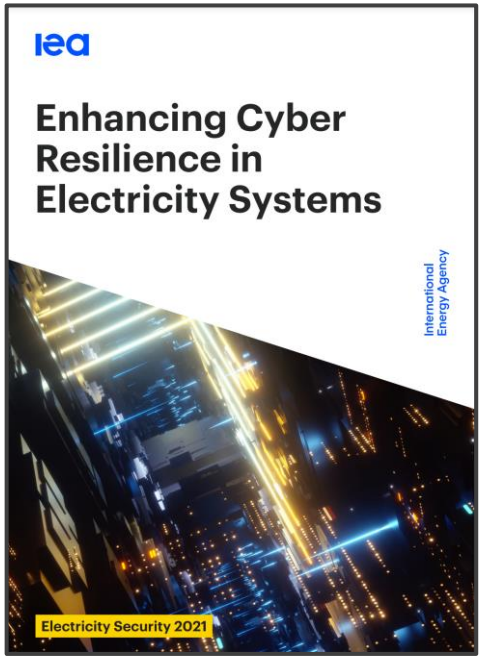
La cybersécurité est un enjeu grandissant partout dans le monde. Des lois dédiées à la cyber sont adoptees partout dans le monde :

- **Union européenne :** Directive NIS (2022)
- **USA :** Cybersecurity Act (2022)
- **Autres pays :** Singapour (Cybersecurity Act 2018), Australie (Security of Critical Infrastructure Act 2021)…

Ces lois générales ne traitent pas des spécificités du secteur électrique.

EVOLUTION DES PRATIQUES

Analyses de l'AIE



- ***Date:*** avril 2022
- ***Agence internationale de l'énergie (IEA)***
- Ce rapport donne des conseils aux décideurs politiques, aux sociétés d'électricité et aux autres parties prenantes sur la manière dont les politiques et les actions pourraient améliorer la cyber-résilience des systèmes électriques.

EVOLUTION DES STANDARDS INTERNATIONAUX

Des actions fortes sont nécessaires pour renforcer la résilience

- S'il n'est pas possible de prévenir totalement les cyberattaques, les réseaux électriques doivent **être conçus pour être plus cyber résilients**.
- **Les décideurs politiques, les régulateurs, les opérateurs de systèmes et les entreprises de la chaîne de valeur de l'électricité** ont tous un rôle important à jouer dans le renforcement de la cyber-résilience du système.
- L'amélioration de la cyber-résilience est un **processus continu**, et la **responsabilité collective de toutes les parties prenantes de la chaîne de valeur de l'électricité**.

EVOLUTION DES STANDARDS INTERNATIONAUX

Les lois de cybersécurité générales sont insuffisantes pour traiter la complexité de la cybersécurité. Des textes spécifiques sont nécessaires pour les completer.

- **Textes réglementaires sectoriels**
- **Normes techniques internationales (ISO / IEC)**
- **Codes de reseau**
  - Le Code de réseau européen sur la cybersécurité (NCCS)
  - **Les codes de réseau nationaux** :
    - The Oman Grid Code Version 3.0 (2020);
    - The Kenya electricity Grid Code (2021);
    - The Indian Grid Code (2023)
    - …

.2

Partage d’expérience : le code de réseau de la Malaisie

PARTAGE D'EXPÉRIENCE

Cybersecurity Code (Malaisie)

- **Aucune disposition traitant de la cybersécurité dans le code de réseau actuel (GCPM 2020)**
- **L'importance du sujet cyber a été identifié par le client (GSO) et confirmé par un benchmark international fait par RTEi**
- **RTEi a formulé 14 recommandations pour intégrer la cyber dans le code de réseau**

- RTEi a rédigé, en partant de réseau, un nouveau code, traitant de la cybersécurité
- Le contenu du code a été défini en prenant en compte les meilleures pratiques actuelles en matière de cybersécurité

Avec le nouveau code, la cybersécurité deviant un theme central du code de reseau de la Malaisie. Les utilisateurs ont de nouvelles obligations à respecter. Le code apporte un cadre institutionnel pour des échange sur le theme de la cybersécurité entre les acteurs.

PARTAGE D'EXPÉRIENCE

Les principaux thèmes du Cybersecurity Code (Malaisie)

- Gouvernance de la cybersécurité
- Identification des cybermenaces
- Détection et traitement des cyberincidents
- Formations et sensibilisations à la cybersécurité
- Exigences techniques de sécurité
- Obligations concernant les achats
- Audits cybersécurité

8

Conclusions

CONCLUSIONS

Sur le droit de la cybersécurité

- Le droit de la cybersécurité est un **droit en pleine expansion**
- Le droit de la cybersécurité est essentiellement un droit de l'**organisation de la protection** envers les cybermenaces (prévention et anticipation des crises)
- Le droit de la cybersécurité touche **de plus en plus d'acteurs**
- L'enjeu va au-delà de la protection des entreprises et des personnes : intérêt majeur de la **protection des nations**
- Un cadre performant de cybersécurité est un argument **d'attractivité économique**. Le cadre juridique participe de cette démarche.

CONCLUSIONS

Sur les sociétés d'électricité et la cyber

- Les sociétés d'électricité sont pleinement concernées par l'enjeu cybersécurité
- Elles doivent être conformes au droit édicté au niveau national mais aussi régional s'il existe.
- L'application de **textes spécifiques au secteur de l'électricité** et complémentaires (normes internationales, codes de réseau cyber…) est une pratique en expansion.
- La **coordination entre les acteurs** est un enjeu grandissant.
- Dans tous les cas, la société doit **anticiper le risque cyber.** Passer par des principes et règles écrites est une bonne pratique.

CONCLUSIONS

Un écueil à éviter

- Les décalages importants qui peuvent se former entre les règles de cybersécurité, les instruments juridiques, et les capacités opérationnelles des acteurs (Etats comme sociétés).

→ Avoir des règles **adaptées et concertées**
→ Mettre en place des **processus de « compliance »**

MERCI POUR VOTRE ATTENTION

INTERVENANTS :

cesar.clause@rte-international.com

henri.maria@rte-international.com