THÈME DU WEBINAIRE

Cybersécurité : quels outils juridiques pour protéger les infrastructures électriques ? Focus sur les codes de réseau.

Henri Maria est avocat au barreau de Paris, spécialisé en droit de l'énergie.

Il accompagne divers acteurs institutionnels et privés dans la mise en œuvre de projets de réformes, la rédaction de cadres normatifs sectoriels, et l'élaboration de stratégies juridiques adaptées aux défis énergétiques contemporains.

Son parcours lui a notamment permis d'explorer des thématiques innovantes, comme la cybersécurité des systèmes électriques. Il a notamment contribué à l'élaboration de codes de réseau et à l'étude des règles applicables aux infrastructures critiques.

*Le présent webinaire est basé sur le rapport intitulé « **Les codes de réseau : un outil au service du renforcement de la cybersécurité du secteur électrique ?** » et produit dans le cadre de l'Energy Facility de l'AFD.*

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 »)

Définitions de cybersécurité : état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.

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, ancien Directeur général de GRTgaz

La cybersécurité, qui concerne la sécurité et la souveraineté numérique de chaque État, présente des enjeux économiques, stratégiques et politiques qui vont donc au-delà de la seule Sécurité des systèmes d'information.

INTRODUCTION

Le 9 décembre 2024…

Key electricity distributor in Romania warns of ‘cyber attack in progress’

One of Romania's most important energy services companies has announced it is currently tackling an ongoing cyberattack.

Electrica Group, which is listed on the Bucharest and London stock exchanges and provides energy to more than 3.8 million customers in Romania, published a note to investors on Monday warning of a “cyber attack in progress.”

“Teams of specialists are working closely with the national cybersecurity authorities to manage and resolve the incident, aiming to address the situation as quickly as possible, identify the source of the attack, and limit its impact,” the company’s chief executive Alexandru Chirita stated.

Définitions de cybersécurité : état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.

Source : https://therecord.media/electric-distributor-cyberattack-romania

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.

SOMMAIRE

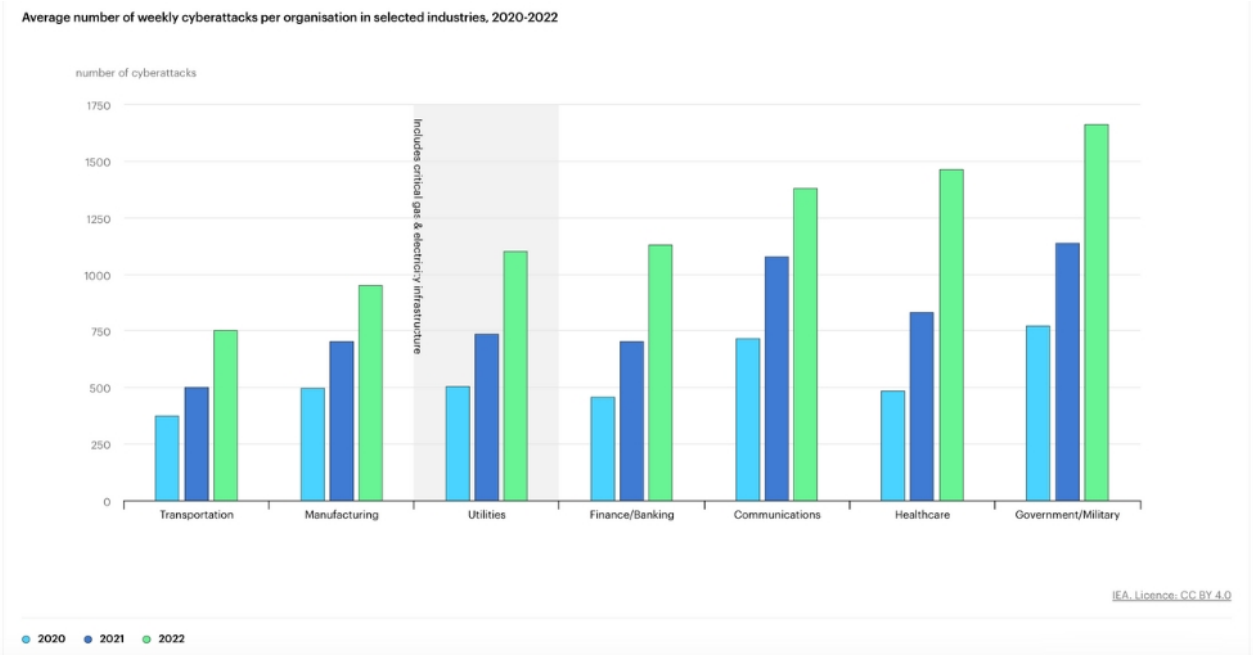
1

Cybersécurité du secteur électrique

CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une recrudescence des cyberrisques

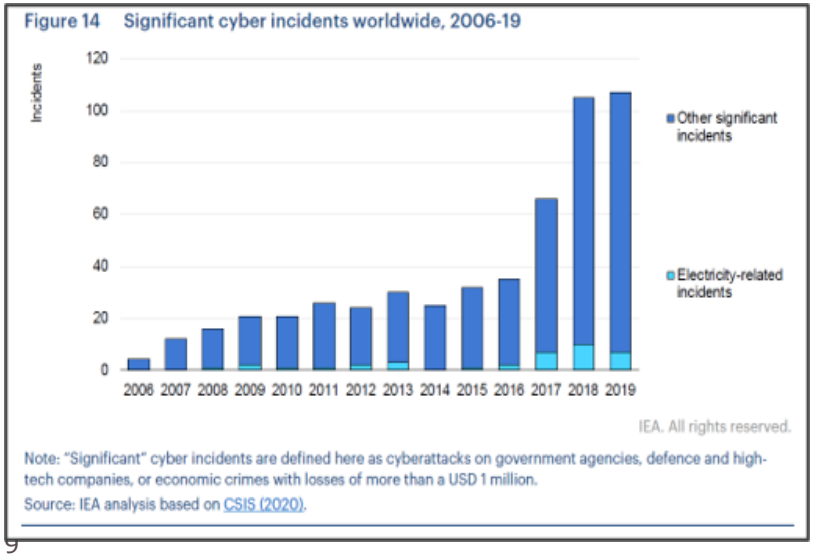
Entre 2020 et 2022, le nombre moyen de cyberattaques contre les services publics dans le monde a plus que doublé.

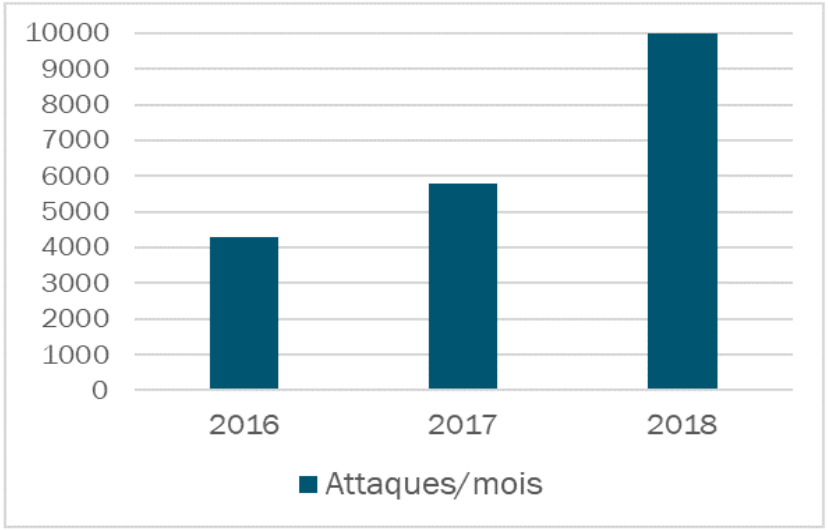


CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une recrudescence des cyberrisques

Pour le secteur électrique, la menace de cyberattaque est aussi croissante et les attaques sont de plus en plus sophistiquées.





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

CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une recrudescence des cyberrisques

La cyberattaque du 23 décembre 2015 sur le réseau électrique ukrainien est la première à avoir causé une interruption massive de fourniture d'électricité.

- Les pirates ont utilisé un malware appelé *BlackEnergy* pour **accéder aux systèmes de gestion du réseau**. Ils ont également perturbé les communications internes des opérateurs, compliquant la reprise en main du système.
- L'attaque a permis l'**accès à distance aux systèmes SCADA**, permettant aux cybercriminels de couper des postes électriques Haute tension/Moyenne tension.
- **225 000 clients** de plusieurs distributeurs d'électricité ukrainiens ont été touchés par des coupures de courant qui ont duré environ six heures.

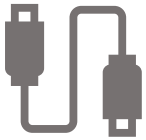
CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une recrudescence des cyberrisques

La numérisation du système électrique a de nombreux bénéfices…

…mais aussi des inconvénients

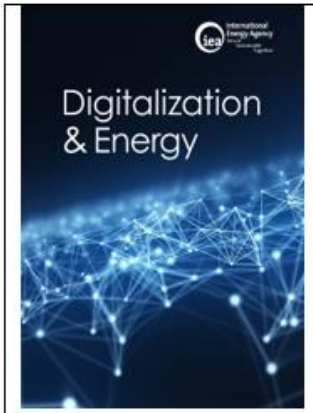
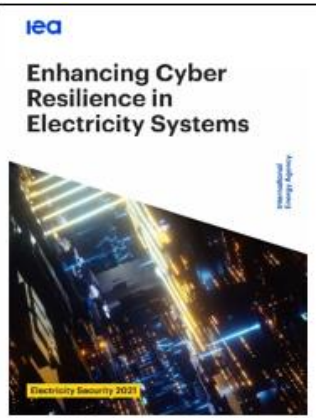
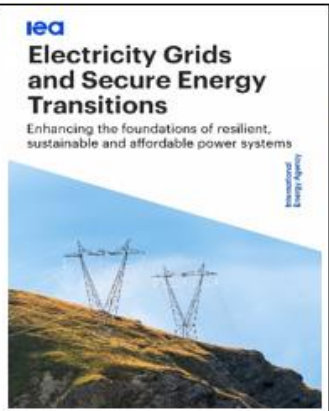
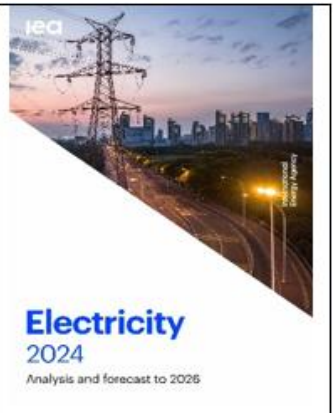
- Les technologies numériques présentent de nombreux atouts pour améliorer la gestion du système électrique dans son ensemble.
- Elles contribuent à optimiser l'efficacité énergétique, à réduire les coûts, à minimiser les interruptions de service et à favoriser une transition plus rapide vers les énergies renouvelables.



- L'augmentation de la connectivité et le recours croissant à l'automatisation dans l'ensemble du réseau électrique en amplifient la vulnérabilité face aux menaces cybernétiques.
- Chaque nouveau point de connexion devient une porte d'entrée potentielle pour des attaques malveillantes, rendant essentiel le renforcement des mesures de cybersécurité afin de protéger les infrastructures critiques et d'assurer la résilience du réseau face à ces risques grandissants.

CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une prise de conscience internationale

			
IEA (2017), *Digitalisation and Energy*, IEA, Paris	IEA (2021), *Enhancing cyber resilience in electricity systems, IEA,* Paris	*IEA (2023), Electricity Grids and Secure Energy Transitions, IEA, Paris*	IEA (2024), *Electricity 2024*, IEA, Paris
https://www.iea.org/reports/digitalisation-and-energy	https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems	https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions	https://www.iea.org/reports/electricity-2024

CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

Une multiplication des initiatives légales et règlementaires

Hong Kong Proposes the Introduction of a Legal Framework for Regulating Critical Infrastructures

The Proposed Framework is the first concrete step towards the introduction of cybersecurity obligations on organisations.

9 oct. 2024

Biden Issues Cyber Executive Order in Last Days of Term

President Biden's Executive Order strengthens cybersecurity through improved standards, threat information sharing, software supply chain...

First Network Code on Cybersecurity for the electricity ...

24 mai 2024 — The new **Network Code** on **Cybersecurity** has been developed in response to t growing digitalisation and interconnection of national power systems ...

La directive NIS2 : une refonte majeure du paysage de la cybersécurité en Europe

En partenariat avec Mailinblack, la cybersécurité centrée sur l'utilisateur. ... Adoptée en janvier 2023, la directive NIS2 (Network and...

UK proposes New Cyber Security and Resilience Bill to Boost the UK's Cyber Defences

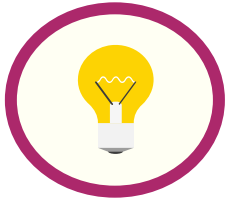
During the King's Speech on 17 July 2024, the newly appointed UK Prime Minister announced the UK Government's intention to introduce a new...

Senado aprobó en general proyecto para la protección de infraestructura crítica

En condiciones de iniciar su debate en particular quedó el proyecto para la protección de la infraestructura crítica del país, luego de que...

CYBERSÉCURITÉ DU SECTEUR ÉLECTRIQUE

En synthèse



- Le secteur de l'énergie en général et de l'électricité en particulier est un des plus visés par les cyberattaques.
- Recrudescence des cyberattaques à l'encontre des infrastructures électriques partout dans le monde.
- Si peu d'entre elles aboutissent à des interruptions massives des services, elles sont une menace grandissante dont l'impact potentiel doit faire l'objet d'une considération sérieuse.
- Les pouvoirs publics prennent des mesures (stratégies et politiques) pour renforcer la cybersécurité : un cadre juridique de la cybersécurité se met progressivement en place partout dans le monde.

2

Panorama des outils juridiques pour la cybersécurité

PANORAMA DES OUTILS JURIDIQUES

La notion d'infrastructure critique

Infrastructure critique

Systèmes, installations, actifs

Services essentiels
ou vitaux pour la société ou l'économie

Gravité des conséquences de la défaillance

*La notion d'infrastructure critique est évolutive et assez vague, car elle dépend du **contexte national**, des menaces en évolution (terrorisme, cyberattaques, catastrophes naturelles) et des avancées technologiques.*

→ La notion est née aux USA dans les années 1990 en réponse à l'émergence de nouvelles menaces, notamment terroristes.

PANORAMA DES OUTILS JURIDIQUES

L'identification des infrastructures critiques

Chaque pays définit ses infrastructures critiques en fonction de ses priorités stratégiques et de sa vulnérabilité.

Dans tous les pays ayant adopté une réglementation sur les infrastructures critiques, l'énergie y est identifiée. Les infrastructures du secteur électrique sont évidemment considérées dans ce cadre.

PANORAMA DES OUTILS JURIDIQUES

Les infrastructures et systèmes d'information critiques

Systèmes d'information critiques (SIC)	Infrastructures d'Information Critiques (IIC)
Les systèmes informatiques et de communication qui soutiennent ces infrastructures critiques. Ils sont considérés comme critiques dans la mesure où une cyberattaque ou une défaillance technique pourrait perturber le fonctionnement des secteurs vitaux.	Ensemble des réseaux, systèmes et ressources nécessaires pour stocker, traiter et transmettre des informations critiques.
C'est un sous-ensemble des IIC, souvent spécifique à un secteur ou une entité. Exemple : Système SCADA d'une centrale électrique	Comprend l'ensemble des ressources à l'échelle nationale ou supranationale. Exemple : Réseaux Internet, systèmes télécoms

Le réseau de transport d'électricité repose sur des systèmes d'information critiques qui sont essentiels à son fonctionnement sécurisé.

PANORAMA DES OUTILS JURIDIQUES

Un cadre juridique associé

- **Droit international et régional**

➢ *Recommandation sur la sécurité numérique des activités critiques* adoptée par le Conseil de l'OCDE le 11 décembre 2019. Elle remplace la Recommandation de 2008 sur la protection des infrastructures d'information critiques. https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0456

➢ Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil

Certains cadres juridiques supranationaux influencent la manière dont les systèmes d'information critiques sont encadrés. Cependant, la cybersécurité des systèmes d'information et infrastructures critiques est donc indissociable de la sécurité et de la souveraineté nationale et passe donc par des lois et décrets propres à chaque pays.

PANORAMA DES OUTILS JURIDIQUES

Contenu standard des lois de protection des infrastructures critiques

- **Identification des infrastructures critiques :** Définition des opérateurs essentiels (OIV, OSE, CI), cartographie des infrastructures critiques et des risques associés…
- **Mise en place de mesures de cybersécurité :** Obligation d'évaluer et de renforcer la sécurité des SI critiques, adoption de référentiels et de normes (ISO..), mise en œuvre d'une politique de Sécurité des Systèmes d'Information intégrant une politique de contrôle des accès et de cloisonnement des réseaux, responsable de la sécurité des systèmes d'information (RSSI ou CISO – Chief Information Security Officer)
- **Obligations de signalement et de gestion des incidents :** Notification rapide aux autorités en cas d'incident grave, élaboration de plans de réponse et de reprise d'activité…
- **Contrôles et audits :** obligations d'audits réguliers, contrôle des autorités compétentes, cadre de sanctions en cas de non-conformité...
- **Coopération et échanges d'informations :** partage d'informations entre acteurs critiques et autorités, participation à des exercices de simulation et de crise…

Les lois de protection des infrastructures critiques établissent un cadre réglementaire essentiel visant à renforcer la résilience et la cybersécurité des services vitaux.

Elles imposent aux acteurs concernés des obligations de sécurisation, de surveillance et de gestion des incidents, tout en favorisant une coopération renforcée entre les secteurs public et privé.

PANORAMA DES OUTILS JURIDIQUES

Les standards techniques internationaux

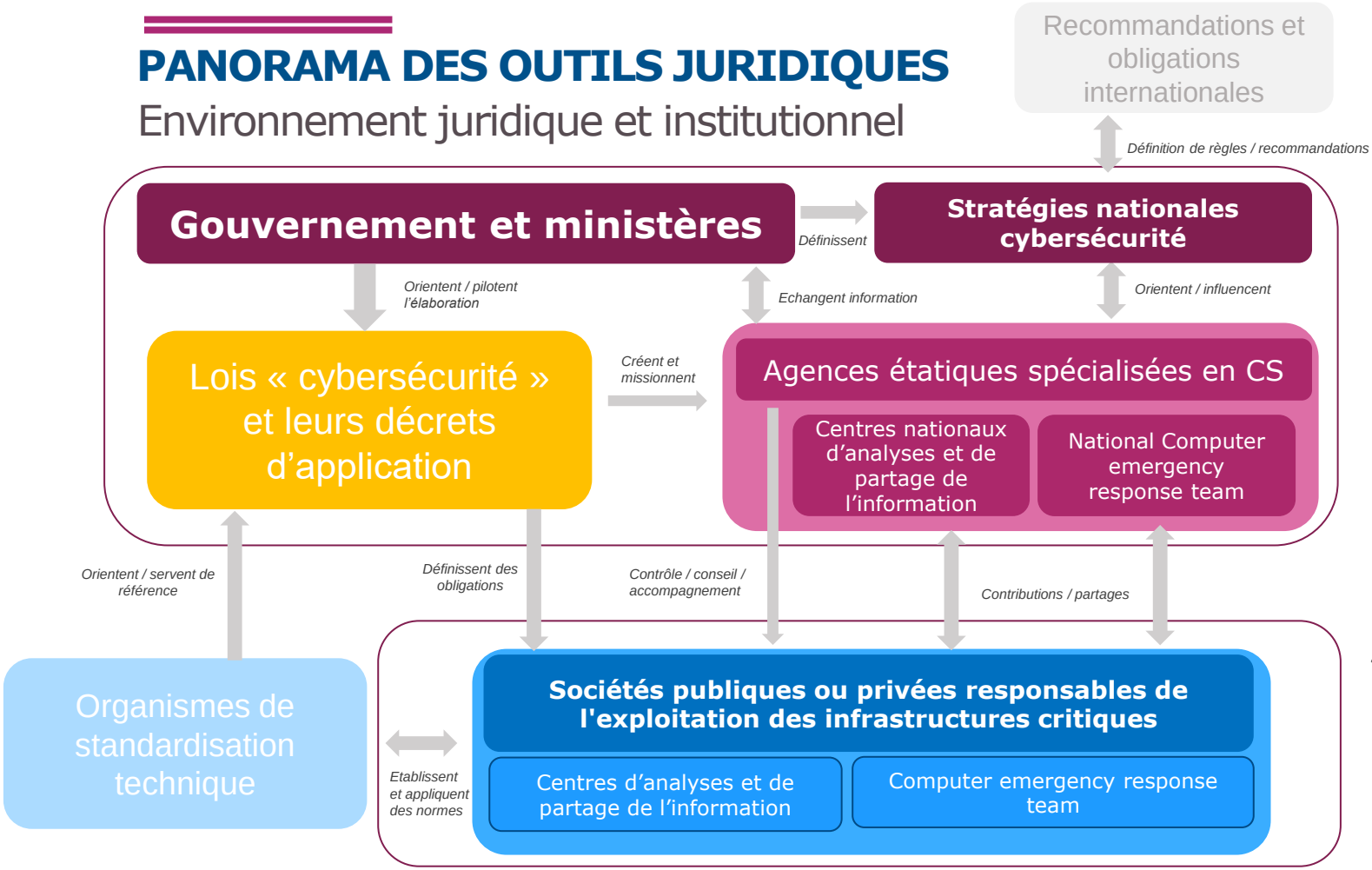
- Qu'est-ce qu'une norme technique ? Définition de l'OMC : « *Document approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques pour des produits ou des procédés et des méthodes de production connexes, dont le respect n'est pas obligatoire* » .

- Une norme d'application volontaire peut devenir une norme juridique obligatoire. Bien qu'une norme soit par principe d'application volontaire, les pouvoirs publics peuvent, par exception, rendre tout ou partie d'une norme d'application obligatoire, en prenant un texte réglementaire spécifique à cet effet.

Exemples de normes techniques en matière de cybersécurité : IEC (62443 Réseaux de communication industriels - Sécurité informatique des réseaux et des systèmes), NERC CIP, ISO 27001…

PANORAMA DES OUTILS JURIDIQUES

Environnement juridique et institutionnel



Sphère des recommandations et règles internationales

Sphère de « l'Etat stratège », législateur et contrôleur

Sphère des opérateurs d'infrastructures critiques

PANORAMA DES OUTILS JURIDIQUES

Quid des codes de réseau ?

- Les **codes de réseau** ou « **grid code** » désigne un document qui établit juridiquement les exigences techniques pour le raccordement et l'exploitation d'un système électrique d'une manière qui garantisse un fonctionnement fiable, efficace et sûr dans un contexte d'ouverture du marché de l'électricité (la gestion du système électrique tend à dépendre d'une pluralité d'acteurs).

- Corpus organisé de règles opposables aux acteurs du secteur, les codes de réseau ont vocation à permettre l'accès des tiers aux réseaux dans des conditions transparentes et non discriminatoires tout en donnant aux opérateurs de réseaux les prérogatives nécessaires pour atteindre ou conserver une fiabilité technique optimale.

- Ils sont généralement élaborés par les **opérateurs de réseaux** et adoptés par les pouvoirs publics.

- Ces deux dernières décennies, de nombreux pays ont adopté ce type de document.

PANORAMA DES OUTILS JURIDIQUES

Contenu standard des codes de réseau

CODE DE RESEAU

Code de raccordement

Le code de raccordement a pour objet de définir les conditions techniques, juridiques et financières du raccordement d'une nouvelle installation au réseau.

Code d'exploitation

On trouve notamment dans le code d'exploitation les standards pour une exploitation sûre, coordonnée et efficace du système électrique national (performances du RPT, analyses et limites de sécurité, défense et reconstitution…)

Code de comptage

Le code de comptage clarifie les responsabilités et spécifie les exigences relatives à la mesure et des données d'énergie

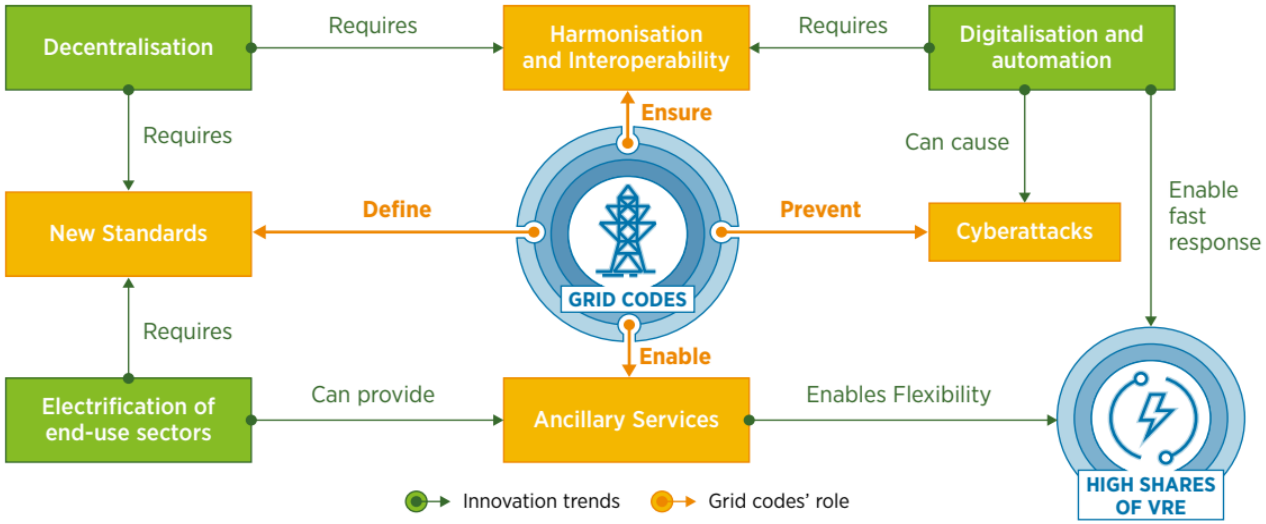
Code de planification

Le code de planification spécifie les critères et procédures techniques et de conception à appliquer par le GRT dans la planification et le développement du réseau électrique de transport

PANORAMA DES OUTILS JURIDIQUES

La cybersécurité et les codes de réseau

La cybersécurité est en train de devenir un sujet incontournable des codes de réseau. L'IRENA l'a souligné dans un récent rapport : « *Les codes de réseau évoluent vers la recommandation de normes et l'amélioration de la cybersécurité dans les systèmes électriques, tout en assurant l'harmonisation et l'interopérabilité* ».



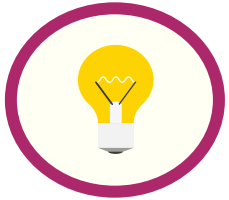
PANORAMA DES OUTILS JURIDIQUES

La cybersécurité et les codes de réseau

- Plusieurs pays ont intégré des dispositions en lien avec le sujet de la cybersécurité dans leurs codes de réseau ;
- L'Union Européenne a publié le 28 mai 2024 son premier code de réseau sur la cybersécurité pour le secteur de l'électricité (« Network Code on Cybersecurity for the electricity sector » ou « NCCS »).

PANORAMA DES OUTILS JURIDIQUES

En synthèse



- Les lois visant à protéger les infrastructures critiques ont intégré la dimension cyber et incluent de manière générale des exigences pour les systèmes d'information.
- Les opérateurs d'électricité sont généralement soumis à des obligations spécifiques émanant du cadre des infrastructures critiques.
- Les codes de réseau ont évolué pour intégrer des règles spécifiques pour les opérateurs et utilisateurs du réseau d'électricité.
- L'analyse menée dans le rapport a permis de comparer différents cas spécifiques pour mesurer la pertinence de l'insertion de règles de cybersécurité dans les codes de réseau à l'aune des cadres juridiques et institutionnels en vigueur dans chaque pays et essayer d'en tirer des recommandations. Le contenu des règles insérées dans les codes de réseau n'est pas uniforme selon le code de réseau étudié.

3

Benchmarking des cadres nationaux

BENCHMARKING DES CADRES NATIONAUX

Introduction

Les pays qui ont été sélectionnés pour l'étude sont les suivants :

- France
- Grande-Bretagne
- Kenya
- Etats-Unis
- Inde

Etats centralisés vs. Etats fédéraux

Les États fédéraux, tels que les États-Unis ou l'Inde, présentent une structure complexe où le pouvoir est partagé entre un gouvernement central et des entités régionales autonomes, chacune gérant souvent des portions distinctes du système électrique national. Ces pays se caractérisent par des réseaux électriques interconnectés qui couvrent plusieurs régions, mais qui sont soumis à des régulations variées

FRANCE

Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	Stratégie nationale pour la sécurité du numérique (2015)
Autorités publiques chefs de fil	▪ Ministère des armées ; ▪ Ministère de l'Intérieur.
Agence nationale dédiée à la cybersécurité	L'Agence nationale de la sécurité des systèmes d'information (ANSSI) (2009).
Centre national d'alerte et de réaction aux attaques informatiques	Le CERT-FR, porté par la Sous-Direction Opérations de l'ANSSI. A noter qu'au niveau européen, un réseau de coordination en cas de crise a été créé récemment (EU-CyCLONe).
Centre d'analyse et de partage d'informations	Oui au niveau européen : EE-ISAC - European Energy Information Sharing & Analysis Centre.
Identification et protection des Infrastructures Critiques	
Loi encadrant les « infrastructures critiques »	Un cadre spécifique vise à protéger les installations d'importance vitale dans le Code de la Défense (art. L.1332-1 à L.1332-7).

- Au sein des Secteurs d'activité d'importance vitale (SAIV), des opérateurs d'importance vitale (OIV) ont été désignés.
- En 2013, un cadre spécifique aux les systèmes d'information d'importance vitale (SIIV) a été créé.

FRANCE

Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	Pas de compétences légales explicites mais implication ponctuelle pour favoriser le développement de la cybersécurité dans le secteur de l'énergie.
Groupe de travail ou instance technico-administrative	La CRE a lancé fin 2020 un groupe de travail sur la cybersécurité comprenant les acteurs des secteurs du gaz et de l'électricité.
Textes réglementaires / directives spécifiques	Pour les OIV du secteur de l'électricité : Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Approvisionnement en énergie électrique » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.
Code de réseau	La DTR de RTE contient des dispositions spécifiques pour la cybersécurité.

- Les exigences décrites dans la DTR en matière de cybersécurité couvrent des sujets techniques liés au raccordement au réseau de transport et plus particulièrement la connexion au réseau de téléconduite de RTE.
- Les exigences couvrent également la coordination entre RTE et ses clients pour l'utilisation de ce réseau et plus largement pour leurs échanges d'informations.

GRANDE-BRETAGNE

Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	La *National Cyber Strategy 2022*
Autorité publique responsable	Le *Government Communications Headquarters* (GCHQ), sous la responsabilité du Secrétaire d'État britannique aux Affaires étrangères et du Commonwealth.
Agence nationale dédiée à la cybersécurité	Le National Cyber Security Centre (NCSC) (2016)
Centre national d'alerte et de réaction aux attaques informatiques	La *Incident Management team*, au sein du NCSC.
Centre d'analyse et de partage d'informations	Le CiSP (expertise générale).
Identification et protection des infrastructures critiques	
Loi encadrant les « infrastructures critiques » et leurs systèmes d'information	*The Network and Information Systems Regulations 2018 (NIS Regulations)*.

- Avant 2016 : plusieurs agences couvraient la sécurité de l'information, la réponse aux cyberattaques, la protection des infrastructures critiques… Elles ont toutes été regroupées dans la **NCSC**, qui a large spectre de missions.
- Avant 2018 et les NIS Regulations (transposition européenne) il n'y a avait pas de cadre juridique précis de la protection des infrastructures critiques).

GRANDE-BRETAGNE

Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	L'Ofgem a des compétences en matière de cybersécurité des opérateurs de services essentiels des secteurs de l'électricité et de l'aval gazier.
Groupe de travail ou instance technico-administrative	▪ Le *Cyber Security Working Group (*CSWG), sous l'égide de l'Energy Networks Association. ▪ Le *Energy Emergencies Executive Cyber Security Task Group* (E3CC), sous-groupe du comité gouvernemental *UK Energy Emergencies Executive*.
Textes réglementaires / directives spécifiques	Le DESNZ et l'Ofgem ont publiés des guides afin d'aider les opérateurs du secteur électrique concernés par la réglementation NIS 2018 à appliquer la règlementation.
Code de réseau	Plusieurs codes encadrent les activités du secteur électrique, dont le *Grid Code*

- Implication très forte de l'Ofgem en matière de cybersécurité : elle a été désignée comme autorité compétente au côté du dép. ministériel de l'énergie (DESNZ) pour déployer la règlementation NIS pour le secteur du gaz et de l'électricité. 5 guides publiés depuis 2020.
- Les codes de réseau administrés par National Grid ESO ne font pas mention du terme « cybersécurité » et ne contiennent pas de dispositions spécifiques.

KENYA

Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	La *National Cybersecurity Strategy* (2022)
Autorité publique responsable	- Le *National Security Council (*compétent en matière de défense nationale en général) ; - Le *Ministry of Interior and National Administration* (autorité de tutelle du NC4).
Agence nationale dédiée à la cybersécurité	Le « National Computer and Cybercrimes Coordination Committee » (NC4).
Centre national d'alerte et de réaction aux attaques informatiques	Le *National KE-CIRT/CC*
Centre d'analyse et de partage d'informations	Le *National KE-CIRT/CC*
Identification et protection des Infrastructures Critiques	
Loi encadrant les « infrastructures critiques » et leurs systèmes d'information	Le *Computer Misuse and Cybercrime Act N°5 of 2018* (CMCA) + Les *Computer Misuse And Cybercrime (Critical Information Infrastructure And Cybercrime Management) Regulations, 2024*.

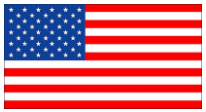
- Le Kenya s'est pleinement saisi de la problématique cyber ces dernières années (la stratégie de 2022 en témoigne). Loi de 2024 pour établir un cadre approprié aux infrastructures d'information critiques.
- Avant 2018 et les NIS Regulations (transposition européenne) il n'y a avait pas de cadre juridique précis pour la protection des infrastructures critiques). L'agence NC4 (2018) permet de progresser sur ce thème (rôle de conseil et d'édiction de normes) notamment pour les IC.

KENYA

Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	Le Plan stratégique 2020 – 2023 de l'EPRA montre une prise de conscience des enjeux en matière de cybersécurité dans l'industrie électrique (mais elle n'a pas d'attributions spécifiques)
Groupe de travail ou instance technico-administrative	La création de groupes de travail technique (*cybersecurity technical working groups* – CTWG) est prévue par la stratégie nationale établie en 2022.
Textes réglementaires / directives spécifiques	Non.
Code de réseau	Le *Kenya National Transmission Grid Code (KNTCG)* contient un chapitre spécifique sur la cybersécurité.

- L'EPRA n'a pas de compétence spécifique en matière de CS mais a approuvé le KNTCG en 2021 dans une version qui contient des dispositions sur la CS (ch. 21).
- Le KNTCG présente un cadre complet et pédagogique pour la gestion de la cybersécurité, abordant un grand nombre de domaines :
- La majorité des dispositions sont formulées sous forme de recommandations et non d'authentiques règles juridiques

ETATS-UNIS



Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	La *National Cybersecurity Strategy 2023*
Autorité publique responsable	Le département de la Sécurité intérieure des États-Unis (DHS)
Agence nationale dédiée à la cybersécurité	La Cybersecurity and Infrastructure Security Agency (CISA) (2018)
Centre national d'alerte et de réaction aux attaques informatiques	Le National Cybersercurity and Communications Integration Center (NCCIC) (fait partie du CISA)
Centre d'analyse et de partage d'informations	Chaque secteur critique possède son propre Information Sharing and Analysis Center (ISAC) (le E-ISAC pour l'électricité)
Identification et protection des Infrastructures Critiques	
Loi encadrant les « infrastructures critiques » et leurs systèmes d'information	*Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) 2001*. *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22) du 30 avril 2024.

- Pays très avancé en matière de cybersécurité, politique forte depuis le Patriot Act (2001).
- Une agence au rôle centrale : la CISA. Travaille avec les agences sectorielles, les gouvernements locaux, et le secteur privé.
- Un texte central : le NSM-22. Puis des lois et règlementations sectorielles (pas de grande loi fédérale sur la protection des infrastructures critiques).

ETATS-UNIS

Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	La *Federal Energy Regulatory Commission* (FERC) a le pouvoir de superviser la fiabilité du système électrique (*Energy Policy Act 2005*). Cela inclut le pouvoir d'approuver les normes de fiabilité obligatoires en matière de cybersécurité.
Groupe de travail ou instance technico-administrative	Plusieurs groupes rassemblant des acteurs de l'énergie ont été mis en place dans le cadre du *Critical Infrastructure Partnership Advisory Council* (CIPAC) établi par Département de la sécurité intérieur : *Cybersecurity Capability Maturity Model (C2M2) Working Group*, *Control Systems Working Group*.
Textes réglementaires / directives spécifiques	*Order N°706* de la FERC (et textes complémentaires associés) rendant opposables les normes CIP.
Code de réseau	Il existe de la documentation technique pour chacun des opérateurs de systèmes/réseau (ISO ou RTO), mais la cybersécurité est traitée au niveau fédéral et non dans ces documents.

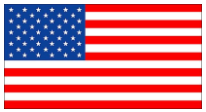
- Depuis 2008, la FERC examine et approuve les normes CIP (*Critical Infrastructure Protection*) qui sont élaborées par la NERC. Chacune d'entre elles est associé à un plan de déploiement.
- Les normes CIP sont reconnues internationalement comme des références en matière de protection des infrastructures critiques du secteur électrique.

ETATS-UNIS

Agence du gouvernement fédéral des États-Unis qui a compétence dans le domaine du commerce inter-États et des tarifs de gros de l'électricité, les permis d'exploitation des centrales hydroélectriques et le prix du transport gazier et pétrolier.

Le North American Electric Reliability Corporation ou NERC est un organisme sans but lucratif nord-américain fondé en 1968 chargé de faire appliquer des normes de fiabilité pour les réseaux de transport de l'électricité des États-Unis, du Canada et de certaines régions du Mexique.

ETATS-UNIS



Référence	Nom	Date
CIP-002-5.1a	Cyber Security - BES Cyber System Categorization	27/12/2016
CIP-003-8	Cyber Security - Security Management Controls	01/04/2020
CIP-004-7	Cyber Security - Personnel & Training	01/01/2024
CIP-005-7	Cyber Security - Electronic Security Perimeter(s)	01/10/2022
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	01/07/2016
CIP-007-6	Cyber Security - System Security Management	01/07/2016
CIP-008-6	Cyber Security - Incident Reporting and Response Planning	01/01/2021
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	01/07/2016
CIP-010-4	Cyber Security — Configuration Change Management and Vulnerability Assessments	01/10/2022
CIP-011-3	Cyber Security — Information Protection	01/01/2024
CIP-012-1	Cyber Security – Communications between Control Centers	01/07/2022
CIP-013-2	Cyber Security - Supply Chain Risk Management	01/10/2022
CIP-014-3	Physical Security	16/06/2022
CIP-015-01	Requirements for Internal Network Security Monitoring (INSM)	05/09/2024

INDE

Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	▪ *National Cyber Security Strategy (2020),* ▪ *National Information Security Policy and Guidelines* (NISPG).
Autorité publique responsable	▪ Le *National Security Council* (NSC), ▪ La *Cyber And Information Security (C&Is) Division* (Ministry of Home Affairs).
Agence nationale dédiée à la cybersécurité	▪ *National Critical Information Infrastructure Protection Center* (NCIIPC), ▪ *National Cyber Coordination Centre* (NCCC), ▪ *Indian Cybercrime Coordination Centre* (I4C).
Centre national d'alerte et de réaction aux attaques informatiques	CERT-In (Indian Computer Emergency Response Team).
Centre d'analyse et de partage d'informations	ISAC India.
Identification et protection des Infrastructures Critiques	
Loi encadrant les « infrastructures critiques » et leurs systèmes d'information	*The Information Technology Act, 2000 (amended 2008), Information Security Practices and Procedures For Protected System Rules (2018)*

- Règles récentes concernant la protection des infrastructures critiques (2018) basée sur la loi de 2000.
- Plusieurs agences en parallèle se partagent des missions liées à la cybersécurité.
- Fragmentation des responsabilités entre plusieurs agences et de l'absence d'une autorité centralisée unique

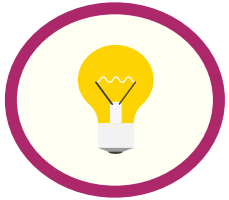
INDE

Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	Oui mais limitée.
Groupe de travail ou instance technico-administrative	Le *Cyber Security Coordination Forum*.
Textes réglementaires / directives spécifiques	*CEA (Cyber Security in Power Sector) Guidelines, 2021*.
Code de réseau	Oui, le *Indian Electricity Grid Code* (IEGC) complété par des codes de réseaux étatiques (State Grid Codes).

- En véritable besoin de renforcement de la CS existe dans plusieurs secteurs dont l'électricité. En 2021, la Central Electricity Authority (CEA) a adopté une règlementation spécifique pour le secteur de l'électricité. Les règles élaborées sont techniques et organisationnelles.
- En 2023, l'actualisation du Code de réseau Indien (IEGC) a été l'occasion d'insérer un chapitre sur la cybersécurité, qui n'apporte pas de nouveauté règlementaire par rapport à la règlementation de 2023.
- Avant, les codes de réseau de chaque Etat avaient leur propre règle sur ce sujet.

PANORAMA DES OUTILS JURIDIQUES

En synthèse



- On retrouve les outils essentiels de la cybersécurité dans chacun des pays étudiés.
- Les pays les plus avancés en la matière ont concentré les missions d'expertise au sein d'une agence spécialisée forte.
- Des règlementations et normes spécifiques au secteur de l'électricité mais contenu variable
- Plusieurs trajectoires différentes prises au niveau des codes de réseau : traitent ou non la cybersécurité, éléments techniques ou organisationnels…

4

Benchmarking des cadres régionaux

BENCHMARKING DES CADRES RÉGIONAUX

Introduction

- La multiplication des échanges commerciaux d'énergie entre pays apporte de nombreux bénéfices au système.
- Elle étend cependant à une échelle plus large certaines problématiques, notamment les risques et menaces dont ceux de nature « cyber ».
- La mise en place d'échanges régionaux nécessite le développement d'infrastructures physiques mais également l'adoption d'un cadre politique, technique et institutionnel permettant la bonne gestion du système.
- Dans ce contexte, les normes permettant l'exploitation des réseaux transfrontaliers sont de plus en nombreuses et des dispositions spécifiques pour la cybersécurité sont en train de voir le jour.

BENCHMARKING DES CADRES RÉGIONAUX

L'Amérique du Nord

- Emergence de règles dédiées à la cybersécurité par le biais de la North American Electric Reliability Corporation (NERC).

- Les normes CIP de la NERC sont appliquées au Canada à la condition, comme pour toutes les autres normes de la NERC, qu'elles soient approuvées par les autorités locales, dans le respect du droit en vigueur. Chaque province peut décider de la manière dont elle intègre les normes de la NERC, y compris les CIP et donc les adopter intégralement, les modifier ou ne pas les adopter.

- Au Mexique, l'adoption des normes CIP n'est pas aussi systématique que dans les provinces canadiennes. L'application est volontaire dans les régions où elles sont jugées nécessaires (interconnexions avec les Etats-Unis).

BENCHMARKING DES CADRES RÉGIONAUX

L'Union européenne

- Règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil en établissant un ***code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité***.

- Elaboré par DSO Entity et l'ENTSO-E, en collaboration avec l'ACER.

- Adopté par la Commission européenne.

- Ce code de réseau fournit une définition claire des rôles et obligations des différents acteurs devant intervenir.

- Il contient 49 articles exposant de règles pour améliorer le traitement de la cybersécurité sectorielle et notamment :
  - Des règles sur l'évaluation des risques cyber,
  - Des exigences minimales communes,
  - La certification en cybersécurité des produits et services,
  - La surveillance, le reporting et la gestion de crise.

BENCHMARKING DES CADRES RÉGIONAUX

L'Union européenne

- Le NCCS met en place un processus structuré, à développer en différentes étapes au cours de plusieurs années et passant par l'élaboration de « modalités », « conditions », « méthodes », ainsi que des plans.

- Les GRT et GRD ont l'obligation d'élaborer une documentation technique permettant de déployer les exigences de cybersécurité pour les réseaux électriques.

Article NCCS	Documents
Art. 18 § 1	Méthodes d'évaluation des risques de cybersécurité
Art. 23	Rapport d'évaluation complète des risques de cybersécurité en lien avec les flux transfrontaliers d'électricité
Art. 29	Contrôles minimaux et avancés de cybersécurité conformément
Art. 33 et 34	Cartographie des contrôles de cybersécurité de l'électricité par rapport aux normes y compris les contrôles minimaux et avancés de cybersécurité dans la chaîne d'approvisionnement
Art. 35	Recommandation relative à la passation de marchés dans le domaine de la cybersécurité
Art. 37 § 8	Méthode/échelle de classification des cyberattaques
Art. 22	Plans régionaux d'atténuation des risques de cybersécurité

BENCHMARKING DES CADRES RÉGIONAUX

Le WAPP (CEDEAO)

- Un code de réseau régional est actuellement en cours de finalisation au sein des instances régionales de l'EEEOA

- Le Code d'exploitation comporte des dispositions techniques spécifiques à la cybersécurité.
  - Mise en place d'un groupe de travail en charge de la cybersécurité
  - Exigences spécifiques aux systèmes SCADA
  - Lignes directrices spécifiques concernant l'infrastructure TIC
  - Obligation d'autocertification.

5

Conclusions & recommandations

CONCLUSIONS ET RECOMMANDATIONS

Sur le droit des infrastructures critiques

- De nombreux pays ont fixé des obligations légales et réglementaires portant sur l'identification des infrastructures critiques et leurs systèmes d'information et les exigences techniques à appliquer en matière de cybersécurité.
- Les infrastructures électriques sont systématiquement identifiées comme critiques et se voient donc appliquer des règles spécifiques, appliquées aux acteurs publics comme privés.
- La maturité et la profondeur des règles varient en fonction des pays, mais de bonnes pratiques sont communément admises.

- Les sociétés d'électricité doivent se préoccuper de connaître le cadre en vigueur, au niveau national et régional, ainsi que les normes internationales. Elles doivent avoir du personnel (experts juridiques et techniques) compétents en matière de cyber.

- Les sociétés d'électricité peuvent encourager les pouvoirs publics à établir des règles spécifiques aux infrastructures critiques, incluant le système électrique, et aider à définir son contenu (logique de coopération/collaboration).

CONCLUSIONS ET RECOMMANDATIONS

Sur les codes de réseau (1/2)

- Les codes de réseau sont un véhicule juridique pertinents pour établir les règles techniques visant la résilience du système électrique et l'exploitation fiable du réseau.
- La cybersécurité y trouve donc naturellement sa place même si elle reste une problématique avant tout nationale et étatique en raison de la dimension sécurité intérieure voire défense nationale.
- Dans les Etats fédéraux, la cybersécurité doit être coordonnée au niveau fédéral.

- Les gestionnaires de réseau doivent considérer le sujet de la cybersécurité dans les règles de raccordement et d'exploitation du réseau et faire éventuellement évoluer le code de réseau national en concertation avec les autres acteurs.
- Les opérateurs d'électricité qui élaborent les codes et les autorités qui les approuvent doivent veiller à respecter leurs compétences et mission.

CONCLUSIONS ET RECOMMANDATIONS

Sur les codes de réseau (2/2)

- Les codes de réseau sont des documents publics. Il peut donc être judicieux de chercher à exclure du code de réseau certaines spécifications ou exigences dont la publication pourrait dévoiler une partie des dispositifs de protection du système électrique.
- L'établissement de marchés de l'électricité régionaux doit encourager les pays à établir une coopération accrue en matière de cybersécurité incluant un cadre juridique et institutionnel harmonisé concernant la gestion et le traitement des cyberrisques.

- Les gestionnaires de réseau doivent protéger la confidentialité des règles cyber les plus sensibles concernant le système électrique.
- Tous les acteurs du secteur électrique (publics comme privés) doivent s'efforcer de coopérer sur le sujet de la cyber et de se coordonner pour avancer conjointement dans le renforcement de la sécurité.
- Cette logique de coopération peut dépasser le niveau national ou même le secteur de l'électricité.

CONCLUSIONS ET RECOMMANDATIONS

Recommandations finales

- Les sociétés d'électricité sont pleinement concernées par l'enjeu cybersécurité. En particulier, les gestionnaires de réseau sont
- Elles doivent anticiper le risque cyber notamment en recrutant formant le personnel.
- Des décalages importants peuvent se former entre les règles de cybersécurité, et les capacités opérationnelles des acteurs (Etats comme sociétés).

  → Avoir des règles adaptées et concertées
  → Des règles diffusées, expliquées et appliquées
  → Mettre en place des processus de « compliance »

Merci de votre attention !