STRATEGIE D'ACCOMPAGNEMENT AU RENFORCEMENT DES CAPACITES (RC) DES OPERATEURS DANS LE CADRE DE LA DIGITAL ENERGY FACILITY COMPOSANTE 1B

CONTRAT N° AFD/ENU/EGI/2021/CC/BHKN°29

Les codes de réseau : un outil au service du renforcement de la cybersécurité du secteur électrique ?

Version 1.1

6 mai 2025

Références		
Ce rapport a été élaboré dans le cadre de la composante 1b de la Digital Facility Energy (DEF) de l'Agence Française de Développement par : RTE international Tour La Fayette, 2 Place des Vosges, 92400 Courbevoie, France https://www.rte-international.com/		
Date : 29/10/2024	Version : 1.1	
Auteur :	**Contributeur :**	**Vérificateur :**
Henri Maria Expert juridique secteur électrique	Nicolas Stakowski Juriste et ingénieur en système électrique	Philippe Michal Directeur Performance des systèmes électriques (PSE)

Avertissement

Ce rapport repose essentiellement sur des données publiques disponibles sur Internet au moment de sa rédaction. Les informations ont été compilées, analysées et interprétées sans validation préalable par les États, institutions ou autre organismes et entreprises mentionnés. Par conséquent, les analyses présentées sont fournies à titre indicatif et sont susceptibles de variations ou d'inexactitudes. L'auteur décline toute responsabilité quant à d'éventuelles divergences avec les informations officielles ou à jour.

GLOSSAIRE

Code	Description
ACER	Agency for the Cooperation of Energy Regulators
AFD	Agence française de développement
AIE	Agence internationale de l'énergie
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARREC	Autorité de Régulation Régionale du secteur de l'Electricité de la CEDEAO
CA	Communications Authority of Kenya
CAF	Cyber Assessment Framework
CAISO	California Independent System Operator
CCA	Centre for Cyber Assessment
CEA	Central Electricity Authority of India
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CENACE	Centro Nacional de Control de Energía
CERC	Central Electricity Regulatory Commission
CERT	Computer Emergency Response Team
CERT UK	Computer Emergency Response Team of the United Kingdom
CESG	Communications-Electronics Security Group
CFE	Comisión Federal de Electricidad
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CiSP	Cyber Security Information Sharing Partnership
CMCA	Computer and Misuse and Cybercrimes Act N°5 of 2018
CPNI	Centre for the Protection of National Infrastructure
CRE	Commission de régulation de l'énergie
CRE	Comisión Reguladora de Energía
CSIRT	Computer security incident response team
CSWG	Cyber Security Working Group

DEF	Digital Energy Facility
DESNZ	Department for Energy Security and Net Zero
DNO	Distribution Network Operator
DTR	Documentation technique de référence de RTE
EEEOA	Système d'échange d'énergie électrique ouest africain
E-ISAC	Electricity Information Sharing and Analysis Center
ENTSO-E	European Network of Transmission System Operators
DSO Entity	Association for all sizes of Distribution System Operators (DSOs) in Europe
E3CC	Energy Emergencies Executive Cyber Security Task Group
GCHQ	Government Communications Headquarters
GCI	Global Cybersecurity Index
I4C	Indian Cybercrime Coordination Centre
ICS	Industrial Control System
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEGC	Indian Electricity Grid Code
IIoT	Industrial Internet of Things
IRENA	International Renewable Energy Agency
ISACs	Information Sharing and Analysis Centers
ISO	International Organization for Standardization
ISO	Independent System Operator
IT	Information Technology
KNTGC	Kenya National Transmission Grid Code
KPLC	Kenya Power and Lighting Company
KHNP	Korea Hydro & Nuclear Power
NC4	National Computer and Cybercrimes Coordination Committee
NCCC	National Cyber Coordination Centre
NCCIC	National Cybersecurity and Communications Integration Center
NCCS	European Network Code on Cybersecurity
NCII	National Critical Information Infrastructure
NCIIPC	National Critical Information Infrastructure Protection Centre
NCSC	National Cyber Security Centre

NERC	North American Electric Reliability Corporation
NETS	National Electricity Transmission System
NIS	Directive européenne « Network and Information Security »
NIS 2018	Network and Information Systems Regulations 2018
NIST	National Institute of Standards and Technology
NKCC	National KE-CIRT/CC (Kenya Computer Incident Response Team – Coordination Centre)
Ofgem	Office of Gas and Electricity Markets
OIV	Opérateur d'importance vitale
OES	Operators of Essential Services
OSE	Opérateurs de services essentiels
OSM	Opérateur du Système Marché
OT	Operational Technology
REC	Directive européenne « Résilience des entités critiques »
RIIO	Revenue Incentives Innovation Outputs
RTE	Réseau de transport d'électricité
RTEi	RTE international
RTO	Regional Transmission Organization
SAIV	Secteurs d'activités d'importance vitale
SCADA	Supervisory Control and Data Acquisition
SERC	State Electricity Regulatory Commissions
SGC	State Grid Code
SIIV	Systèmes d'information d'importance vitale
TIC	Technologies de l'information et de la communication
UE	Union européenne
WAN	Wide Area Network
WAPP	West African Power Pool

TABLE DES MATIERES

GLOSSAIRE 3
TABLE DES MATIERES 6
TABLE DES FIGURES 8
TABLE DES TABLEAUX 8
PROPOS PRELIMINAIRES 9
RESUME EXECUTIF 11
INTRODUCTION 12
1. Renforcer le cadre juridique pour faire face aux cybermenaces 14
1.1. L'émergence des cybermenaces dans le secteur électrique 14
1.1.1. Le secteur électrique : une cible privilégiée pour les cyberattaques 14
1.1.2. Une prise de conscience internationale 16
1.2. Outils juridiques et institutionnels pertinents en matière de cybersécurité 17
1.2.1. La loi au service de la protection des infrastructures critiques 17
1.2.2. Les codes de réseau : un outil au service de la résilience du système électrique 20
2. Cybersécurité : Une Intégration Croissante dans les Codes de Réseau Électrique 23
2.1. La France 23
2.1.1. Protection des infrastructures critiques et de leurs systèmes d'information 23
2.1.2. Règles de cybersécurité du secteur de l'électricité 25
2.1.3. La Documentation technique de référence de RTE : le code de réseau de transport français 26
2.1.4. Tableau de synthèse 29
2.2. La Grande-Bretagne 30
2.2.1. La protection des infrastructures critiques et de leurs systèmes d'information 30
2.2.2. Règles spécifiques au secteur de l'électricité 32
2.2.3. Le Grid Code et les autres codes « électricité » britanniques 32
2.2.4. Tableau de synthèse 35
2.3. Le Kenya 36
2.3.1. La protection des infrastructures critiques et de leurs systèmes d'information 36
2.3.2. Règles spécifiques au secteur de l'électricité 38
2.3.3. Le « Kenya National Transmission Grid Code » (KNTGC) 38
2.3.4. Tableau de synthèse 40
2.4. Les Etats-Unis d'Amérique 41
2.4.1. Protection des infrastructures critiques et de leurs systèmes d'information 41
2.4.2. Règles de cybersécurité du secteur de l'électricité 43

2.4.3. Business practice manuals et operating procedures : les codes de réseau à l'américaine 44
2.4.1. Tableau de synthèse 45
2.5. L'Inde 46
2.5.1. La protection des infrastructures critiques et de leurs systèmes d'information 46
2.5.2. Règles spécifiques au secteur de l'électricité 48
2.5.3. Le Indian Electricity Grid Code 50
2.5.4. Tableau de synthèse 51
3. Un outil normatif en devenir au niveau supranational 53
3.1. Le développement de la collaboration multilatérale par l'établissement de règles communes : le cas de l'Amérique du Nord 53
3.1.1. Des pionniers de la coopération en matière de fiabilité du système électrique 53
3.1.2. Le traitement des cyberrisques 55
3.1.3. Une coopération à approfondir 55
3.2. Le Code européen « cybersécurité » : un modèle de coopération élevé pour un marché régional fortement intégré 56
3.2.1. La cybersécurité du secteur de l'énergie : un défi pris en compte au niveau européen 56
3.2.2. Genèse de l'établissement d'un code de réseau européen pour la cybersécurité des échanges électriques transfrontaliers 56
3.2.3. Contenu du code de réseau européen NCCS 57
3.3. Le Code régional de l'EEEOA 58
3.3.1. Présentation de l'EEEOA 58
3.3.2. Le projet de Code de réseau régional 59
3.3.3. La cybersécurité dans le projet de code régional 59
Annexe 1 : Synthèse du benchmarking – Codes de réseau nationaux 60
Annexe 2 : Synthèse du benchmarking – Codes de réseau régionaux 61

TABLE DES FIGURES

Figure 1 : Lexique cyber de l'AIE (traduit de l'anglais).....13
Figure 2 : La numérisation du secteur électrique : des bénéfices et des inconvénients...17
Figure 3 : Limites de propriété et de responsabilité - schéma de principe de la connexion du réseau local au réseau de téléconduite de RTE (Art. 4.7.1 § 6.2 de la DTR). 28

TABLE DES TABLEAUX

Tableau 1 : Cyberattaques réussies sur les infrastructures électriques.....14
Tableau 2 : Rapports de l'AIE d'intérêt sur le sujet de la cybersécurité du secteur de l'électricité.....16
Tableau 3 : Principales exigences de l'arrêté du 11 août 2016 25
Tableau 4 : Les codes de l'industrie électrique britannique.....33
Tableau 5 : Synthèse des dispositions du chapitre dédié à la cybersécurité du KNTGC...39
Tableau 6 : Normes CIP actuellement en vigueur.....43
Tableau 7 : Structure et contenu synthétique des lignes directrices du CEA pour la cybersécurité du secteur électrique (2021) 48
Tableau 8 : Synthèse des dispositions de cybersécurité du IEGC (Chapitre 8) 51
Tableau 9 : Modalités, conditions, méthodes et plans à élaborer en application du NCCS 58

PROPOS PRELIMINAIRES

La Digital Facility Energy (DEF), est un programme portant sur la prise en compte de la digitalisation pour l'amélioration l'intégration des énergies renouvelables au réseau électrique, de l'accès à l'énergie électrique, et des performances des sociétés d'électricité tout en réduisant les pertes techniques et commerciales. Ce programme est financé par l'Union européenne et mis en œuvre par l'Agence Française de Développement.

Qu'est-ce que la Digital Energy Facility ?

La Digital Energy Facility est un programme financé par l'Union européenne et mis en œuvre par l'Agence française de développement.

- Budget : 23,5 millions d'euros (dont 3 millions d'euros affectés à la gestion, à la communication et à l'évaluation du programme).
- Localisation : pays éligibles à l'aide publique au développement du Comité d'aide au développement (CAD) de l'OCDE à l'exception des pays en pré-adhésion à l'UE. Focus sur les pays d'Afrique subsaharienne.
- Durée : de décembre 2019 à décembre 2025 (décembre 2027 pour le volet de l'amorçage).

Le secteur de l'énergie, notamment celui de l'électricité, doit actuellement faire face à des changements fondamentaux qui perturbent la structure du système électrique : jusque-là centralisé, unidirectionnel, basé sur le carbone et centré sur la production, le réseau devient décentralisé, multidirectionnel, décarboné et centré sur le consommateur.

La digitalisation est cruciale pour ce nouveau réseau d'énergie flexible et décentralisé, car elle facilite la gestion de la demande énergétique, améliore la planification du réseau et permet de mettre en œuvre de nouveaux modèles économiques tels que les *minigrid* (mini-réseaux) et les *offgrid* (systèmes autonomes), ce qui contribue à accroître l'accès à l'énergie.

RAPPELS SUR LA DEF ET SES QUATRE COMPOSANTES

RTE international a été mandaté par l'AFD pour la réalisation de la Composante 1b de la DEF qui vise à renforcer les capacités des sociétés d'électricité en matière de digitalisation. C'est dans ce contexte qu'a été formulé une thématique d'étude portant sur la cybersécurité et les codes de réseau au niveau international.

L'étude présentée ci-après vise à rappeler les enjeux de la cybersécurité des infrastructures électriques et propose une analyse sur l'opportunité d'encadrer les acteurs sectoriels avec des règles insérées au sein des codes de réseau. Des comparaisons internationales nourrissent la réflexion sur ce sujet novateur qui va sûrement connaître des évolutions dans les prochaines années.

Cette étude comparative permet en outre d'identifier des bonnes pratiques et des opportunités d'amélioration dans les codes de réseau électrique des différents pays.

RESUME EXECUTIF

La cybersécurité est une préoccupation de plus en plus forte pour toutes les infrastructures essentielles, et notamment celles du secteur électrique.

- La sécurité des infrastructures d'informations critiques est cruciale car une défaillance ou une cyberattaque contre ces systèmes peut entraîner des perturbations majeures sur les infrastructures physiques qu'elles soutiennent.
- Le secteur de l'électricité est pleinement concerné par les enjeux de cybersécurité en raison de son exposition de plus en plus forte (digitalisation) et des attaques dont le nombre est en hausse.

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 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.

- Les règles de raccordement et d'exploitation doivent désormais intégrer les spécifications techniques propres à la sécurisation du système électrique dans son aspect cyber.
- Le respect des compétences des acteurs est une problématique juridique de premier ordre. La cybersécurité est un sujet qui emporte des problématiques de sécurité intérieure, voire de défense nationale. Les opérateurs d'électricité qui élaborent les codes et les autorités de régulation qui les approuvent généralement doivent veiller à respecter leurs compétences et mission et celles des autorités publiques et autres organismes impliqués dans la cybersécurité du secteur.
- Les règles adoptées au sein des codes de réseau ne doivent pas enfreindre ou (réitérer sans apporter de compléments) des dispositions légales ou réglementaires prises à un niveau supérieur, notamment les dispositions concernant les infrastructures critiques et leurs systèmes d'information.
- Dans les Etats fédéraux, la cybersécurité doit être coordonnée au niveau fédéral et non par les opérateurs ou autorités étatiques, et ce afin de garantir un niveau de sécurité uniforme sur tout le territoire et des échanges sûrs d'énergie. Cela exclut l'intégration de dispositions sur ce sujet dans des codes de réseau élaborés au niveau infra-national.
- 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 coordonné concernant la gestion et le traitement des cyberrisques.

INTRODUCTION

Le développement mondial de l'Internet a entraîné des risques croissants pour les systèmes connectés, exposant les infrastructures critiques, telles que les réseaux électriques, à des menaces variées, allant de la prise de contrôle des équipements à la destruction de données ou à la perturbation intentionnelle de leur fonctionnement. Ces menaces exigent une vigilance accrue et des mesures renforcées en matière de cybersécurité pour garantir la résilience et la protection des infrastructures vitales.

Cela conduit inévitablement les pouvoirs publics à s'interroger sur les actions à mener et les exigences à faire peser sur les acteurs privés et publics pour améliorer la cybersécurité. Au sein du secteur électrique, elle inclue une interrogation sur l'opportunité d'inclure des règles spécifiques dans les règles techniques des opérateurs de réseau, les codes de réseau.

Les codes de réseau sont un ensemble de règles et de spécifications techniques qui régissent la planification, le raccordement, l'exploitation et la maintenance des systèmes électriques, ainsi que le fonctionnement du marché de l'électricité. Ils sont conçus pour assurer la sécurité, la fiabilité, la qualité et l'efficacité du réseau électrique dans un contexte de multiplication des acteurs. Or, la numérisation des systèmes électriques les expose de plus en plus à des cybermenaces. Les cyberattaques à l'encontre des infrastructures critiques ou essentielles, notamment celles du secteur électrique, sont en hausse constantes ces dernières années.

Dans ce contexte se pose la question de l'adoption de règles propres à la cybersécurité au sein même des codes de réseau. Cette question se justifie d'autant plus que l'ouverture progressive des marchés de l'électricité a amené des acteurs de plus en plus nombreux à intervenir dans la gestion de ce système par des interfaces numériques et connectées. L'application d'une stratégie de défense demande alors d'établir de règles communes pour l'implémenter.

A ce titre, plusieurs pays ont déjà intégré au sein de leurs codes de réseau des règles ou principes concernant la cybersécurité. Au niveau régional, l'Union européenne vient récemment d'adopter un code de réseau sur la cybersécurité dans le secteur de l'électricité.

Ces évolutions récentes alimentent la réflexion sur les meilleures pratiques à déployer en matière de cybersécurité des réseaux électriques et interroge sur la place et le rôle des codes de réseau :

- Comment les codes de réseau s'insèrent-ils dans le paysage juridico-institutionnel de la cybersécurité ?
- Les codes de réseau constituent-ils un véhicule juridique nécessaires et pertinents pour mettre en œuvre une meilleure cybersécurité du système électrique ?
- Existent-ils des dispositions standards en la matière ?

Pour répondre à ces questions, la présente étude pose un regard international sur le sujet. Elle procède à la comparaison des codes de réseau de plusieurs pays et d'ensembles régionaux, analysant leurs orientations en matière de traitement de la cybersécurité pour le secteur électrique. Elle prend en compte le cadre institutionnel et réglementaire de la cybersécurité des zones analysées, notamment pour comprendre le traitement réservé aux infrastructures critiques. L'analyse comparative menée a vocation à identifier les bonnes pratiques internationales et les opportunités d'amélioration des codes de réseau existants dans différents pays. Elle est destinée à la fois aux décideurs, afin de mieux intégrer ce sujet au niveau de la gouvernance et de réglementation sectorielle, mais aussi aux équipes opérationnelles intervenant sur les thématiques cyber, afin de pouvoir comparer leurs pratiques à celles d'autres organisations similaires.

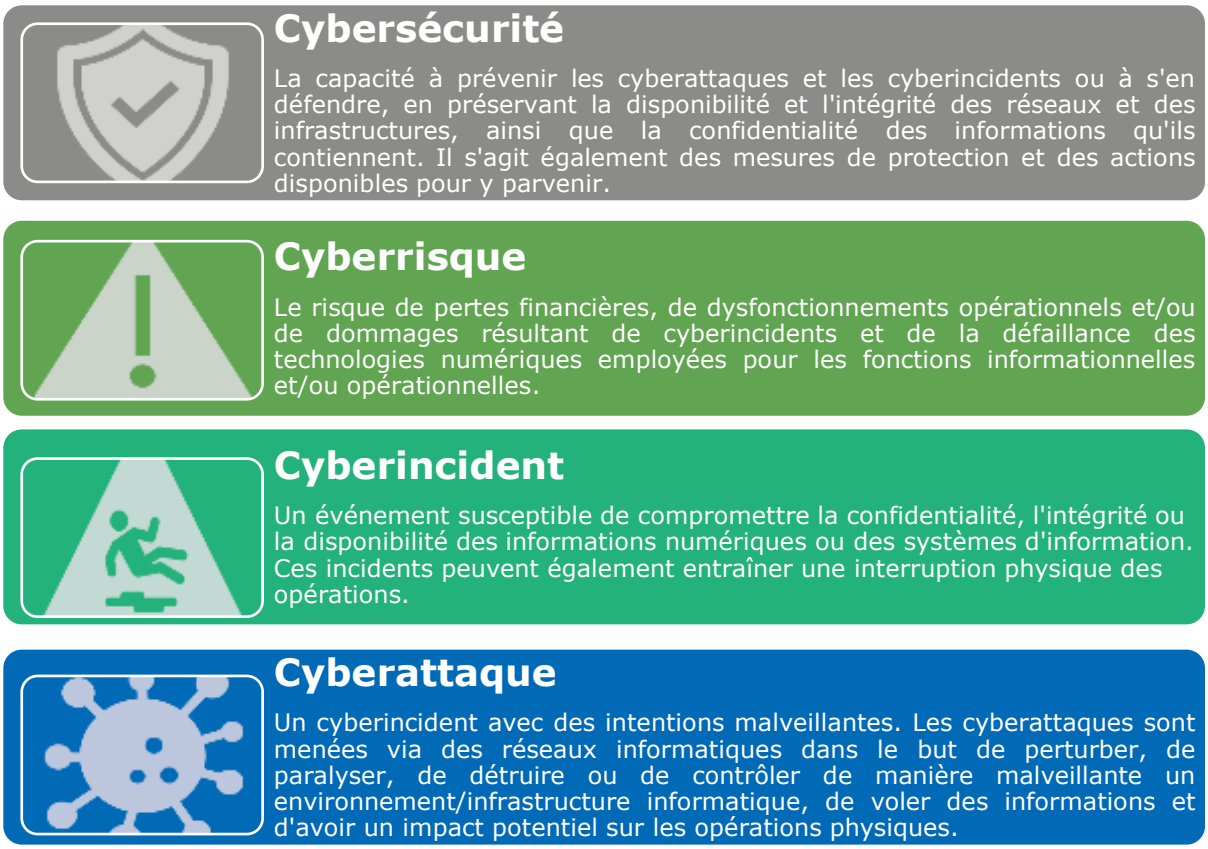


Figure 1 : Lexique cyber de l'AIE (traduit de l'anglais)

1. RENFORCER LE CADRE JURIDIQUE POUR FAIRE FACE AUX CYBERMENACES

Le secteur de l'électricité fait face à des menaces croissantes dans le cyberespace, avec des cyberattaques et cyberincidents pouvant entraîner des conséquences graves dans le monde physique. Étant donné la multiplicité des acteurs impliqués dans la gestion et l'exploitation des infrastructures électriques, il devient impératif d'harmoniser et de renforcer leur niveau de protection. Cela nécessite notamment l'adoption d'un cadre légal et réglementaire approprié imposant des obligations strictes et cohérentes à toutes les parties prenantes.

1.1. L'émergence des cybermenaces dans le secteur électrique

1.1.1. Le secteur électrique : une cible privilégiée pour les cyberattaques

Le secteur de l'énergie en général et de l'électricité en particulier est un des plus visés par les cyberattaques. L'industrie énergétique connaît en effet une transformation numérique profonde, modifiant les méthodes de production, de transformation, de stockage, de transport et de consommation de l'énergie. L'expansion significative des dispositifs de l'Internet industriel des objets (IIoT) s'est accompagnée d'une connectivité accrue et conduit à une augmentation sans précédent du volume des données. Les systèmes électriques modernes sont de plus en plus interconnectés et automatisés, notamment grâce aux réseaux intelligents (*smart grids*) et aux systèmes de gestion avancée des infrastructures énergétiques.

Toutes ces évolutions technologiques offrent de nombreux avantages, tels que l'amélioration de l'efficacité énergétique, la gestion intelligente des réseaux, et une meilleure intégration des sources d'énergie renouvelable. Cependant, elles exposent le secteur à de nouvelles formes de vulnérabilités et de risques. Elles créent de nouvelles opportunités pour les cyberattaquants de pénétrer dans le réseau et de compromettre la sécurité des systèmes de contrôle industriels (ICS) qui supervisent les opérations des infrastructures électriques.

Le réseau électrique est donc devenu est une cible de choix en raison de son rôle central dans le fonctionnement des sociétés modernes. Toute perturbation majeure dans l'approvisionnement en électricité peut avoir des effets en cascade sur d'autres infrastructures critiques, entraînant des pannes massives, des interruptions de services essentiels, et des conséquences économiques et sociales graves. S'attaquer au réseau d'électricité permet de toucher par effet domino la quasi-totalité des activités essentielles au bon fonctionnement de la société.

Le tableau ci-dessous rassemble les principales cyberattaques réussies contre les infrastructures électriques depuis le début des années 2000.

Tableau 1 : Cyberattaques réussies sur les infrastructures électriques

Date	Pays	Description
17 déc. 2016	Ukraine	• Des cybercriminels ont attaqué un poste électrique Haute tension à Kiev, la capitale de l'Ukraine.

		• Le malware appelé Industroyer (ou CrashOverride) a été utilisé. Il est considéré comme l'un des malwares les plus sophistiqués ciblant spécifiquement les systèmes de contrôle industriels (ICS). • Cette attaque a provoqué une panne d'électricité d'environ une heure dans une partie de Kiev et de ses environs, affectant des centaines de milliers de personnes.
23 déc. 2015	Ukraine	• 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.
Déc. 2014	Corée du Sud	• Attaque visant la Korea Hydro & Nuclear Power (KHNP), l'opérateur gérant les réacteurs nucléaires et les systèmes hydroélectriques de Corée du Sud. • Les cybercriminels ont réussi à infiltrer les systèmes de l'entreprise et à voler des informations sensibles, tel que des schémas techniques, des manuels d'instructions pour les réacteurs nucléaires et des informations personnelles sur les employés de la KHNP. Cependant, les systèmes critiques directement liés à la gestion des réacteurs n'ont pas été affectés, car ils étaient isolés physiquement des réseaux externes. • L'attaque n'a pas perturbé directement les opérations des centrales nucléaires, mais elle a créé une grande inquiétude quant à la sécurité des infrastructures critiques sud-coréennes.
2013	Etats-Unis	• La cyberattaque a ciblé le Bowman Avenue Dam, un petit barrage situé à Rye Brook, dans l'État de New York. • Les cybercriminels ont réussi à pénétrer dans les systèmes de contrôle du barrage. Ils ont accédé aux systèmes SCADA. • Bien que l'attaque n'ait pas causé de dégâts physiques ou d'interruptions majeures, elle a suscité une vive inquiétude. Elle a révélé la vulnérabilité des infrastructures critiques, même les plus petites, aux cyberattaques.
Octobre 2001	Etats-Unis	• L'attaque a ciblé le California Independent System Operator (CAISO), l'opérateur du système électrique en Californie. • Les cybercriminels ont réussi à accéder aux systèmes informatiques de CAISO et à s'immiscer dans l'exploitation du réseau électrique. • Cette attaque n'a pas entraîné de pannes majeures ou de perturbations directes dans la distribution d'électricité, mais

		elle a mis en évidence des faiblesses dans la cybersécurité des systèmes de gestion des infrastructures critiques.

Une recrudescence des cyberattaques à l'encontre des infrastructures électriques est constatée 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.

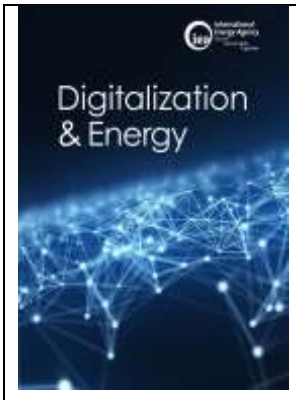
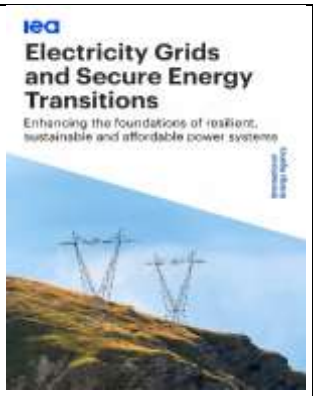
1.1.2. Une prise de conscience internationale

La prise de conscience par les États de l'émergence des cybermenaces, en particulier dans le cadre des infrastructures critiques comme les réseaux électriques, s'est accélérée au cours de la dernière décennie notamment sont l'effet des cyberattaques ci-avant présentées. Des attaques ont montré que les systèmes d'énergie et d'autres infrastructures critiques étaient vulnérables à des cyberattaques sophistiquées.

De manière générale, les Etats ont pris conscience que dans un contexte d'ouverture du système électrique à une pluralité d'acteurs, il n'était pas possible de déployer une stratégie de défense sans la mise en place de règles de nature juridique. Ils ont ainsi créé ou renforcé le cadre juridique s'appliquant aux infrastructures critiques et à leurs systèmes d'informations. De nombreuses stratégies et politiques visant à protéger les infrastructures critiques et à prévenir les cyberattaques majeures ont ainsi vu le jour.

Le renforcement de la cybersécurité est désormais un impératif qui évolue au fur et à mesure des évolutions technologiques et donc des menaces associées. Ces dernières années, l'Agence internationale de l'énergie (AIE) a plusieurs fois souligné dans ses rapports la nécessité de réhausser la cybersécurité du secteur de l'électricité, pointant la hausse constante des attaques constatées et la croissance continue des menaces. Le tableau ci-dessous mentionne plusieurs rapports récents de l'AIE contenant des développements sur ce sujet d'importance crucial.

Tableau 2 : Rapports de l'AIE d'intérêt sur le sujet de la cybersécurité du secteur de l'électricité

			
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

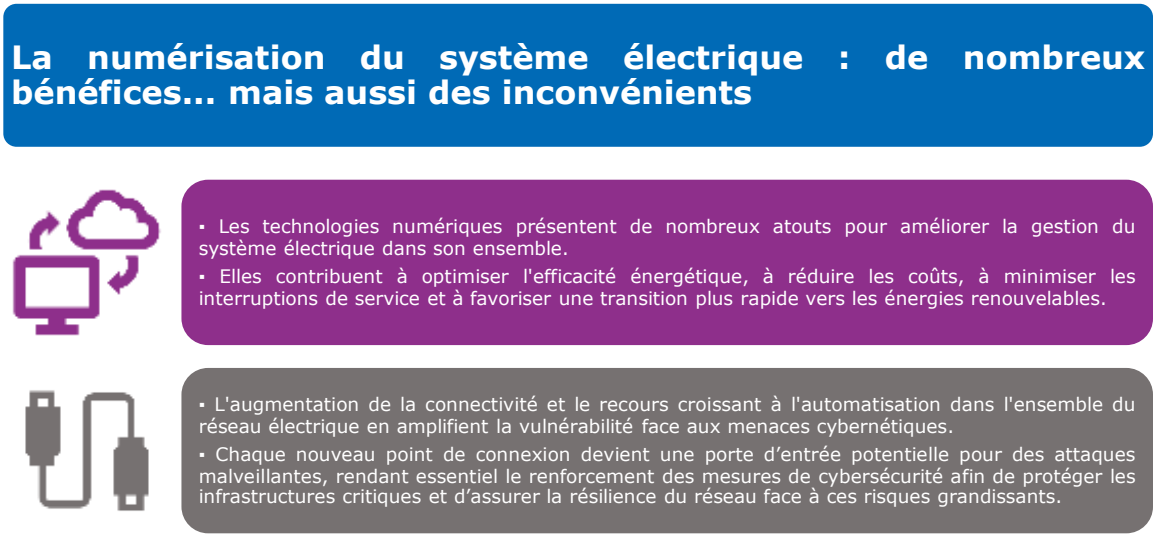


Figure 2 : La numérisation du secteur électrique : des bénéfices et des inconvénients

1.2. Outils juridiques et institutionnels pertinents en matière de cybersécurité

L'adoption d'un cadre juridique et institutionnel adapté au traitement des cybermenaces fait partie des mesures fondamentales pour répondre à cet enjeu. Pour les Etats, le renforcement de la cybersécurité des infrastructures électriques s'inscrit dans une démarche plus large de rehaussement des exigences de sûreté de toutes les infrastructures qui sont au service des activités les plus importantes d'un pays. Un cadre légal propre aux « infrastructures critiques » s'est ainsi progressivement développé partout dans le monde devenant aujourd'hui un standard juridique quasi-incontournable. Dans ce contexte, les codes de réseau se positionnent comme des outils complémentaires, spécifiques au secteur de l'électricité et en particulier aux réseaux de transport d'électricité.

1.2.1. La loi au service de la protection des infrastructures critiques

Dans de nombreux pays, des lois et décrets ont été adoptés pour protéger les infrastructures électriques en imposant aux gestionnaires de ces infrastructures des règles de sécurité strictes.

- **La notion d'infrastructure critique**

La notion « d'infrastructure critique » est apparue dans les textes officiels vers le milieu des années 1990 aux Etats-Unis, en réponse à l'émergence de nouvelles menaces, notamment terroristes. Elle est donc associée à des préoccupations de sécurité nationale.

Les infrastructures critiques sont celles qui apportent des services essentiels à la société et dont le fonctionnement défectueux ou la destruction affaiblirait considérablement la

défense ou l'économie du pays concerné, voire pourrait causer des dommages physiques ou la mort.

Par définition, une défaillance majeure d'un ou plusieurs opérateurs (publics ou privés) en charge de la gestion de ces infrastructures critiques peut provoquer un chaos économique, perturber des services essentiels, déstabiliser un État, et même menacer directement la sécurité des citoyens. Ces infrastructures sont notamment celles de secteurs particulièrement importants : transports, communications, services financiers, santé, approvisionnement en eau, agriculture. Le secteur de l'énergie en fait évidemment partie tant il est au centre de nos systèmes économiques et de nos modes de vie actuels.

Le concept d'infrastructure critique s'est diffusé en dehors des États-Unis dans de nombreux pays dans un contexte de renforcement de la prise en compte des menaces pour la sécurité nationale. Des ministères et agences spécifiques ont été chargés de sa mise en œuvre. Il se concrétise par la mise en place de règles propres à ce type d'infrastructures et visant leur identification et le durcissement de leur sécurité et de leur résilience. La qualification d'infrastructure critique est un levier pour des exigences sécuritaires : une fois une infrastructure qualifiée de critique, elle peut être soumise à une surveillance et des exigences spécifiques.

Il est important de souligner que les infrastructures critiques, essentielles au bon fonctionnement d'une nation, peuvent être détenues ou exploitées aussi bien par le secteur public que par le secteur privé. Qu'elles relèvent de l'une ou l'autre sphère, ces infrastructures sont stratégiques pour la sécurité nationale. Par conséquent, l'État a un rôle fondamental à jouer en tant que garant de cette sécurité. Il lui incombe de veiller à la protection de ces infrastructures en s'assurant de la cohérence des politiques de sécurité et du respect d'un niveau d'exigence uniforme et adapté par tous les opérateurs, qu'ils soient publics ou privés.

Cette intervention de l'État est d'autant plus cruciale face à des menaces en constante évolution, qu'elles soient physiques, cybernétiques ou d'ordre naturel. Dans ce cadre, l'État doit non seulement imposer des normes de sécurité strictes, mais aussi coordonner les efforts de l'ensemble des acteurs concernés, afin de garantir la résilience et la continuité des services essentiels pour la population et l'économie du pays.

- **L'édiction d'exigences propres à la cybersécurité des systèmes d'information critiques**

Les vulnérabilités potentielles des infrastructures critiques sont physiques mais également cyber. En effet, les infrastructures critiques reposent et dépendent aujourd'hui quasi-systématiquement sur des systèmes et réseaux d'information interconnectés. Les systèmes d'information industriels (ou systèmes de contrôle industriel, tels que les SCADA) sont de plus en plus utilisés pour surveiller et contrôler des processus industriels dans divers secteurs comme l'énergie. La vulnérabilité croissante des systèmes d'information critiques est notamment le résultat de la convergence toujours plus grande entre les technologies de l'information (IT) et les technologies opérationnelles (OT).

Par prolongement à la notion d'infrastructure critique s'est donc aussi développée la notion **de système d'information critique**. Un cadre juridique protecteur associé a vu le jour encouragé par les instances internationales telles que l'OCDE qui a adopté une

Recommandation *sur la protection des infrastructures d'information critiques* le 30 avril 2008[1].

En bref :

Un système d'information industriel est qualifié de système d'information critique lorsqu'il joue un rôle essentiel dans le maintien des services vitaux pour la société, c'est qui est souvent le cas dans les processus industriel du secteur électrique.

Les lois visant à protéger les infrastructures critiques ont donc intégré la dimension cyber et incluent de manière générale des exigences pour les systèmes d'information.

Une des règlementations les plus abouties en la matière est celle édictée par l'Union européenne : la directive « Sécurité des réseaux et de l'information » (dite « Directive NIS », de son nom anglais *Network and Information System Security*)[2]. Ce texte a été adoptée le 6 juillet 2016 avec pour objectif d'augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activité en mettant en place des règles de gouvernance de la cybersécurité, de coopération, et en déterminant des obligations spécifiques pour les fournisseurs de services numériques et les Opérateurs de Services Essentiels, définis comme les entités publiques ou privées qui fournissent un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques, dont la fourniture dudit service est tributaire des réseaux et des systèmes d'information et pour lequel un incident pourrait aboutir à une suspension de fourniture dudit service. Cette définition inclut donc un certain nombre d'acteurs du secteur électrique.

Plusieurs obligations développées notamment par la Directive NIS sont devenues des standards internationaux :

- **Identification des opérateurs de services essentiels/d'infrastructures critiques** ;
- **Identification des systèmes d'information critiques / essentiels** : à la charge des opérateurs, cette obligation constitue la base permettant d'analyser les risques et adopter des mesures de sécurité adaptées ;
- **Mise en œuvre de mesures techniques et organisationnelles appropriées pour gérer les risques** ;
- **Obligation de signalement des incidents de cybersécurité aux autorités compétentes** : exiger des opérateurs d'infrastructures critiques qu'ils signalent les incidents permet une meilleure coordination et réponse en cas de crise.

[1] Cette recommandation a été abrogée par le Conseil le 11 décembre 2019 et remplacée par la Recommandation *sur la sécurité numérique des activités critiques* [OECD/LEGAL/0456].
[2] La directive NIS a récemment été révisée (adoption de la Directive NIS 2 en décembre 2022). Le nouveau texte renforce et d'élargit les obligations dans une optique d'améliorer encore la cybersécurité au niveau européen.

De même, différents outils peuvent être mis en place par l'adoption de textes législatifs ou réglementaires et contribuer à renforcer la cybersécurité de ces infrastructures :

- **L'adoption de stratégies nationales de cybersécurité :** les stratégies nationales permettent d'établir un cadre général pour la cybersécurité. Elles définissent généralement les priorités nationales, les objectifs et les moyens à mobiliser. Elles incluent généralement la stratégie de sécurisation des infrastructures critiques ;
- **La création d'agence nationales dédiées à la cybersécurité :** ces agences spécialisées ont tendance à se généraliser partout dans le monde. Différentes missions peuvent leur être attribuées mais elles sont globalement en charge de concentrer l'expertise juridique et technique en matière de cybersécurité et de coordonner les efforts au niveau national. Elles veillent à la mise en œuvre des mesures de protection des systèmes d'information des infrastructures critiques, et interviennent souvent en soutien aux opérateurs de ces infrastructures ;
- La création de **centres d'analyse et de partage d'informations** : ces centres, également appelés **Information Sharing and Analysis Centers (ISACs)**, facilitent l'échange d'informations entre acteurs publics et privés sur les menaces, les vulnérabilités, et les bonnes pratiques de sécurité entre les opérateurs d'infrastructures critiques ;
- Les **CERT** (*computer emergency response team*) ou **CSIRT** (*computer security incident response team*) sont des équipes chargées d'organiser la réaction aux incidents de sécurité informatique, créées pour détecter, analyser et répondre aux cyberattaques. Ils jouent un rôle essentiel dans la cybersécurité des infrastructures critiques en fournissant un soutien technique, en surveillant les menaces et en coordonnant les réponses en cas de cyberincident. Les CERT peuvent être nationaux, sectoriels ou internes à une organisation.

Les **normes techniques internationales**, telles que celles du NIST ou de l'ISO/IEC, fournissent un cadre méthodologique pour aider les États et les entreprises à gérer la cybersécurité des infrastructures critiques. Ces normes sont souvent intégrées ou mentionnées dans les législations nationales comme des références obligatoires ou des recommandations.

1.2.2. Les codes de réseau : un outil au service de la résilience du système électrique

1.2.2.1. Un outil incontournable pour la fiabilité du système électrique

Le terme « code de réseau » ou « grid code » en anglais est largement utilisé pour désigner un document (ou un ensemble de documents) qui établit juridiquement les exigences techniques et autres pour le raccordement et l'utilisation 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.

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

Le rôle des codes de réseau selon l'IRENA

*« La mise en œuvre de ces codes donne aux gestionnaires de réseau **l'assurance que les actifs connectés au réseau ne mettront pas en péril la sécurité de l'approvisionnement en électricité**. L'établissement d'un code de réseau est une étape importante dans **l'ouverture du secteur de l'électricité** aux développeurs privés ou aux nouveaux exploitants de centrales et permet une intégration efficace des producteurs d'EnR intermittentes. L'objectif des codes de réseau est multiple et consiste notamment à **assurer la coordination entre les différents acteurs, à accroître la transparence, la sécurité du réseau, la fiabilité et l'intégration des EnR**. Les codes de réseau énumèrent les exigences techniques à respecter pour assurer le bon fonctionnement du système et instaurer la confiance entre les acteurs du réseau électrique. Ils englobent différents aspects du système électrique, tels que les marchés, l'exploitation, la planification et le raccordement ».*

Extrait traduit de l'anglais du rapport : IRENA (2022), Grid codes for renewable powered systems, International Renewable Energy Agency, Abu Dhabi. ISBN: 978-92-9260-427-1

Les codes de réseau sont conçus pour assurer la sécurité, la fiabilité, la qualité et l'efficacité du réseau électrique. En ce sens, ils participent à la rationalisation, à la sécurisation et à la modernisation des pratiques en faisant émerger des standards d'exploitation dans le contexte de marchés de l'électricité de plus en plus ouverts où la gestion du système électrique tend à dépendre d'une pluralité d'acteurs.

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

1.2.2.2. Un véhicule réglementaire utilisé pour introduire des règles de cybersécurité

Au cœur du fonctionnement technique du système électrique, les codes de réseau sont un outil contribuant à affronter les défis et menaces rencontrés actuellement dans le secteur de l'électricité. Des évolutions technologiques majeures sont en œuvre et modifient les pratiques et les exigences qui étaient autrefois en vigueur : intégration des énergies renouvelables, développement de nouvelles technologies (*smart grids*, batteries, interconnexions…). La cybersécurité en fait partie étant donné qu'elle est des éléments incontournables pour la sécurité l'exploitation du réseau.

La cybersécurité est en train de devenir un sujet incontournable des codes de réseau. L'IRENA l'a souligné dans le rapport précité : « *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 ».*

Le gestionnaire du réseau électrique n'a, en principe, pas la compétence pour établir les règles de cybersécurité applicables aux acteurs privés, car ces règles relèvent généralement des prérogatives de l'État, dans le cadre de ses pouvoirs de police et de protection de la sécurité intérieure. Toutefois, on observe que de plus en plus de codes de réseau intègrent des dispositions dédiées à la cybersécurité :

- Plusieurs pays ont intégré des dispositions techniques en lien avec ce sujet 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 »).

Ces codes, qui sont gérés par les opérateurs de réseau et souvent approuvés par les autorités de régulation sectorielles, introduisent des obligations de sécurité pour les acteurs connectés au réseau, bien que la compétence traditionnelle en matière de cybersécurité demeure celle des autorités publiques. Cette situation découle de la nécessité de protéger l'intégrité du réseau électrique, considéré comme une infrastructure critique.

L'interconnexion croissante des systèmes électriques et l'évolution des menaces, notamment les cyberattaques, ont poussé les gestionnaires de réseaux à jouer un rôle actif dans l'élaboration et l'application de règles de cybersécurité. Ces dernières s'imposent non seulement aux opérateurs eux-mêmes, mais aussi aux entités privées qui interagissent avec le réseau, afin de prévenir toute vulnérabilité pouvant mettre en danger le système électrique.

Cependant, on constate que le contenu des règles insérées dans les codes de réseau n'est pas uniforme selon le pays ou l'opérateur concerné, et qu'il n'y a pas encore clairement de contenu standard concernant la cybersécurité. L'analyse comparative menée dans ce rapport vise à 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.

La liste des pays étudiés dans ce rapport a été établie sur la base de plusieurs critères croisés et principalement leur niveau de maturité concernant la réponse institutionnelle et juridique en matière de cybersécurité et l'existence de dispositions dédiées à la cybersécurité au sein de leurs codes de réseau.

2. CYBERSECURITE : UNE INTEGRATION CROISSANTE DANS LES CODES DE RESEAU ÉLECTRIQUE

2.1. La France

La France s'est impliquée dans le sujet de la cybersécurité à partir du milieu des années 2000. Plusieurs rapports officiels ont mis en évidence le constat selon lequel la multiplication des attaques informatiques étaient inévitables dans les années à venir, et que la France n'était pas prête à y faire face. Les pouvoirs publics ont mis en place les moyens nécessaires pour créer un cadre permettant d'atténuer les vulnérabilités constatées. C'est ainsi qu'ont été posées les bases d'une cybersécurité à la française, reconnue aujourd'hui pour sa solidité.

2.1.1. Protection des infrastructures critiques et de leurs systèmes d'information

2.1.1.1. Stratégie

La France est dotée d'un document de politique générale de cybersécurité intitulé « Stratégie nationale pour la sécurité du numérique (2015). Ce document évoque de prime abord l'objectif de renforcement de la sécurité des infrastructures critiques : « *La France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace. Elle consolidera la sécurité numérique de ses infrastructures critiques et œuvrera pour celle de ses opérateurs essentiels à l'économie* ».

Il est essentiel de noter qu'en tant qu'État membre de l'Union européenne, la France est tenue de respecter et de mettre en œuvre le droit de l'UE, ainsi que de suivre les politiques communes définies au niveau européen, notamment en ce qui concerne la cybersécurité.

2.1.1.2. Cadre légal

La protection des infrastructures critiques en France relève à la fois d'une logique de défense militaire et de sécurité intérieure. Son cadre juridique donc été mis en place par des lois successives de programmation militaire. Les règles en vigueur sont rassemblées au sein du Code de la défense.

En 2006, un dispositif appelé Secteur d'activité d'importance vitale (SAIV) a été instauré pour protéger les opérateurs essentiels à la survie de la nation contre diverses menaces, telles que le terrorisme, le sabotage, les cyberattaques, ainsi que contre les risques naturels, technologiques ou sanitaires. Ces opérateurs, identifiés par les ministères compétents, sont officiellement désignés comme « Opérateurs d'importance vitale » (OIV) par arrêté[3]. Cette notion correspond à la version française des « infrastructures critiques » évoquées précédemment. L'énergie fait partie de ces secteurs. La liste de leurs infrastructures critiques, dénommés « Points d'importance vitales » est classée « secret défense ».

[3] La France compte environ 300 entreprises dans 12 secteurs d'activité et organismes publics et privés considérés comme des « Opérateurs d'importance vitale » (OIV) par le Code de la défense, c'est-à-dire dont les activités ont été jugées indispensables au bon fonctionnement et à la survie de la nation.

Pour faire face à l'augmentation en quantité et en sophistication des attaques informatiques, l'article 22 de la Loi de programmation militaire de 2013 a complété le dispositif de protection des « infrastructures d'importance vitale ». La sécurité des systèmes d'information critiques a été renforcé par la création **d'un dispositif spécifique aux Systèmes d'information d'importance vitale (SIIV), notamment :**

- Les OIV doivent identifier et déclarer leurs systèmes d'information d'importance vitale ;
- Les OIV doivent notifier directement l'ANSSI des incidents affectant leurs SIIV ;
- L'ANSSI définit les règles techniques et organisationnelles de sécurité des systèmes d'information devant être appliquées par l'opérateur à ses SIIV. Elles sont au nombre de 20 et adressent les thématiques suivantes : gouvernance et pilotage de la sécurité informatique, maîtrise des risques, maîtrise des systèmes d'information, gestion des incidents de sécurité, protection des systèmes d'information. Les exigences sont définies pour chaque SAIV dans des arrêtés sectoriels pris par le Premier ministre.

Comment déterminer si un système d'information est un SIIV ?

« Pour déterminer si un système d'information (SI) est un SI d'importance vitale (SIIV), les Opérateurs d'importance vitale (OIV) doivent mener, selon la méthode de leur choix, une analyse des impacts sur leurs activités vitales qui peuvent résulter d'une atteinte à la sécurité ou au fonctionnement du système. Les OIV doivent impérativement mener ces analyses pour certains types de systèmes d'information pré déterminés pour leur secteur d'activité ». (Source : https://cyber.gouv.fr/)

2.1.1.3. Principales institutions

- **L'ANSSI**

En 2009, le décret n° 2009-834 du 7 juillet 2009 crée l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Elle constitue un service du Premier ministre et est placée sous l'autorité du secrétaire général de la défense et de la sécurité nationale. Au cœur du dispositif de cyberdéfense français, l'ANSSI a pour mission de veiller à la sécurité des systèmes d'information de l'État, mais également de conseiller et de soutenir les administrations et les opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

L'ANSSI est dans une démarche globale d'ouverture et de partage d'outils permettant d'accompagner la sécurisation des opérateurs OIV ou OSE. L'ANSSI peut également déclencher des contrôles de sécurité afin d'évaluer le niveau de sécurité de l'OIV.

- **La CRE**

La Commission de régulation de l'énergie (CRE) est une autorité administrative indépendante française créée le 24 mars 2000, chargée de veiller au bon fonctionnement du marché de l'énergie et d'arbitrer les différends entre les utilisateurs et les divers

exploitants, en suivant les objectifs de la politique énergétique. Sa compétence de régulateur s'étend aux marchés du gaz et de l'électricité.

Bien qu'intervenant marginalement sur le sujet de la cybersécurité, la CRE n'a pas de compétence réglementaire attribuée officiellement dans ce domaine.

2.1.2. Règles de cybersécurité du secteur de l'électricité

Le Premier ministre détient en France le pouvoir d'édicter les règlements en lien avec la cybersécurité des opérateurs électriques. L'arrêté du 11 août 2016 a fixé les règles de sécurité que les opérateurs d'importance vitale du sous-secteur « approvisionnement en énergie électrique » sont tenus de respecter pour protéger leurs systèmes d'information. Le tableau ci-dessous présente certaines dispositions de ce décret :

Tableau 3 : Principales exigences de l'arrêté du 11 août 2016

Intitulé de l'exigence	Principe
Déclaration des systèmes d'information d'importance vitale	L'OIV doit identifier et transmettre à l'ANSSI la liste de systèmes d'information d'importance vitale (SIIV).
Déclaration des incidents de sécurité	L'OIV doit notifier directement l'ANSSI les incidents affectant leurs SIIV. Les types d'incidents à notifier sont spécifiques aux secteurs et précisés à l'annexe IV de l'arrêté du 11 août 2016.
Règle relative à la politique de sécurité des systèmes d'information	L'OIV élabore, tient à jour et met en œuvre une politique de sécurité des systèmes d'information (PSSI).
Règle relative à l'homologation de sécurité	L'OIV procède à l'homologation de sécurité de chaque SIIV, en mettant en œuvre la procédure d'homologation prévue par sa PSSI. Dans le cadre de l'homologation, un audit de la sécurité du SIIV doit être réalisé.
Règle relative à la cartographie	L'OIV doit être en mesure de fournir à l'ANSSI, pour chaque système d'information d'importance vitale (SIIV), les éléments de cartographie précisés dans l'arrêté.
Règle relative au maintien en conditions de sécurité	L'OIV élabore, tient à jour et met en œuvre une procédure de maintien en conditions de sécurité des ressources matérielles et logicielles de ses SIIV, conformément à sa politique de sécurité des systèmes d'information.
Règle relative au traitement des incidents de sécurité	L'OIV élabore, tient à jour et met en œuvre une procédure de traitement des incidents affectant le fonctionnement ou la sécurité de ses SIIV, conformément à sa politique de sécurité des systèmes d'information.
Règle relative au traitement des alertes	L'OIV met en place un service de permanence lui permettant de prendre connaissance, à tout moment et sans délai, d'informations transmises par l'ANSSI relatives à des incidents, des vulnérabilités et des menaces. Il met en œuvre une procédure pour traiter les informations ainsi reçues et le cas échéant prendre les mesures de sécurité nécessaires à la protection de ses SIIV. L'opérateur communique à l'ANSSI les coordonnées (nom du service, numéro de téléphone et adresse électronique) tenues à jour du service de permanence.
Règle relative à la gestion de crises	L'OIV élabore, tient à jour et met en œuvre une procédure de gestion de crises en cas d'attaques informatiques majeures, conformément à sa PSSI.
Règle relative à l'authentification	L'OIV protège les accès aux ressources de ses SIIV, que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification basé sur un

	élément secret. Il doit respecter certaines règles précisées dans le décret.

Bien d'autres règles opérationnelles sont édictées par ce décret, notamment des règles relatives à l'authentification, aux droits d'accès, aux comptes d'administration, aux accès à distance, etc.

Un arrêté du Premier ministre du 14 septembre 2018 adopté sur proposition de l'ANSSI, a fixé le même type de règles à une autre catégorie d'opérateurs dénommés les « Opérateurs de services essentiels » (OSE) dont font partie certains acteurs du secteur de l'électricité. Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Elles définissent les mesures appropriées pour prévenir les incidents qui compromettent la sécurité des réseaux et systèmes d'information utilisés pour la fourniture des services essentiels ou pour en limiter l'impact afin d'assurer la continuité de ces services essentiels.

Les OIV comme les OSE sont tenus d'appliquer les règles de renforcement de leur cybersécurité ci-avant énoncées à leurs frais.

2.1.3. La Documentation technique de référence de RTE : le code de réseau de transport français

La Documentation technique de référence de RTE (DTR) constitue un ensemble de prescriptions, droits et obligations qui régissent d'une manière générale les interactions de nature technique et contractuelle entre RTE, le gestionnaire de réseau de transport et l'opérateur du système, et ses clients. Cette DTR fait figure de documentation applicative des dispositions analogues à un code de réseau.

Cette documentation ne contient donc pas à proprement parler de section explicitant la stratégie ou l'organisation de RTE en matière de cybersécurité, qui reste interne à l'opérateur. En revanche, en présentant les exigences de RTE vis-à-vis de ses clients pour accéder à son réseau de télécommunication, la DTR reflète pour une part certains enjeux et aspects structurants de cette organisation consistant en général à faire peser sur le client des obligations de sécurité en échange de son accès au réseau de données de l'opérateur.

2.1.3.1. Analyses des dispositions de la DTR en lien avec la cybersécurité

Les exigences de RTE en matière de connexion à son réseau de téléconduite concernent plus particulièrement la mise en place par RTE d'un réseau de télécommunication en propre, les conditions de raccordement des réseaux télécom des clients au réseau de téléconduite de RTE et la coordination entre RTE et ses clients pour l'utilisation de ce réseau et plus largement pour leurs échanges d'informations.

- **Un réseau de télécommunication dédié**

La DTR définit le « réseau de téléconduite RTE » comme le « *réseau de télécommunications longue distance qui supporte les échanges de téléconduite, de téléphonie de sécurité et de sauvegarde entre les centres de conduite de RTE et du Client* » (Art. 8.25.1 §4 de la DTR).

Ce réseau de télécommunication, qui fait l'objet d'une infrastructure télécom dédiée (physiquement séparé du réseau utilisé pour Internet) est opérée en IP par un protocole spécifique dénommé INUIT, établissant un plan d'adressage (Art. 8.25.1 §3 de la DTR).

Pour assurer la maîtrise de cette infrastructure :

- RTE exige que la connexion de ses clients à ce réseau de téléconduite RTE se fasse à un point de connexion établi sur son territoire de desserte, en France métropolitaine continentale (Art. 4.7.1, § 6.1 de la DTR) ;
- RTE conserve la responsabilité exclusive de la maintenance et l'exploitation de ce réseau (Art. 4.7.1, § 6.2 de la DTR).

- **Les conditions de raccordement du réseau télécom du client au réseau de téléconduite RTE**

Parmi les obligations du client pour se raccorder au réseau de puissance de RTE, le client doit se conformer aux règles de raccordement de son réseau télécom au réseau de téléconduite RTE. Ces règles sont émises dans un « **cahier des charges télécom-téléconduite** » annexé à la convention de raccordement et dont la trame est publiée dans la DTR (sous réserve de certaines annexes non publiées et uniquement transmises au client au moment de leur raccordement).

Les règles de connexion au réseau de télécommunication de RTE émises dans ce cahier des charges concernent le « réseau local » du client défini par la DTR de RTE comme le réseau « *situé sur un Site Client, et sur lequel sont connectés les équipements de téléconduite en interface avec RTE* ». Elles s'appliquent également en cas de connexion au réseau de télécommunication de RTE des « centres de conduite » des clients (c'est-à-dire « regroupant en un même lieu la conduite de plusieurs installations de production »), si ceux-ci sont établis sur des sites différentes de leurs installations raccordées au réseau de puissance.

Pour assurer le partage des informations, RTE transmet un plan d'adressage au client (Art. 8.25.1 §7.1.1 de la DTR).

En ce qui concerne les engagements du client, la DTR prévoit d'abord le principe d'encapsulation du réseau local à l'intérieur des sites du client : par exemple, en ce qui concerne le raccordement des producteurs, « *les équipements de téléconduite du client sont installés sur les sites de production ou dans un centre de conduite* ».

Plus précisément, les différents cas de figure d'organisation du Client sont décrits dans le cahier des charges téléconduite (Article 8.25.1 de la Documentation Technique de Référence). On retrouve les cas de figure suivants :

- Cas 1 : conduite locale sur le même site que la production ;
- Cas 2 : conduite déportée de la production ;
- Cas 3 : conduite centralisée de la production (centre de conduite déportée, site de téléconduite déportée des sites de production).

Une fois définis les réseaux des clients soumis aux prescriptions de RTE, la DTR énonce le principe de responsabilité du client sur l'exploitation et la maintenance de son « réseau local » (Art. 4.7.1, § 6.2 de la DTR), dont les limites sont définies par le schéma de principe ci-dessous :

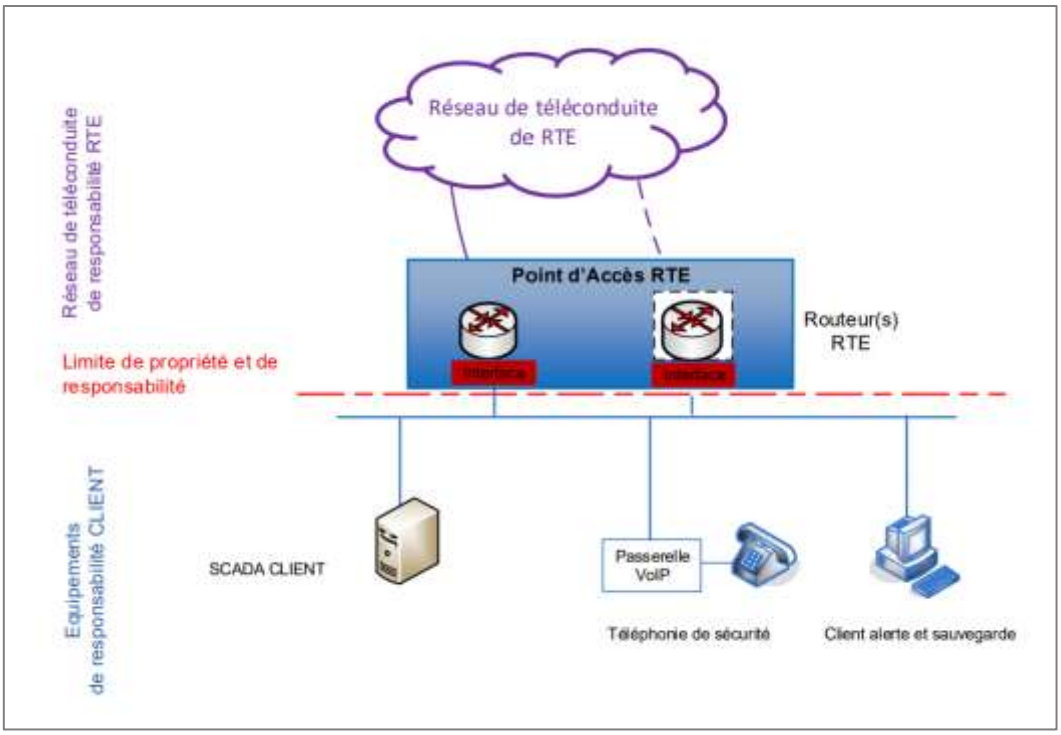


Figure 3 : Limites de propriété et de responsabilité - schéma de principe de la connexion du réseau local au réseau de téléconduite de RTE (Art. 4.7.1 § 6.2 de la DTR).

En outre, à l'issue de la mise en service de ses équipements, et préalablement aux premiers échanges d'informations avec RTE, le Client doit fournir à RTE :

- Une attestation de réalisation des systèmes dédiés aux échanges d'informations en conformité avec les cahiers des charges annexés à la convention de raccordement ;
- Un schéma qui représente l'architecture technique de ces systèmes : équipements de sécurité, de télécommunication et de téléconduite (matériels et logiciels), connexions éventuelles avec le système d'information du Client ;
- Un plan qualité des systèmes dédiés aux échanges d'informations, précisant les dispositions retenues pour l'administration, l'exploitation, la maintenance ainsi que le traitement des dysfonctionnements des équipements du Client ;
- Une **attestation de conformité aux exigences spécifiques non publiées de cybersécurité de RTE**.

- **La coordination opérationnelle entre RTE et ses clients pour l'utilisation du réseau de téléconduite de RTE**

De nombreuses dispositions sont mises en œuvre pendant la phase d'exploitation de l'installation raccordée au réseau pour assurer le maintien dans le temps de la sécurité opérationnelle.

Préalablement à la mise en exploitation des échanges d'informations avec l'installation du client, puis pendant toute sa durée de vie, RTE et le Client programment et réalisent des essais visant à en vérifier le bon fonctionnement et le respect des performances attendues (cf. trame de contrôle de conformité pour une unité de production : article 8.3.3 de la Documentation Technique de Référence). Le résultat de ces tests est consigné dans un PV

de recette. L'absence de non-conformités susceptibles d'affecter la sûreté du système électrique et/ou la sécurité des personnes et des biens conditionne l'accès au réseau définitif de l'installation (Art. 4.7.1 § 6.4 de la DTR).

Si la recette comporte des réserves imputables à l'une des parties (ou des tiers placés sous sa responsabilité), la levée de ces réserves ainsi que la réalisation des essais de recette complémentaires pourront être portées à la charge de cette partie. En outre :

- Le client a l'obligation de prévenir RTE en cas de modification du « réseau local ». Dans ce cas, RTE évalue la nécessité de réaliser une nouvelle mise en exploitation s'accompagnant d'un programme d'essais (Art. 4.7.1 § 7.2 de la DTR) ;
- Le client a l'obligation de recourir au réseau de télécommunication de RTE pour les échanges (Art. 8.25.1 § 7.1.1, §7.2.2) ;
- La communication se fait par des ordres standardisés par interface de sécurité ou téléphonie de sécurité, avec spécifications techniques réalisées selon des documentations non publiques ;
- Les consignes à exécuter en matière d'exploitation de l'installation sont prévues dans un manuel non public concernant :
  - Le suivi des journaux de sécurité et de remontée des alertes de sécurité ;
  - Les dispositions à prendre en cas d'alerte d'exploitation avérée.

2.1.4. Tableau de synthèse

FRANCE	
Informations générales	
Indice mondial de cybersécurité (GCI 2020)	97,6/100
Classement (GCI 2020)	9ème
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).
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	Pas d'ISAC national : plusieurs structures assurent la fonction. 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).
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.

2.2. La Grande-Bretagne

La Grande-Bretagne est une référence en matière de cybersécurité. Depuis le Brexit, le Royaume-Uni a maintenu une grande partie des exigences européennes issues de la Directive NIS de 2016, tout en développant sa propre stratégie nationale de cybersécurité.

2.2.1. La protection des infrastructures critiques et de leurs systèmes d'information

2.2.1.1. Cadre stratégique

Une stratégie nationale est établie par le Gouvernement du Royaume-Uni dont la version la plus récente a été publiée en 2022. Elle plaide pour une meilleure coopération entre le gouvernement et le secteur privé. La stratégie vise à transférer la responsabilité de la cybersécurité des citoyens vers les organisations les mieux placées pour gérer les risques cybernétiques. Le Gouvernement britannique met en exergue la nécessité pour le secteur public et pour les opérateurs réglementés d'infrastructures critiques d'améliorer le traitement des cyberrisques.

2.2.1.2. Cadre légal

La Grande-Bretagne a adopté le texte *Network and Information System Regulations* en 2018 (NIS 2018), en application de la Directive européenne NIS. Cette réglementation est restée en vigueur après le Brexit, sous réserve de quelques amendements de forme. Le texte contient des dispositions s'appliquant notamment aux opérateurs de services essentiels (OES) opérant dans les secteurs de l'énergie, du pétrole, des transports, des soins de santé, de l'eau potable et des infrastructures numériques.

Les tâches de sécurité assignées aux OES dans le cadre de NIS 2018 sont détaillées dans l'article 10 :

- L'OES doit prendre des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques posés à la sécurité du réseau et des systèmes d'information sur lesquels repose son service essentiel. Les mesures doivent, compte tenu de l'état de la technique, garantir un niveau de sécurité des réseaux et des systèmes d'information adapté au risque encouru ;

- L'OES doit prendre des mesures appropriées et proportionnées pour prévenir et minimiser l'impact des incidents affectant la sécurité du réseau et des systèmes d'information utilisés pour la fourniture d'un service essentiel, en vue d'assurer la continuité de ces services.

Les OES doivent tenir compte de toute orientation pertinente émise par l'autorité compétente lorsqu'ils s'acquittent de ces deux obligations.

Les OES ont également l'obligation de notifier par écrit à l'autorité compétente tout incident ayant un impact significatif sur la continuité du service essentiel fourni par l'OES.

Chaque secteur désigne donc une autorité compétente chargée de publier des orientations techniques en matière de cybersécurité et d'en contrôler la mise en œuvre. Ces autorités doivent s'engager au côté des industriels, publier des orientations, rencontrer des représentants des OES et mettre en œuvre un cadre d'évaluation comprenant un programme d'audit.

En juillet 2024, un projet de loi sur la cybersécurité et la résilience (*Cyber Security and Resilience Bill)* a été déposé afin de renforcer les défenses du Royaume-Uni contre l'augmentation des cyberattaques et de protéger les infrastructures essentielles du pays.

2.2.1.3. Principales institutions

- **Le NCSC**

Le *National Cyber Security Centre* (NCSC) est une organisation du gouvernement britannique qui fournit des conseils et du soutien aux secteurs public et privé sur la manière d'éviter les menaces à la sécurité informatique. C'est l'autorité technique nationale du Royaume-Uni en matière de cybermenaces.

Créée en 2016, le NCSC est rattaché au *Government Communications Headquarters* (GCHQ), lui-même placé sous l'autorité du Secrétaire d'État britannique aux Affaires étrangères et du Commonwealth.

Le NCSC a un large spectre de missions. Il a absorbé et remplacé le CESG (le service de sécurité de l'information du GCHQ), le *Centre for Cyber Assessment* (CCA), le *Computer Emergency Response Team UK* (CERT UK) et s'est vu transférer les compétences du *Centre for the Protection of National Infrastructure* (CPNI) dans le domaine de la cybernétique.

Depuis sa création, le NCSC a joué un rôle central dans les efforts visant à renforcer la résilience des infrastructures critiques nationales. Il a notamment permis d'élaborer une cartographie des systèmes d'information des infrastructures critiques nationales, permettant une amélioration de la compréhension des risques.

- **L'Ofgem**

L'*Office of Gas and Electricity Markets* (Ofgem) est le régulateur britannique pour les secteurs de l'électricité et du gaz. Bien que son rôle principal soit de surveiller les marchés de l'énergie et de protéger les consommateurs, l'Ofgem a également un rôle croissant en matière de cybersécurité.

En effet, depuis l'entrée en vigueur des règles *Network and Information System (NIS) Regulations* en 2018, c'est elle qui a été désignée pour l'électricité et le gaz, conjointement avec le département ministériel dédié à l'énergie (DESNZ), comme « autorité compétente ». A ce titre elle doit publier les conseils et informations facilitant aux OES de son secteur l'application des règles de NIS 2018. L'Ofgem est également chargé de veiller

au respect des exigences de ces règles et doit à ce titre réaliser les enquêtes et infliger des amendes en cas de non-conformité.

2.2.2. Règles spécifiques au secteur de l'électricité

Le DESNZ et l'Ofgem ont produit des guides pour aider les opérateurs du secteur de l'électricité et du gaz à se conformer aux obligations des règles NIS 2018 :

- **Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain (DESNZ, 2023)** : ce guide a pour but d'aider les opérateurs de services essentiels (OES) dans le secteur de l'énergie en Grande-Bretagne à se conformer aux dispositions de NIS 2018. Ce document résume les obligations des OES ainsi que les rôles et compétences des autorités compétentes. Il fournit également des conseils sur le processus et les seuils de notification des incidents ;
- **NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain (Ofgem, 2022)** : l'objectif de ce guide est de présenter les attentes de l'Ofgem en matière d'OES, et il sous-tend l'approche d'engagement collaboratif recherchée par l'AC et la communauté OES pour assurer la conformité aux réglementations NIS ;
- **NIS Supplementary Guidance and CAF Overlay for DGE Sector (Ofgem, 2022) :** ce document fournit aux OES du secteur de l'électricité et de l'aval gazier des orientations pour les aider à atteindre et à démontrer les résultats en matière de sécurité du cadre d'évaluation cybernétique (*Cyber Assessment Framework - CAF*) du NCSC ;
- **RIIO-2 Cyber Resilience Guidelines (Ofgem, 2020)** : lignes directrices sur la cyber-résilience à l'intention des opérateurs de réseaux de gaz et d'électricité et de leurs parties prenantes, en relation avec le contrôle des prix des réseaux appelé *Revenue Incentives Innovation Outputs* (RIIO). Ce document sert de guide opérationnel pour aider les professionnels de la sécurité au sein des entreprises de réseau à développer la cybersécurité et la résilience de leur réseau et de leurs systèmes d'information ;
- **Network and Information Systems Enforcement Guidelines and Penalty Policy (Ofgem, 2022)** : l'objectif de ces lignes directrices est d'expliquer les politiques et processus de l'Ofgem dans le cadre de son pouvoir de contrôle et de sanction d'inexécution des règles de NIS.

2.2.3. Le Grid Code et les autres codes « électricité » britanniques

Le *Grid Code* détaille les exigences techniques pour le raccordement et l'utilisation du réseau national de transport d'électricité (NETS). Le *Grid Code* a notamment pour but de :

- Permettre le développement, la maintenance et l'exploitation d'un système efficace, coordonné et économique pour le transport de l'électricité ;
- Faciliter la concurrence dans la production et la fourniture d'électricité ;
- Promouvoir la sécurité et l'efficacité des systèmes de production, de transport et de distribution d'électricité dans la zone de l'opérateur du système de transport national d'électricité.

C'est l'opérateur du système électrique britannique « ESO » qui est l'administrateur du *Grid Code*.

Toutefois, ce document n'est pas l'unique code applicable en Grande-Bretagne. D'autres documents spécifiques au secteur de l'électricité appelés « codes » sont en vigueur. On dénombre en effet plusieurs « industry codes » qui rassemble les règles applicables aux utilisateurs de l'infrastructure et du marché de l'électricité. Les titulaires de licence dans le secteur de l'électricité sont tenus de respecter ces codes spécifiques édictés dans le cadre de cette industrie. Le tableau suivant répertorie les codes qui ont été analysés dans le cadre de la présente étude :

Tableau 4 : Les codes de l'industrie électrique britannique

Code	Administrateur	Objet
The Grid Code	National Grid ESO	Le *Grid Code* détaille les exigences techniques pour la connexion et l'utilisation du réseau national de transport d'électricité (NETS).
Connection Use of System Code (CUSC)	National Grid ESO	Le CUSC est le cadre contractuel pour le raccordement et l'utilisation du réseau national de transport d'électricité (NETS).
System Operator - Transmission Operator Code (STC)	National Grid ESO	La STC définit les critères et la méthodologie pour la planification et l'exploitation du réseau national de transport d'électricité (NETS).
Security and Quality of Supply Standard (SQSS)	National Grid ESO	LE SQSS définit les critères et la méthodologie pour la planification et l'exploitation du réseau national de transport d'électricité (NETS).
Distribution Code	Energy Networks Association	Le code de distribution contient des procédures visant à permettre une gestion efficace des situations techniques quotidiennes dans l'industrie de la distribution d'électricité, en tenant compte d'un large éventail de conditions opérationnelles susceptibles d'être rencontrées dans des circonstances normales et exceptionnelles.
Smart Energy Code (SEC)	SECAS	Le Smart Energy Code (SEC) définit les droits et obligations du DCC, des fournisseurs d'énergie, des opérateurs de réseaux et des autres parties concernées par la gestion de bout en bout des compteurs intelligents en Grande-Bretagne.

Le *Grid Code* ne contient pas de sections spécifiques sur la cybersécurité, d'exigences en matière de sécurité informatique ou les règles connexes. De même pour les autres codes complémentaires administrés par National Grid ESO. En revanche des dispositions spécifiques ont été identifiées dans le Distribution Code et le Smart Energy Code.

2.2.3.1. Le Distribution Code

Les entreprises de distribution d'électricité titulaires d'une licence, ou gestionnaires de réseaux de distribution (DNO) en Grande-Bretagne, sont tenues de disposer d'un code de distribution détaillant les paramètres techniques et les considérations relatives au raccordement à leurs réseaux électriques et à l'utilisation de ceux-ci. Tous les DNO appliquent actuellement la même version du code, qui est mis à jour par le *Distribution Code Review Panel*. Toutes les modifications du Code sont approuvées par l'Ofgem.

Le Distribution Code prévoit des exigences renforcées en matière de cybersécurité portant sur les *Restoration Contractors*, définis comme les producteurs ou autres clients ayant une

obligation contractuelle de fournir les services nécessaires au rétablissement après une mise à l'arrêt totale ou d'un arrêt partiel (prestataires de services de restauration du système).

- Les *Restauration Contractors* doivent veiller à ce que tous leurs appareils de communication et de télémétrie soient cyber-sécurisés. En particulier, ils doivent s'assurer que toutes les communications entre la station de télémesure (ou appareil terminal du DNO), et l'appareil de *Restauration Contractors* sont également résilientes la perte de l'alimentation principale pendant au moins 72 heures (DPC6.7.3) ;
- Les *Restoration Contractors* sont tenus de garantir que leur équipement est sécurisé contre les cyberattaques et les intrusions, conformément aux normes du Network and Information System Security (NIS) Regulations (DPC6.8.4) ;
- Au moins tous les trois ans, tous les *Restauration Contractors* doivent fournir l'assurance que l'ensemble de leur équipement est cybersécurisé, comme exigé par l'article DPC6.8.4 (DOC5.7.3.6(b)).

Les *Restoration Contractors*, en tant qu'auxiliaires externes au DNO dans le schéma de restauration du réseau, peuvent représenter un maillon plus faible dans la chaîne de sécurité. C'est pourquoi ces dispositions spécifiques ont été intégrées.

2.2.3.2. Le Smart Energy Code (SEC)

Le *Smart Energy Code (*SEC) est un accord multipartite qui définit les droits et les obligations des fournisseurs d'énergie, des opérateurs de réseau et des autres parties concernées par la gestion des compteurs intelligents en Grande-Bretagne. Le SEC est appliqué dans le cadre de la licence délivrée au *Data and Communications Companies* (DCC), qui a été créée pour gérer l'infrastructure de communication des compteurs intelligents. Le titulaire de la licence DCC, les fournisseurs d'énergie et les opérateurs de réseau sont tenus par leurs licences d'adhérer au SEC et de se conformer à ses dispositions. La SEC est gérée par un groupe technique spécifique (le SEC Panel), sous le contrôle, le cas échéant, de l'Ofgem. Gemserv est l'administrateur et assure le secrétariat du *Smart Energy Code*.

Le Smart Energy Code (SEC) fournit des lignes directrices détaillées sur la cybersécurité pour les systèmes de comptage intelligents au Royaume-Uni. Le code exige que les utilisateurs mettent en place et maintiennent des mesures de cybersécurité solides, guidées par des normes internationales telles que ISO/IEC 27001 : 2013. Les utilisateurs doivent mettre en œuvre un système de gestion de la sécurité de l'information (SGSI) complet qui aborde divers aspects, notamment la protection des données, la gestion des actifs et le contrôle d'accès. Ce SGSI doit être régulièrement revu et mis à jour afin d'atténuer efficacement les risques de sécurité. En outre, le sous-comité de sécurité joue un rôle crucial en maintenant le cadre des contrôles de sécurité, en menant des évaluations des risques et en veillant à ce que l'architecture de sécurité soit à jour dans son intégralité.

La mise en place de ces règles se justifient par le fait qu'au Royaume-Uni, le comptage est réalisé par les fournisseurs et non par les gestionnaires du réseau de distribution. Dans ce contexte, la mise en place du comptage dit intelligent demandait une organisation spécifique des rapports des fournisseurs et d'opérateurs spécifiques du back bone télécom pour en assurer l'exploitation, et la cybersécurité. En France, l'ensemble de ces préoccupations est directement pris en charge par le gestionnaire de réseau de distribution seul.

2.2.4. Tableau de synthèse

Grande-Bretagne	
Informations générales	
Indice mondial de cybersécurité (GCI 2020)	99,54/100
Classement (GCI 2020)	2ème
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).
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
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)*.
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 chacun produit des guides afin d'aider les opérateurs du secteur électrique concernés par la réglementation NIS 2018 à appliquer les dispositions en vigueur : - *DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain* (2023) ; - *NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain* (2022) ; - NIS Supplementary Guidance and CAF Overlay for DGE Sector (2022) ; - RIIO-2 Cyber Resilience Guidelines (Ofgem, 2020) ;

	- Network and Information Systems Enforcement Guidelines and Penalty Policy (2022).
Code de réseau	Plusieurs codes encadrent les activités du secteur électrique, dont le *Grid Code* ; Deux d'entre eux ont des dispositions spécifiques pour la cybersécurité.

2.3. Le Kenya

La cybersécurité au Kenya est un domaine en pleine évolution, reflétant les efforts du pays pour s'adapter à l'augmentation rapide de la connectivité numérique et à la montée des cybermenaces. Ces dernières se concrétisent comme le montre l'attaque du 27 juillet 2023, où une cyberattaque a touché à la fois plusieurs organisations publiques et privées notamment l'opérateur d'électricité *Kenya Power and Lighting Company* (KPLC).

2.3.1. La protection des infrastructures critiques et de leurs systèmes d'information

2.3.1.1. Cadre stratégique

Le document de stratégie cybernétique le plus récent au Kenya s'intitule *The National Cybersecurity Strategy.* Il a été publié en 2022, remplaçant la précédente stratégie datant de 2014. Un des piliers essentiels de cette stratégie est le renforcement de la cybersécurité des infrastructures critiques d'information. Il y est souligné que le gouvernement kenyan est engagé à mettre en œuvre diverses initiatives afin d'améliorer la cybersécurité et la résilience de ces infrastructures.

Parmi les mesures en projet pour atteindre cet objectif, on retrouve l'élaboration d'un cadre de protection des infrastructures d'information critiques, l'identification et classification de ces infrastructures, la mise en œuvre de mesures de cybersécurité de base (contrôles de sécurité physique et technique, y compris les mesures d'urgence et de récupération en cas de crise), établissement d'un cadre pour le partage et la communication d'informations et la réponse aux incidents.

2.3.1.2. Cadre légal

Le 9 février 2024, le texte *Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024* est entré en vigueur. Pris en application du *Computer Misuse and Cybercrimes Act N°5* de 2018, il ouvre véritablement une nouvelle ère dans la lutte contre les cybermenaces au Kenya.

Ce texte fournit des règles visant à assurer la protection des infrastructures d'information critiques ainsi que surveiller, prévenir, détecter et répondre aux menaces de cybersécurité dans le cyberespace du Kenya.

Concernant les obligations spécifiques aux opérateurs d'infrastructures d'informations critiques, ceux-ci doivent notamment :

- Effectuer une évaluation des risques dans un délai de douze mois après l'entrée en vigueur des règlements afin d'identifier et de prioriser les menaces internes et externes potentielles ;

- Réaliser des évaluations annuelles des risques cybernétiques et des analyses d'impact sur les activités, produits, services, fonctions commerciales et processus ;
- Veiller à ce que l'infrastructure abritant les informations critiques soit située au Kenya. Tout projet de localisation d'informations critiques en dehors du Kenya doit être approuvé par le comité, afin de garantir le respect des normes de sécurité ;
- Effectuer des examens périodiques des programmes de sensibilisation à la cybersécurité pour s'assurer de leur adéquation et de leur pertinence ;
- Nommer un responsable de la sécurité de l'information (CISO) pour superviser les questions de cybersécurité.

2.3.1.3. Principales institutions

- **Le NC4**

Le *National Computer and Cybercrimes Coordination Committee (NC4)* est une entité multi-agences établie par le *Computer and Misuse and Cybercrimes Act N°5 of 2018* (CMCA) pour coordonner les questions de cybersécurité nationale afin de permettre la détection, la prévention, la réponse, l'enquête et la poursuite rapides et efficaces des abus informatiques et des cybercrimes. Il a vocation à faciliter la coopération internationale dans le traitement des questions informatiques et de cybercriminalité au Kenya.

Le NC4 a plusieurs attributions en lien avec la protection des infrastructures critiques :

- **Conseiller sur la sécurité des infrastructures critiques** : NC4 conseille le gouvernement kenyan, notamment le Conseil de sécurité nationale, sur les aspects de sécurité liés aux infrastructures d'information critiques.
- **Établir de normes et codes de pratique** : L'un des rôles clés du NC4 est de développer des codes de bonnes pratiques et des normes de performance en cybersécurité pour les propriétaires des infrastructures critiques, en garantissant leur intégrité, disponibilité et confidentialité.
- **Développer un cadre national de sécurité** : Le NC4 est chargé de la gestion des infrastructures publiques nationales clés (*National Public Key Infrastructure* - NPKI) et développe des cadres pour garantir la disponibilité, l'intégrité et la confidentialité des infrastructures critiques.

- **Le NKCC**

Le *National KE-CIRT/CC* (*Kenya Computer Incident Response Team – Coordination Centre*) est l'entité nationale responsable de la réponse aux incidents de cybersécurité au Kenya. Il est géré par la *Communications Authority of Kenya* (CA) et joue un rôle crucial dans la surveillance, la détection et la réponse aux cybermenaces à l'échelle nationale, et participe ainsi à la protection des infrastructures critiques.

- **Les « Cybersecurity Operation Centers »**

Le texte *Critical Information Infrastructure and Cybercrime Management Regulations,* adopté en 2024, prévoit l'établissement des centres opérationnels de cybersécurité (COC) : le centre national des opérations de cybersécurité (NCOC), les centres sectoriels des opérations de cybersécurité (SCOC) et le centre des opérations de cybersécurité pour les infrastructures d'information critiques (CIICOC) :

- Le NCOC sera le principal centre national de surveillance et d'investigation en matière de cybersécurité ;

- Les SCOC se concentreront sur les menaces spécifiques à chaque secteur ;
- Les CIICOC seront chargés de la surveillance en temps réel, de la détection et de l'analyse des menaces pesant sur les infrastructures critiques.

Ces centres sont en cours de création et joueront un rôle central dans le traitement des cybermenaces en fournissant des informations en temps réel et en garantissant des réponses rapides aux cyberincidents. On note que l'organisation choisie prend en compte tant les spécificités des infrastructures critiques que des différents secteurs économiques. Dans ce cadre, une attention particulière sera sans nul doute portée sur le secteur de l'énergie.

- **L'EPRA**

L'Autorité de régulation de l'énergie et du pétrole (EPRA) a succédé à la Commission de régulation de l'énergie (ERC) en 2019, avec un mandat élargi, entre autres, à la régulation de l'amont pétrolier et charbonnier. L'EPRA régule la production, l'importation, l'exportation, la transmission, la distribution, la fourniture et l'utilisation de l'énergie électrique, à l'exception de l'autorisation des installations nucléaires. Le Plan stratégique 2020 – 2023 de l'EPRA montre une prise de conscience des enjeux en matière de cybersécurité dans l'industrie électrique mais l'organisation institutionnel et juridique actuelle au Kenya ne donne pas d'attributions spécifiques en la matière à l'EPRA.

2.3.2. Règles spécifiques au secteur de l'électricité

Le cadre juridique de la protection des infrastructures critiques est très récent au Kenya. A ce jour, aucun texte juridique ou guide spécifique au secteur de l'électricité n'a été publié. Si des règles techniques spécifiques doivent être adoptées, elles le seront par le NC4 qui dispose de cette compétence.

2.3.3. Le « Kenya National Transmission Grid Code » (KNTGC)

Le KNTGC établit les aspects techniques de la planification, du raccordement, de l'exploitation et de l'utilisation du réseau de transport national du Kenya, ainsi que les relations entre l'opérateur du réseau (SO), le gestionnaire du réseau de transport et les autres parties prenantes.

On y identifie quelques dispositions traitant de la sécurité des données, notamment l'article 20.4.8: (e) qui dispose que les parties assurent une sécurité raisonnable contre l'accès non autorisé, l'utilisation et la perte d'informations (c'est-à-dire qu'elles disposent d'une stratégie de sauvegarde) pour les systèmes qui contiennent les informations.

Mais l'essentiel des dispositions encadrant explicitement le sujet de la cybersécurité sont rassemblées au sein d'un **chapitre spécifique**. Dans sa version la plus récente, adoptée en avril 2021, le KNTGC intègre en effet un nouveau chapitre (Chapter 21) sur la cybersécurité. Concernant son contenu :

- En introduction, il est rappelé quelques généralités sur la nécessité de renforcer la cybersécurité du réseau électrique et le contexte stratégique de cette thématique au Kenya ;

- Les rédacteurs contextualisent le chapitre en citant des normes techniques américaines et en faisant référence aux meilleures pratiques en la matière en Inde et en Europe ;

- Le chapitre fournit des recommandations pour élaborer des contrôles de cybersécurité afin de répondre aux défis de sécurité potentiels liés à la modernisation du réseau électrique du Kenya en traitant les sujets suivants :
    - Développement de contrôles et de procédures de gestion de la sécurité de l'information ;
    - Systèmes de cybersécurité ;
    - Gestion de l'accès aux systèmes ; et
    - Mise en place d'une défense contre les menaces par la formation, la sensibilisation et la surveillance.

La structuration plus précise de ce chapitre est résumée dans le tableau ci-dessous.

Tableau 5 : Synthèse des dispositions du chapitre dédié à la cybersécurité du KNTGC

Ref. article	Description
21.3.1 People and Policy	Cette section met en avant l'importance des politiques et procédures comme outils contre les violations de sécurité. Elle décrit les exigences en matière de documentation et de cohérence avec les objectifs opérationnels sécurisés. Elle souligne également l'importance de définir les responsabilités du personnel et de le former à la cybersécurité.
21.3.2 Operational Security	Cette section traite de la sécurité opérationnelle, en mettant l'accent sur l'évaluation des risques et leur atténuation, le contrôle des accès aux systèmes critiques, la surveillance, et la journalisation des activités pour détecter d'éventuelles anomalies. Elle inclut également des directives pour la gestion sécurisée des actifs, notamment leur déclassement ou redéploiement, ainsi que la gestion des correctifs pour maintenir la sécurité des systèmes à jour. Enfin, des évaluations régulières de la vulnérabilité sont recommandées afin de minimiser les risques.
21.3.3 Physical and Logical Security	Cette section décrit les mesures de protection des actifs physiques, du personnel et des systèmes numériques contre des risques tels que l'incendie, le vol, le vandalisme et l'accès non autorisé. Un plan de sécurité physique documenté, approuvé par la direction, doit être mis en œuvre et maintenu.
21.3.4 Network Security	Cette section traite de la protection des données transitant via le réseau. Cela comprend l'autorisation d'accès aux données, ainsi que la prévention et la surveillance des accès non autorisés, des abus, modifications ou dénis de services.
21.3.5 Platform Security Risks	Cette section se concentre sur les risques liés aux systèmes d'exploitation et aux autres logiciels sur lesquels les applications de l'organisation sont exécutées.
21.3.6 Application Security	Cette section traite des logiciels développés en interne ou achetés sur mesure. Ces applications doivent être conçues avec la sécurité comme priorité dès le début du processus de développement pour éviter les failles susceptibles d'être exploitées par des attaquants.

21.3.7 Unique Security Requirements and Controls	Cette section aborde les pratiques de sécurité spéciales nécessaires pour la modernisation du réseau, notamment le réseau intelligent.

L'intégration de la cybersécurité dans le KNTGC a été réalisée avec un effort certain de pédagogie. Les règles édictées sont relativement générales et sont formulées sous forme de recommandations et non d'obligations juridiques à proprement parler. Ainsi, on note par exemple que contrairement aux autres chapitres du code :

- Ce ne sont pas des exigences techniques propres au système électrique ;
- Le ou les destinataires des normes ne sont pas identifiables.

Le chapitre 21 du KNTGC présente un cadre complet pour la gestion de la cybersécurité, abordant des domaines allant de la gestion des politiques de sécurité à la protection des infrastructures critiques comme les systèmes SCADA et AMI, mais formulé sous formes de recommandations.

On comprend que ce corpus de dispositions insérées dans le code de réseau a vocation à parer, au moins partiellement, à l'absence d'autres textes juridiques disposant les exigences propres aux infrastructures critiques au Kenya.

2.3.4. Tableau de synthèse

Kenya	
Informations générales	
Indice mondial de cybersécurité (GCI 2020)	81,7/100
Classement (GCI 2020)	51ème
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*.

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.
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* contient un chapitre spécifique sur la cybersécurité.

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.

La suite de ce chapitre examine comment deux de ces Etats, les Etats-Unis et l'Inde, gèrent la question du cadre normatif de la cybersécurité des réseaux électriques.

2.4. Les Etats-Unis d'Amérique

Les Etats-Unis sont reconnus comme un des pays les plus avancés du monde en matière de cybersécurité. Ce pays a été parmi les premiers pays à reconnaître l'importance de protéger les infrastructures critiques et les systèmes informatiques contre les cyberattaques et c'est aux Etats-Unis que sont nées les premières normes et règles juridiques pour renforcer la cybersécurité.

2.4.1. Protection des infrastructures critiques et de leurs systèmes d'information

2.4.1.1. Cadre stratégique

La stratégie nationale de cybersécurité actuellement en vigueur a été édictée en mars 2023, et son premier pilier s'intitule « Defend critical infrastructure ». Il démontre la volonté des Etats-Unis de renforcer la cybersécurité des infrastructures critiques.

2.4.1.2. Cadre légal

Aux États-Unis, il n'existe pas une unique loi fédérale qui imposerait des obligations de cybersécurité à toutes les infrastructures critiques. Plusieurs lois sectorielles, directives présidentielles et règlements spécifiques définissent des obligations pour différents secteurs d'infrastructures critiques.

Le texte central en matière de politique applicable est le Mémorandum de sécurité nationale sur la sécurité et la résilience des infrastructures critiques (NSM-22) qui a récemment remplacé la directive présidentielle *PPD 21 : Critical Infrastructure Security and Resilience*.

Publié le 30 avril 2024 par le Conseil de sécurité nationale (NSC) de la Maison Blanche, la NSM-22 renforce la stratégie américaine en matière de cybersécurité et de protection des infrastructures critiques. Un Plan national de gestion des risques liés aux infrastructures 2025 permet le déploiement des efforts du gouvernement fédéral pour sécuriser et protéger les infrastructures critiques au cours des prochaines années.

2.4.1.3. Principales institutions

Le cadre institutionnel et juridique de la cybersécurité aux États-Unis repose sur un ensemble d'agences et d'organisations, dont certaines ont un focus spécifique sur le secteur de l'électricité. Parmi ces acteurs, on distingue, d'une part, les organismes chargés de la cybersécurité générale (CISA, NCCIC), et d'autre part, les entités spécialisées dans la régulation et la sécurisation du secteur de l'électricité, telles que la FERC, la NERC et l'E-ISAC.

- **La CISA**

La *Cybersecurity and Infrastructure Security Agency (*CISA) est une agence fédérale américaine sous la supervision du département de la Sécurité intérieure des États-Unis, créée le 16 novembre 2018 par la loi *Cybersecurity and Infrastructure Security Agency Act* de 2018. La CISA fournit des orientations pour aider les États, les collectivités locales et les partenaires industriels à identifier les secteurs d'infrastructures critiques et les travailleurs essentiels nécessaires au maintien des services et des fonctions dont les Américains dépendent quotidiennement. Par ailleurs, la CISA :

- Organise des exercices de cybersécurité et de sécurité physique avec des partenaires gouvernementaux et industriels afin de renforcer la sécurité et la résilience des infrastructures critiques ;
- Réalise des évaluations spécialisées de la sécurité et de la résilience des infrastructures critiques du pays. Ces évaluations volontaires aident la CISA et ses partenaires à mieux comprendre et gérer les risques pesant sur les infrastructures critiques. Les évaluations portent sur les vulnérabilités des infrastructures, les interdépendances, les lacunes en matière de capacités et les conséquences de leur perturbation ;
- Collabore avec la communauté des systèmes de contrôle industriel (SCI) pour faire face aux cyber-événements opérationnels urgents ainsi qu'aux risques à long terme liés aux SCI ;
- Offre une large gamme de produits et de services gratuits pour soutenir les efforts de gestion des risques de cybersécurité de la communauté ICS.

- **Le NCCIC**

Le *National Cybersecurity and Communications Integration Center* (NCCIC) est un centre de gestion, de réponse aux incidents et de connaissance de la situation cybernétique fonctionnant 24 heures sur 24 et 7 jours sur 7 qui fait partie du CISA. Il s'agit d'un point nodal national d'intégration de la cybernétique et des communications pour le gouvernement fédéral, la communauté du renseignement et les forces de l'ordre. Le NCCIC partage des informations entre les partenaires des secteurs public et privé afin de les sensibiliser aux vulnérabilités, aux incidents et aux mesures d'atténuation. Les utilisateurs

de cyber-systèmes et de systèmes de contrôle industriels peuvent s'abonner gratuitement à des produits, des flux et des services d'information.

Dans le cadre de sa mission, le NCCIC réalise des évaluations de la cybersécurité pour les propriétaires et les opérateurs d'infrastructures critiques afin de renforcer la cybersécurité de leurs systèmes de contrôle industriel (ICS).

- **La FERC**

La *Federal Energy Regulatory Commission* (FERC) est une agence indépendante qui réglemente le transport interétatique du gaz naturel, du pétrole et de l'électricité. La FERC réglemente également les projets de gaz naturel et d'hydroélectricité. La 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.

- **La NERC**

La *North American Electric Reliability Corporation* (NERC) est une autorité de régulation internationale à but non lucratif dont la mission est d'assurer la réduction effective et efficace des risques pour la fiabilité et la sécurité du réseau. La NERC été désignée par la FERC comme entité de référence en matière de fiabilité de l'électricité (*Electricity Reliability Organization*). Elle a par conséquent élaboré des normes de fiabilité en matière de cybersécurité pour la protection des infrastructures critiques (*Critical Infrastructure Protection* - CIP) qui ont été ensuite soumises à examen et à approbation de la FERC.

- **L'E-ISAC**

Créé en 1999, l'*Electricity Information Sharing and Analysis Center* (E-ISAC) renforce la capacité du secteur à se préparer et à répondre aux menaces, vulnérabilités et incidents cybernétiques et physiques en fournissant une analyse de qualité et un partage rapide des informations de sécurité sur la manière d'atténuer les menaces complexes et en constante évolution qui pèsent sur le réseau. Cela comprend une veille 24/7, une analyse interne experte des incidents en cours et une série de produits et de services analytiques. L'E-ISAC est ouvert à tous les propriétaires et exploitants de réseaux électriques et de gaz naturel d'Amérique du Nord, ainsi qu'à certaines organisations partenaires.

2.4.2. Règles de cybersécurité du secteur de l'électricité

Le 18 janvier 2008, la FERC a publié l'ordonnance n° 706 approuvant les premières versions des normes de fiabilité dites « CIP » élaborées par la NERC. Les normes initiales ont progressivement évolué et ont été complétées par de nouvelles normes afin de renforcer la cybersécurité du secteur. Actuellement la liste des normes CIP en vigueur est la suivante :

Tableau 6 : Normes CIP actuellement en vigueur

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

Ces normes sont obligatoires aux Etats-Unis et sont déployées conformément aux plans de mise en œuvre associés à chaque norme et élaborés par la NERC. A noter qu'une nouvelle norme CIP vient récemment d'être finalisée par la NERC : la « CIP-015-01 Requirements for Internal Network Security Monitoring (INSM) ».

2.4.3. Business practice manuals et operating procedures : les codes de réseau à l'américaine

Aux États-Unis, il n'existe pas de « codes de réseau » au sens strict, comme on peut les trouver dans d'autres pays. Cependant, des acteurs opérationnels – principalement les opérateurs de systèmes électriques indépendants (*Independent System Operators*, ou ISO) et les organisations régionales de transmission (*Regional Transmission Organizations*, ou RTO) – élaborent et se conforment à des ensembles de règles et de normes qui remplissent des fonctions similaires à celles des codes de réseau.

Les ISO et RTO établissent des tarifs, procédures et règles d'exploitation spécifiques à leur région. Ces documents, soumis à l'approbation de la Federal Energy Regulatory Commission (FERC), régissent les aspects techniques et commerciaux du réseau. Ils comprennent des règles qui, dans certains cas, peuvent s'apparenter aux éléments que l'on retrouve dans les codes de réseau européens.

En matière de cybersécurité, les ISO et RTO ne peuvent pas élaborer de règles de manière totalement autonome. Cependant, ils jouent un rôle clé dans l'application des normes de cybersécurité obligatoires, notamment les normes *Critical Infrastructure Protection* (CIP) élaborées par la *North American Electric Reliability Corporation* (NERC), qui sont appliquées à l'échelle du réseau interconnecté nord-américain. Ces normes assurent la sécurité des infrastructures critiques, y compris la cybersécurité des systèmes de contrôle et des données sensibles.

Une affaire de sécurité nationale

Aux États-Unis, l'élaboration des règles de cybersécurité pour le secteur États plusieurs raisons liées à la nature du réseau électrique et à la nécessité d'une coordination nationale face aux menaces cybernétiques.

Le réseau est interconnecté à travers les États, et que les cybermenaces ne respectent pas les frontières étatiques. Cela nécessite une coordination et une réponse nationales pour garantir la sécurité du réseau dans son ensemble.

En revanche, les États et les opérateurs locaux peuvent définir certaines règles spécifiques concernant le fonctionnement de leurs réseaux électriques, car ces questions sont souvent plus locales et relèvent de la gestion quotidienne des services publics.

La FERC a régule les aspects liés au fonctionnement global et la sécurité du réseau électrique interconnecté, que ce soit en matière de régulation de marché ou de fiabilité technique.

2.4.1. Tableau de synthèse

USA	
Informations générales	
Indice mondial de cybersécurité (GCI 2020)	100/100
Classement (GCI 2020)	1er
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)
Centre national d'alerte et de réaction aux attaques informatiques	Le NCCIC
Centre d'analyse et de partage d'informations	Il existe plusieurs ISAC dont le E-ISAC, propre au secteur électrique.
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.
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.

2.5. L'Inde

Depuis un peu plus d'une décennie, l'État indien a pris des mesures pour renforcer sa cybersécurité. Elles semblent cependant encore insuffisantes. Le pays souffre d'un retard dans l'application de mesures cohérentes et efficaces alors même qu'il fait face à un développement important de ses infrastructures, notamment dans le secteur énergétique.

2.5.1. La protection des infrastructures critiques et de leurs systèmes d'information

2.5.1.1. Cadre stratégique

En 2013, l'Inde a publié sa Stratégie nationale de cybersécurité qui met l'accent sur la protection des infrastructures critiques. Cependant, le déploiement de cette stratégie est jugé incomplète et de nombreux défis persistent.

2.5.1.2. Cadre légal

La loi *Information Technology Act, 2000* est la principale législation régissant la cybersécurité en Inde. En application de cette loi ont été adoptées les *Information Security Practices and Procedures for Protected System Rules* en 2018. Ces règles sont venues cadrer les obligations des organisations possédant des infrastructures critiques d'information en Inde, leur imposant des normes strictes de sécurité et une coordination avec le NCIIPC pour protéger ces systèmes contre les cybermenaces. Ces règles s'appliquent aux systèmes informatiques critiques désignés comme "Systèmes Protégés" par le gouvernement. Elles définissent les pratiques de sécurité à suivre pour ces systèmes afin de prévenir les cyberincidents et assurer la sécurité des infrastructures critiques d'information.

Malgré ces avancées légales et institutionnelles, il est souvent souligné que la mise en œuvre reste inégale et que le cadre de cybersécurité de l'Inde souffre d'un manque de coordination et de ressources.

2.5.1.3. Cadre institutionnel

- **Le NCIIPC**

Créé en 2013 sous l'égide de la *National Technical Research Organisation* (NTRO), le *National Critical Information Infrastructure Protection Center* (NCIIPC) joue un rôle central dans la cybersécurité nationale. Il est responsable de la protection des infrastructures critiques d'information en Inde. Il les identifie et les supervise, veille à leur protection contre les cyberattaques et travaille en étroite collaboration avec CERT-In pour coordonner la réponse en cas de cybermenaces.

- **Le NCCC**

Le National Cyber Coordination Centre (NCCC) est une agence de cybersécurité et de cybersurveillance en Inde. Elle a pour mission de filtrer les métadonnées des communications et de coordonner les activités de collecte de renseignements d'autres agences.

- **Le I4C**

Le *Indian Cybercrime Coordination Centre* (I4C) est une initiative du ministère de l'intérieur du gouvernement indien visant à lutter contre la cybercriminalité dans le pays de manière coordonnée et globale. Le I4C travaille sous l'égide du ministère de l'intérieur Indien afin de créer un cadre et un écosystème efficaces pour la prévention, la détection, l'investigation et la poursuite de la cybercriminalité dans le pays. Il s'attache à résoudre les problèmes liés à la cybercriminalité pour les citoyens, notamment en améliorant la coordination entre les différentes agences chargées de l'application de la loi et les parties prenantes, en faisant évoluer la capacité globale de l'Inde à lutter contre la cybercriminalité et en améliorant le niveau de satisfaction des citoyens.

- **La CEA**

La Central Electricity Authority (CEA) conseille le gouvernement sur les questions de politique et formule des plans pour le développement des systèmes électriques. Il s'agit d'une institution constituée en vertu de l'article 3(1) de la loi sur l'approvisionnement en électricité de 1948, qui a été remplacée par l'article 70(1) de la loi sur l'électricité de 2003.

- **La CERC**

La Central Electricity Regulatory Commission (CERC) a pour objectif de promouvoir la concurrence, l'efficacité et l'économie sur les marchés de l'électricité en gros, d'améliorer la qualité de l'approvisionnement, de promouvoir les investissements et de conseiller le gouvernement sur la suppression des obstacles institutionnels afin de combler le fossé entre l'offre et la demande et de favoriser ainsi les intérêts des consommateurs.

La CERC est notamment responsable de l'élaboration et de l'adoption du code de réseau indien (IEGC) qui vise à améliorer l'exploitation et la gestion des réseaux de transport régionaux. Le CERC s'est saisi du sujet de la cybersécurité en élaborant des dispositions incluent dans l'IEGC.

- **Les SERC**

Les *State Electricity Regulatory Commissions* (SERC) sont des organismes administratifs qui ont été créés par la loi sur l'électricité de 1998, mais avec un rôle renforcé par une loi de 2003. Présent dans chaque État, ces commissions ont pour rôle de réguler le secteur de l'électricité à l'échelle locale et donc de compléter l'action du régulateur national CERC. Elles fixent les tarifs, régulent le processus d'achat et d'approvisionnement en électricité des titulaires de licences de distribution, délivrent les licences pour les gestionnaires de transport et de distribution, facilitent le transit de l'électricité à travers le réseau de leur Etat… Les commissions ont également un pouvoir de règlement des différends entre les opérateurs du secteur ainsi qu'entre les distributeurs et les consommateurs.

Enfin, les SERC doivent élaborer un Code de réseau de leur Etat (*State Grid Code*, SGC) conforme au Code de réseau national ainsi que spécifier (ou faire respecter) les normes concernant la qualité, la continuité et la fiabilité du service. De ces missions découlent de fait une compétence en matière de cybersécurité.

2.5.2. Règles spécifiques au secteur de l'électricité

La *Central Electricity Authority* (CEA) a été formellement missionnée par la réglementation en vigueur (*Technical Standards for Connectivity to the Grid - Regulations 2019*) pour rédiger des dispositions, sur la cybersécurité, destinées au secteur de l'électricité.

C'est dans ce cadre qu'elle a adopté des lignes directrices sur la cybersécurité dans le secteur de l'électricité en 2021 (***CEA Cyber Security in Power Sector Guidelines 2021***). Ce document contient les principes cardinaux applicables en la matière ainsi que les exigences techniques. C'est la première fois que des lignes directrices en matière de cybersécurité sont créées pour ce secteur en Inde. Leur contenu est décrit dans le tableau ci-dessous :

Tableau 7 : Structure et contenu synthétique des lignes directrices du CEA pour la cybersécurité du secteur électrique (2021)

Ref. article	Nom	Description
Article 1	Cyber Security Policy	▪ Les entités responsables doivent suivre des principes fondamentaux, comme l'isolation stricte des systèmes OT (technologie opérationnelle) des systèmes IT connectés à Internet. ▪ La conformité à la norme ISO/IEC 27001 et aux contrôles spécifiques au secteur est requise. ▪ La politique de cybersécurité doit être revue annuellement par des experts et approuvée par le Conseil d'administration.
Article 2	Appointment of CISO	Obligation de nommer un CISO ainsi qu'un adjoint. Les CISO doivent régulièrement mettre à jour leurs informations auprès des autorités sectorielles et veiller au respect des règles de cybersécurité.
Article 3	Identification of Critical Information Infrastructure (CII)	Les entités doivent soumettre les détails de leurs actifs cyber à NCIIPC pour consultation, afin d'identifier et de notifier les CII. Un

		examen des CII doit être effectué au moins une fois par an.
Article 4	Electronic Security Perimeter	Les entités doivent identifier, documenter et évaluer le périmètre de sécurité électronique. Une évaluation de vulnérabilité doit être effectuée tous les 6 mois, et les vulnérabilités doivent être corrigées rapidement.
Article 5	Cyber Security Requirements	Les entités doivent avoir une division dédiée à la sécurité de l'information fonctionnant 24/7. Un système de détection d'intrusions et des tests réguliers de sécurité doivent être mis en place.
Article 6	Cyber Risk Assessment and Mitigation Plan	Les entités doivent documenter un plan d'évaluation et de mitigation des risques cyber, approuvé par le Conseil d'administration et révisé trimestriellement.
Article 7	Phasing out of Legacy System	Les technologies IT dans les systèmes électriques doivent être modernisées. Un plan de remplacement des systèmes en fin de vie doit être élaboré et approuvé.
Article 8	Cyber Security Training	Un programme annuel de formation en cybersécurité doit être mis en place pour tout le personnel ayant accès aux systèmes critiques. Les nouveaux employés doivent suivre cette formation avant d'accéder aux systèmes.
Article 9	Cyber Supply Chain Risk Management	Les entités doivent s'assurer que les clauses contractuelles liées à la cybersécurité sont incluses dans chaque appel d'offres pour des équipements ou systèmes TIC.
Article 10	Cyber Security Incident Report and Response Plan	Les incidents doivent être rapportés selon le format de CERT-In, une analyse des causes doit être effectuée, et des mesures correctives doivent être mises en place pour éviter la récurrence.
Article 11	Cyber Crisis Management Plan(C-CMP)	Les entités doivent élaborer un plan de gestion de crise en cybersécurité, le soumettre aux CERT sectoriels pour révision, puis le faire approuver par le Conseil d'administration.
Article 12	Sabotage Reporting	Un processus pour identifier et signaler les sabotages doit être inclus dans la politique de cybersécurité. Le CISO est responsable de signaler tout acte de sabotage.
Article 13	Security and Testing of Cyber Assets	Les entités doivent effectuer régulièrement des mises à jour logicielles, des tests de pénétration, et des évaluations de vulnérabilité sur leurs actifs cyber, en se conformant aux standards de sécurité.
Article 14	Cyber Security Audit	Un audit de sécurité informatique doit être effectué au moins tous les six mois par un auditeur certifié, avec traitement des

		vulnérabilités critiques dans un délai d'un mois.
Annexure A	FAT & SAT	Décrit les processus de tests de conformité pour les systèmes SCADA et les équipements de communication, selon les normes internationales (IEC 61850, IS 15953).
Annexure B : 1	List of designated laboratories for cyber security conformance testing	Énumère les laboratoires désignés pour tester la conformité des équipements aux protocoles de communication et aux normes de cybersécurité.
Annexure B : 2	Details of tests for various identified products	Fournissent des détails techniques sur les procédures de test des unités terminales à distance, des dispositifs électroniques intelligents et des compteurs intelligents, ainsi que les critères pour tester les équipements provenant de sources externes.
Annexure B : 3	Testing Criteria	
Annexure B : 4	Type Tests	

Ces lignes directrices spécifiques au secteur de l'électricité s'appliquent à toutes les entités responsables (*Responsible Entities*) définies par une liste assez large, ainsi que les intégrateurs de systèmes, les fabricants d'équipements, fournisseurs/vendeurs, prestataires de services, équipementiers en matériel et logiciels informatiques engagés dans le système d'alimentation électrique indien.

Elles forment un ensemble qui semble abouti, dans lequel on retrouve les thématiques importantes de la cybersécurité du système électrique. Elles sont le signe de la volonté de concentrer au niveau fédéral la compétence de définition des exigences techniques en la matière, en rappelant toutefois tous les autres textes et normes importants en la matière et en listant les responsabilités reposant sur les acteurs du système.

2.5.3. Le Indian Electricity Grid Code

Le Code de réseau électrique indien (*Indian Electricity Grid Code*, IEGC) est une réglementation établie par l'autorité de régulation de l'électricité fédérale en Inde, (*Central Electricity Regulatory Commission*).

L'IEGC définit les règles et les lignes directrices et les normes techniques que doivent respecter les différents acteurs du secteur afin de planifier, développer, entretenir et exploiter le réseau électrique de la manière la plus sûre, la plus fiable, la plus économique et la plus efficace possible et afin d'assurer une saine concurrence dans la production et la fourniture d'électricité.

Dans sa version la plus récente datant de 2023, l'IEGC s'est doté d'un nouveau chapitre dédié à la cybersécurité qui comporte seulement quatre articles. Ils sont présentés dans le tableau ci-dessous.

Tableau 8 : Synthèse des dispositions de cybersécurité du IEGC (Chapitre 8)

Ref. article	Synthèse
50. General	Cet article présente l'objet du chapitre (protéger le réseau national sous l'aspect cyber) puis il rappelle aux parties qu'elles ont l'obligation d'avoir un cadre de cybersécurité conforme à la loi et aux règlements en vigueur dans ce domaine.
51. Cyber Security Audit	Cet article rappelle l'obligation des parties de réaliser des audits de cybersécurité conformément à la réglementation en vigueur.
52. Mechanism of reporting	Cet article rappelle l'obligation des parties de signalement des cyberattaques et élargit les destinataires de ce signalement.
53. Cyber Security Coordination Forum	Cet article crée un forum de coordination spécifique pour la cybersécurité du secteur de l'électricité.

A noter qu'avant la publication des guidelines cybersécurité du CEA, les SERC avaient pu prendre l'initiative d'intégrer des dispositions spécifiques de cybersécurité dans les State Grid Codes. Cela a été le cas pour la *Maharashtra Electricity Regulatory Commission* et son code de réseau approuvé en 2020, lequel contient un chapitre 64 intitulé « Cyber Security ».

On comprend de l'analyse du nouveau cadre juridique fédéral indien depuis 2021 que les régulateurs locaux n'auront plus ni le besoin ni la compétence d'édicter au sein de leurs codes de réseaux étatiques des exigences particulières qui risqueraient de s'écarter de la doctrine nationale.

2.5.4. Tableau de synthèse

Inde	
Informations générales	
Indice mondial de cybersécurité (GCI 2020)	97,5/100
Classement (GCI 2020)	10ème
Stratégies et acteurs de la cybersécurité	
Documentation de stratégie nationale cybersécurité	▪ *National Cyber Security Strategy 2013,* ▪ *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)*
Cybersécurité du secteur électrique	
Implication de l'autorité de régulation de l'énergie en matière de cybersécurité	Oui mais implication légère.
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).

3. UN OUTIL NORMATIF EN DEVENIR AU NIVEAU SUPRANATIONAL

La multiplication des échanges commerciaux d'énergie entre pays apporte de nombreux bénéfices au système. Cependant, elle étend à une échelle plus large certaines problématiques, notamment les risques et menaces dont ceux de nature « cyber ».

Progressivement, les échanges entre pays laissent place à une intégration plus forte à travers la construction de marchés régionaux de l'électricité. L'intégration régionale permet notamment le renforcement de la sécurité d'approvisionnement, augmente l'accessibilité de l'énergie par une meilleure efficacité économique et accentue la pénétration des énergies renouvelables intermittentes.

Ce mode de coopération transfrontalière connaît une dynamique de développement dans de nombreuses régions dans le monde, notamment en Afrique. Toutefois, elle apporte également de nouvelles problématiques techniques et des défis à relever. En matière de cybersécurité, l'interconnexion des réseaux étend le champ des menaces à un système plus vaste, au nombre d'acteurs et d'infrastructures plus élevé et rencontre encore plus fortement des domaines régaliens d'intervention de l'Etat.

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.

3.1. Le développement de la collaboration multilatérale par l'établissement de règles communes : le cas de l'Amérique du Nord

3.1.1. Des pionniers de la coopération en matière de fiabilité du système électrique

Les pays d'Amérique du Nord ont été les premiers à doter leur secteur électrique de normes de cybersécurité communes et obligatoires. Une culture technique et institutionnelle forte établie de longue date a permis l'émergence de règles dédiées à la cybersécurité par le biais de la *North American Electric Reliability Corporation* (NERC).

La *North American Electric Reliability Corporation* (NERC) a été créée le 1er juin 1968 sous le nom de *National Electric Reliability Council* en réponse au *Northeast blackout*, panne électrique de grande ampleur qui s'est produit le 9 novembre 1965 et qui a privé d'électricité plus de 30 millions de personnes aux Etats-Unis et au Canada. La mission donnée à la NERC était donc d'accroître la fiabilité de l'approvisionnement en électricité pour l'Amérique du Nord.

3.1.1.1. Canada et Etats-Unis : les fondateurs d'une coopération internationale au service de la fiabilité du système électrique

La NERC est dès l'origine un organe de collaboration internationale puisque des représentants des industries électriques du Canada et les Etats-Unis y sont intégrés.

L'importance des échanges d'électricité entre le Canada et les Etats-Unis ainsi que la prise de conscience croissante des menaces cyber ont motivé le renforcement de la coopération entre les deux Etats en la matière. En effet, les deux voisins nord-américains disposent d'un réseau d'électricité hautement interconnecté avec plus de 35 lignes de transport transfrontalières. Chaque province canadienne située le long de la frontière américaine est interconnectée électriquement avec au moins un État américain voisin. Finalement, ce sont environ 70 TWh d'électricité qui traversent la frontière chaque année, pour un flux financier d'environ 3 milliards de dollars[4].

Cependant, les règles de fiabilité édictées ne sont pas directement opposables (elles sont d'application volontaire).

En 2007, les provinces canadiennes ont commencé à intégrer formellement les normes de fiabilité de la NERC dans leurs propres législations. La structure fédérale du Canada fait que chaque province est responsable de son réseau électrique et a des processus d'adoption et d'application des normes différents. Les principales provinces électriques comme l'Ontario, le Québec, la Colombie-Britannique et l'Alberta ont adopté les normes NERC à travers leurs régulateurs locaux.

3.1.1.2. L'élargissement au Mexique

Le Mexique a rejoint la NERC plus tardivement. Bien que certaines interconnexions électriques entre le Mexique et les États-Unis datent des années 1980, le Mexique n'a adopté officiellement les normes de la NERC qu'à partir de 2011, après des réformes du secteur de l'énergie visant à améliorer l'intégration et la modernisation de son infrastructure électrique.

En 2011, la *Comisión Federal de Electricidad* (CFE), qui est l'opérateur principal du réseau mexicain, est devenue membre de la NERC, en particulier pour le nord du pays qui est interconnecté avec le Texas et la Californie. À la suite des réformes énergétiques de 2013-2014, l'amélioration de la fiabilité du système électrique mexicain est devenue une priorité pour permettre l'ouverture du marché. Cette dynamique a conduit au renforcement de la coopération avec la NERC.

La *Comisión Reguladora de Energia (*CRE), le régulateur mexicain, a approuvé le 3 mars 2016, la Resolución RES/151/2016, qui contient le premier code de réseau (*Código de Red*). Ce code de réseau contient les critères pour « *l'efficacité, la qualité, la fiabilité, la continuité, la sécurité et la durabilité du système électrique national* » au Mexique, et la version initiale a adopté dix normes de fiabilité similaires à celles de la NERC, afin de maintenir la coordination et la sécurité de l'exploitation.

En mars 2017, le NERC, la *Comisión Reguladora de Energía* (CRE) et le CENACE ont signé un protocole d'accord de coopération américano-mexicaine en matière de fiabilité du système électrique. Cet accord indiquait notamment que la CRE et le CENACE s'engagent à déployer des efforts raisonnables pour collaborer avec la NERC à l'élaboration d'une procédure en vue de l'adoption éventuelle des normes de fiabilité de la NERC et de leur inclusion dans le Code de réseau électrique mexicain ou dans tout autre instrument réglementaire.

[4] Données issues du site Internet d'*Electricity Canada* : www.electricity.ca. Consultée le 09/07/2024.

3.1.2. Le traitement des cyberrisques

Pendant plusieurs décennies, les cyberrisques n'étaient pas reconnus comme menace importantes mais certaines circonstances ont amené la NERC à s'emparer de ce sujet dont la plus considérable a été les attentats du 11 septembre 2001.

C'est dans ce contexte que le Conseil d'administration du NERC a approuvé, le 13 août 2003, la mise en œuvre de la norme *Urgent Action Cyber Security Standard 1200 (UA 1200)* qui rassemblait un ensemble de dispositions temporaires visant à renforcer la cybersécurité des systèmes électriques. Le processus a été approfondi et a abouti sur la formulation des normes CIP, déjà présentées dans le présent rapport.

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).

3.1.3. Une coopération à approfondir

Le Canada, le Mexique et les États-Unis coopèrent en vue d'améliorer la fiabilité de leurs réseaux électriques. Le Groupe trilatéral de supervision de la fiabilité des réseaux électriques en place entre ces trois pays vise à renforcer la coopération en matière de fiabilité des systèmes électriques en Amérique du Nord, en lien avec les normes de la NERC. Ce groupe facilite l'échange d'informations, la coordination et la mise en œuvre des normes communes de fiabilité.

Toutefois, l'application des normes reste dépendante de système institutionnel et juridique de chaque Etat et ne constitue donc pas un droit supranational en la matière. La diffusion des normes NERC et notamment des CIP est donc basé sur un système de coopération, de consensus technique et d'adoption volontaire plutôt que sur un système d'opposabilité directe.

Par ailleurs, la coopération via l'application des normes du NERC est apparue comme insuffisante pour traiter le sujet à la hauteur des enjeux actuels. En décembre 2016 une stratégie commune afin de renforcer la sécurité et la résilience de leur réseau électrique. Le document intitulé *Joint United States-Canada Electric Grid Security and Resilience Strategy* (Stratégie conjointe États-Unis-Canada pour la sécurité et la résilience du réseau électrique) décrit un objectif commun : celui de disposer d'un réseau électrique sécurisé et résilient, capable de résister aux dangers et de se rétablir à la suite de perturbations. Pour y arriver, la priorité est de réduire le risque systémique pour le réseau électrique en combinant et en alignant les efforts organisationnels, techniques et politiques dans les secteurs public et privé. Les gouvernements canadien et américain ont établi un Comité de politique bilatéral inter-agences pour examiner les efforts passés et actuels afin de réaliser cet objectif.

3.2. Le Code européen « cybersécurité » : un modèle de coopération élevé pour un marché régional fortement intégré

3.2.1. La cybersécurité du secteur de l'énergie : un défi pris en compte au niveau européen

Depuis une décennie, l'Union européenne se préoccupe de plus en plus de la cybersécurité dans le secteur de l'énergie. En 2016, un rapport commandé par le Parlement européen a fourni une évaluation des politiques et législations européennes existantes traitant de la cybersécurité dans le secteur de l'énergie et a établi une liste de recommandations législatives et non législatives[5]. La communication conjointe du Parlement et du Conseil de 2017 sur la cybersécurité[6] a reconnu l'importance de considérations et de besoins spécifiques à chaque secteur au niveau de l'UE, incluant le secteur de l'énergie.

La directive NIS de juin 2016, révisée en 2022, est le texte de référence pour la cybersécurité dans l'UE et inclut 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 et les fournisseurs de technologies, afin d'atteindre un niveau supérieur de cybersécurité compte tenu des exigences spécifiques et en temps réel identifiées pour le secteur de l'énergie, des effets en cascade et de la combinaison de technologies obsolètes et de pointe[7]. Ces orientations visent à aider les parties prenantes à prendre en compte les exigences spécifiques du secteur de l'énergie lors de la mise en œuvre des normes de cybersécurité reconnues au niveau international.

3.2.2. Genèse de l'établissement d'un code de réseau européen pour la cybersécurité des échanges électriques transfrontaliers

C'est dans ce contexte qu'est née l'idée d'établir un code de réseau spécifique à la cybersécurité du secteur électrique au niveau européen. Ce projet a commencé à se concrétiser avec l'article 59 (2)(e) Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité qui a donné à la Commission européenne l'habilitation nécessaire pour adopter des actes délégués en ce qui concerne l'établissement de codes de réseau dans les domaines des « *règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité, y compris des règles sur les exigences minimales communes, la planification, la surveillance, les rapports et la gestion de crise* ».

---

[5] Parlement européen, Direction générale des politiques internes de l'Union, Cottle, E., Meckler, S., Antia, U. and Healey, D., *Cyber security strategy for the energy sector*, Publications Office, 2016.

[6] JOIN(2017) 450 final du 13.09.2017 : « Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide ».

[7] Commission européenne, "COMMISSION RECOMMENDATION of 3 April 2019 on cybersecurity in the energy sector," {SWD(2019) 1240 final}, Bruxelles, 3.04.2019.

Pour rappel, les codes de réseau européens sont un ensemble de plusieurs règlements techniques qui trouvent initialement leur fondement dans le Règlement (CE) n° 714/2009. Ils sont adoptés par la Commission européenne et implémentés dans les États membres. Ils sont d'application immédiate (effet direct). Les codes de réseau doivent faciliter l'harmonisation, l'intégration et l'efficacité du marché européen de l'électricité.

Conformément à l'Article 59(4) du Règlement (UE) 2019/943, la Commission européenne a invité l'ACER le 28 janvier 2021 à rédiger des lignes directrices pour un code réseau sur la cybersécurité. L'ACER a publié ses travaux le 22 juillet 2021. Ont suivi plusieurs années de travaux de rédaction, menés par l'ENTSO-E, DSO Entity, et l'ACER, en coopération avec l'ENISA, qui ont abouti en 2024 à l'adoption du Règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 dit « code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité » ou NCCS (acronyme anglais). Il est entré en vigueur le 13 juin 2024.

3.2.3. Contenu du code de réseau européen NCCS

Le NCCS fixe des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité, y compris des règles sur les exigences minimales communes, la planification, la surveillance, les rapports et la gestion de crise (article 1er). Le NCCS crée par ses 49 articles des dispositifs et des obligations, notamment il :

- Oblige chaque État membre de l'UE à désigner une autorité compétente d'ici au 13 décembre 2024 afin de garantir la mise en œuvre correcte du code réseau et de superviser les entités qui effectuent des processus ayant un impact suffisamment important sur les flux d'électricité transfrontaliers (appelées « entités à impact élevé et critique ») (article 4) ;
- Prévoit trois types d'évaluations des risques de cybersécurité : à l'échelle de l'Union, au niveau régional et au niveau des États membres, ainsi qu'un rapport complet d'évaluation des risques transfrontaliers (articles 18, 19, 20, 21, 23) ;
- Établit des règles de gestion des risques de cybersécurité par les entités à impact élevé et critique (articles 26 et 27) ;
- Contient des dispositions relatives à la gestion des crises de cybersécurité (articles 40 et 41) ;
- Inclut un cadre commun de cybersécurité pour le secteur de l'électricité avec des contrôles de cybersécurité minimaux et avancés, couvrant la sécurité de la chaîne d'approvisionnement et un système de gestion de la cybersécurité, ainsi que des dispositions sur sa vérification (articles 33 et 34) ;
- Prévoit l'élaboration de recommandations concernant les marchés publics liés à la cybersécurité (article 35) ;
- Contient des règles pour la détection des cyberattaques ainsi que pour la gestion et le partage des informations relatives aux cyberattaques, aux menaces et aux vulnérabilités non corrigées activement exploitées (article 37) ;
- Envisage des exercices de cybersécurité au niveau des entités, des États membres, des régions et des régions transfrontalières (article 43, 44, 45) ;
- Établit les principes de protection des informations confidentielles (article 46 et 47).

La démarche nouvelle menant à ce nouveau code de réseau dédié à la cybersécurité d'une zone transnationale part du constat suivant : la gestion des cyberrisques est d'importance

stratégique dans le secteur de l'électricité, et le contexte des systèmes électriques de plus en plus numérisés et interconnectés fait que les mesures prises au niveau national sont insuffisantes pour traiter ces risques. Dès lors, il convient de mettre en place un cadre commun de règles et de procédures afin de développer une coopération efficace au niveau européen.

L'approche déployée par le NCCS est une approche fondée sur les risques : elle vise à recenser les processus, les ressources d'appui et les entités qui les exploitent qui ont un impact sur les flux transfrontaliers d'électricité.

Le NCCS implique de nombreux acteurs du secteur électrique. Les entités peuvent être considérées comme « à fort impact » ou « à impact critique » en fonction du degré d'impact d'éventuelles cyberattaques sur leurs opérations et par conséquent être soumises à des obligations spécifiques.

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 sont des acteurs majeurs du NCCS dans le sens où ils ont l'obligation d'élaborer une documentation technique permettant de déployer les exigences de cybersécurité pour les réseaux électriques. Ainsi, les GRT doivent élaborer, en coopération avec la DSO Entity, des propositions de modalités et conditions ou de méthodes et de plans puis les soumettent pour approbation, aux autorités compétentes concernées ainsi qu'à l'ACER, pour information. Le NCCS donne un cadre procédural assez précis pour l'élaboration de ces documents d'application du code qui ont vocation à être évalués et amendés régulièrement.

Tableau 9 : Modalités, conditions, méthodes et plans à élaborer en application du NCCS

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

L'ACER surveille la mise en œuvre du NCCS et participe activement à son déploiement au côté des autres acteurs.

3.3. Le Code régional de l'EEEOA

3.3.1. Présentation de l'EEEOA

Le Système d'échange d'énergie électrique ouest africain (EEEOA, plus connue sous son acronyme anglais WAPP), est une organisation créée en 1999 sous l'égide de la CEDEAO. Son objectif principal est de promouvoir et de développer un marché régional de l'électricité en Afrique de l'Ouest, en intégrant les réseaux électriques nationaux des pays membres

pour permettre des échanges d'électricité transfrontaliers, et ainsi améliorer l'accès à une énergie fiable et abordable dans la région.

3.3.2. Le projet de Code de réseau régional

Un code de réseau régional est actuellement en cours de finalisation au sein des instances régionales de l'EEEOA, et notamment en attente d'approbation par l'autorité de régulation régionale, l'ARREC. Le projet code de réseau régional vise à établir un cadre réglementaire harmonisé pour le fonctionnement et l'exploitation des systèmes électriques interconnectés dans la région.

3.3.3. La cybersécurité dans le projet de code régional

Parmi l'ensemble de codes, le Code d'exploitation est celui qui comporte des dispositions techniques spécifiques à la cybersécurité. Le Code d'exploitation traite de « l'exploitation fonctionnelle des Systèmes électriques en relation avec les interconnexions transfrontalières ». Il contient des dispositions prévoyant les dispositifs suivants :

- **Mise en place d'un groupe de travail en charge de la cybersécurité** : L'OSM doit mettre en place des groupes de travail pour l'assister dans ses activités d'exploitation fonctionnelle. Il est prévu l'établissement d'un groupe de travail sur les TIC chargé des questions relatives à la cybersécurité des SCADA et du réseau WAN commun pour l'échange de données en temps réel ;
- **Exigences spécifiques aux systèmes SCADA** : ils sont soumis à des directives de cybersécurité et à des auto-évaluations pour vérifier au moins le niveau de sécurité et le cyberrisque à travers les gestionnaires de réseau connectés dans le WAN d'échange d'informations ;
- **Lignes directrices spécifiques concernant l'infrastructure TIC** : L'OSM est chargé d'élaborer, après consultation du groupe de travail évoqué ci-avant, des lignes directrices comprenant l'auto-évaluation des capacités de vulnérabilité et de résilience prouvées par des tests de résilience, l'analyse des scénarios de menaces cybernétiques, l'évaluation des risques et les plans de sécurité, l'organisation des mesures d'atténuation physiques et les procédures de réponse aux attaques ;
- **Obligation d'autocertification** : les gestionnaires de réseau doivent attester du respect d'exigences techniques concernant notamment la séparation physique et fonctionnelle.

Le **Code de Formation des Opérateurs du Système**, qui traite des programmes de formation que le personnel du gestionnaire de réseau exploitant le système électrique doit suivre, pour pouvoir faire face à la complexité du système électrique interconnecté de l'EEEOA, mentionne l'évaluation de la sécurité comme un thème technique à privilégier par les gestionnaires de réseau. Il encourage également les gestionnaires de réseau à établir des accords bilatéraux/multilatéraux de coopération pour une formation commune, afin de poursuivre des objectifs communs en matière de sécurité d'exploitation et d'amélioration des procédures. Sans la citer, on déduit que la cybersécurité entre dans cette attention particulière portée à la sécurité d'exploitation.

ANNEXE 1 : SYNTHESE DU BENCHMARKING – CODES DE RESEAU NATIONAUX

Pays :	France	Grande-Bretagne	Kenya	Etats-Unis	Inde
Code de réseau	**Oui.** La Documentation technique de référence (DTR) de RTE peut partiellement être assimilée à un code de réseau.	**Oui.** The Grid Code. Mais la Grande-Bretagne est dotée plusieurs autres codes pour le secteur électrique.	**Oui.** The Kenya National Transmission Grid Code (KNTGC).	**Oui.** Plusieurs documents élaborés par les opérateurs peuvent partiellement être assimilées à des codes de réseau.	**Oui.** The Indian Electricity Grid Code (IEGC). Complété par des codes de réseaux régionaux (State Grid Codes).
Auteur / approbateur du document	Le gestionnaire du réseau de transport RTE élabore et publie la DTR. Information ou approbation de la CRE suivant les chapitres concernés de la DTR.	NESO supervise le Grid Code (gestion du document et coordination des modifications). Toutes les modifications doivent être examinées par le Grid Code Review Panel et approuvées par ce dernier ou par l'Ofgem.	L'Autorité est responsable de contrôler les activités et la révision du KNTGC et sera informée des recommandations du Kenya National Grid Code Review Committee (comité de révision du code du réseau national du Kenya).	Les opérateurs de réseaux (ISO / RTO) élaborent leurs documentations techniques. La FERC les approuve.	The Central Electricity Regulatory Commission élabore et adopte ce document.
Exigences cybersécurité	**Oui.**	**Non.** Le « Grid Code » ne contient pas de dispositions spécifiques pour la cybersécurité.	**Oui.** Le KNTCG intègre un chapitre dédié à la cybersécurité (Chapitre 21).	**Non.** Les exigences en matière de cybersécurité (normes CIP) sont élaborées au niveau fédéral par la NERC et approuvées par la FERC.	**Oui.** Le IEGC intègre in chapitre dédié à la cybersécurité (Chapitre 8).
Synthèse des exigences du code	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.	N/A	Le KNTCG présente un cadre complet pour la gestion de la cybersécurité, abordant un grand nombre de domaines. Ce chapitre est cependant principalement formulé sous forme de recommandations et non d'authentiques règles juridiques ce qui peut interroger sur l'opérationnalisation et l'effet juridique de ces règles.	N/A	Composé de seulement quatre articles, le chapitre dédié à la cybersécurité : - Rappelle aux parties qu'ils ont l'obligation d'avoir un cadre de cybersécurité conforme à la loi et aux règlements en vigueur dans ce domaine ; - Rappelle l'obligation qu'ont les parties de réaliser des audits de cybersécurité conformément à la réglementation en vigueur ; - Rappelle leur obligation de signalement des cyberattaques et élargit les destinataires de ce signalement ; - Crée un forum de coordination spécifique pour la

					cybersécurité du secteur de l'électricité.

ANNEXE 2 : SYNTHESE DU BENCHMARKING – CODES DE RESEAU REGIONAUX

Pays :	Amérique du Nord	Union européenne	Afrique de l'Ouest (EEEOA)
Code de réseau	**Non.**	**Oui.** 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.	**Oui.** Le Code de réseau de l'EEEOA (pas encore entré en vigueur).
Auteur / approbateur du document	N/A	Elaboré par DSO Entity et l'ENTSO-E, en collaboration avec l'ACER. Adopté par la Commission européenne.	Elaboré par l'EEEOA. Approuvé par l'ARREC.
Exigences cybersécurité	Les règles CIP de la NERC s'appliquent sous certaines conditions aux Etats voisins, le Canada et le Mexique.	**Oui** L'intégralité de l'objet du document porte sur fixation de règles concernant la cybersécurité des flux d'électricité.	**Oui.** Le projet de Code d'exploitation contient plusieurs dispositions visant à renforcer la cybersécurité.
Synthèse des exigences du code	N/A	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.	- Mise en place d'un groupe de travail en charge de la cybersécurité, - Exigences spécifiques aux systèmes SCADA, - Elaboration de lignes directrices spécifiques concernant l'infrastructure TIC, - Obligation d'auto-certification des gestionnaires de réseau.